ÉCOLE 18.06
LA LIBERTÉ PAR LA SOUVERAINETÉ

La journalisation pour la cybersécurité appliquée à l'automobile

Mastère Cyberdéfense

Maxime BAZIN
28 avril 2026

Résumé

La cybersécurité automobile est un domaine en pleine structuration et encore à l'étape de laboratoire. Avec la généralisation des véhicules connectés, la surface d'attaque exposée par les constructeurs et leurs équipements s'est considérablement élargie. Les bus, les interfaces sans-fil, les mises à jour à distance et les infrastructures extérieures constituent déjà des vecteurs d'attaques documentés mais surtout exploités. Face à cette réalité, le secteur dispose aujourd'hui d'un cadre réglementaire naissant comme la norme ISO 21434, le règlement UNECE R155 et le Cyber Resilience Act mais les architectures techniques permettant d'y répondre concrètement restent insuffisantes. Ce mémoire de recherche vise donc à répondre à la question si un système de collecte et d'analyse de journaux appliqué à l'automobile peut-il être une réponse à la surveillance de la sécurité numérique des véhicules connectés. Les connaissances existantes sur le sujet montrent que les outils SIEM d'aujourd'hui sont matures sur leurs offres de services pour la journalisation d'évènements dans le domaine de la sécurité des systèmes d'informations classiques mais leur application au domaine automobile n'est pas encore complète. Certains éditeurs proposent des outils externes à l'existant ou proposent d'absorber les journaux et de les envoyer dans un SIEM déjà implémenté mais cela se heurte à plusieurs contraintes, aucun ne propose pour l'instant nativement un outil capable d'absorber des journaux IT, IoT et OT. L'apport de ce travail par rapport à l'existant réside dans la démonstration qu'un outil open-source généraliste tel qu'Elasticsearch peut être adapté pour ingérer, normaliser et analyser les journaux des bus CAN sans couche intermédiaire. Cette approche me permettrai de traiter dans un même moteur d'analyse des données automobiles et des journaux IT classiques. Les résultats obtenus valident la faisabilité de cette approche, sur plus de onze millions de journaux ingérés, deux règles de détection basées sur les menaces du règlement UNECE R155 ont générées treize alertes uniquement sur l'ensemble de données compromis. Ces résultats restent à l'échelle d'une preuve de concept et appelle à des développements complémentaires.

Glossaire

1. Soupape : Organe mécanique du moteur permettant l'admission des gaz frais et l'évacuation des gaz brûlés. (fr.wikipedia.org)
2. Calculateur : Un calculateur est un système embarqué (électronique et informatique) autonome, souvent en temps réel, spécialisé dans une tâche précise. (fr.wikipedia.org)
3. RFID : « Les puces RFID permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micropuce (également dénommée étiquette ou tag) et d'une antenne qui dialoguent par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. » (cnil.fr)
4. Dispositif : Tout équipement, qui au minimum, sait communiquer avec un réseau. En plus de cette capacité de communication, l'équipement peut intégrer des fonctions de détection à travers des capteurs, d'actionnement, de saisie de données, de stockage et de traitement des données (Recommandation UIT-T Y.2060)
5. Modèle OSI : "Le modèle OSI (Open Systems Interconnection ou interconnexion de systèmes ouverts) est une norme de l'Organisme international de standardisation (ISO) permettant de définir la communication entre des systèmes informatiques à l'aide de protocoles standards. Ce modèle se compose de 7 couches (couches physique, de liaison de données, réseau, transport, de session, de présentation et d'application)." (cnil.fr)
6. Firmware : « Dans un système informatique, un firmware (ou micrologiciel, microprogramme, microcode, logiciel interne ou encore logiciel embarqué) est un programme intégré dans un appareil informatique (ordinateur, photocopieur, automate, disque dur, routeur, appareil photo numérique, etc.) pour qu'il puisse fonctionner. » (https://fr.wikipedia.org/wiki/Firmware)
7. Multiplexage : Le multiplexage est une technique inventée en 1891 par Émile Baudot qui consiste à faire passer plusieurs informations à travers un seul support de transmission. Elle permet de partager une même ressource entre plusieurs utilisateurs. (https://fr.wikipedia.org/wiki/Multiplexage)
8. Syslog : Syslog est l'acronyme de System Logging Protocol et désigne un protocole standard qui sert à envoyer des fichiers du journal système ou des messages ayant trait à

des événements à un serveur dédié appelé serveur syslog. On l'utilise avant toute chose pour collecter différents journaux d'événements auprès de plusieurs machines et pour les transférer vers un emplacement central depuis lequel on pourra les consulter et les examiner. (https://www.paessler.com/fr/it-explained/syslog)

9. SNMP : SNMP est un protocole de couche applicative qui transmet des données de gestion entre les dispositifs réseau. (https://www.fortinet.com/fr/resources/cyberglossary/simple-network-management-protocol)
10. WMI : WMI est un système de gestion interne de Windows qui prend en charge la surveillance et le contrôle de ressources systèmes via un ensemble d'interfaces. Il fournit un modèle cohérent et organisé logiquement des états de Windows. (https://fr.wikipedia.org/wiki/Windows_Management_Instrumentation)
11. API : Une API (application programming interface ou « interface de programmation d'application ») est une interface logicielle qui permet de « connecter » un logiciel ou un service à un autre logiciel ou service afin d'échanger des données et des fonctionnalités. (https://www.cnil.fr/fr/definition/interface-de-programmation-dapplication-api)
12. RGPD : Le règlement général sur la protection des données (RGPD) est un texte réglementaire européen qui harmonise les règles de traitement des données à caractère personnel dans toute l'Union européenne. (https://www.economie.gouv.fr/entreprises/gerer-son-entreprise-au-quotidien/assurer-sa-cybersecurite-et-la-protection-de-ses/le)
13. Machine Learning : L'apprentissage automatique (machine learning en anglais) est un champ d'étude de l'intelligence artificielle qui vise à donner aux machines la capacité d'« apprendre » à partir de données, via des modèles mathématiques. Plus précisément, il s'agit du procédé par lequel les informations pertinentes sont tirées d'un ensemble de données d'entraînement. (https://www.cnil.fr/fr/definition/apprentissage-automatique)
14. CTI : La Cyber Threat Intelligence définit la recherche, l'analyse et la modélisation de la menace cyber. Elle permet de décrire une menace ou une attaque informatique au travers d'éléments contextualisés et/ou d'indicateurs compréhensibles par des hommes ou des machines. (https://www.sekoia.io/fr/glossaire/quest-ce-que-la-cti/)
15. Active Directory (abrégé AD) : Active Directory est un service d'annuaire développé par Microsoft qui stocke des informations sur les objets d'un réseau et met ces informations à

la disposition des utilisateurs et des administrateurs. Pour le réseau d'entreprise, Active Directory fonctionne comme un système organisationnel complet. Il fonctionne comme un répertoire central qui surveille les utilisateurs, les ordinateurs et les ressources tout en contrôlant les autorisations d'accès sur l'ensemble du réseau. (https://www.fortinet.com/fr/resources/cyberglossary/active-directory)

16. Malware : Un malware est un logiciel malveillant qui intervient dans le but de nuire à l'utilisateur de l'ordinateur. C'est une forme de cyberattaque et l'objectif est de voler des données personnelles, financières ou commerciales. (https://www.oracle.com/fr/cloud/malware-logiciel-malveillant/)
17. HTTPS : Le protocole de transfert hypertexte sécurisé (HTTPS) est la version sécurisée du protocole HTTP, principal protocole utilisé pour l'envoi de données entre un navigateur Web et un site Web. HTTPS est chiffré afin de renforcer la sécurité du transfert de données. (https://www.cloudflare.com/fr-fr/learning/ssl/what-is-https/)
18. Numéro VIN : Le Vehicle Identification Number, « code VIN », appelé également « Numéro d'identification du véhicule », « Numéro dans la série du type » ou encore tout simplement « Numéro de série du véhicule », est un code alphanumérique unique qui est donné à chaque véhicule automobile depuis 1954. (https://fr.wikipedia.org/wiki/Vehicle_Identification_Number)
19. RFC : RFC est l'acronyme en anglais pour Request for Comments (demandes de commentaires). Les RFC sont une série numérotée de documents officiels décrivant les aspects et spécifications techniques d'Internet ou de différents matériels informatiques. (https://kb.planethoster.com/glossaire/rfc/)

Sommaire

Liste des figures

Préface

Durant la convention de « leHACK 2025 », j'ai eu la chance d'assister à l'atelier présenté par Gaël MUSQUET, le titre étant « Car Hacking » et me passionnant depuis quelques temps pour le monde automobile j'ai tout de suite été captivé par ses explications. Quand il nous a fait comprendre les problèmes et l'état actuel du parc automobile et de ses capacités à se défendre, notamment en France, j'ai été interloqué, étant dans le milieu, de voir à quel point les Français et nos constructeurs industriels avaient pris du retard sur la question de la cybersécurité.

C'est pourquoi j'ai décidé d'en faire mon sujet de mémoire de recherche, d'autant plus que par mon expérience professionnelle passée et surtout présente je suis très sensibilisé à ces questions de sécurité et plus récemment autour de celle des objets qui m'entourent. Au sein de mon ancienne entreprise, Cegedim.cloud, spécialisée dans le stockage et le traitement de données de santé, j'ai été dans l'équipe sécurité, chargé de développer un système de haute disponibilité pour le SIEM (security information & event management) dans ce qui était la nouvelle infrastructure cloud ultra-sécurisée SecNumCloud. C'est donc dans ce contexte de conditions de sécurité strictes, de souveraineté et de gestion des données sensibles, le tout en devant aussi s'occuper des exigences du Groupe que j'ai évolué. Dans l'entreprise qui m'a embauchée en août, La Royale Investissements France, l'un de leurs sujets les plus captivants est la dynamisation de la ville de Molsheim à travers l'immobilier et doivent donc déployer dans leurs bâtiments rénovés des équipements de domotique nouvelle génération, tous interconnectés et donc j'ai pour projet de mettre en place des moyens de sécurité sur le produit que mon collègue Alexandre et moi-même sommes en train de concevoir pour contrôler un ensemble d'équipement de domotique disséminé partout dans la ville.

C'est donc avec ce bagage en cybersécurité que je vais aborder mon mémoire de recherche afin de devenir un ingénieur à la fin de mon cursus.

Présentation de l'entreprise

Ma première expérience professionnelle s'est faite au sein de Cegedim.cloud que j'ai rejoint lors de ma première année de BTS. En première et deuxième année de BTS j'ai été dans l'équipe support de premier niveau pour l'ensemble des 6000 utilisateurs du groupe. J'avais pour mission l'administration des boîtes mails utilisateurs, des boîtes mails partagées et des listes de diffusion. Je faisais aussi du support via le call center pour aider les gens à distance sur leurs problèmes de VPN, de suite Office, d'application Zoom et plus généralement des postes de travail. Chaque appel faisait l'objet d'un ticket que je devais créer dans notre outil de ticketting interne. Ensuite, en année de licence d'informatique générale spécialisée en cybersécurité j'ai pu rejoindre l'équipe sécurité de cette même entreprise et j'avais pour mission la gestion et la maintenance des outils de sécurité tel que Splunk pour le SIEM interne, F5 pour le Web Application Firewall et SentinelOne, l'anti-virus pour les postes et serveurs. Je devais regarder tous les matins à J+1 les alertes remontées par SentinelOne sur l'infrastructure et vérifier si c'était des faux ou vrais positifs. J'ai aussi à plusieurs reprises mené des campagnes de sensibilisation pour les collaborateurs du groupe avec des mails de phishing via l'application GoPhish. J'ai aussi eu pour mission de faire des revues de sécurité pour les différentes applications mises en place par le groupe en lançant des tests automatisés et en produisant des rapports à la suite de ceux-ci. Durant cette année, j'avais deux projets, le premier étant la mise en place d'une infrastructure à haute disponibilité pour le SIEM de l'environnement SecNumCloud et le second était la migration de notre ancienne infrastructure Splunk vers une nouvelle mieux organisée.

L'entreprise dans laquelle je travaille actuellement se nomme La Royale Investissements France (LRIF) et y ai un poste d'Administrateur d'infrastructures sécurisées. Cette entreprise est une holding du groupe La Royale créé en 2023 regroupant des entreprises dans les domaines des technologies de jeu, financières, du marketing et de l'immobilier. La holding est basée à Molsheim, 67120 et se concentre sur la proximité ainsi que le sponsoring des activités dans la ville de

Molsheim comme certains clubs de sport ou encore le patrimoine de la ville en rachetant des bâtiments dans le but de les rénover tout en gardant le charme alsacien grâce aux Architectes des Bâtiments de France. Cette volonté de re-dynamisation se traduit aussi dans l'investissement de l'Ecole 18.06 qui a pour mission de former des futurs ingénieurs informatiques mais aussi les politiciens de demain. Durant cette année d'alternance, j'ai pu effectuer diverses missions variées. Avec un alternant de troisième année de Bachelor informatique, nous avons commencés par mettre en place le réseau de l'Ecole 18.06 en commençant, alors même que l'Ecole n'était pas encore ouverte, par le branchement du routeur et des commutateurs puis leur brassage. Ensuite, nous avions pour projet la supervision de l'état global du réseau et avons donc conceptualisés un ELK (Elasticsearch, Kibana, Logstach) avec des tableaux de bord que nous avons reliés au routeur afin de récupérer les informations dont nous avions besoin (taux de disponibilité etc.) Enfin, nous avons engagés notre projet de domotique avec un temps de recherche sur les technologies autour de l'IoT et leur fonctionnement dans le cadre de la domotique et une analyse de marché sur les solutions déjà existantes et notamment celles qui étaient souveraines afin de porter les valeurs de l'entreprise. Nous avons donc mis en place, localement, pour garder les données en interne, un serveur avec le système d'exploitation d'Home Assistant pour commencer à le paramétrer selon les besoins du cahier des charges qui nous a été confiés en début d'alternance avec un premier déploiement au sein de l'École qui nous a laissés faire nos tests.

Introduction

L'industrie automobile a su s'imposer comme l'un des secteurs industriels les plus florissants du XXème siècle grâce à ses innovations constantes depuis sa naissance à la fin du XIXème siècle. Son premier grand tournant industriel est l'adoption du Taylorisme, théorisé par l'ingénieur Frederick Winslow Taylor qui prône une organisation scientifique du travail visant à maximiser la productivité ouvrière. C'est l'industriel Henry Ford qui va le plus loin dans cette logique en introduisant, 1913, la ligne d'assemblage mobile pour la production de sa Ford T, ce n'est plus un personne seule qui fabrique une voiture dans son intégralité mais une chaîne où chaque ouvrier intervient sur une tâche précise et répétée. Ce modèle désormais désigné comme étant le « Fordisme », s'impose progressivement comme standard mondial tant il révolutionne la rapidité et le coût de fabrication.

Cette Ford T marque alors un tournant dans le monde automobile, qui le fait alors passer d'un statut de luxe, réservée aux hautes sphères des privilégiés car tout était artisanal et fait main, le faisant passer à un statut plus modeste, fait pour être vendue à moindre coût et pour une classe dite « moyenne ». Mais c'est aussi pendant cette démocratisation de l'automobile que durant les « années folles », le monde voit apparaître des constructeurs qui, justement vont faire le choix de garder leurs lignes directrices, comme l'entreprise Bugatti, qui produit en 1926, seulement six exemplaires de son modèle « Royale » vendue à 500 000 francs et est donc réservée à la fine fleur de l'époque.

Les ingénieurs français ne se feront pas attendre avant de révolutionner à leur tour cette industrie avec de nombreux progrès techniques, toujours utilisés dans les voitures actuelles. La Citroën Traction, mise en fabrication en 1934, présente de nombreuses innovations comme la carrosserie monocoque (pas de châssis), un aérodynamisme amélioré, un moteur à soupapes[1] en tête (en haut du moteur), la traction avant (les roues avant apportent la motricité) ou encore les freins hydrauliques (utilisation de liquide de frein). Et des innovations, les industriels automobiles ne cesseront jamais de compter là dessus et connaitront un certain

essor après la Seconde Guerre Mondiale, alors qu'il faut tout reconstruire, le marché est très prisé par les américains mais n'est pas abandonné pour autant par les Européens, avec la sortie de la mythique 2CV de Citröen en France, la Volkswagen Coccinelle en Allemagne ou encore les petites Fiat en Italie et Mini en Angleterre. De nouvelles marques émergeront, pendant que d'autres périront et d'autres encore consolideront leurs positions et s'imposeront comme des leaders dans leurs marchés respectifs.

Ces innovations ont changées de nature au fil du temps, de leur design jusqu'à leur moteur, les constructeurs se sont aussi concentrés sur la sécurité routière qu'accompagnent l'avènement de nouvelles infrastructures routières. En 1965, c'est plus d'un million et demi de personnes qui sont mortes sur les routes américaines en 20 ans, ce bilan est plus lourd que celui des dernières guerres. C'est seulement en 1971, il y a 54 ans, que les Australiens votent pour le port obligatoire de la ceinture de sécurité dans les automobiles. C'est aussi par cette prise de conscience que le moteur à traction avant revendique sa supériorité face au moteur à propulsion grâce à ses propriétés plus sécuritaires.

C'est dans cette période que l'électronique et l'informatique embarquée se généralise dans l'industrie automobile, faisant apparaître un ensemble de technologies comme l'allumage commandé des moteurs (son alimentation en carburant est commandé par de l'électronique). L'injection et l'allumage seront donc désormais gérés par un « calculateur[2] » selon plusieurs paramètres comme les températures de l'air, du moteur ou la dépression interne, pression externe etc. Les boîtes de vitesses automatiques profitent elles aussi de la généralisation de l'informatique au sein des voitures, permettant un passage des vitesses plus adaptables selon les envies du constructeur les rendant plus joueuses ou au contraire plus confortables. Les systèmes embarqués se généralisent aussi dans les suspensions, la transmission etc. Tous les composants de nos voitures sont désormais sous contrôle d'un calculateur informatique afin d'optimiser l'ensemble de la structure. Mais comme évoqué plus tôt, l'une des priorités des constructeurs était

la sécurité (sécurité active et passive) et la propagation des systèmes informatiques ont fortement participé à l'amélioration de celle-ci. Les conducteurs ont pu voir apparaître l'ABS (de l'anglais Anti-Blocking System) empêchant les roues de se bloquer pendant un gros freinage ou encore l'ESP (Electronic Stability Program) qui vise à améliorer le contrôle, l'adhérence et corriger la trajectoire de la voiture si nécessaire, un système qui s'active principalement sur route mouillée.

Ces systèmes embarqués devenus des obligatoires sont réfléchis dès la conception des véhicules modernes et la sécurité informatique devient progressivement un sujet de plus en plus important pour les constructeurs et tous les autres acteurs utilisant des systèmes embarqués dans leurs produits. C'est pourquoi dans mon entreprise, La Royale Investissements France, nous avons un sujet de cybersécurité autour de la domotique, notamment, afin de concevoir un produit de domotique utile aux activités de dynamisation de territoires à travers l'immobilier sans pour autant oublier la sécurité du produit en lui-même dont je suis en charge. C'est dans cette optique, en m'intéressant à la cybersécurité des systèmes embarqués que j'ai compris que ces systèmes avaient encore de nombreuses lacunes malgré les efforts des constructeurs et que des dérives grandissantes apparaissaient au fur et à mesure des années compromettant la sécurité informatique et donc routière du moyen de transport préféré des Français.

Je profite aussi de cette introduction à mon sujet pour préciser que l'automobile, par définition désigne le fait de se mouvoir par soi-même mais depuis lors a connu quelques déformations et est devenue le terme définissant les voitures côtoyant le quotidien des Français aujourd'hui, c'est pourquoi dans ce mémoire, je ne me concentrerai que sur les « voitures », que je désigne aussi comme « automobile ».

Problématique

Vous avez pu comprendre en introduction que le contexte de l'industrie automobile s'était toujours profondément transformé au fil des années. De nos jours, les constructeurs souhaitent moins se dépasser dans leurs performances mécaniques mais plutôt proposer à leurs consommateurs des expériences de conduite confortables et tout en silence notamment grâce à l'hybridation et l'électrification du parc automobile poussée principalement par des réglementations écologiques européennes exigeantes forçant petit à petit la majeure partie des marques à revoir leur catalogue de produits. Cette transformation s'accompagne d'une augmentation des systèmes embarqués et connectés au sein de nos véhicules de tous les jours. Les constructeurs veulent être les premiers à développer les voitures du futur grâce à ces systèmes, ceux que nous voyons dans nos films de science-fiction favoris mais comme dans tout bon film, il faut un bon méchant. Ces méchants profitent de ces changements pour trouver de plus en plus de failles puisque les systèmes se développent mais la sécurité nécessaire n'arrive pas à suivre. Ce mémoire de recherche est donc destiné à confirmer ou infirmer l'hypothèse qu'une solution de cybersécurité puisse être implantée à travers des systèmes embarqués à destination des industries via un système de collecte, de normalisation et d'analyses de journaux conforme aux nouvelles réglementations en vigueur, pour améliorer la détection des menaces pesant sur les véhicules connectés.

Un système de collecte et d'analyse de journaux appliqué à l'automobile peut-il être une réponse à la surveillance de la sécurité numérique des véhicules connectés ?

1. Internet des objets (IoT)

1.1. Présentation de l'IoT

1.1.1. Le concept d'IoT

Le concept d'IoT (Internet of Things) naît en 1999, c'est Kevin Ashton un informaticien britannique qui invente cette expression en faisant de la recherche sur les réseaux RFID[3]. Depuis le début du XXIème siècle, ce concept a bien évolué notamment avec le nombre grandissant d'objets connectés au quotidien, la place de plus en plus importante de l'intelligence artificielle et les données numériques récoltées dans le quotidien.

Aujourd'hui, l'internet des objets regroupe tous les objets dit « connectés », qui en plus de leur fonction principale, peuvent envoyer et / ou recevoir des informations via des réseaux de télécommunications sans-fil (Wi-Fi, Bluetooth, réseaux mobiles etc. dont je préciserai le fonctionnement dans une prochaine partie). L'objet peut aussi être équipé de capteurs récupérant des données (par exemple, les montres connectées qui récupèrent les mouvements, la fréquence cardiaque etc.) et transmet ces données à un autre système conçu pour stocker et analyser ces données. Ces données, une fois collectées et analysées, permettent d'automatiser des actions, d'anticiper des comportements ou de déclencher des alertes sans intervention humaine, ce qui constitue l'un des apports fondamentaux de l'IoT par rapport aux systèmes informatiques traditionnels.

Selon Cisco Internet Business Solutions Group, l'Internet des Objets ne serait né qu'au moment où le nombre d'objets connectés a dépassé le nombre d'humains peuplant la Terre, c'est-à-dire dans les années 2008-2009. En 2010, le nombre d'appareils connectés aurait atteint 12,5 milliards pour 6,8 millards de personnes. En 2020, l'estimation monte à 21,7 milliards d'appareils connectés dont 11,7 milliards d'objets connectés auxquels il faut rajouter 10 milliards de téléphones, tablettes et ordinateurs (qui ne comptent pas comme étant de l'IoT). Cette croissance exponentielle du nombre d'objets connectés s'accompagne d'une augmentation

proportionnelle de la surface d'attaque exposée aux attaques informatiques : chaque objet connecté constitue une porte d'entrée potentiel pour un attaquant, ce qui fait de la sécurité de l'IoT un enjeu croissant. Je peux illustrer cet enjeu avec l'article de Radio France **[RadioFrance.2026]** par Adrien Serriere du 26 février 2026 qui explique le piratage involontaire récent de 7000 aspirateurs robots de la marque chinoise DJI. Un informaticien français qui souhaitait simplement reprogrammer son robot afin de pouvoir le contrôler avec sa manette de Playstation a pu accéder accéder aux données de ces appareils à leur insu. Samy Azdoufal finit par découvrir qu'il a non seulement accès aux données de son aspirateur mais aussi à celles de 7000 autres dont le niveau de la batterie, l'accès à la caméra, au micro et à la localisation des appareils. Selon moi, je pense que cette affaire très médiatisée, puisque j'en ai entendu parler pour la première fois à la radio, a pu alerter les gens sur les dangers de l'Internet des Objets qui devient une préoccupation grandissante.

1.1.2. Aperçu technique de l'IoT

Lors de mes recherches sur la définition de ce qu'était l'Internet des Objets, j'ai pu trouver les travaux de l'Union Internationale des télécommunications qui, grâce à leur recommandation Y.4000/Y.2060 du 15 juin 2012 me permet d'aborder un plan plus technique de l' « Internet of Things » **[ITUT.2012]**. L'IoT y est représentée comme une « infrastructure mondiale » permettant de disposer de services en interconnectant des objets physiques ou virtuels grâce aux « technologies de l'information et de la communication » (TIC) pouvant communiquer ensemble. Selon l'encyclopédie libre Wikipédia : « Les technologies de l'information et de la communication sont les outils et les systèmes qui permettent de créer, transmettre, stocker et partager des informations ». (https://fr.wikipedia.org/) L'internet des objets ajoute une dimension nouvelle aux TIC traditionnelles qui fournissaient déjà la possibilité de communiquer à tout moment et en tout lieu, l'IoT permet désormais de communiquer avec n'importe quel objet dans un écosystème numérique comme présenté dans la figure ci-dessous.

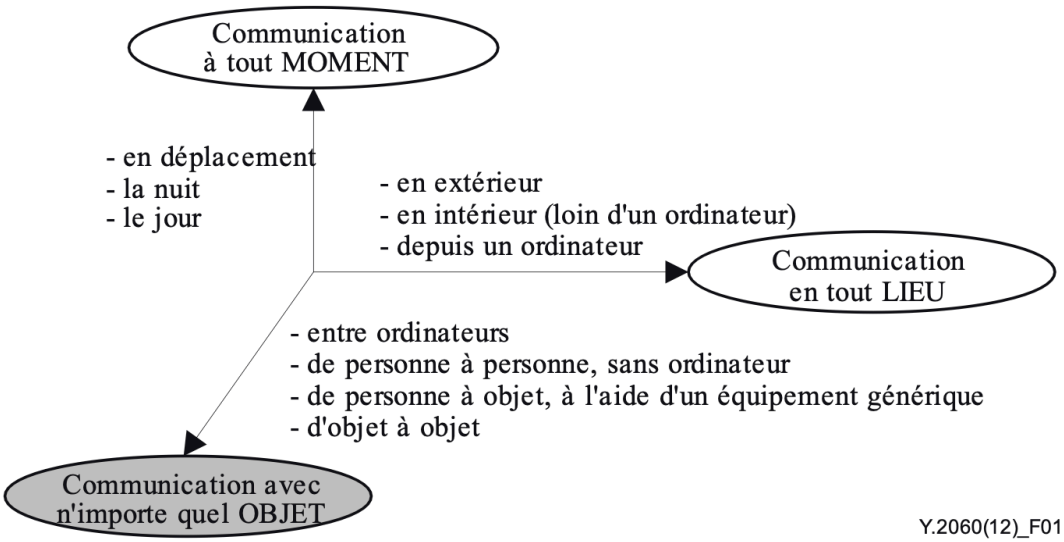

Figure 1 : Nouvelle dimension apportée par l'IoT

J'estime que ce schéma représente l'évolution de l'informatique et de comment les communications entre services ont évolué dans le temps. Dans ses débuts, l'informatique nécessitait une personne assise devant un poste fixe à piloter un ordinateur depuis sa chaise. Les améliorations de la connectivité ont permis la communication en tout lieu, c'est à dire depuis n'importe où, le poste fixe à proprement parlé a disparu et je l'ai notamment observé au sein des entreprises où j'ai fait mes cinq années d'alternance où la plupart des postes professionnels sont désormais des ordinateurs portables qui permettent la communication en tout lieu. Ces évolutions ont aussi permis la communication à tout moment, elle n'est plus limitée dans le temps ni demandant une surveillance humaine constante. C'est là qu'intervient l'IoT et la nouvelle dimension qu'apporte cette technologie en permettant la communication avec n'importe quel objet d'un écosystème numérique, ce ne sont plus deux ordinateurs qui communiquent entre eux via des réseaux classiques mais bien l'avènement d'un réseau universel où n'importe quel objet un temps soit peu connecté nous entourant devient un système permettant la réception ou l'envoi de données. Cette nouvelle façon de communiquer est permise grâce à l'introduction de nouvelles méthodes de communications, à savoir la communication de personne à objet (éteindre ou allumer sa lumière depuis son

téléphone par exemple), la communication d'objet à objet ou « machine to machine » (M2M) (récupération de la température ambiante d'une pièce via un capteur sur son serveur) ou encore l'introduction d'équipements génériques (montres, frigos ou voitures etc.)

L'internet des Objets s'appuie sur trois modes de communications principaux, le premier étant la communication via le réseau ainsi qu'une passerelle c'est-à-dire que les "dispositifs[4]" sont capables de communiquer via un réseau de communication (IP (Internet Protocol), etc.) mais aussi via les passerelles que génèrent les interfaces des dispositifs permettant un réseau plus large entre les équipements. Le second mode de communication est la communication uniquement via un réseau de communication « classique » comme l'Ethernet, le Wi-Fi ou les données cellulaires mais n'ont pas besoin d'une passerelle donc d'un autre équipement pour accéder à ce réseau. Enfin, le dernier mode de communication est la communication directe donc les dispositifs communiquent entre eux sans infrastructure réseau comme des réseaux locaux. Ils peuvent communiquer via Bluetooth, des réseaux de capteurs, des bus de données CAN (controller area network) etc.

1.1.3. Caractéristiques fondamentales de l'IoT

Pour qu'un équipement soit considéré comme un objet de l'IoT, il se doit de respecter plusieurs caractéristiques et fondements pour le distinguer des autres objets électroniques. Tout d'abord, un dispositif doit pouvoir être interconnectable entre plusieurs appareils, un dispositif IoT ne peut fonctionner seul, il a besoin d'une infrastructure réseau ou d'autres dispositifs pour communiquer. Pour communiquer et créer cette interconnectivité l'Internet des Objets n'utilise pas le modèle standard donc OSI[5] mais un modèle réduit comme 6LoWPAN (IPv6 Low power Wireless Personal Area Networks) qui transporte des paquets réseau IPv6 via le protocole de communication IEEE 802.15.4 qui est destiné aux équipements de faible consommation, de faible portée et de faible débit. Pour définir ces paquets et les faire communiquer le protocole MQTT (Message Queuing Telemetry Transport) est généralement utilisé qui contrairement au 6LoWPAN qui se situerait plutôt dans la

couche réseau, le MQTT, lui, se situerait dans la couche application. MQTT est un protocole de messagerie léger fonctionnant sur un modèle de publication et d'abonnement dit « publish/subscribe », un dispositif publie des données sur un canal thématique appelé « topic » géré par un serveur central nommé « broker » et tous les dispositifs abonnés à ce « topic » reçoivent automatiquement ces données sans avoir à interroger directement la source. Cette architecture est particulièrement adaptée aux environnements de l'IoT puisqu'elle minimise la bande passante consommée et ne nécessite pas de connexion permanente entre les appareils, le « broker » (ou courtier en français) se chargeant de conserver les messages jusqu'à ce que le destinataire soit disponible pour les recevoir. C'est ce protocole qui permet d'indiquer sur le réseau quels sont les données échangées et de leur structure. Ils s'appuient sur de nombreux autres protocoles situés dans différentes couches du modèle OSI réduit que je détaillerai dans la partie suivante mais c'est en cela que les dispositifs peuvent communiquer tous entre eux malgré leurs fonctions différentes et leurs réseaux distincts.

Un dispositif IoT peut aussi changer d'état à l'instar d'un serveur informatique "classique" qui se doit d'être de respecter un certain taux de disponibilité, un dispositif lui, change continuellement d'état passant de l'état de réveil à celui de veille et ainsi de suite. Un dispositif n'a pas besoin d'être constamment disponible mais seulement lorsqu'il en a besoin pour remonter les informations qui sont demandées par l'utilisateur tout en s'adaptant à l'environnement dynamique dans lequel il peut être installé (par exemple la vitesse ou l’emplacement géographique qui sont des valeurs changeantes). La dynamique des dispositifs doit aussi se faire sur le nombre qu'un réseau est capable d'accueillir, ce qui peut nécessiter un protocole de découverte automatique de services comme le fait Home Assistant via son interface web à l'aide de plusieurs protocoles permettant cette découverte (mDNS (multicast Domain Name Service), MQTT discovery, SSDP (Simple Service Discovery Protocol), Bluetooth etc.)

Pour finir, l'IoT ne doit pas se contenter de transporter des informations sur un réseau donné mais de donner un sens à l'action que permet le dispositif, c'est pour cela qu'il faut réussir à garder une certaine cohérence entre l'objet "physique ou virtuel" et ses représentations sur l'interface. Les dispositifs doivent pouvoir faire tout cela et intégrer nativement des protections comme la Root of Trust (RoT) qui utilise des puces sécurisées (exemple TPM (Trusted Platform Module)) qui stocke des clés de chiffrement permettant le démarrage d'un objet uniquement avec le logiciel autorisé via le Measured Boot et certifie donc de sa viabilité sur le réseau).

1.1.4. Modèle de référence de l'IoT

Comme évoqué précédemment, l'Internet des Objets n'utilise pas le modèle OSI ni TCP/IP standard utilisé par les serveurs ou les ordinateurs de tous les jours mais un modèle réduit pour convenir à ses besoins.

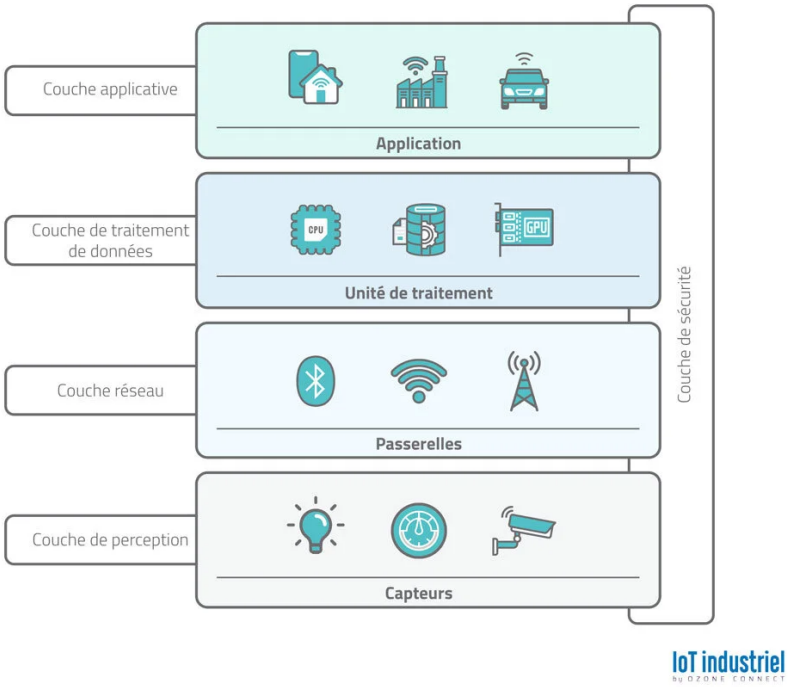

Figure 2 : Architecture IoT

La figure ci-dessus présente l'architecture adopté par l'IoT et définit à la façon du modèle OSI comment les données transitent entre dispositifs et interfaces

logicielles. La couche la plus basse, la couche de perception "[...] est responsable de convertir des signaux analogiques en données numériques et vice versa." (https://iotindustriel.com/) C'est donc cette première couche qui se charge de traduire les signaux émis par les différents dispositifs selon leur fonctions aux couches plus hautes, elle agit "comme un pont entre les mondes réel et numérique".

La seconde couche, la couche réseau représente la collecte des données, leur transmission et s'occupe d'interconnecter les appareils entre eux ou à l'infrastructure réseau global. Pour cela, elle s'appuie de la connexion Ethernet, des réseaux cellulaires, du 6LoWPAN ou du Wi-Fi. Certaines technologies acceptent aussi le NFC (Near Field Communication), le Bluetooth ou le Zigbee.

La couche de traitement des données a pour rôle d'accumuler, stocker et traiter les données de la couche précédente. Cette couche a aussi un rôle de définition de pertinence de la donnée, contrairement aux données en temps réel, les données en temps non réel doivent être définies afin de répondre aux besoins de l'utilisateur pour les placer correctement afin de les stocker le plus efficacement possible dans la solution de stockage. Enfin, la couche va abstraire les données pour améliorer la compréhension entre les différents dispositifs en masquant les détails du matériel améliorant l'interconnectivité entre les appareils.

Ensuite, la couche application est l'interface utilisateur grâce à laquelle celui-ci interagit avec les données récupérées comme par exemple Home Assistant qui propose une solution clé en main afin de gérer ses appareils IoT.

Enfin, la couche de sécurité, transverse à toutes les autres couches de l’infrastructure et regroupe toutes les solutions de sécurité mises en places afin de protéger l'infrastructure. Il s’y trouve des mécanismes de gestion des accès (authentification, autorisation, confidentialité, intégrité etc.) ou des pare-feux, anti-virus etc. Ces solutions sont mises en parallèle avec les besoins utilisateurs et l'application mise en place pour correspondre aux exigences de sécurité requises.

1.2. Usages professionnels de l'IoT

1.2.1. Gestion de l’énergie

La gestion de l'énergie et de l'empreinte carbone devient petit à petit une donnée importante pour les entreprises, d'autant plus que nous, citoyens, sommes grandement sensibilisés aux questions portant sur l'écologie ces dernières années. Ce sujet est porté par la Responsabilité Sociétale des Entreprises (RSE) qui conceptualise, sur la base du volontariat, une démarche pour les entreprises d'intégration de questions sociales, économiques et environnementales. Une norme ISO, la 50001 vient aussi argumenter cette priorité croissante pour la gestion de l'énergie par les entreprises en les aidant à élaborer un système de management de l'énergie. C'est ainsi que naquît le projet "Enercare" de mon ancien employeur, cegedim.cloud, permettant aux entreprises louant des services cloud de mesurer toutes les minutes, leur empreinte carbone en collectant le PUE (Power Usage Effectiveness) et les facteurs de leurs émissions de CO2 annuels **[CegedimCloud.2026]**.

L'Internet des Objets et ses concepts évoqués plus tôt deviennent donc des acteurs potentiels dans cette gestion de l'énergie ainsi que des coûts économiques et environnementaux et ce dans différents secteurs. Par exemple, dans le domaine de l'immobilier et donc de la domotique, qui est mon projet majeur cette année chez La Royale Investissements France. Pour mon alternance, j’ai été mis en binôme avec un second alternant de 3ème année de bachelor informatique, Alexandre, du fait de son profil plus axé sur le développement que le mien qui est plus axé sur le réseau par mon parcours scolaire, nous pouvons nous apporter conjointement de l’aide sur divers sujets et être complémentaires sur nos missions dont l’une d’elle consiste en l’élaboration d’une solution de gestion centralisée d'équipements de domotique pour les investissements immobiliers destinés à re-dynamiser la ville de Molsheim en Alsace et inclure alors dans notre solution un moyen de surveillance de la consommation énergétique des logements, des commerces ou de l'école. Pour cela, nous nous servons de dispositifs de compteur d'énergie intelligents Zigbee, ce

qui fait que lorsqu'un courant électrique passe à travers le capteur celui-ci enregistre la consommation en temps réel et renvoie les informations via le réseau et affiche les données sur l'interface utilisateur (Home Assistant dans notre cas) nous permettant de surveiller sa consommation. Ces technologies peuvent tout aussi bien s'appliquer aux secteurs de l'industrie (par exemple l'industrie automobile) en installant différents capteurs sur les machines (presses, robots, cabines de peinture etc.) ou sur des actionneurs pour les piloter et réduire la charge quand ils sont en veille par exemple. Cette surveillance permet aux industriels de passer d'un compteur général d'usine à un suivi machine par machine et ligne par ligne.

Mais, je constate, notamment par mon expérience professionnelle, que les entreprises et notamment les grandes structures accordent une priorité grandissante à leur empreinte carbone et à leur consommation énergétique, non seulement pour des raisons d'image, mais également pour gagner un avantage concurrentiel grâce à la Responsabilité Sociétale des Entreprises et à son label vendeur face aux clients. Cette constatation est confirmée par l'arrivée d'un terme désignant le fait qu'une entreprise ou une organisation souhaite se donner une image plus éco-responsable qu'elle ne l'est vraiment. Le « greenwashing » ou « écoblanchiement » en français désigne alors les entreprises manipulant l'information pour entrer dans ce sens. L'écologie préoccupe de plus en plus la jeunesse et les entreprises souhaitent se conformer à ces nouveaux principes mais doivent le faire sincèrement.

1.2.2. Confort et productivité

Après avoir passé en revue comment l'Internet des Objets pouvait aider les entreprises à gérer leur énergie et leur consommation, je peux désormais aborder l'idée selon laquelle l'IoT permet aussi d'optimiser le confort et la productivité des employés au sein d'une entreprise. De nouveaux termes anglophones sont apparus associant l'IoT aux besoins d'une entreprise, comme le « smart office » qui définit les endroits de travail devenus intelligents grâce à l'incorporation de dispositifs permettant l'optimisation, l'efficacité et le rendement de ces espaces de travail.

Premièrement, l'IoT permet l'amélioration du confort environnemental de façon autonome, des capteurs mesurent en continu la température, l'humidité, la luminosité et la présence dans les bureaux et salles de réunion permettant d'optimiser automatiquement ces éléments selon les besoins. Si des systèmes CVC sont mis en place alors ces équipements de chauffage, ventilation et climatisation peuvent être automatisés pour améliorer leurs performances, leur réactivité et leur adaptabilité afin de réduire l'empreinte carbone de l'entreprise et ainsi réduire les couts opérationnels de ces équipements. Ensuite, l'Internet des Objets permet l'organisation du personnel et des espaces de travail, en positionnant des capteurs de présence ou d'occupation de bureau, le suivi en temps réel des postes et de la disponibilité de certaines salles devient possible. Cela permet aux équipes managériales d'accroître leur vue globale sur les bureaux occupés afin de ne pas sous-utiliser certains équipements ou laisser à l'abandon certaines salles. Cela permet aussi de récolter des statistiques quant aux utilisation régulières de certaines salles de réunions selon des heures, des jours ou des périodes définies et de prédire les taux d'occupation de celles-ci et ainsi de permettre une meilleure organisation des salles dans un bâtiment. Aussi, l'apparition de chaises et bureaux connectés permettent l'accroissement du taux de productivité des employés grâce à leurs capacités d'adopter plusieurs positions et ainsi personnaliser le cadre de travail de chacun selon leurs préférences, leurs problèmes de santé etc. Mais l'IoT ne s'arrête pas à fournir un confort de travail simplement dans les bureaux mais aussi dans la chaîne de production. En effet, en plaçant des dispositifs, généralement des capteurs spécifiques sur différents équipements d'une chaîne de production, les données récupérées peuvent permettre à une équipe de maintenance de pouvoir visualiser en temps réel les besoins d'une machine donnée et ainsi prédire les travaux de maintenance à réaliser avant que la machine ne tombe en panne ou encore qu'une imprimante ne manque de papier et bloque le travail de certains.

Ce sont tous ces dispositifs placés à des endroits stratégiques qui permettent le maintien en condition opérationnel des salles de réunion, des postes de travail et

des machines servant le quotidien des employés d'une entreprise et leur permettent d'améliorer leur productivité grâce à des conditions de travail améliorées via des dispositifs IoT.

1.2.3. Sécurité et contrôle d'accès

L'Internet des Objets dans un cadre professionnel ne s'arrête pas là et peut se mettre au service de la sécurité. L'IoT permet la centralisation en temps réel de la sécurité et des contrôles d'accès de façon plus fine et automatisée que les solutions de badge ou de clés classiques. L'introduction de contrôles d'accès dits « intelligents » se fait à travers différents nouveaux modes de fonctionnement dont des serrures et contrôleurs connectés pouvant gérer plusieurs modes d'authentification via une plateforme centrale afin de gérer la sécurité selon les besoins. Un contrôleur connecté peut désormais gérer simultanément une carte ou un badge RFID qu'ils soient physiques ou sur un smartphone, une authentification biométrique (empreintes digitales, iris ou visage) donnant accès à des zones plus ou moins privilégiées selon le mode d'authentification et les droits d'accès des utilisateurs. Ces droits d'accès contrôlables via la plateforme dédiée se modifient en temps réel selon les besoins (rôles, zones, créneau horaire etc.) mais peuvent aussi être révoquées instantanément lorsque par exemple un collaborateur se voit dans l'obligation de quitter son poste de travail et ne peut donc accéder à d'autres salles afin de commettre des actions illégales ou de se venger. Toutes ces actions sont possibles sans avoir besoin de remettre de nouvelles clés physiques à chaque fois qu'un besoin est changé pour un collaborateur. Ces nouveaux modes de contrôles d'accès permettent aussi une meilleure traçabilité et supervision puisque les contrôleurs génèrent des évènements horodatés (qui, quand, où, quelle porte) et peuvent faire l'objet de contrôles réguliers ou de supervision si une alerte malveillante est déclenchée. Ce fût une partie de mon travail au sein de l'équipe sécurité chez Cegedim.cloud, qui lors de sa certification SecNumCloud a dû renforcer ses mécanismes de contrôles d'accès dans ses baies serveurs mais aussi dans les espaces de travail afin de n'autoriser l'accès qu'aux collaborateurs ayant un

besoin d'accéder à un espace certifié SecNumCloud, je devais alors toutes les deux semaines effectuer une révision des accès à ces différents espaces et analyser toute alerte ayant été levée par les contrôleurs d'accès. Si un badge n'était pas resté assez longtemps sur le lecteur ou si la porte était resté trop longtemps ouverte, je devais alors investiguer sur les causes de ces journaux alarmants et vérifier si ces alertes étaient légitimes ou non et pour cela je pouvais m'aider notamment des caméras de surveillance donnant sur les différents contrôleurs de badges et ainsi classer les différents journaux selon leur niveau de risque.

Mais ces nouvelles méthodes de gestion des contrôles d'accès et d'authentification sur des équipements physiques ne sont pas exemptés de failles de sécurité, ces serrures modernes étant reliées à Internet sont particulièrement sensibles à différentes attaques utilisées par des pirates souhaitant s'introduire dans des bâtiments ou encore des auditeurs de sécurité « Red Team » exploitant ces failles pendant leurs audits de sécurité physique. Les auditeurs de sécurité spécialisés en Red Team simulent des attaques réelles via des scénarios qu'ils auront eux-même définis afin de tester la sécurité globale d'un système d'information (tel que je l'ai vu en cours durant mon BTS, un « SI » est un ensemble de ressources permettant de collecter, stocker, traiter et distribuer de l'information) ainsi que la sensibilisation des employés. Leurs audits visent à démontrer les impacts et conséquences d'une attaque et de mettre au défi les équipes de défense qui ne sont généralement pas au courant de l'audit et les confronter sur leurs temps de détection et de réaction. Ces auditeurs vont alors tenter d'exploiter des failles de sécurité réelles sur les serrures et contrôleurs d'accès tel que l'absence de secure boot permettant d'introduire un firmware[6] malveillant permettant le déverrouillage à la demande, la désactivation des logs et l'exfiltration de clés et de secrets ou bien l'utilisation de protocoles non chiffrés comme le protocole HTTP qui est défini par le Robert comme étant « le protocole de transmission permettant à l'utilisateur d'accéder à des pages web par l'intermédiaire d'un navigateur » ou encore le protocole Telnet qui est défini dans le glossaire de Lenovo en tant que « protocole réseau qui vous permet de vous

connecter et de communiquer avec des ordinateurs distants via un réseau TCP/IP », ou encore le FTP qui est défini par Fortinet comme « protocole réseau standard utilisé pour le transfert de fichiers d'un hôte à un autre sur un réseau basé sur TCP, tel qu'Internet. » Ces protocole peuvent permettre l'ouverture ou la fermeture des portes en rejouant les paquets et et ainsi ouvrir la porte sans badge. L'interface d'administration avec des mots de passes par défaut devient aussi une source d'attaque très pertinente et souvent la cause principale de l'introduction d'acteurs malveillants dans le système d'informations car c'est une faille bien connue et souvent exploitée notamment dans le domaine de l'IoT.

Ce ne sont que trois exemples parmi tant d'autres mais il en existe encore qui ne sont peut-être pas encore découvertes au moment où j'écris, je souhaite simplement à travers eux appuyer le fait que ces nouveaux contrôleurs ne sont pas des modes de contrôles inviolables et qu'ils doivent être implémentés correctement pour éviter de laisser ces failles nuire à la sécurité d'une infrastructure toute entière.

1.3. L'IoT dans le transport

1.3.1. Transport agricole

Durant le cours présenté par Aurélien Bouvard, RSSI chez Kuhn Group, j'ai bien compris à quel point l'Internet des Objets pouvait devenir un élément technologique central pour certains secteurs d'activités notamment le sien, la construction de matériel agricole. En effet, il nous a présenté, à mes camarades de classe et moi-même un cours sur les normes et les référentiels pour la cybersécurité en général mais via a sa pédagogie vivante, il n'a pas hésité à nous parler de son environnement et de son travail au quotidien dans ce groupe et de l'importance qu'avait pris l'IoT ainsi que l'intelligence artificielle dans les travaux de recherche et développement et ce depuis plusieurs dizaines d'années car l'Internet des Objets aide aussi les agriculteurs dans leur métier en les allégeants de certaines tâches grâce à l'automatisation et la mise en place de solutions agricoles autonomes. Pour y

arriver, les constructeurs ont besoin de dispositifs pour récolter toutes les informations nécessaires à l'autonomisation de leurs véhicules sans pour autant laisser de côté les avis et l'expérience des professionnels qui ont des besoins tous bien différents selon l'exploitation, la région etc.

Ces dispositifs vont capturer plusieurs données télématiques sur les équipements roulants des agriculteurs afin de récupérer un suivi GPS (Global Positioning System) **[LeRobert]** pour étudier les parcours de ces machines, le temps de fonctionnement du moteur, la consommation de carburant et le comportement de conduite afin d'établir des itinéraires plus optimisés et ainsi réduire les trajets à vide pour améliorer les rendements de l'agriculture. Ces données renvoyées à l'interface d'administration de l'agriculteur via le réseau lui permettent toujours de surveiller et contrôler son exploitation. Malgré la ruralité et la vastité des champs dans les campagnes les données arrivent toujours à bon port grâce à des réseaux de longue portée et bas débit comme par exemple, le protocole LoRaWAN (Long Range Wide Area Network ou réseau étendu à longue portée) **[Wattsense.2025]** qui propose une connectivité étendue ainsi qu'une faible consommation énergétique qui en fait une des solutions optimales dans l'implantation de dispositifs IoT permettant aux objets connectés d'échanger des données via des passerelles réseau et de les transmettre à un serveur.

Qualité du signal radio LoRaWAN

	Indicateurs	LoRaWAN					
		SF7	SF8	SF9	SF10	SF11	SF12
RSSI Puissance en réception d'un signal reçu	Mauvais	< -117 dBm	< -120 dBm	< -123 dBm	< -127 dBm	< 129 dBm	< -130 dBm
	Moyen	< 107 dBm	< -110 dBm	< -113 dBm	< -117 dBm	< -119 dBm	< -120 dBm
	Bon	> -107 dBm	> -110 dBm	> -113 dBm	> -117 dBm	> -119 dBm	> -120 dBm
SNR Qualité de la transmission	Mauvais	< 0 dB	< -5 dB	< -8 dB	< -10 dB	< -12 dB	< -15 dB
	Moyen	< 10 dB	< 5 dB	< 2 dB	< 0 dB	< -2 dB	< -5 dB
	Bon	> 10 dB	> 5 dB	> 2 dB	> 0 dB	> -2 dB	> -5 dB

Figure 3 : Qualité du signal radio LoRaWan

Ce graphique présente la portée du signal ainsi que le « spreading factor » ici représenté par les sigles « SF X » qui est la capacité du protocole à régler dynamiquement le facteur d'étalement, plus un facteur d'étalement est faible, plus le temps d'émission sera court et donc le débit de données sera plus élevé, mais la résistance au bruit donc les obstructions sera moindre, il faut donc trouver un bon compromis selon nos besoins pour obtenir la connectivité la plus optimale possible. Cela permet au protocole de s'adapter selon les environnements de transmission afin de préserver au mieux la batterie des capteurs et gagner en efficacité énergétique. C'est donc en majeure partie grâce à ce protocole réseau et les passerelles ainsi que d'autres méthodes de communication à longue portée, dont je ne détaillerai pas le fonctionnement, que les données, même dans un environnement à grande ampleur peuvent continuer à transiter et faire profiter les exploitants de terrains agricoles de l'IoT et de ses fonctions pour intégrer une démarche dite de « smart farming » ou « agriculture intelligente » au plus grand nombre.

1.3.2. Transport routier de marchandises

Après vous avoir démontré comment l'IoT pouvait aider la culture de nos terres, je souhaite désormais aborder le secteur d'activités du transport de marchandises des chauffeurs routiers et de comprendre comment l'IoT pouvait améliorer leur quotidien sur les routes.

Les dispositifs, comme pour l'agriculture, s'ils sont prévus pour, peuvent remonter tout type d'informations GPS ainsi que la vitesse, la consommation carburant, le temps moteur et les codes défauts de chaque véhicules à travers le réseau OBD (On-board diagnostics) que je présenterai plus en détails dans les parties suivantes. Les données récoltées sur le réseau interne sont envoyées à une passerelle embarquée via le protocole MQTT évoqué plus tôt et sont enfin acheminées vers la plateforme centrale , généralement en cloud, grâce aux réseaux cellulaires (antennes 4G, 5G…). Ces données récoltées permettent une gestion de la flotte de véhicules centralisée, elle-même permettant comme dans les autres

secteurs d'analyser les données collectées et d'optimiser chaque aspect du transport tel que l'optimisation des itinéraires, la réduction des trajets à vide ainsi que l'amélioration de l'éco-conduite des chauffeurs mais aussi pour planifier des maintenances sur les véhicules qui le nécessiteraient. L'IoT permet aussi une nouvelle dimension dans la sécurité et la sûreté des chauffeurs grâce à la géolocalisation en continu permettant de retrouver un véhicule n'importe où, des alertes en cas de déviation de trajet, d'arrêt non prévu ou d'ouverture de porte anormal renforçant la lutte contre le vol, la fraude et le détournement de cargaison, une menace grandissante de nos jours tant les reportages sur les conditions de travail et la peur des chauffeurs me paraissent être un sujet toujours plus important.

L'usage de l'Internet des Objets dans ce contexte ne s'arrête pas aux chauffeurs mais s'étend jusque dans ce qu'ils transportent, en effet l'IoT permet une certaine traçabilité des marchandises transportées sur la chaîne du froid notamment grâce aux capteurs intégrés ils permettent de suivre les conditions de transports des produits sensibles que ce soit de l'alimentaire ou bien du pharmaceutique. Les données généralement envoyées à travers le réseau cellulaire permet la transmission en temps réel de ces informations et ainsi déclencher des alertes en cas de dépassement de seuil afin de garantir et fournir des preuves sur le maintien de la chaîne du froid.

1.3.3. Transports en commun

Avant de rentrer dans le coeur du sujet de mon mémoire de recherche, je souhaitais aussi exprimer comment l'IoT pouvait aussi aider les infrastructures de transports en commun en les rendant plus intelligentes afin d'optimiser les trajets de ces transports empruntés par des milliers voire des millions de personnes chaque jour en France.

En effet, l'Internet des Objets grâce à son champ d'application multiples permet aux infrastructures de bus, métros, tramways, trains etc. d'être plus intelligents et interconnectés permettant une dynamique optimisée pour les voyageurs. C'est

grâce à l'IoT que sans s'en rendre de nombreux voyageurs peuvent consulter sur l'application de mobilité de leur ville, dans combien de temps sera le prochain bus etc. Les dispositifs capturant les données GPS et les données des accéléromètres sont renouvelés environ toutes les 10 à 60 secondes pour les transports en question ce qui permet d'estimer avec une certaine précision le temps d'attente qui sera affiché sur les tableaux d'informations dans les rues ou les gares selon le transport. Dans une vidéo publiée sur la plateforme Youtube **[YouTube.2017]**, il y a déjà 8 ans, le Directeur Général de Kéolis Bordeaux Métropole présente les dispositifs intégrés dans les bus qui parcourent la ville permettant la surveillance des bus passant par la machine à laver grâce à des puces RFID installées dans les véhicules qui sont ensuite lues par les machines contrôlant ainsi le passage ou non des bus par le lavage. Les données GPS permettent aussi de traquer la position des bus dans la « zone de lavage ». Pour moi, il est vrai que cet aspect ne me paraissait pas important à première vue mais il indique que ces passages en machine participent au bien-être des usagers et donc à l'image de marque que ceux-ci peuvent avoir d'eux, ce qui pour une entreprise est primordial.

De nos jours, l'IoT peut aussi être accompagnée par l'intelligence artificielle dans des capteurs aidant les infrastructures à effectuer des maintenances prédictives (plaquettes de frein des bus etc.) afin d'éviter les incidents et empêcher des arrêts d'exploitation ce qui serait imputable à l'entreprise et mettrait la confiance de ses usagers en péril. Au-delà des maintenances prédictives, les capteurs peuvent aussi capturer les taux d'affluence dans les transports afin de mieux réguler les services de transports et ainsi permettre, dans les horaires de pointes les plus fortes de mieux gérer les flottes de transports et mieux réguler les passages.

2. Voiture connectée

2.1. Sécurité routière

2.1.1. Évolution de la sécurité routière

Avant de vouloir apprendre à sécuriser une voiture connectée, je trouve qu'il est important d'aborder la question de la sécurité routière, plus palpable par les automobilistes et ce qui est le plus exposé par l'État à travers les différentes campagnes de sensibilisation que je peux voir à la télévision.

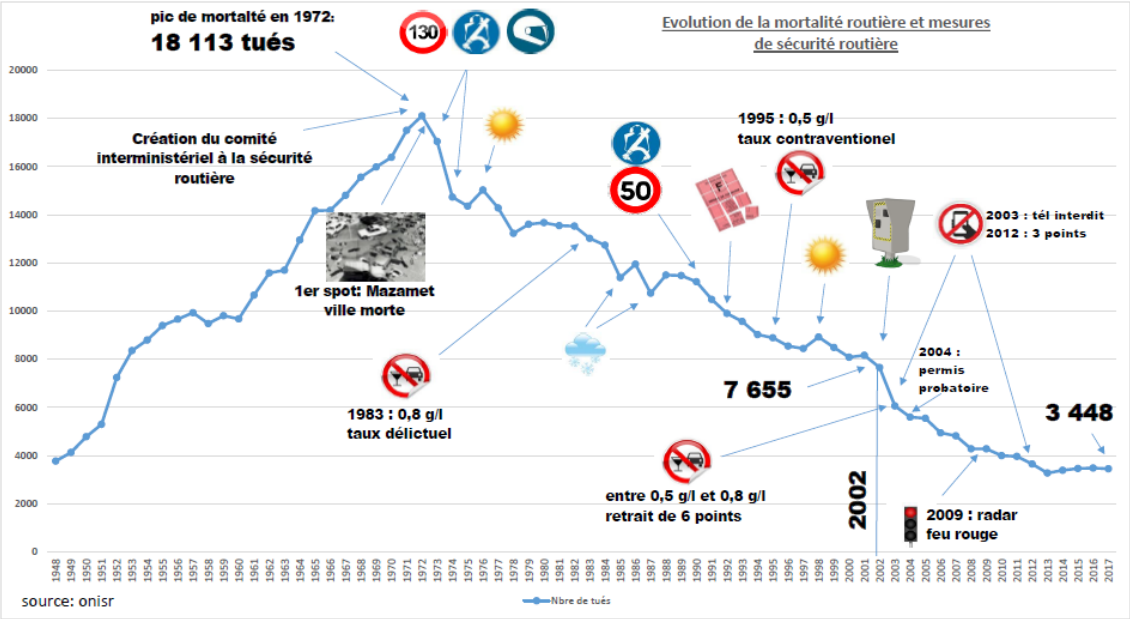

Figure 4 : Taux de mortalité routière en France

Le graphique ci-dessus provient de l'Observatoire national interministériel de la sécurité routière (onisr) **[ONISR]** et présente l'évolution du taux de mortalité routière en France depuis l'année 1948 jusqu'à 2017 ainsi que les principales évolutions en terme de sécurité routière démontrant les impacts positifs qu'elles ont eus sur le taux de mortalité. En 1972 il est observable que 18 113 personnes sont tuées sur les routes en une année, un chiffre record à cette époque, c'est cette même année que l'État prend conscience du danger pour ses citoyens et décide de créer en juillet 1972, un comité interministériel de la sécurité routière dédié à définir la politique de

sécurité routière et à maintenir son application. Les changements apportés par le comité sont multiples, il introduit les limitations de vitesses sur les routes et autoroutes, l'obligation du port de la ceinture de sécurité pour les places avant et obligation du port du casque pour les usagers de deux roues. Il est important aussi de noter l'apparition en 1983 du taux maximum de grammes d'alcool par litre de sang, fixé à 0,8g/L qui une fois dépassé devenait un délit alors qu'autrefois ce n'était qu'une simple contravention et un délit à partir de 1,2g/L. Les véhicules deviennent aussi plus sûrs grâce aux efforts de chaque constructeur automobile avec l'anti-blocage des roues (ABS) puis l'apparition des airbags et enfin du contrôle technique en 1985. Le permis à points est lui, instauré en 1992 permettant ainsi de réduire le taux de mortalité sur nos routes. En 2002, le téléphone est interdit au volant et en 2009, les radars aux feux rouges font leur apparition progressive. Ce sont toutes ces évolutions, qu'elles soient techniques au sein des véhicules que juridiques qui permettent de réduire chaque année le nombre d'accidents mortels sur nos routes.

2.1.2. Types de sécurité routière

Aujourd'hui quand il faut définir la sécurité routière, il faut savoir qu'il en existe deux types, à savoir la sécurité passive et la sécurité active **[Ornikar.2026b]**. Ces deux types, bien qu'ils soient différents restent complémentaires afin d'assurer une sécurité optimale pour les conducteurs automobiles. La sécurité active se concentre sur les dispositifs (différents de ceux vus en IoT) permettant la réduction des risques d'accidents, elle agit en prévention du risque. Il y a dans cette catégorie des équipements internes au véhicule comme l'anti-blocage des roues aussi appelé ABS (de l'allemand : Antiblockiersystem) **[Wikipedia.2026i]** qui est un système d'assistance au freinage limitant le blocage des roues et donc le dérapage, il y a aussi un système de contrôle de la trajectoire qui porte le sigle ESP (Electronic Stability Program) **[RooleMedia.2025]** et permet l'amélioration du contrôle et de l'adhérence du véhicule en corrigeant la trajectoire si nécessaire, mais encore l'aide (ou assistance) au freinage d'urgence (AFU) **[Wikipedia.2025a]** et aide les conducteurs à compenser leurs tendances naturelles à ne pas assez appuyer sur la

pédale de frein et d'autres équipements. Tous ces dispositifs sont reliés à une multitude de capteurs connectés à la voiture et fonctionnaient jusqu'alors en circuit fermé dans le véhicule mais depuis l'arrivée et la généralisation de l'IoT, la voiture pourrait devenir capable d'anticiper les dangers qu'elle ne voit pas encore. Grâce aux communications en temps réel, le véhicule pourrait recevoir des informations de toute sorte d'infrastructure, que ce soit une autre voiture, des infrastructures routières (feux tricolores, météo, embouteillages etc.) mais aussi des organes internes du véhicule, comme la durée de vie des consommables (freins, pneus, liquides etc.) afin de prévenir au mieux en avertissant le conducteur afin d'éviter une éventuelle panne ou un risque accidentel sur la route.

À cela s'ajoute donc la sécurité passive, qui agit plutôt comme une protection au véhicule, elle permet surtout la réduction des conséquences à un accident si jamais un conducteur et la sécurité active n'ont pas réussi à l'éviter. Cette catégorie se compose de tous les éléments nécessaires à cette tâche, comme par exemple, les ceintures de sécurité, les airbags, la cellule de survie **[Ornikar.2026a]** désignant la partie rigide de l'habitacle où se trouvent ses occupants censée se déformer le moins possible en cas d'accident etc. À mon sens c'est cette partie de la sécurité routière qui est la plus démonstrative et dont les gens se préoccupent le plus, c'est ce qui en fait une partie importante pour les constructeurs et en l'objet d'une bataille commerciale entre les constructeurs assurant chacun avoir la meilleure conception de la sécurité chaque année.

Des dispositifs IoT peuvent aussi s'ajouter à cet ensemble d'équipements et deviennent de plus en plus populaires avec par exemple, un capteur de crash nommé eCall **[Wikipedia.2025l]** qui détecte les chocs ou le déclenchement des airbags et appelle directement le 112, le numéro unique d'urgence européen puisque cet équipement est une initiative de la Commission européenne et vise à être équipé sur tous les modèles de voiture à partir de 2035 malgré qu'il soit devenu obligatoire depuis 2018. Cet équipement permet la géolocalisation, le sens de circulation, la vitesse avant impact, le nombre de ceintures bouclées ainsi que

l’intensité du choc. Ces données permettent aux secours de dimensionner leurs interventions et de diminuer par deux leur temps d’arrivée sur les lieux, diminuant considérablement la mortalité post-accident sur nos routes.

2.1.3. Normes et référentiels

Quand je veux parler de normes et de référentiel pour la sécurité routière, la première chose qui me vient en tête c’est forcément le code de la route **[Wikipedia.2026d]**, c’est le manuel pour apprendre à conduire et comprendre comment la sécurité routière est défini. C'est ce texte de loi qui selon sa définition sur Wikipédia : "[...] est l'ensemble de lois et règlements relatifs à l'utilisation des voies publiques par les [...] automobilistes et routiers." Cet ensemble de règles, si elles ne sont donc pas respectées peuvent alors mener à des sanctions comme des amendes ou des peines de prison, c'est dans ce cadre que la sécurité routière évolue.

Mais, les normes ne s'appliquent pas seulement aux usagers de la route mais aussi aux véhicules qu'ils empruntent, les constructeurs doivent se soumettre à certaines réglementations européennes s’ils veulent vendre des véhicules neufs au sein de l'UE. Depuis le 7 juillet 2024, les nouveaux véhicules doivent se soumettre à la norme GSR 2 (Global Safety Regulation) **[LArgus.2024]**, elle prévoit l'ajout de nouvelles aides à la conduite obligatoires comme la direction assistée, la détection de trafic en marche arrière, les systèmes d'alerte de somnolence, la perte d'attention du conducteur et le freinage d'urgence automatique. Les constructeurs automobiles seront aussi chargés de mettre en place un système de "boîte noire" **[LArgus.2022]** enregistrant les données du véhicule avant, pendant et après un accident servant aux autorités dans le cadre d'investigations et cela tout en restant anonyme, le propriétaire ne doit pas pouvoir être identifié grâce aux enregistrements et ne doivent pas être retenues contre le conducteur ni par les forces de l'ordre ni par les assurances, une nouveauté qui a beaucoup fait réagir dans le monde automobile.

Toutes ces nouveautés doivent participer à l'amélioration de la sécurité du véhicule en lui même mesuré par l'organisme Euro NCAP ("European New Car Assessment Program" ou "Programme européen d'évaluation des nouveaux véhicules") créé en 1997 **[Wikipedia.2026e]**. Cet organisme n'est pas une "norme" au sens juridique strict mais est un programme d'évaluation de la sécurité des véhicules neufs, toutefois cet organisme a su s'imposer comme "standard" puisque les constructeurs se fient à leurs tests pour estimer la sécurité de leurs véhicules. Leurs évaluations se composent de plusieurs crashs tests dont certains sont même mis en ligne sur leur chaîne YouTube **[EuroNCAP]** et au final, les véhicules se voient attribuer une note sur 5 étoiles après une moyenne faite sur l'évaluation de différentes catégories comme l'occupation des adultes, des enfants, la vulnérabilité des autres usagers de la route et les aides à la sécurité. Ces tests bien que non obligatoires, permettent aux constructeurs d'avoir un avantage concurrentiel sur leur image ou sur le marketing les poussant à développer alors des voitures plus sécurisées, c'est en cela que l'Euro NCAP est devenu un référentiel de choix pour les fabricants.

En revanche, il existe bien une norme de management appliquée à la sécurité routière, la norme ISO 39001 **[ISO.2012]**, qui définit comment une organisation interagissant avec la route doit organiser son système pour réduire les morts et les blessés graves sur lesquels elle a une influence, elle ne remplace pas la loi mais impose d'identifier et de montrer comment les organisations appliquent ces exigences légales au travers d'un système de management de type "RTS" (Road Traffic Safety) qui se décompose de la même manière qu'une norme pour la cybersécurité (par exemple la norme ISO 27001) avec des analyses, de la surveillance, de la planification, des supports, des améliorations etc. Ce sont toutes ces normes et règlementations qui permettent d'assurer que chaque jour les routes sont un peu plus sécurisées.

2.2. Communication sans-fil

2.2.1. Réseau cellulaire

Pour qu'une voiture soit définie comme connectée, il lui faut, une connexion. Les dispositifs connectés d'une voiture peuvent émettre et recevoir des paquets sur un réseau via différents modes de connexion comme celui utilisé par nos téléphones mobiles intelligents, le réseau de téléphonie mobile. N'étant pas le coeur de mon sujet de mémoire, je ne vais seulement présenter les concepts de base du réseau. Ce réseau fonctionne sur la base de réseaux cellulaires dont l'usage a été spécifiquement pensé pour les équipements mobiles.

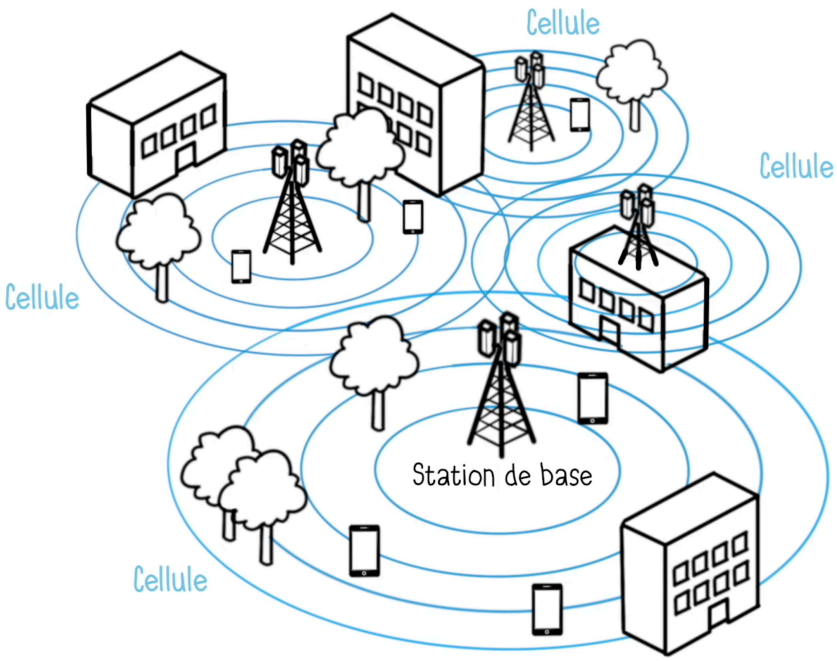

Figure 5 : Schéma représentant le fonctionnement en cellules

Comme le montre le schéma ci-dessus le réseau cellulaire tire son nom de sa topologie car il est segmenté en cellules avec des stations de base au sein de chacune d'entre elles s'occupant de la transmission radio aux différents canaux de signalisation permettant la communication. C'est grâce à ce mode de fonctionnement qu'un utilisateur est capable de se déplacer dans une large zone et

reste connecté à Internet tant qu'une station de base est disponible dans la zone. Ces stations de base sont elles-même reliées à un coeur de réseau qui s'occupe de communiquer avec les opérateurs de téléphonie mobile pour récupérer l'abonnement reliées aux cartes SIM installées dans les différents téléphones.

Après avoir présenté succinctement le réseau cellulaire, je vais me concentrer sur l'accès au réseau 5G étant le plus performant (cent fois plus de débit que la 4G) et fiable actuellement (il supporte jusqu'à un million de mobile au kilomètre carré), couvrant aussi une bonne partie du territoire français devenant ainsi la technologie clé pour les véhicules connectés. Grâce aux améliorations en matière de virtualisation et de cloud, la technologie 5G ne s'appuie plus sur les infrastructures de la téléphonie mobile puisqu'elle est gérée via des logiciels et non des équipements. Elle améliore alors l'accès à la connectivité dans les zones rurales mal desservies et dans les endroits où le réseau 4G ne suffit plus due à l'augmentation constante du nombre d'appareils nécessitant une connexion au réseau, ce que la 5G peut couvrir car elle admet un nouveau spectre radio le Multiple Input, Multiple Output ou MIMO qui permet à un plus grand nombre de transmetteurs et récepteurs de faire transiter les données à travers le réseau. Cette gestion basée sur une couche logicielle et non physique permet aussi une amélioration « […] les expériences numériques grâce à l'automatisation basée sur l'apprentissage automatique. » **[Cisco]** Cette automatisation permet ainsi de satisfaire les besoins grandissants en connectivité avec le moins de latence possible de l'ordre des millisecondes (véhicules autonomes, équipements dans la santé etc.) cette automatisation grâce à l'apprentissage automatique mais aussi l'Intelligence Artificielle et le Deep Learning (sous-ensemble de l'apprentissage avec des algorithmes fonctionnant comme le cerveau humain apprenant à partir d'une étendue certaine de quantités de données) **[OracleFrance.2022]**.

2.2.2. Technologie Wi-Fi

Le wifi, principalement connu pour ses usages domestiques est aujourd'hui devenu une technologie essentielle au bon fonctionnement de nombres d'infrastructures puisqu'elle permet un accès sans fil à Internet ou à un réseau local à un nombre important de personnes avec sa couverture étendue. Contrairement à ce que la plupart de gens peuvent penser le « Wi-Fi » n'est pas l'acronyme de « Wireless Fidelity » mais est une marque déposée et correspond à la certification délivrée par la « Wi-Fi Alliance » (anciennement Wireless Ethernet Compatibility Alliance, WECA jusqu'en 2003) et voit son nom être inspiré du Hi-Fi qui signifie High Fidelity **[Wikipedia.2026k]**.

Finalement, le nom réel et technique du wifi est « IEEE 802.11b Direct Sequence » et agit dans les couches physiques et liaison de données du modèle OSI. La couche physique permet de définir « la modulation des ondes radioélectriques » (fr.wikipedia.org) que va recevoir la carte réseau prévue à cet effet (certaines cartes réseau n'acceptent pas le wifi et ne permettent seulement la liaison avec le réseau Ethernet). Ces ondes varient entre 2,4GHz, 5GHz et 6GHz, la fréquence avec la valeur la plus élevée étant celle pouvant gérer le plus grand nombre de données grâce à son débit plus important. En revanche, la fréquence la plus élevée n'est pas toujours celle dont les utilisateurs ont besoin, tout dépend de ce que nous recherchons, par exemple la fréquence 2,4GHz offre une portée bien plus importante que le 6GHz mais le débit est moindre comparée à celle-ci.

La couche liaison de données s'occupe de faire le lien entre le bus de la machine et la couche physique, un mode de fonctionnement proche de celui du protocole Ethernet. La couche se sépare en deux entités distinctes, l'une d'entre elle, la sous-couche LLC pour Logical Link Control sert d'interface entre les protocoles de la couche trois et la technologie spécifique du support. La seconde sous-couche est la MAC pour Media Access Control, c'est là que tout se joue pour le sans-fil puisque contrairement à l'Ethernet, le wifi doit gérer un milieu rempli d'ondes distinctes et éviter les collisions en implémentant le principe de CSMA/CA (Carrier Sense

Multiple Access with Collision Avoidance) **[Wikipedia.2026c]**, un algorithme distribuant les données sur le réseau lorsqu'il est libre et si il est occupé, l'algorithme va venir choisir un nombre tiré aléatoirement pour attendre avant de retenter la transmission évitant ainsi que toutes les machines ne discutent en même temps dès que le canal se libère.

Le wifi a aussi connu de belles évolutions en terme de sécurité informatique puisque son chiffrement, alors en WEP (Wired Equivalent Privacy) est passé en WPA (Wi-Fi Protected Access) puis en WPA2 et enfin en WPA3 que nous connaissons aujourd'hui, assurant un meilleur niveau de chiffrement lors des communications. En effet, les réseaux sans-fils sont très prisés des attaques MITM (Man-In-The-Middle) **[Wikipedia.2025b]** avec des techniques d'écoute sur le réseau par des personnes n'ayant pas accès au réseau, alors les clés WEP étaient très facilement cassables car le chiffrement RC4 **[Wikipedia.2025g]** n'était que sur 24 bits et la clé ne changeait jamais devenant ainsi vulnérables aux attaques statistiques. Après de trop nombreuses faiblesses trouvées dans ce protocole, les chercheurs en cryptographie ont développé le WPA utilisant le protocole de chiffrement TKIP **[Wikipedia.2021]** qui employait des solutions proches de celles du WEP et aussi en utilisant du chiffrement dynamique contrairement au WEP. Le WPA introduit aussi le Message Integrity Check qui vérifie l'intégrité des messages afin de repérer toute tentative de manipulation de la donnée. L'évolution du WPA, le WPA2 vient encore renforcer la structure en s'appuyant sur l'emploi de la méthode de chiffrement AES (Advanced Encryption Standard) **[Wikipedia.2026b]** au lieu de TKIP. Le WPA2 introduit également le WPA2-Enterprise conçu pour les réseaux d'entreprise utilisant une méthode d'authentification centralisée. Enfin, le WPA3 est introduit pour venir encore renforcer la sécurité des réseaux sans-fil apportant des évolutions comme le chiffrement individuel et une sécurité renforcée des réseaux ouverts.

Le Wi-Fi, dans un véhicule moderne, joue un rôle important pour connecter les occupants, les équipements embarqués et parfois même l'environnement proche (maison, IoT etc.) Les IVI (In-Vehicle Infotainment) sont systématiquement multi-

interfaces dont Wi-Fi et cellulaire pour l'accès IP permettant ces systèmes de pouvoir communiquer avec des serveurs dans le cloud et ainsi bénéficier d'une navigation connectée, de streaming ou des mises à jours de certains contenus. Le point d'accès wifi ou « hotspot » wifi utilise la connexion cellulaire soit du téléphone du propriétaire soit elle est intégrée au véhicule permettant de diffuser Internet à bord via un AP (Access Point) utilisant la norme 802.11. Une étude (MDPI - Open Access Journals) prend le wifi comme base de communication entre l'IVI et les autres ressources du véhicules (caméras, écrans de sièges etc. via un réseau IP interne).

2.2.3. Bluetooth

La technologie Bluetooth est une technologie de communication très appréciée dans les réseaux d'objets connectés, elle simplifie la connexion entre des appareils électroniques en supprimant le lien physique et en remplaçant les câbles entre plusieurs appareils. Cette technologie naît dans les années 1990 chez l'entreprise Ericsson et décide que cette nouvelle technologie porterait le nom de « Bluetooth », une référence qui est directement inspiré du surnom anglicisé du roi viking danois « Harald Ier dit Harald à la dent bleue » **[Wikipedia.2025f]** qui est connu pour avoir unifié les tribus danoises mais aussi pour avoir rassemblé le Danemark et la Norvège durant son règne de même manière que le Bluetooth relie les équipements entre eux et les unifie. Le logo mélange plusieurs lettres de l'alphabet runique inspiré de Harald, le ᛒ et le ᚼ.

Le Bluetooth est donc composé de deux normes de télécommunications à savoir le Bluetooth classique et le Bluetooth Low Energy (LE) optimisé pour ne consommer qu'une faible quantité d'énergie, ces deux normes permettent l'échange entre plusieurs appareils à courte portée en utilisant des ondes radio sur des fréquences entre 2,402GHz et 2,480GHz qui est une bande de fréquence aussi utilisée par le Wi-Fi. Ces normes Bluetooth sont gérées par un organisme dédié, le Bluetooth Special Interest Group (SIG) **[Wikipedia.2025c]** qui est fondé en 1998 par Ericsson et qui s'associe à Intel, IBM, Nokia et Toshiba pour former l'organisme. Pour fonctionner le bluetooth établit un réseau sans-fil personnel éphémère nommé

« piconet » (ou picoréseau en français) ne subsistant que lorsqu'une connexion est demandée et est composé d'un appareil maître pouvant s'appairer jusqu'à 7 appareils esclaves actifs ou 255 appareils esclaves en mode « parked » (les appareils sont connectés mais n'ont pas d'adresses physiques dans le picoréseau). Le dispositif « maître » initialise la connexion et va contrôler le piconet ainsi que les appareils sous-jacents qui eux, ne feront que répondre aux demandes de l'appareil maître et ne peuvent discuter entre eux. Le picoréseau prévoit dans son fonctionnement de pouvoir interconnecter plusieurs picoréseaux entre eux pour obtenir un réseau maillé et faire communiquer tous les appareils entre eux. Chaque appareil bluetooth se distingue de manière unique par son adresse nommée « BD_ADDR ». Ce code de 48 bits reprend la structure de celle des adresses Ethernet, spécifié dans la norme IEEE 802-2001. Cette structure se compose de la « Low Address Part » (LAP) sur 24 bits qui correspond au numéro de série du module Bluetooth, la « Non Significant Address Part) sur 16 bits et la « Upper Address Part » sur 8 bits.

La technologie Bluetooth a plusieurs usages au sein d'un véhicule, il permet de connecter des appareils électroniques comme des téléphones permettant la réception d'appels, la lecture de contenus multimédias et d'autres mécanismes de l'appareil connecté sans avoir besoin de le toucher directement, c'est ce qui est appelé « kit main libres » **[Vroomly.2022]** comprenant un haut-parleur et un microphone directement intégrés dans le véhicule et est autorisé par le code de la route à condition que l'attention du conducteur n'en soit pas affectée.

Comme tout type de connectivité, le Bluetooth possède ses propres failles de sécurité malgré ses améliorations tout du long de sa durée de vie grâce au Bluetooth SIG qui met à jour la technologie afin de prévenir les problèmes. L'introduction d'un code PIN (succession d'un certain nombre de chiffres) afin d'appairer les appareils entre eux constitue une protection contre certains types d'attaque mais reste quand même assez faible dans certains cas puisque certains appareils ont des codes par défaut ou facilement devinables. Par exemple et selon mon expérience personnelle, pour s'appairer au système d'infodivertissement de

certains véhicules, le code est quatre fois 0, ce qui constitue une faille de sécurité dans ce système de connectivité.

2.3. Communication physique

2.3.1. Electronic Control Unit (ECU)

Les unités de commandes électroniques **[Wikipedia.2025k]** (Electronic Control Unit en anglais, simplifié « ECU ») sont devenus des indispensables dans un véhicule, les éléments électroniques étant de plus en plus nombreux en a résulté de la multiplication de systèmes capables de pouvoir les contrôler et les exploiter. Ceux-ci peuvent être matérialisés par des calculateurs embarqués ou des systèmes embarqués commandant les dispositifs internes au véhicule grâce à des capteurs ou actionneurs. Le principal contrôleur d'une voiture reste celui présent dans le bloc moteur défini comme étant son « cerveau » puisqu'il va venir collecter constamment des informations pour contrôler d'autres dispositifs. Ces dispositifs sont apparus à la fin des années 1990 à la fin des moteurs carburateurs. Un moteur à carburateur est un moteur essence dont l'alimentation en carburant est gérée par un dispositif mécanique qui mélange l'air et l'essence avant l'entrée dans le moteur, sans aide électronique, ce qui veut aussi dire que sa maintenance et son réglage était manuel qui le rendait instable aux variations de température, d'altitude ou de charge. Ces systèmes se sont fait remplacer par des injecteurs électroniques beaucoup plus modulables afin de mieux gérer les combustions moteur (dosage carburant et contrôle de l'allumage) pour les normes anti-pollution et les exigences de consommation. Ce système électronique permet effectivement le contrôle des propriétés du moteur pour l'optimiser en faisant ce qui se fait appeler des « stages » **[ECUAUTO21.2025]**, une méthode de débridage du calculateur du moteur, une méthode proscrite en France puisqu'elle change les données inscrites sur la carte grise mais j'ai aussi pu comprendre en participant à des rassemblements de passionnés d'automobile, que cette pratique restait tout de même très populaire afin

de gagner en performance selon les modifications apportées au véhicule. Grâce à l'inclusion qu'ont fait preuve les passionnés à mon égard, j'ai pu comprendre énormément de choses dont le principe de ces stages, allant généralement de 1 à 3 qui apportent des performances différentes mais les contraintes qui accompagnent ces modifications moteur doivent forcément être suivies de modifications matériels au sein du bloc moteur comme le remplacement du filtre à air d'origine pour un filtre à air sport permettant une meilleure respiration du moteur. Le premier stage étant une simple reprogrammation sur le calculateur du moteur ne nécessite pas de modification hardware et plus le chiffre de stage augmente plus les modifications sont importantes et plus les pièces moteur doivent pouvoir supporter ces modifications. Ces expériences avec des passionnés d'automobile m'ont beaucoup appris sur ce domaine de la modification et comprendre leurs motivations et leurs projets m'ont fascinés me permettant de me rapprocher de leur communauté et m'ont poussés à m'y intéresser encore plus intensément.

Du point de vue de la cybersécurité, les contrôleurs électroniques sont des cibles de choix dans les attaques puisque les ECU sont tous interconnectés via des bus comme CAN (Area Network) que je détaillerai dans la partie suivante, souvent sans chiffrement ni authentification ce qui permet d'y interpréter différentes attaques contre les calculateurs. Un ECU compromis ou un appareil tiers branché peut envoyer de fausses trames sur le bus pour simuler un autre ECU et provoquer des actions dangereuses contrôlées par le système embarqué. En y injectant du code malveillant expressément préparé pour les ECU peut permettre de désactiver les sécurités que gère le système embarqué comme les aides à la conduite ou certains éléments de sécurité de l'habitacle. En résumé dès lors qu'un système embarqué contrôle une fonction du véhicule, celui-ci devient vulnérable aux injections de code malveillant.

2.3.2. Types de BUS

Pour s'interconnecter et pouvoir tous communiquer entre eux, les systèmes embarqués utilisent différents types de bus pour subvenir à leurs besoins. Ils ont

tous leur spécificité et leur usage, comme vu, ci-dessus, le bus CAN, est le bus le plus utilisé. Ces réseaux en série succèdent aux faisceaux point à point qui reliaient chaque fonction électrique par des fils dédiés, sans réseau partagé, créant un réseau de câbles de quelques kilomètres dans le véhicule. Chaque nouvelle fonction ajoutée au véhicule (ABS, airbags etc.), augmentait le nombre de fils ce qui augmentait peu à peu le poids, la complexité et le risque de pannes tout en rendant le diagnostic toujours plus difficile. Le bus CAN, conçu par Bosch à partir de 1983, présenté en 1986 et normalisé par ISO 11898 en 1993. Il permet, grâce à son système de multiplexage[7], de récupérer des informations de plusieurs calculateurs, au travers d'un seul et même câble et de faire transiter les informations en les faisant communiquer à tour de rôle. L'introduction de cette méthode de communication a donc permis la démultiplication des calculateurs et des capteurs pour un même système puisque depuis son implantation dans les automobiles, de nombreux industriels se sont emparés de cette technologie, comme l'aéronautique, pour l'embarquer dans leurs systèmes. Le bus CAN est un bus de données dit « de série bidirectionnel half-duplex », ce qui veut dire que les informations qui transitent dans le bus ne peuvent avoir qu'une seule direction à la fois mais tout de même fonctionner dans les deux sens.

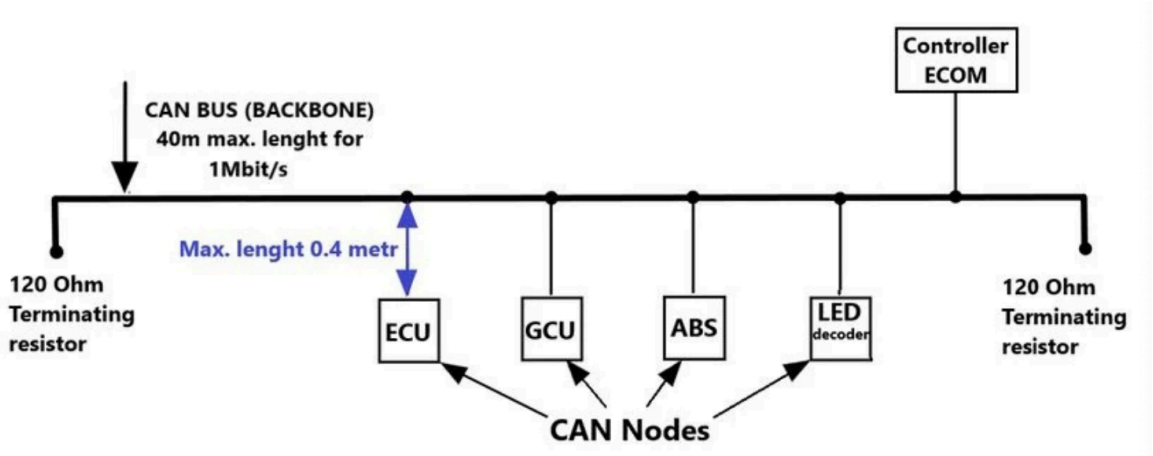

Figure 6 : Représentation d'un bus CAN

Les équipements reliés au bus CAN sont appelés des « noeuds » et peuvent tous communiquer entre eux, ils sont reliés par des paires torsadées (l'un désigné en CAN High et l'autre en CAN Low pour pouvoir envoyer des 0 et des 1, si les deux fils ont le même voltage, il n'y a pas de différence donc c'est un bit à 1 qui est envoyé, en revanche lors d'un changement le CAN High monte à 3,5V et le CAN Low descend à 1,5V envoyant un bit à 0) et suivent la technique CSMA/CR, un autre protocole permettant d'éviter les collisions dans les communications, un seul ECU à la fois peut transmettre des informations et tous les autres sont en écoute et choisis de les recevoir ou de les ignorer. Cette communication ne se fait non pas par tour de parole, mais selon la priorité définie par l'identifiant de trame, plus il est petit plus le message sera prioritaire sur le réseau (le calculateur pour les freins/ABS envoyant un message avec l'identifiant 0x100 sera prioritaire face à un message de l'autoradio pour changer la station qui envoie un message avec l'identifiant 0x500).

Une alternative aux bus CAN, à moindre coût puisqu'il n'utilise qu'un fil par câble et à faible vitesse pour les capteurs et actionneurs, le bus de données LIN (Local Interconnect Network ou Réseau Interconnecté Local en français), est normalisé par l'ISO 17987 et désigne un protocole se basant sur une configuration type « maître - esclave » comme le Bluetooth vu plus tôt. Ce bus est principalement utilisé pour les éléments de confort du véhicule comme les vitres électriques, la climatisation, les éclairages ou encore le verrouillage centralisé du véhicule, des exemples parmi tant d'autres permettant aux bus CAN de se décharger de ces fonctions de confort afin de l'alléger et se concentrer sur les fonctions essentielles au bon fonctionnement de la voiture. Un cluster LIN ne supporte que 16 noeuds comptant un calculateur maître et quinze esclaves, le maître surveillant l'ensemble du bus s'assurant du respect des communications par les noeuds, lui seul pouvant demander des informations.

Quant aux fonctions de multimédia, c'est le bus de données MOST (Media Oriented Systems Transport) qui vient faire les liaisons audio/vidéo dans les voitures « premium » avec son réseau en anneau, les données ne circulant que dans un sens,

évitant ainsi les collisions. Il est décliné en trois vitesses, la première est le « MOST25 » avec une connexion de 25Mbit/s, le « MOST50 » pour une vitesse de 50Mbit/s et enfin le « MOST150 » pour une connexion à 150Mbit/s. Cette dernière déclinaison se distingue par l'introduction d'un canal Ethernet via de la fibre optique, introduite en 2007 elle est configurable entre 0 et 150Mbit/s amplifiant l'efficacité de la transmission des paquets IP.

Enfin, pour ce qui demande de la bande passante à haut débit, j'aurais pu évoquer la technologie de bus de données FlexRay permettant d'obtenir un niveau de transfert de données assez important mais vu son déclin face à la technologie Ethernet, je préfère me concentrer sur celle-ci. Aussi surprenant que cela puisse paraître, Ethernet est bel et bien présent dans les automobiles modernes, une version durcie, résistante à l'environnement d'une automobile, certes. En effet, la transmission via les bus CAN ayant un débit assez réduit (5Mbit/s maximum) pour pouvoir supporter toutes les nouvelles technologies comme les capteurs ADAS (Advanced Driver Assistance System désignant les caméras de recul HD, les radars, les capteurs LIDAR) mais aussi les écrans haute résolution, la connectivité avec Apple CarPlay ou Android Auto et les mises à jour OTA (Over The Air) qui génèrent un grand nombre de données et sont impossibles à traiter pour les bus classiques. Ethernet vient alors apporter 100 à 1000 fois plus de bande passante tout en restant une technologie assez bon marché puisqu'elle est déjà bien implantée dans le domaine de l'informatique en général. C'est notamment grâce à cette évolution, que je me rends compte que l'informatique se déplace de plus en plus de son carcan original et vient s'implanter de plus en plus dans nos vies quotidiennes à travers différents domaines.

2.3.3. OBD (on-board diagnostics)

Comme j'ai pu l'expliquer à travers mes parties précédentes, l'automobile moderne connaît un essor important concernant sa connectivité, malheureusement qui dit augmentation de systèmes connectés dit aussi augmentation des endroits potentiels d'où peuvent provenir un incident. Pour palier à cela, les constructeurs ont

développé un système de diagnostic embarqué accessible via une prise se nommant OBD qui est le raccourci pour On-Board Diagnostics et permet de lire les défauts et données en temps réel depuis les calculateurs. Ainsi, le système OBD surveille et collecte des données de l'ensemble du véhicule pour rapporter l'état du moteur ou autres systèmes électroniques permettant aux techniciens de repérer d'où peuvent provenir les pannes pouvant survenir. Ils surveillent ces dispositifs en se connectant à un connecteur généralement placé sous le tableau de bord, la prise OBD via une valise de diagnostic. Cette valise peut lire la plupart des codes défauts communs aux différents constructeurs, si certains d'entre eux sont différents, il faudra alors que le technicien se munisse d'une valise spécifique au constructeur.

C'est en 1988, que les Etats-Unis imposent la mise en conformité de tous les véhicules légers et camions vendus à la norme OBD-I, contraignant les constructeurs à implanter cette technologie pour le contrôle de tous les composants électriques ayant une influence sur les émissions. En 1996, la norme évolue en OBD-II, elle est toujours obligatoire sur les véhicules américains mais apparaît aussi en 2000 (d'abord pour les moteurs essences puis se généralise aux moteurs diesel en 2003) pour nous, européens, sous le nom d'European On-Board Diagnostics ou EOBD reprenant la norme OBD-II tout en l'adaptant au contexte européen. Cette nouvelle version étend la surveillance aux autres systèmes vitaux du véhicule comme par exemple le système antipollution, la transmission ou encore les différents capteurs de sécurité ainsi que du stockage de ces données dans la mémoire du véhicule.

Cette prise n'est pas exempte de contraintes techniques puisqu'elle doit pouvoir être facilement accessibles pour les techniciens, en étant présente au sein de l'habitacle et à moins de 61cm du volant. Cette contrainte rend donc cette prise vulnérable à des attaques puisqu'elle est la porte d'entrée la plus simple vers les autres bus internes d'un véhicule. Un attaquant se branchant sur la prise OBD via une valise pirate ou trafiquée peut se faire passer pour un ECU légitime et envoyer des messages sur le réseau CAN malveillant, ce protocole n'ayant ni chiffrement ou authentification. L'attaquant peut alors envoyer de fausses informations aux

calculateurs, mais aussi provoquer une attaque DoS, une attaque par déni de service est, comme j'ai pu l'apprendre durant mes cours ou en voyant les effets à travers mes expériences professionnelles, cette attaque est une attaque cyber rendant indisponible un service donné en lui envoyant un très grand nombre de requêtes, interrompant ainsi son fonctionnement normal. Alors, en envoyant un certain nombre de requêtes sur le réseau CAN, celui peut être considéré comme défectueux et être éjecté résultant de l'indisponibilité d'un module précis (airbag, ABS, direction assistée etc.) Cette prise peut aussi être utilisée par des acteurs malveillants pour soutirer le véhicule à son propriétaire, en entrant dans le véhicule (effraction, relais d'ouverture sans-clé...), y connecter une valise malveillante contenant des clés constructeurs volées pour ouvrir une session de diagnostic constructeur, différente de la session OBD, lui permettant ainsi d'enregistrer une nouvelle clé ou de désactiver l'anti-démarrage. Aussi, depuis quelques temps, se démocratisent les dongles OBD connectés par Bluetooth remplaçant ainsi la connexion filaire et facilitant le diagnostic du véhicule à distance mais permettant alors à un attaquant qui compromettrait l'un de ces dongles de pouvoir envoyer ses différentes attaques à distance, attaques prouvées par des chercheurs de San Francisco dans cette vidéo sur YouTube (https://youtu.be/-CH9BvFlrGs?si=jfvy4cwdj4_OI2AW) datant de 2016, je peux clairement les voir activer les essuie-glaces mais aussi les freins d'une Corvette alors même qu'elle est en train de rouler, ce qui peut représenter un réel danger pour les utilisateurs de ce genre de boîtier.

3. Security Information and Event Management

3.1. Les composants d’un SIEM

3.1.1. Collecteurs de données

Avant de rentrer dans les détails de son fonctionnement, il faut comprendre ce qu'est un SIEM (Security Information and Event Management). Le SIEM est apparu au début des années 2000 et désigne une plateforme centralisée qui permet la

collecte, l'analyse et la corrélation en temps réel de journaux et évènements de sécurité provenant de n'importe quel type de systèmes. Cette centralisation permet une efficacité accrue sur la détection des menaces sur l'ensemble d'un système d'informations par l'équipe en charge de cette solution mais facilite aussi la réponse aux incidents de sécurité lorsque cela est nécessaire **[Microsoft]**.

La première étape de cette solution est donc de collecter des données (journaux, évènements...) à travers des chaînes de capteurs, des agents ou des connecteurs réseau pour capturer les évènements qui se passent sur les hôtes et/ou le réseau, puis de pré-traiter ces données et enfin de les injecter de manière fiable et sécurisée dans le serveur central. Dans un premier temps, pour pouvoir capturer les évènements nécessaires et donc alimenter notre solution SIEM, des agents peuvent être installés sur des serveurs ou des postes c'est ainsi qu'au sein de Cegedim.cloud, j'avais la charge de mettre à jour les agents Splunk ou de réinstaller les agents de certains serveurs lorsque ceux-ci n'envoyaient plus de journaux. Ces agents vont s'occuper de récupérer des journaux sur des systèmes (journaux systèmes, activité des utilisateurs…), des applications, des équipements réseau grâce à des sondes (IDS/IPS pour Intrusion Détection System et Intrusion Prévention System) **[Varonis.2025]**, des solutions de sécurité ou encore de l'IoT (des capteurs peuvent être intégrés aux systèmes IoT pour générer des évènements de sécurité) mais aussi de normaliser l'ensemble des journaux récupérés puisque le SIEM doit gérer des formats très variés tout en pouvant fournir une vue unifiée et exploitable pour l'analyste. Il existe deux formats de collecte, le mode agent-based que nous venons d'introduire et d'expliquer mais il existe aussi un second mode de collecte, le mode agentless qui va, lui en revanche, aller questionner via des requêtes les services concernés par la collecte de données via des protocoles standards (syslog[8], SNMP[9], WMI[10], API[11]) ou recevoir des données directement depuis les équipements réseau (comme j'ai fait pour le routeur de l'École 18.06 qui envoie directement des journaux au SIEM qu'Alexandre et moi avons mis en place) ou des équipements de sécurité, ce qui est utile lorsque l'installation d'agents n'est pas disponible.

3.1.2. Traitement / agrégation

Ces données, une fois récupérées par des agents qu'ils soient agent-based ou agentless ou récupérées via des fichiers de journaux importés manuellement vont ensuite être traitées par le SIEM afin d'en exporter les champs utiles tel que l'horodatage (un des champs des plus importants pour reconstruire la chronologie des évènements), l'IP source ainsi que l'IP de destination, l'utilisateur quand cela est possible avec de garantir la non-répudiation (comme je l'ai appris dans de nombreux cours, ces propriétés sont la base de la cybersécurité et la non-répudiation est l'assurance qu'une action réalisée par un utilisateur après l'authentification de ce dernier ne pourrait être remis en cause), les applications concernées, les actions, les codes de retour etc. Cette étape est essentielle puisqu'un journal brut tel qu'il est récupéré n'est pas directement exploitable ni optimisé par un analyste car il doit traiter de nombreuses données par jour et ne peut perdre du temps à varier ses compréhensions de journaux selon les systèmes sur lesquels ils sont récupérés, comme un langage, la donnée est donc après cette étape est convertie dans un langage commun pour favoriser le traitement et l'analyse mais aussi comparer les différentes données.

Ces journaux une fois normalisé, voient leurs unités d'informations découpées afin de rendre la recherche pour l'analyste plus efficace. Pour enrichir les évènements, les SIEM peuvent ajouter du contexte externe comme de la géolocalisation IP, la criticité de la machine qui serait défini au préalable en interne, la réputation d'une adresse IP ou la zone réseau de l'organisation etc. Pour enrichir les évènements récupérés le SIEM peut aussi faire un travail pour éliminer les évènements redondants, trop verbeux ou sans valeur de sécurité immédiate afin de réduire le « bruit », ce qui permettrai à un analyste de n'avoir à inspecter que des journaux utiles. L'agrégation permet ainsi de réduire le volume de données en consolidant des évènements répétitifs et ainsi de faire apparaître des séquences d'attaque qui seraient invisibles dans des logs séparés, je peux prendre l'exemple des attaques DoS (déni de service) que j'ai pu expliquer précédemment dans le

cadre des voitures connectées, si le SIEM récupère des logs uniques de connexion, celles-ci ne valent rien, c'est une fois mises entre elles et concordantes que ces données prennent de la valeur et prouvent ainsi une tentative d'attaque par déni de service.

Au-delà des évènements de sécurité, le SIEM récupère aussi de la donnée utile afin de mesurer les activités de différentes sources, je pense à la récupération de l'usage des processeurs ou du stockages sur certains serveurs applicatifs qui doivent être surveillés afin de fournir le plus de disponibilité possible aux utilisateurs.

3.1.3. Stockage / Restitution

Le rôle d'un SIEM permet la collecte, l'agrégation et la restitution de journaux mais l'une de ses principales fonctions qui en fait une solution de sécurité, à mon avis, très importante pour les entreprises est le stockage de ces journaux qui en font la constitution de preuves en cas d'incident menant à des répercussions juridiques. Le SIEM permet de disposer d'un historique complet des événements de sécurité pour faire de l'analyse forensique et constituer une chronologie de ce qui aurait pu se produire afin de présenter ces preuves devant un tribunal le moment venu.

L'historique permet aussi de pouvoir constituer un historique fiable pour détecter les tendances d'attaques se produisant sur une infrastructure. Lors de ma précédente expérience à Cegedim.cloud, dans l'équipe sécurité, le SIEM que nous exploitions avec la solution « Splunk » était l'application la plus utilisée en terme de recherches et d'analyses puisque grâce à notre historique et notre politique de stockage et de traitement des données, nous pouvions détecter plus rapidement des évènements qui pouvaient s'avérer être des faux positifs et ainsi les référencer dans nos documents de traitement pour alimenter notre gouvernance et améliorer notre efficacité pour ne pas passer plus de temps que nécessaire sur une alerte donnée. Au-delà des alertes de compromissions, le SIEM nous permettait de respecter nos exigences de conformité, puisque notre activité principale était le stockage et le traitement de données sensibles (notamment des données de santé),

nous étions certifiés HDS (Hébergeur de données de santé) **[AFNORCertification]** et avions donc des audits de conformité réguliers et devions donc présenter des preuves de conformité aux auditeurs. Évidemment, ces logs ne sont pas stockés indéfiniment, cela poserait évidemment des problèmes de stockage mais aussi de confidentialité, c'est pour cela qu'à Cegedim.cloud, nous ne stockions les journaux que 3 mois dans notre stockage principal avec lequel nous pouvions encore interagir avec les journaux très simplement sur notre interface Splunk puis passé ces 3 mois, nous les envoyions dans des stockages secondaires dits « froids » **[PureStorage.2026]** (donc archivés ne permettant pas l'accès direct au contenu pour des données qui ne le nécessitent pas) pendant encore 9 mois afin de les récupérer en cas de nécessité. Au bout d'un an au total les journaux sont donc supprimés de notre infrastructure afin de rester conforme au RGPD[12] et les certifications **[Inkivari]**.

Comme je l'ai expliqué précédemment l'un des rôles du SIEM est de permettre aux analystes de parcourir facilement les journaux collectés, selon la temporalité, les hôtes, les utilisateurs ou les types d'évènements et pour leur faciliter la tâche les développeurs de solution de SIEM ont intégrés la mise en place de tableaux de bord.

3.2. Fonctionnement d'un SIEM

3.2.1. Cycle de vie d'un évènement

Le cycle de vie d'un évènement dans un SIEM suit un parcours tracé, de sa génération jusqu'à son stockage indexé en passant par la collecte, le traitement, la corrélation et enfin son stockage consultable pour l'investigation et l'audit pour finir archivé.

Tout commence sur la source, le système d'exploitation, l'application métier, la base de données, un équipement réseau ou une solution de sécurité, lorsque l'un de ces équipements va générer lors d'un évènement significatif, une authentification,

une erreur, un accès à un fichier, sa modification, sa suppression, une modification de configuration, une alerte de sécurité etc. Un journal (log) est donc une trace écrite et horodatée d'un fait observé par la source (d'où l'observateur d'évènements sur Windows) destiné à permettre le diagnostic, la traçabilité et l'audit sur un système donné. L'évènement, une fois détecté est enregistré en fichier de journaux (généralement des fichiers en .log qui peuvent communément être retrouvés sur Linux ou Windows), à ce stade le log ne contient généralement que la date, l'heure, l'origine, parfois le niveau de sévérité, l'identifiant d'évènement, le message correspond à l'évènement, potentiellement l'utilisateur concerné, une adresse IP, un processus, un code retour etc. Ces premières informations sont importantes pour la suite puisqu'elles vont permettre de conditionner la qualité de l'exploitation et la capacité de corrélation entre plusieurs évènements. Aussi, plus il y a d'informations fiables et cohérentes, plus il sera facile de filtrer et d'agréger les évènements plus tard dans le SIEM. Ces premières données, sous format de journaux, sont d'abord stockées en local sur la machine source, cela permet de garder une trace en cas d'indisponibilité du collecteur et de l'envoyer plus tard vers un serveur distant via l'agent, le protocole syslog ou autre intégration native de la solution.

Une fois que les évènements arrivent sur le système de supervision, ils ne sont pas encore exploitables c'est pour cela qu'ils doivent être triés puis normalisés afin de répondre aux exigences du SIEM. Leurs différents formats seront convertis, les champs extraits, les horodatages seront harmonisés, la structure corrigée, le bruit supprimé etc. C'est aussi à ce moment là qu'intervient l'enrichissement des journaux avec des données contextuelles que j'ai pu expliquer dans la partie 3.1.2. L'objectif de ces étapes est d'obtenir des évènements homogènes afin qu'ils puissent être analysés dans une interface unique sous le même format avec des éléments de message brut transformés en informations utiles. Ces évènements vont être indexés, pour une recherche rapide, via des structures internes permettant de trier les évènements et ainsi les retrouver plus rapidement dans le flux d'informations engrangés par le SIEM. Ces journaux resteront stockés « à chaud » dans un stockage

facile d'accès pendant un certain temps défini par l'organisation puis seront envoyés dans un stockage « à froid » ce qui veut dire qu'ils seront archivés mais récupérables en cas de nécessité. Le cycle de vie de l'évènement s'arrête au moment où il est supprimé par l'organisation (généralement au bout d'un an pour respecter les directives du RGPD).

3.2.2. Détection et corrélation

Tout le long de son cycle de vie, un journal collecté est amené à être mis en relation avec plusieurs autres journaux qui constituent ensemble un signal, c'est là qu'intervient la corrélation.

Le SIEM permet de détecter plusieurs journaux provenant de différentes sources afin de déterminer si ou un plusieurs signaux peuvent constituer ensemble une alerte qui ne serait visible qu'en corrélant ces évènements puisque seuls ils ne vaudraient pas grand chose. Après la normalisation de leurs caractéristiques principales puis enrichissement des données, le SIEM applique à son flux de journaux un ensemble de règles de filtrage et de corrélation permettant de détecter des répétitions ou des anomalies pouvant révéler une menace qui serait ensuite analysée afin d'en évaluer la vraisemblance et ainsi constituer une alerte ou non si cela n'est pas nécessaire. Comme j'ai pu le voir dans mon cours de cette année de « Réaction à un évènement cyber et gestion de crise », une alerte est avant tout un signal indiquant qu'un évènement potentiellement anormal s'est produit sans pour autant signifier qu'un incident de sécurité affectant la disponibilité, l'intégrité ou la confidentialité du système d'informations n'est confirmé, celle-ci peut être considérée comme faussement positive ou vraie positive dépendant de la situation et des évènements relevés ainsi que des règles et des documents mis en place par l'organisation dans son SMSI (Système de Management de la Sécurité de l'Information prévu par l'ISO 27001) par exemple **[FeelAgile.2026]**.

Ainsi, après avoir regroupé plusieurs évènements et les avoir mis en corrélation, si une règle de filtrage est satisfaite et qu'une alerte est créée, le SIEM va venir

enrichir cette même alerte en indiquant la règle qui a été déclenchée, l'entité principalement touchée, le contexte, la criticité, le tag MITRE ATT&CK (Base de données mondiale recensant les tactiques et techniques utilisées par les cyber-attaquants) etc. Cette alerte est ensuite envoyée vers l'équipe sécurité pour la transmettre à l'équipe en charge du système potentiellement corrompu afin qu'elle puisse traiter l'alerte et l'escalader si nécessaire via un ticket en priorisant celui-ci selon la sévérité et l'actif touché, c'est généralement le rôle de l'analyste SOC (Security Operations Center). Ces règles de filtrage sont assez explicites, elles décrivent un chemin d'actions attendues, comme un algorithme. Elles peuvent être définies par des conditions sur des champs (champs générés après l'agrégation et l'enrichissement), des seuils (tant d'échecs en moins de X minutes), des fenêtres temporelles et parfois des logiques de séquence pour modéliser le potentiel chemin d'attaque d'un acteur malveillant (reconnaissance, exploitation, élévation de privilèges autrement dit ce qui est retrouvable sur la base de MITRE ATT&CK). Ces règles peuvent être maintenues à jour manuellement en mettant à jour la liste des filtres et en maintenant à jour la liste des sources critiques, des nouveaux chemins d'attaque etc. mais elle peut aussi être mise à jour grâce à l'intégration de règles comportementales et/ou du machine learning[13] pour construire une base de référence de comportements normaux des utilisateurs, un système ou une application. Cette méthode permet aussi la détection de chemins d'attaque qui n'ont pas encore été découvertes et qui n'ont donc pas de signature, une méthode fort utile aussi pour la détection de compte compromis ou l'exfiltration de données anormales ainsi que les scénarios d'authentification suspectes. Ainsi, le moteur de corrélation ne se limite pas à produire une alerte par évènements, il regroupe souvent plusieurs évènements liés dans un même « incident », qu'il soit avéré ou non afin de donner une vision plus globale à l'analyste. Ce regroupement lui permet ainsi de réfléchir en termes de scénarios et non pas en termes de lignes de journaux.

3.2.3. Exploitation

Les tableaux de bord agrègent des indicateurs issus du SIEM (volumes d'alertes, types de menaces, sources générant le plus de bruit etc.) permettant de vérifier en un coup d'oeil sur l'état global de la sécurité du systèmes d'informations.

Figure 7 : Exemple de tableau de bord sur Splunk

Comme je peux l'observer sur l'exemple de tableau de bord venant du fournisseur de solutions, Splunk, tout est fait pour que l'analyste en charge du périmètre puisse organiser et plus simplement interpréter l'immense quantité de données injectée chaque jour et ainsi améliorer son efficacité grâce aux tableau de bord alimentés par les données en temps réel. Je peux aussi observer sur l'exemple, une analyse globale selon des niveaux de criticité, le nombre total d'alerte relevées selon leur urgence, la chronologie avec des statistiques et tout cela est représenté par un code couleur bien défini afin, encore une fois, d'alléger le travail de l'analyste. Mais ces tableaux de bord hauts en couleur ne servent pas seulement aux analystes en charges de la surveiller la sécurité du système d'informations mais servent aussi à présenter des résultats au RSSI et à la direction puisque la compréhension est simplifiée, elle est compréhensible de tous et permettent le suivi des risques et détecter les écarts par rapport à la situation normale. Pour étayer mes propos, à

Cegedim.cloud, au sein de l'équipe sécurité dans laquelle j'évoluais, nous avions préparé un tableau de bord spécialement conçu pour permettre la surveillance des actifs qui seraient les plus critiques pendant la période des Jeux Olympiques, qui nous le savions allait être une période où la France et ses infrastructures allait être la cible d'une multitude d'attaques puisque nous allions être au centre du monde pendant deux mois. Cette interface interactive permet aussi la navigation entre alertes ou indicateurs (IP, utilisateur, domaine etc.) facilitant les reconstitutions chronologiques et permettant d'établir une réponse aux incidents plus précise et visuelle lors de l'établissement du rapport d'incident.

Ces réponses à incident se voient être de plus en plus automatisées grâce à l'installation de SOAR (Security Orchestration, Automatisation and Response) **[IBM]**, des solutions se greffant directement au SIEM pour orchestrer et automatiser une partie de la réponse à incident. Elles récupèrent les alertes générées par le SIEM et les enrichissent de nouveau selon le contexte (recherche CTI[14], tests via des machines bac à sable, recherche de réputation de la potentielle adresse IP malveillante etc.) et peuvent aussi déclencher des actions techniques sur les autres solutions de sécurité (blocage sur les pare-feux, anti-virus etc.) Le SOAR peut être vu comme étant le « chef d'orchestre » des solutions de sécurité en exécutant des actions prédéfinies réduisant ainsi la charge des analystes qui n'ont plus à aller bloquer une menace sur chaque équipement de sécurité un à un, réduisant alors aussi le temps moyen de réponse à incident. Le SIEM est ainsi particulièrement soumis à l'amélioration continue, chaque incident améliore les règles de corrélation, les enrichissements et les actions du SOAR selon les menaces ainsi que ses réponses aux incidents et permettant au moment de l'agrégation de réduire toujours plus significativement le bruit inutile, améliorant aussi les compréhensions de scénarios d'attaques et les capacités d'analyse avancées.

3.3. Quelques cas d'usage pour un SIEM

3.3.1. Détection d'intrusions

Afin de donner plus de sens à mes propos, je vais pouvoir maintenant évoquer quelques cas d'usage typique pour un SIEM plus en détails.

Dans le cadre de potentiels détections d'intrusions, la corrélation d'évènements joue un rôle majeur afin de mettre en lumière les évènements qui pourraient indiquer qu'une intrusion ou une compromission s'est avérée, pour cela l'analyste doit se baser sur un socle de journaux « prioritaires » comme les journaux sur les identités avec les logs d'authentification réussie ou échouée, les tentatives d'authentification via le multi-facteurs, les élévations de privilèges ou les logs des terminaux avec les processus, les indices de persistance, les alertes anti-virales ou encore des logs provenant du réseau avec les alertes sur les flux sortants par exemple (potentielle extraction de données).

Pour pouvoir détecter une attaque par brute-force (attaques par dictionnaires donc le fait de tester plusieurs combinaisons jusque trouver la bonne) sur un environnement Active Directory[15] **[ITConnect.2024]**, donc Windows, une équipe SOC doit être en mesure de pouvoir analyser des « Event ID » donc des identifiants d'évènements. Au sein de Cegedim.cloud, il était devenu tellement régulier pour moi de travailler avec ces identifiants que j'ai fini par les connaître par coeur (ce qui n'est plus le cas aujourd'hui), que ce soit au support de premier niveau afin de mieux comprendre pourquoi un compte utilisateur pouvait être bloqué ou bien au sein de l'équipe sécurité ou je devais analyser des journaux pour comprendre si une compromission était avérée ou non et déclencher un ticket incident si cela était nécessaire. Je pouvais ainsi rapidement reconnaître dans un évènement si il s'agissait d'une authentification échouée ou réussie. Puisqu'ils sont au coeur de la surveillance sur Windows et comme chaque action sur une machine de ce système d'exploitation génère des identifiants d'évènements distincts, il devient alors plus simple pour un SIEM de pouvoir corréler plusieurs évènements ensemble, ainsi la

détection d'intrusions par attaque brute-force peut se faire assez simplement en regardant des évènements ayant le même identifiant et le même nom d'utilisateur ou la même machine hôte. Ainsi le SIEM devient en capacité et a le pouvoir d'en déduire d'une attaque potentielle si l'horodatage est assez rapproché. Plusieurs échecs venant d'un même compte utilisateur mais dans des temps assez éloignés pour qu'un utilisateur ait le temps de retaper son mot de passe ne déclencherait donc pas d'alerte, au contraire d'évènements se produisant à 0,3 secondes d'intervalle.

Le SIEM peut aussi détecter des connexions depuis des pays inhabituels et est l'un des signaux les plus efficaces concernant la compromission de comptes, cela se base sur l'enrichissement de la géolocalisation via adresse IP. Ce type d'alerte est d'autant plus surveillée depuis la démocratisation du télétravail puisqu'il permet de savoir d'où provient la connexion et d'en déduire la connexion légitime ou illégitime, un employé se connectant dans un pays étranger à une heure inhabituelle pourrait traduire de la compromission d'un compte. Aussi, le SIEM permet de détecter via la corrélation temporelle et des journaux de connexion, ce qui est nommé « le voyage impossible », autrement dit un employé qui se connecte à 9h00 à Paris, puis se reconnecte à 9h30 à Singapour, ces journaux indiquent tous les deux des tentatives de connexion réussies mais celles-ci sont physiquement impossibles. Ainsi, ces deux évènements corrélés peuvent déclencher une alerte puis être re-qualifiés par un analyste SOC en un incident de sécurité puisque l'authentification de l'utilisateur n'est plus fiable, ne garantissant plus la propriété de la non-répudiation.

Lors d'une intrusion par un tiers malveillant au sein d'un système d'informations, d'autres journaux restent intéressants à surveiller, ceux qui collectent les actions effectuées par des comptes à privilèges. Lors d'une attaque avancée, il faut repérer les mouvements suspects de ces comptes pouvant perpétrer des actions frauduleuses comme l'utilisation soudaine de commandes Powershell pour manipuler des droits administrateur ou encore l'ajout d'un autre compte dans un groupe à haut privilèges (Domain Admin, Entreprise Admin) qui génèrent des

journaux caractérisés par les « Event ID » numéros 4728 et 4756. Pour éviter cela, il faut durcir la sécurité de ces comptes spécifiques et limiter leurs droits à ce dont ils ont besoin ainsi que surveiller de près et mettre des alertes dès qu'un Event ID 4728 ou 4756 est généré.

3.3.2. Conformité

La conformité est devenue un principe essentiel pour les organisations, elle est le résultat de pressions réglementaires, contractuelles et d'assurance qui s'accumulent. Le SIEM aide donc à répondre à ces exigences réglementaires pour faciliter les audits de conformité, qui est comme, l'intervenant M. THIROINE, l'a défini en cours de « Conduite d'un audit de sécurité », l'évaluation du niveau de conformité et/ou de sécurité de la gouvernance, des politiques ainsi que des procédures de sécurité mises en oeuvre pour assurer le maintien en condition de sécurité du système d'informations. Pour arriver à cela, le stockage et le classement des journaux de sécurité est primordial pour assurer aux auditeurs, mais aussi aux clients de la maturité de l'organisation sur les questions de cybersécurité en se conformant aux recommandations de l'ANSSI (Agence Nationale sur la Sécurité des Systèmes d'Information), de la CNIL principalement pour le RGPD qui est la norme européenne incontournable au vu des sanctions prévues en cas de non-respect de cette règle (jusqu'à 4% du chiffre d'affaires mondial).

Les journaux deviennent donc des preuves permettant aux auditeurs de pouvoir vérifier qu'une politique de sécurité a bien été appliquée ou de pouvoir reconstituer la chronologie d'un incident. Ainsi, les logs se doivent d'être fiables, horodatés, protégés contre l'altération et conservés pendant la durée légale. Cette durée est définie par les règles de l'organisation allant de 6 mois à 3 ans selon les contextes (comme je l'ai évoqué, à Cegedim.cloud, nous traitions des données de santé et conservions nos logs pendant 1 an). La plupart des normes imposent aux organisations de pouvoir identifier la source des journaux, de séparer les logs sensibles et les logs techniques, de définir des règles de purge, d'archivage et de pseudonymisation si nécessaire. Justement, pour répondre aux exigences du RGPD

en matière de surveillance, il impose aux organisations de garantir les propriétés de confidentialité, d'intégrité et de traçabilité de toutes les opérations concernant des données à caractère personnel ce qui implique de pouvoir répondre aux questions des auditeurs sur les personnes qui y ont accès à ces données, depuis quand, depuis où et pourquoi. Pouvoir répondre à ces questions, me fait repenser aux accès sur les environnements SecNumCloud au sein de Cegedim.cloud qui étaient très stricts, avec des accords de confidentialité, l'envoi du casier judiciaire etc. Tout cela était surveillé et journalisé afin de prouver aux auditeurs de certification que seuls ceux en ayant le besoin peuvent avoir accès à ces environnements fermés, c'est le principe du moindre privilège.

Une autre norme prouvant la maturité des organisations sur les questions de cybersécurité, la norme ISO 27001 qui exige la mise en place d'un Système de Management de la Sécurité de l'Information qui soit vivant, améliorable et opérationnel. Cela implique, pour les auditeurs, de pouvoir récupérer des preuves de surveillance active, de détection, de traitements des évènements et de révision périodique puisque ce système ne doit pas être figé et alimenté seulement avant les audits, il peut et doit servir à tous les collaborateurs de l'organisation pour trouver de l'information utile. Cette mouvance est permise par le SIEM mis en place, grâce aux différentes automatisations, il permet d'entretenir et de tenir à jour le SMSI et autres besoins en réglementations en offrant sa surveillance continue et ses preuves de contrôle du cycle de vie de l'entreprise via les accords, les modifications et les suppressions des identités et des droits, ceci étant permis tant que les journaux sont accessibles dépendamment des règles de stockage imposés par l'organisation et des réglementations en vigueur.

3.3.3. Réponse aux incidents

La réponse aux incidents ne se limite pas à solutionner un problème lorsque celui-ci éclate. La réponse aux incidents permet que ce genre d'évènements négatifs ne se reproduisent pas en mettant en place et en faisant vivre les politiques de sécurité, une analyse des risques, des outils technologiques et tout autre document

ou outil visant à limiter l'impact d'un incident. La surveillance en continue permise grâce au SIEM permet à l'équipe d'analystes d'avoir entre leurs mains et sous leur responsabilité, le fil conducteur de toute l'investigation, ce qui permettra en cas de crise, reporter aux équipes concernées, ce qui s'est passé avant, pendant et après l'attaque et ainsi faire évoluer l'organisation selon les choix qui seront pris. La réponse aux incidents s'appuyant sur le SIEM vient reprendre tous les éléments expliqués plus tôt et les mets en pratique afin de fournir des pièces et des preuves permettant de comprendre toute la complexité (ou parfois la simplicité) d'un incident survenant dans une entreprise.

Le SIEM joue donc un élément prédominant dans la réponse aux incidents et cela avant même que ledit incident ne soit déclaré à travers sa collecte permanente, tous les jours, à toutes les heures sur l'ensemble du système d'informations. Sans cette collecte automatisée, il faudrait aller chercher manuellement les journaux concernés sur les machines une par une, potentiellement incomplets, déjà écrasés ou supprimés par l'attaquant, ce gain de temps justifie à lui seul l'usage d'un SIEM pour une organisation. Ensuite, lorsqu'une alerte se déclenche, le SIEM a déjà recueilli toutes les informations nécessaires à l'investigation par un analyste qui va se charger de récupérer des données sur ce qui s'est passé mais aussi sur la chronologie des évènements afin de remonter à la source de l'alerte et comprendre si cela s'avère être une alerte illégitime auquel cas il mettrait à jour la documentation nécessaire à limiter les alertes faussement positives ou si cette alerte s'avère être une vraie positive, qu'il pourrait re-qualifier d'incident de sécurité si cela est nécessaire. Le SIEM permet aussi de gagner du temps sur cet aspect là, puisque grâce à l'enrichissement des données via des sources externes (réputation adresse IP, fichiers associés à des malwares[16] etc.) Cette rapidité de réponse à l'incident est primordial, puisque réduire la fenêtre d'action d'un attaquant en contenant la menace au plus vite permet de réduire significativement les impacts de l'attaque en cours. Le temps de réponse est aussi fort important dans le cadre de la remédiation et de communication apportée aux clients puisqu'il devient peu à peu une métrique

capitale, aux enjeux économiques lourds de conséquences, car selon mon expérience, la plupart des clients attendent des temps de réponse sur les incidents en cours les plus faibles pour éviter des temps d'inactivité (donc pas toujours de production de richesses) étant donné que cela représente pour eux un réel impact financier. Une entreprise avec une certaine maturité cyber vise en moyenne une détection en moins de 24 heures et une remédiation en moins de 72 heures.

Le SIEM est aussi un outil très puissant dans les analyses post-incident, puisque permettant de retracer la chronologie des évènements, il permet à des analystes forensique de pouvoir déterminer ce qui a pu provoquer l'incident. Ils analysent les dommages subis et les traces laissées par les attaquants permettant de reconstituer l'attaque et constituer un dossier contenant des éléments exploitables pour la justice. D'après le cours vu en première année de Mastère Cyberdéfense sur la forensique, pour que les preuves soient recevables par la justice, elles doivent être toutes horodatées et reproductibles par un technicien via le rapport fourni, elles doivent aussi être non destructives pour le support de stockage d'où elles proviennent, tout doit être recopié à l'identique sur un support externe afin de garder les preuves originales en l'état. Ces éléments vont aussi servir par la suite, d'un point de vue technique à améliorer la qualité de sécurité de l'entreprise attaquée en menant les actions préventives nécessaires sur les points faibles et stratégiques de l'organisation.

1. Le SIEM au service de l'automobile

4.1. Identifier les données exploitables dans une voiture connectée

4.1.1. Nature des données collectées

Les données récupérées pour un SIEM au service de l'automobile peuvent être regroupées en quatre grandes familles tel que la télémétrie, les évènements techniques des ECU et des passerelles ainsi que les journaux des fonctions critiques et enfin les métadonnées de sécurité liées à la connectivité et aux identités. La télémétrie des informations comme la vitesse, l'odométrie (le compteur kilométrique), les accélérations, les freinages, l'état de la batterie, la consommation, les cycles de charge (voiture électriques ou hybrides), les états d'allumage ou encore des indicateurs d'usage comme les temps d'arrêt et les trajets. Dans un contexte de surveillance de flotte, ces données sont utiles pour vérifier l'éco-conduite ou comprendre certains problèmes techniques pouvant survenir, dans mon contexte de SIEM, ces données sont importantes pour vérifier si les données sont cohérentes, par exemple un déplacement géographique incompatible avec l'état du véhicule ou une consommation anormale après un évènement suspect.

Les calculateurs, eux, génèrent des évènements très variés comme le démarrage, l'arrêt, la réinitialisation, la présence d'un défaut interne, une surcharge du processeur, une perte de synchronisation temporelle (qui peut prévenir d'un problème potentiel, comme au sein d'un ordinateur). J'ai eu l'opportunité de pouvoir m'entretenir avec M.BOUVARD Aurélien, RSSI de chez Kuhn Group mais aussi notre professeur de la matière « Normes et Référentiels » qui a pu me confirmer lors de notre entretien de la réalité du terrain à laquelle il était lui-même confronté que les journaux fonctionnels que les calculateurs génèrent et les journaux de sécurité associés constituaient en effet les journaux prioritaires à récupérer. Ces données traversent des passerelles, qui génèrent elles-mêmes des évènements de routage, de filtrage, de traduction de protocole (CAN, Ethernet etc.), d'authentification etc. Récupérer ces données est pertinent pour un SIEM destiné à l'automobile puisque

cela permet de contrôler si une trame a été refusée, si une passerelle a modifié un message, si un ECU a redémarré de manière inattendue ou si un composant a envoyé un volume inhabituel de messages permettant de repérer si un ECU a pu être compromis par un attaquant et si oui, lequel permettant d'investiguer plus en profondeur par la suite via la forensique sur cet élément **[MISC.2025b]**.

En ce qui concerne les fonctions critiques, le SIEM collecte des évènements détaillés et horodatés liés au freinage, à l'info-divertissement et à la recharge. En ce qui concerne le freinage, ce qui peut être surveillé par exemple, ce serait les activations des aides à la conduite ABS et ESP, les demandes de freinage automatique, les conflits de commande ou les erreurs de capteurs associés. Pour l'info-divertissement le but est de surveiller principalement les accès réseaux, les connexion en Bluetooth ou Wi-Fi, les mises à jour, les applications tierces et les tentatives de persistence. Ces équipements d'info-divertissement sont les portes d'entrée les plus exposées vers l'extérieur ce qui les rend plus vulnérable à des attaques cyber. Étant connecté à la passerelle centrale, souvent développé avec le système d'exploitation Linux, cela en fait un moyen de pivot voire même d'élévation de privilèges, le plus attractif pour les attaquants. La recharge est quant à elle surveillée via les négociations de session, l'état du chargeur embarqué, les erreurs de protocole, les interruptions et les évènements liés à la batterie haute tension. La recharge, bien qu'elle soit une surface d'attaque encore peu connue est particulièrement critique puisqu'elle constitue un lien physique et numérique entre le véhicule et une infrastructure externe. Elle permettrait donc à un attaquant de pouvoir compromettre une borne de recharge et donc de créer un canal d'attaque, qu'il pourrait utiliser à son avantage.

4.1.2. Modes de transit des données

Les données (journaux ECU, évènements de passerelle, télémétrie etc.), préalablement collectées, sont générés par les réseaux internes du véhicule (CAN, Ethernet, LIN etc.) et sont accessibles à un composant de connectivité, le TCU (Telematic Control Unit, en français boîtier télématique connecté), ou alors une

passerelle centrale relié au boîtier. Dans la majorité des architectures actuelles, le TCU se connecte au réseau mobile via un SIM/eSIM embarquée lui permettant d'établir une ou plusieurs sessions IP avec l'opérateur mobile en 4G ou 5G. Ces sessions IP contiennent les données télématiques qui sont encapsulées dans des protocoles applicatifs (HTTPS[17], MQTT etc.)

Le même TCU peut aussi se connecter à un point d'accès Wi-Fi, dans ce cas le véhicule obtient une adresse IP sur le réseau local via DHCP (Dynamic Host Configuration Protocol) **[Fortinet]**, ce protocole est utilisé dans les réseaux pour attribuer dynamiquement des adresses IP à chaque hôte du réseau. Le protocole va envoyer des messages à chaque appareil leur fournissant ce dont ils ont besoin. Ainsi, que ce soit en Wi-Fi ou via le réseau cellulaire, une voiture est capable de remonter ses informations de télématique et de les envoyer via Internet sur des serveurs opérés par les constructeurs ou bien par des fournisseurs tiers de télématique. Utilisant soit une technologie proche du Wi-Fi, soit du C-V2X sur la couche radio cellulaire, les communications V2X (véhicule à véhicule; véhicule à infrastructure; véhicule à réseaux etc.) permettant elles aussi de transmettre des informations télématiques normalisées à travers les infrastructures routières ou les autres véhicules émettant de type de connexion **[FARECO.2019]**. Ces équipements V2X permettent notamment de récupérer des évènements depuis ceux-ci sur les échecs d'authentification, les incohérences ou les anomalies qui elles, peuvent être transmises pour mon infrastructure.

Ces données permettent aux constructeurs d'améliorer leurs produits, ils détectent les pannes récurrentes sur un modèle et peuvent ainsi améliorer les futures versions (apparition de certaines voitures en « phase 2 », c'est le même véhicule mais amélioré sur certains points). Cela leur permettrai aussi d'alerter le propriétaire avant une panne, de pouvoir déployer leurs mises à jour via Internet sur les véhicules nécessitant une correction logicielle (principe très présent sur les modèles type Tesla etc.) **[MISC.2025c]**. Ces données servent aussi au services client pour de l'assistance ou encore de la localisation en cas de vol. Mais, ces données

peuvent aussi être revendus après leur agrégation à des assureurs, des collectivités ou des infrastructures routières. Le but serait donc de récupérer ces données sortant du TCU et transitant par Internet afin de les collecter dans mon infrastructure de SIEM via des API ou flux de messages grâce à un connecteur les transportant vers mon SIEM sur des liens IP chiffrés comme pour n'importe quelle autre application cloud. Pour ensuite récupérer des informations provenant d'une voiture précise à travers le cloud, les données récupérées peuvent être filtrées de ces connexions API ou autre via le numéro VIN[18] ou un identifiant interne du constructeur pour suivre une voiture précise.

La récupération de données peut aussi se faire à travers des outils physiques, comme j'ai pu l'expliquer précédemment notamment avec la prise OBD-II qui permet de récupérer des données de diagnostic. Exporter ces données permettrai de les faire ingérer par le SIEM et de les corréler avec des données d'autres sources comme celles qui auraient été récupérées via le cloud. Certains constructeurs fournissent des outils de diagnostic propriétaires qui vont plus loin que l'OBD-II générique et permettent parfois d'accéder aux journaux internes des ECU, à l'historique des défauts, des journaux de l'info-divertissement etc. Cet outil propriétaire permet aussi parfois de lire des traces réseaux sur les différents bus (CAN, FlexRay, Ethernet) et d'autres journaux d'évènements complexes que je ne pourrai aborder. Aussi, de plus en plus de véhicules récents stockent leurs données sur des supports locaux comme des cartes SD ou micro SD, des clés USB utilisées notamment pour les mises à jour ou encore des mémoires vives démontables en atelier. Comme j'ai aussi pu l'aborder vaguement plus tôt, certains boitiers télématiques vendus sur le net peuvent se brancher directement sur la prise OBD-II sans valise propriétaire et lire ses données (la lecture est aussi possible sur le réseau CAN), ils peuvent stocker en local ou envoyer vers une passerelle locale les données transitant dans le véhicule, malgré les failles de sécurité pouvant en découler, cette méthode peut être intéressante pour récupérer des données intéressantes dans le cadre d'un SIEM pour les automobiles dans le secteur des particuliers. Mais pour les

entreprises gérant un certain nombre de véhicules, récupérer ces données via des méthodes plus traditionnelles serait plus pertinent, un véhicule rentre au dépôt, les données sont collectées puis envoyées dans le SIEM pour les faire analyser.

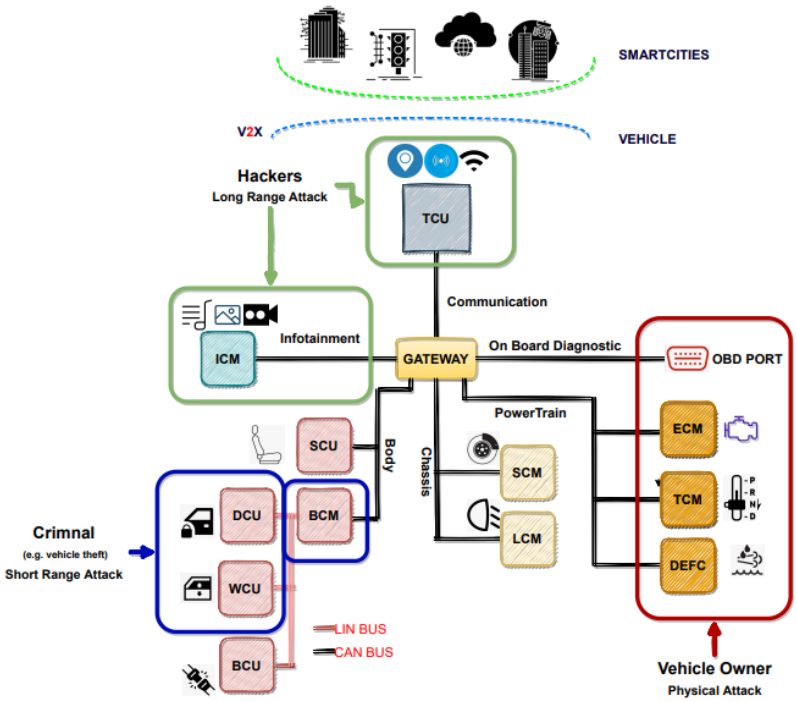

Figure 8: Représentation des différents vecteurs d'attaques pour l'automobile

Cette figure ci-dessus, vient à la fois représenter les différents vecteurs d'attaques pour un véhicule, que ce soit à distance ou en physique et vient aussi étayer mes propos sur les raisons pour lesquelles il faut s'appuyer de ces équipements de confiance pour les protéger et récolter les données nécessaires et les corréler pour éviter ce genre d'incidents.

4.1.3. Contraintes de collecte

Évidemment, le processus de collecte de données ne peut se faire sans se contraindre au cadre normatif qui l'englobe. Ce cadre va déterminer ce qu'il est réellement possible d'observer, à quel rythme et avec quel niveau de confiance. Les normes ISO 21434 et l'UN R155 imposent une logique de cybersécurité sur tout le cycle de vie du véhicule, ce qui inclut la conception, l'exploitation et la maintenance

donc aussi la façon dont les données sont collectées. La collecte de données d'un système automobile pour un SIEM ne doit pas pouvoir créer une nouvelle surface d'attaque exploitable par des attaquants, ni altérer l'intégrité de ces données ou contourner les principes de sécurité du constructeur, ce qui signifie que la collecte de données doit être tracée et justifiable. La collecte de données, notamment de localisation, est considérée comme étant particulièrement sensible pour la vie privée et est donc régulée par la CNIL selon ce que décrit le RGPD puisqu'elle permet d'identifier les déplacements, les habitudes et les lieux fréquentés d'une personne. Il faut donc que le SIEM puisse avoir des mécanismes de distinctions de champs (ce qui a été vu précédemment et est généralement effectué par l'étape de l'agrégation) pour pouvoir les minimiser, les pseudonymiser quand c'est possible, limiter les finalités et définir des durées de conservation des journaux adaptées. Adoptée en 2024 et dont l'application est progressive jusqu'en 2027, vient s'ajouter à ces normes, le Cyber Resilience Act (CRA) qui étend les obligations de cybersécurité à l'ensemble des produits connectés mis sur le marché européen, imposant notamment une surveillance continue après mise sur le marché et un signalement des incidents aux autorités compétentes **[ANSSI.2024]**. Lors de mon entretien avec M. BOUVARD, il a aussi pu me confirmer que cette norme CRA était le coeur de ses discussions actuelles et que cela représentait donc un grand enjeu pour son secteur d'activité, bien qu'il soit différent du véhicule connecté, les similarités avec les engins mécaniques d'agriculture permettent de constater les mêmes problématiques de cybersécurité sur des systèmes embarqués connectés.

Au-delà des contraintes réglementaires, les contraintes techniques sont aussi à prendre en compte. La connectivité d'un véhicule n'est pas toujours stable, lors de longs trajets, la connexion entre la voiture et le SIEM peut être compromise, lorsque le véhicule passe d'une cellule à une autre, dans le cadre du réseau cellulaire, lorsqu'elle traverse une zone blanche (zone où les réseaux cellulaires ne sont pas disponibles), qu'elle passe du mobile au wifi, la connexion peut être momentanément interrompue. Cette instabilité impose que la collecte soit tolérante

aux coupures de réseau, la donnée doit pouvoir être mise en attente puis envoyée lorsque cela est de nouveau possible. Du côté du SIEM, cela ne doit pas forcément refléter d'un incident mais simplement de ce qu'une voiture normale peut traverser. Aussi, la bande passante, notamment sur l'autoroute, n'est pas illimitée ce qui est une contrainte importante au vu du nombre de données générées par les véhicules. La collecte et l'agrégation doivent donc pouvoir faire un mix entre ce qui est nécessaire et ce qui ne l'est pas pour le domaine souhaité, donc la sécurité et la contextualisation dans mon cas pour concilier entre richesse du journal et coût de la transmission.

La collecte des données doit aussi pouvoir assurer les propriétés de cybersécurité d'intégrité et de confidentialité. Concernant l'intégrité, la collecte représente un risque pour cette propriété puisque la donnée peut être altérée, modifiée par un composant compromis ou simplement incomplète à cause d'une coupure réseau. Les chaînes de collecte doivent donc être complétées par des mécanismes de signature, de chiffrement et/ou de contrôle d'authenticité. Dans le cadre de ma solution répondant à la problématique de mon mémoire, l'enjeu n'est donc pas seulement de recevoir l'évènement mais de pouvoir prouver qu'il est arrivé intact, dans le bon ordre et depuis une source identifiée. Comme j'ai pu l'expliquer ci-dessus, les données récoltées peuvent contenir des informations à caractères personnelles comme la localisation, l'usage du véhicule, les identifiants techniques et parfois des éléments indirectement liés à un conducteur ou à un trajet, il faut donc pouvoir assurer la confidentialité des données récoltées. Pour cela, il faut donc protéger à la fois les données en transit mais aussi une fois qu'elles sont stockées dans le SIEM, par exemple, en restreignant l'accès au SIEM aux seules personnes ayant besoin de les consulter. Cette contrainte de confidentialité est d'autant plus importante que le SIEM centralise et croise plusieurs sources augmentant la possibilité de pouvoir reconstituer un comportement individuel. Arriver à cela pourrait permettre, à mon avis, à un attaquant de reproduire le comportement de

l'individu à qui appartient le véhicule afin de passer incognito dans le réseau et ainsi attaquer lorsque le temps serait venu pour lui de le faire.

Comme vu, les contraintes d'une telle solution ne sont donc pas seulement techniques mais aussi juridiques et réglementaires. Il faut penser à la sécurité dès la conception mais aussi à sa conformité afin de garantir que la collecte se fasse dans le respect des réglementations.

4.2. Préparer et intégrer les données dans le SIEM

4.2.1. Centralisation des données

La centralisation des données consiste à rassembler en un point unique l'ensemble des évènements et des journaux issus de la collecte provenant des différentes sources du système de l'automobile. Cette étape dans la conception d'un SIEM est fondamentale puisque c'est la centralisation qui permet que toutes ces données générées de flux dispersés et hétérogènes se retrouvent en un seul et même endroit exploitable à des fins de supervision et de détection. Étant donné qu'un véhicule moderne peut embarquer jusqu'à 150 unités de contrôle électronique et environ 100 millions de lignes de code, ce qui serait quatre fois plus qu'un avion de chasse selon l'UNECE (Commission économique pour l'Europe des Nations unies) et ce nombre devrait passer à 300 millions d'ici 2030 ce qui montre l'ampleur des flux de données qu'il faut centraliser. Sans celle-ci, les données resteraient fragmentées et difficilement reconstituables de bout en bout, ce qui rendrait l'analyse d'un incident plus complexe.

Chacune de ces unités génère des évènements dans des formats propriétaires ou standardisés qui ne sont pas directement compatibles avec les schémas attendus par un SIEM généraliste. Cette étape de centralisation des données joue aussi un rôle de lien entre le monde de l'informatique embarquée et plus généralement de l'internet des objets et le monde de l'informatique. D'un côté les systèmes embarqués produisent des journaux techniques et de l'autre il y a des services cloud,

des serveurs applicatifs, des outils métiers et des environnements d'exploitation. La centralisation permet d'absorber la diversité des sources et de les regrouper pour les rendre accessible à un système de surveillance. C'est ce qui donne au SIEM sa valeur, puisqu'il ne va pas seulement surveiller un appareil seul mais toute une chaîne d'équipements pour les mettre en corrélation entre eux. La centralisation n'est donc pas seulement une question de stockage mais surtout de visibilité globale sur les journaux et évènements.

Lors de mon entretien avec M. BOUVARD concernant mon mémoire, une de ses principales réflexions était sur ce sujet de centralisation des données puisque pour l'instant, rares sont les éditeurs de SIEM à proposer une centralisation de journaux à la fois pour les journaux informatiques dits « classiques » mais aussi, à proposer dans une même solution des journaux pour l'IoT ou les journaux du monde industriel. Cet intéressement encore très récent par le marché (notamment au travers de la norme CRA) justifie ainsi l'intérêt de ma démarche proposée dans ce mémoire et confirme que la centralisation des journaux dans un contexte automobile n'est pas seulement un défi technique mais aussi un enjeu industriel et doit pouvoir s'adapter aux différents concepts techniques que sont l'IT, l'IoT et l'OT (Operational Technology désigne l'ensemble des systèmes matériels et logiciels qui surveillent et contrôlent directement les équipements physiques, les processus industriels et les infrastructures).

4.2.2. Mise en forme et corrélation

Une fois les données centralisées, la remontée vers le SIEM au format brut ne suffit pas. Chaque ECU génère des événements dans un format qui lui est propre avec des trames CAN brutes, des messages UDS (Unified Diagnostic Services, protocole standardisé par la norme ISO 14229 permettant aux outils de diagnostic d'interroger les calculateurs du véhicule pour en extraire des données de fonctionnement, des codes défauts ou des journaux internes), des composants Linux embarqués (infodivertissement, TCU), sorties applicatives propriétaires des fournisseurs de calculateurs etc. Ces formats ne partagent ni la même syntaxe ni les

mêmes champs, le SIEM vient alors normaliser les évènements vers un schéma de données commun que le SIEM peut alors comprendre lui permettant de les corréler entre eux. Plusieurs formats standardisés ont été développés pour faciliter l'interopérabilité des journaux envoyés dans le SIEM comme le CEF (Common Event Format), le LEEF (Log Event Extended Format) et le syslog qui est défini par les RFC[19] 3164 et RFC 5424. Le LEEF étant un format propriétaire développé par IBM pour QRadar serait pertinent pour une organisation si elle gère ses journaux avec cette solution. En revanche, le CEF qui est ouvert et libre d'accès est un format de journalisation standardisé et structuré conçu pour simplifier la collecte, l'intégration et l'analyse d'évènements de sécurité issus de sources multiples. L'avantage du CEF par rapport au syslog est qu'il assure la normalisation des données les rendant immédiatement exploitables pour une analyse par la suite. Dans le contexte de l'automobile, cette normalisation est d'autant plus complexe puisque les données ne sont pas, de base, prévues pour être envoyées dans un SIEM et donc le format de normalisation, doit lui aussi être choisi dépendamment du SIEM cible. Avec l'entretien que j'ai pu avoir avec M. BOUVARD, j'ai pu comprendre que dans son secteur les flux de données transitaient par un hub d'évènements avant d'être stockés dans un format AVRO, un format de stérilisation binaire issu de la fondation Apache. Le format AVRO utilise le JSON pour la définir le type de données et les protocoles. Ce choix a été fait suite à la contrainte rencontrée où lorsque plusieurs utilisateurs tentent simultanément d'accéder au même flux d'évènements, des problèmes de latence et d'interception apparaissent rendant le traitement en temps réel plus compliqué. Le format AVRO, plus compact et optimisé pour la déserialisation rapide à grande échelle, permet de répondre à cette contrainte tout en maintenant une compatibilité avec les outils d'analyse en aval.

Après cette étape de normalisation de l'ensemble des données collectées, le SIEM se retrouve avec des journaux au même format qui deviennent manipulables pour un analyste. En effet, les structures étant désormais communes, il est possible d'interpréter et d'extraire des champs nominatifs de ces journaux comme

l'horodatage, l'identifiant de l'ECU source, le type d'évènement, la valeur associée etc. tel que décrit dans ma partie sur le fonctionnement du SIEM. Les données, bien qu'étant devenues manipulables ne sont pas d'une grande pertinence lorsqu'elles sont laissées telles quelles alors pour les rendre suffisantes à ce qu'elles soit analysables, il faut les enrichir. Dans le cadre d'une automobile, les différents ECU n'ont pas toujours une horloge interne ainsi l'horodatage des journaux, pour maintenir leur cohérence entre eux doivent s'appuyer de l'horloge du TCU, qui via son accès au monde extérieur peut se synchroniser à un serveur NTP (Network Time Protocol) qui a pour fonction de synchroniser son horloge au reste du réseau, garantissant ainsi une certaine cohérence entre l'horodatage des journaux. Il serait aussi bon de pouvoir visualiser de quelle voiture les journaux proviennent et donc d'enrichir ces mêmes journaux de l'identifiant du véhicule (numéro VIN) que j'ai mentionné plus tôt. Il permet ainsi de pouvoir filtrer les journaux centralisés dans un même système sur une seule voiture et permettre au gestionnaire de flotte d'accéder à la fiche technique du dit véhicule avec le modèle, l'année de fabrication, le type de propulsion, les équipements embarqués (ceux-ci peuvent changer selon les options commandées sur le véhicule, par exemple je pense à la caméra de recul qui n'est pas toujours présente) et l'historique des mises à jour logicielles afin de contrôler l'état général du véhicule. Visualiser la flotte de véhicule est un champ aussi très pertinent en lui-même puisqu'il permet de détecter, en cas d'attaque si toute une flotte est touchée par l'attaque ou si le cas est isolé, permettant ainsi de pouvoir répondre à l'incident de manière plus efficace et de le comprendre plus simplement. Aussi, récupérer la version du firmware de l'ECU produisant un évènement est aussi indispensable à l'enrichissement d'un journal puisqu'une voiture qui ne serait pas à jour serait plus à même de subir une cyberattaque et ainsi mettre en danger ses usagers étant donné que des fonctions essentielles comme la direction ou le freinage sont maintenant gérées électroniquement. Ce genre d'informations permet aussi au SIEM de pouvoir prioriser les alertes selon les bulletins de vulnérabilités connus en se basant sur la sévérité du bulletin associé. Cette priorisation peut aussi être corrélée par la criticité de l'ECU produisant l'évènement, en effet comme

mentionné plus tôt, le freinage ou la direction, qui sont gérées électroniquement par leurs ECU respectifs auront une priorisation plus importante dans le SIEM de leur criticité même au sein du véhicule en lui-même.

4.2.3. Organisation et stockage

Une fois que les données sont normalisées et enrichies, elles doivent maintenant être stockées et organisées de manière à être rapidement interrogeables par les analystes et le moteur de corrélation. L'indexation des journaux d'évènements consiste à regrouper les données dans des catégories, à permettre la recherche et à relier les évènements corrélés entre eux. Concrètement chaque champ extrait de l'étape précédente devient une clé d'index sur laquelle des requêtes peuvent être effectuées en quelques millisecondes. L'indexation est une activité extrêmement gourmande en puissance de calcul ce qui provoque une latence entre le moment où les données sont saisies dans le système et celui où elles apparaissent dans les résultats de recherche et les visualisations. Dans le contexte automobile, cette contrainte est amplifiée par le volume de données qui sont envoyés par les ECU puisqu'ils sont des centaines par véhicule multiplié par l'ensemble de la flotte géré. Le débit de données est constant et doit être ingéré, indexé et rendu disponible quasiment en temps réel pour permettre la détection. Tout l'enjeu du SIEM se fait à ce moment là puisque son architecture doit être conçue pour supporter plusieurs axes de recherche simultanés et complémentaires. Un analyste doit pouvoir interroger les différents champs récupérés des journaux pour, par exemple, isoler un véhicule précis, un ECU distinct, un niveau de criticité fonctionnelle et une plage temporelle pour reconstituer une chronologie d'attaque.

Après toutes ces étapes de traitement de la donnée, les journaux doivent maintenant être stockés dans le SIEM et seront soumis à la politique de rétention définie par l'organisation respectant les conditions imposées par la CNIL. En effet, ces journaux de systèmes embarqués ne peuvent être conservés indéfiniment dans le système d'informations. Dans une organisation, cette politique de rétention doit être mûrement réfléchie puisque d'un côté, conserver les journaux le plus longtemps

possible maximise la capacité d'investigation forensique et la détection de menaces persistantes mais peut poser des problèmes de stockage à terme (saturation du SIEM entraînant une indisponibilité ou un accès illégitime au serveur SIEM qui permettrait à un attaquant de pouvoir récupérer un nombre considérable de données utiles). C'est pour éviter cela que le stockage se distingue en deux parties avec le stockage à chaud et le stockage à froid que j'ai pu évoquer dans ma partie sur le fonctionnement du SIEM. Dans un contexte automobile et non-industriel donc moins sensible que s'il l'était le stockage à chaud peut perdurer pendant 6 mois à un an selon les capacités de stockage et aussi selon la criticité des ECU produisant des évènements. Comme évoqué, de nombreux ECU produisent un nombre considérable de journaux et leur criticité peut influer sur la durée de rétention. Ces journaux, passés un certain délai, peuvent être ensuite envoyés dans un stockage à froid (archivage compressé des journaux) pour satisfaire aux obligations de traçabilité et de conformité réglementaire. Le stockage des journaux dans le cadre d'un SIEM appliqué à l'automobile n'est donc pas seulement une décision technique mais aussi une obligation légale encadrée. La CNIL recommande de limiter strictement la durée de conservation des logs dans le cas général de six mois à un an avec une possibilité d'allongement sous certaines conditions justifiées. Ainsi, je peux reprendre l'exemple de Cegedim.cloud, où dans mon équipe, nous gardions les journaux de sécurité pendant 3 mois à chaud puis les envoyions 9 mois dans le stockage à froid avant de les supprimer définitivement. Ce modèle peut être adapté à nos besoins dans l'automobile avec des politiques modulables selon la criticité des systèmes embarqués produisant les journaux.

4.3. Évaluer la capacité d'un SIEM à répondre aux besoins automobiles

4.3.1. Détection d'événements anormaux

La détection d'évènements anormaux constitue la finalité opérationnelle de tout le travail de préparation des données évoqué plus tôt. C'est dans cette partie que le SIEM prend son sens en croisant les journaux normalisés, enrichis et indexés pour identifier des comportements anormaux qui sembleraient anodins à première vue mais qui pourrait transparaître d'une réelle intrusion sur les systèmes embarqués d'un véhicule. L'enjeu de ce contexte automobile n'est pas de se limiter simplement aux journaux IT classiques qui pourraient être récupérés via des passerelles mais aussi de pouvoir disposer d'indicateurs fonctionnels pour savoir ce qui se passe réellement au sein de la machine.

L'un des vecteurs d'attaque les plus critiques sur les véhicules modernes sont les mises à jour OTA (Over-The-Air donc via le réseau sans-fil), elles sont devenues indispensables à certains constructeurs leur permettant de pouvoir appliquer des mises à jour à leur flotte automobile sans avoir à les ramener dans un garage pour le faire, cela se rapproche de ce que fait un logiciel grand public aujourd'hui. Ce canal représente un risque pour la sécurité des automobiles puisque des virus informatiques peuvent être injectés par les processus de mises à jour OTA. D'après l'entreprise Parasoft, ils auraient découvert en 2025 une faille sur le système télématique Starlink, de la marque nippone Subaru, gérant les mises à jour OTA des calculateurs essentiels à la sécurité tels que les modules de contrôle du freinage et de la transmission. Ce système utilisait un système de chiffrement faible exposant les ECU critiques à des manipulations frauduleuses. Dans un SIEM, la détection de ce genre de menaces repose sur plusieurs indicateurs corrélables, par exemple, une mise à jour initiée depuis une adresse IP inhabituelle ou à une heure atypique peut être un premier indice de compromission. Peut aussi être un indice de compromission, une tentative de mise à jour avec une taille de paquet anormalement élevée en comparaison aux précédentes mises à jour peut être un signe de tentative d'injection de code malveillant.

Toujours d'après l'entreprise Parasoft, en 2024, une faille dans le portail client de Kia aurait exposé non seulement les données des utilisateurs mais aussi un accès indirect aux calculateurs télématiques des véhicules connectés. Les attaquants auraient exploité une authentification API faible afin d'envoyer des commandes non autorisées aux ECU modifiant potentiellement leurs configurations (désactivation d'alarmes, du géo-repérage etc.) Dans ce cas là le SIEM doit pouvoir analyser les données reçues via les API et ainsi corréler les requêtes inhabituelles. Le véhicule qui reçoit une commande de déverrouillage à distance alors que le véhicule est en train de rouler ou une rafale de requêtes d'authentification depuis plusieurs adresses IP dont la géolocalisation ne colle pas constituerait un potentiel évènement de sécurité suite à l'analyse des logs par le système de journalisation.

Aussi, je trouve important de mentionner que les bornes de recharge pour les voitures électriques ou hybrides peuvent elles aussi constituer une surface d'attaque **[MISC.2025e]**. Ces attaques sont encore relativement nouvelles mais je pense qu'elles vont tendre à augmenter au fur et à mesure notamment par le fait de l'électrification du parc automobile ainsi que la rapidité du déploiement de ces bornes, elles ont été installées avec des matériels hétérogènes, des firmwares différents et avec des niveaux de sécurité différents. Je pense que les infrastructures françaises n'étaient pas prêtes à devoir répondre à une demande aussi forte et aussi rapide des Français quant à la recharge de leurs véhicules notamment sur les autoroutes puisque les voitures électriques ne sont pas connues pour permettre de rouler sur de longues distances, même si cela tend à évoluer. Le protocole OCPP (Open Charge Point Protocol) est le protocole largement utilisé par les bornes pour communiquer avec les systèmes centraux des opérateurs et celui-ci peut être exposé à des failles si il est mal configuré ou insuffisamment chiffré. Dans l'article de Mickael Duros sur le journal Techno-car, il indique que la société de cybersécurité Saiflow avait publié un rapport, au moment de l'écriture de l'article en 2023, alertant sur les vulnérabilités du réseau des bornes de recharge [. L'exploitation de ces vulnérabilités pouvait permettre aux pirates de déconnecter un chargeur unique à travers une

attaque par déni de service voire même tous les chargeurs connectés à un réseau lors d'une attaque distribuée, ce qui créait une interruption de service pour l'entreprise déployant ces bornes de recharge et donc créer un risque pour eux. Ces attaques pouvaient aussi potentiellement leur permettre de pouvoir charger leurs véhicules gratuitement. Dans ce type d'attaque, la détection passe par la corrélation des journaux de session avec les évènements du véhicule : une session OCPP qui s'interrompt anormalement, un changement de configuration de la borne pendant une session active peuvent constituer des alertes de sécurité qui seraient remontées par le SIEM.

Un dernier aspect que je souhaite aborder c'est la démocratisation des outils d'attaque physique accessibles au grand public. En effet, durant mes recherches au préalable sur le sujet, j'ai pu découvrir l'existence d'un adaptateur CANBus pour le Flipper Zero, qui est à l'origine un outil de test de sécurité assez tendance depuis quelques temps maintenant.

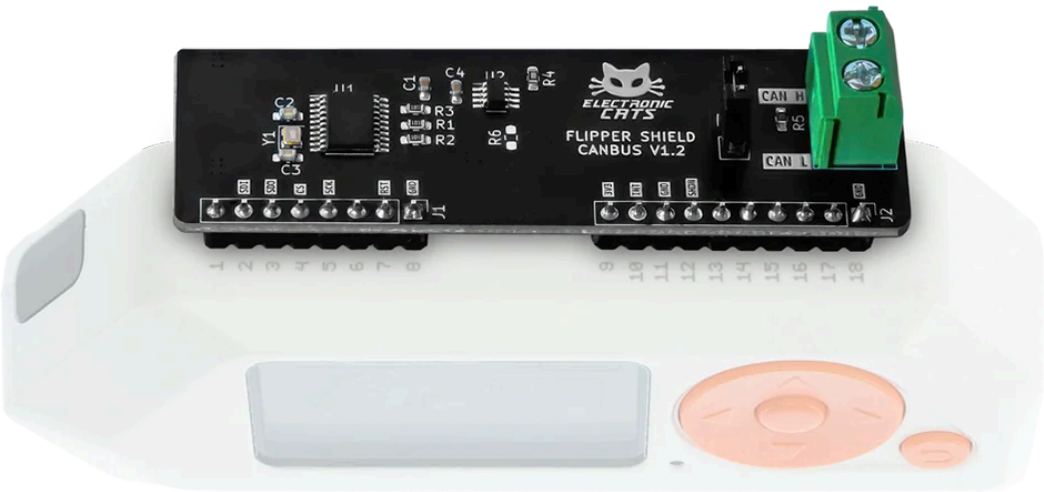

Figure 9 : Module CANBus pour Flipper Zero

En effet, cet outil vendu publiquement, à n'importe qui, permet de connecter le Flipper Zero au protocole CAN d'un véhicule via les connecteurs physiques. L'adaptateur permet d'envoyer des messages CAN-High et CAN-Low et via des scripts Python permet l'interaction avec les ECU en utilisant différents protocoles

CAN notamment le protocoles UDS. Il permet aussi aux utilisateurs de surveiller, envoyer et journaliser des paquets CAN directement depuis l'appareil ce qui signifie qu'il est possible d'analyser et de manipuler le trafic CAN. Ce type d'outil illustre la nécessité pour un SIEM de surveiller les trames CAN et d'en détecter les anomalies. Lorsqu'un attaquant tente d'injecter des trames depuis le Flipper Zero via la prise OBD-II, la fréquence des messages portant un certain identifiant et qui change brusquement peut constituer un signal pour le SIEM en le corrélant aux précédents messages.

4.3.2. Gestion et analyse des incidents

La première mission du SIEM dans la phase d'analyse est de reconstituer précisément la séquence des évènements ayant conduit à l'incident. Le SIEM conserve l'historique des évènements alors en cas d'incident, il permet de reconstituer la chronologie d'une attaque afin d'identifier son origine et son étendue. Dans le contexte de systèmes embarqués dans une voiture cette reconstitution chronologique est plus complexe qu'un système d'informations classiques puisque les évènements proviennent de sources aux temporalités différentes. Certains ECU n'ont pas d'horloge dédiée et doivent alors se baser sur la temporalité du TCU par lesquels passent les évènements avant d'être envoyés dans le cloud, cela explique l'utilisation d'un serveur NTP pour que la synchronisation de la temporalité soit commune à tous.

Analyser un incident ne se limite évidemment pas à la simple reconstruction chronologie d'un évènement, après avoir répondu à la question « quand », nous devons savoir « par où » l'attaquant est donc passé. Cette étape permet de comprendre par où est passé l'attaquant et le chemin qu'il a emprunté pour progresser dans le système. Les vecteurs d'attaques j'ai décrit en 4.3.1, laissent chacun des traces distinctes dans les journaux. L'identification du vecteur repose sur la corrélation entre le premier évènement anormal détecté et les caractéristiques du flux qui l'a précédé. Cette identification est également une exigence réglementaire directe du règlement UNECE R155, qui impose aux constructeurs de documenter et

signaler les incidents de cybersécurité identifiés sur leur flotte aux autorités compétentes **[UNECE.2021]**. Sans identification précise du vecteur, ce signalement s'avérerait incomplet voire impossible.

L'évaluation de l'impact est bien différente du besoin dans un SI classique. Au sein d'une entreprise, l'étude de l'impact se mesure principalement selon la disponibilité, la confidentialité ou l'intégrité des données. Dans un véhicule, une nouvelle dimension s'ajoute à savoir la sécurité physique des occupants de la voiture. Cette évaluation doit répondre à plusieurs questions simultanément tel que reconnaître les ECU qui ont été touchés ou manipulés pour savoir si ce sont des fonctions critiques (le freinage, la direction, les aides à la conduite…) ou bien seulement des fonctions de confort. Il faut aussi identifier si l'attaque s'est limitée à un seul véhicule ou à d'autres véhicules d'une flotte et si le véhicule était en mouvement au moment de l'incident ce qui pourrait aggraver le risque pour les occupants. Le SIEM permet d'automatiquement classifier la gravité de l'incident selon les ECU impliqués. Une fonctionnalité pourrait ne manifester aucune anomalie d'un point de vue informatique mais avoir un comportement aberrant révélant une possible compromission, c'est précisément pour cette raison que l'évaluation de l'impact dans le SIEM appliqué à l'automobile ne peut se limiter aux indicateurs informatiques classiques mais doit intégrer les données fonctionnelles du véhicule.

Chaque incident analysé constitue une source d'apprentissage qui permet d'améliorer les règles de corrélation, de réduire les faux positifs et de renforcer la posture de sécurité globale. Les investigations forensiques suite à un incident identifient les failles exploitées et guide les actions de remédiation. Les données collectées par le SIEM alimentent aussi l'amélioration continue de la sécurité. Cette boucle d'amélioration prend une dimension supplémentaire puisque les règles de corrélation affinées après un incident peuvent être déployées à l'ensemble d'une flotte via une mise à jour OTA. Cette boucle de rétroaction entre l'analyse post-incident réalisée dans le SIEM et la mise à jour des capacités de détection embarquées est ce qui distingue un SIEM appliqué à l'automobile mature d'un

simple système de collecte de journaux. Il transforme chaque incident en protection renforcée pour l'ensemble de la flotte. La mise en place de ce type de systèmes s'inscrit dans une démarche globale incluant des services de gestion de crises, d'analyse et de veille sur la menace, tout cela constituant ainsi un cycle vertueux d'amélioration continue de la sécurité.

4.3.3. Validation de la solution proposée

Afin de valider concrètement la faisabilité d'un SIEM appliqué à l'automobile, j'ai réalisé une preuve de concept en m'appuyant sur une architecture ELK (Elasticsearch, Logstash, Kibana). J'ai choisi de m'appuyer sur cette solution puisqu'elle m'est quelque peu familière, j'ai dû mettre en place une solution de haute disponibilité à Cegedim.cloud puis je l'ai mise en place au sein de l'École 18.06 pour surveiller le trafic du réseau avec l'aide d'Alexandre Peltier et Vincent Peyrouse. Cette architecture étant open-source et reconnue dans le domaine de la gestion des journaux de sécurité nous a permis de l'installer et de l'utiliser via nos propres serveurs garantissant la souveraineté dans le transit des données, qui est la valeur que partagent Cegedim.cloud et l'École 18.06. Le choix de cette solution s'est aussi fait par son aspect généraliste lui permettant d'absorber des sources de données hétérogènes, qui est l'un des principaux points d'attention que m'a partagé M. BOUVARD lors de notre entretien puisqu'il m'expliquait que les principaux éditeurs de solution de journalisation dédiés aux entreprises ne proposaient pas encore de solution pour absorber les données IT classiques ainsi que ses données IoT et OT dans la même solution. En effet, certains éditeurs proposent sur le marché des solutions pour ingérer les journaux des automobiles ou IT mais ne proposent pas encore de solutions liant les deux. D'autres encore, comme la société Upstream Security propose une solution pour la surveillance sur les données des véhicules connectées, alimentant par la suite le SIEM IT classique mais rien n'est encore proposé nativement.

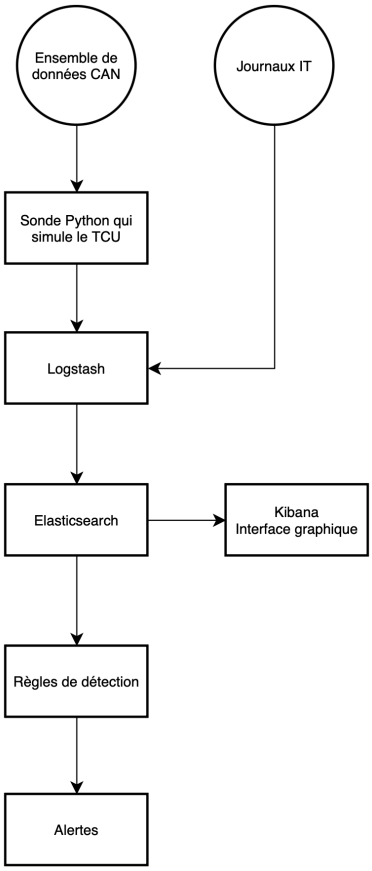

Figure 10 : Flux des données dans ELK

Le flux de données comme illustré dans la figure ci-dessus décrit le chemin complet des données depuis leur source jusqu'à la génération d'alertes. J'ai décidé, pour cette preuve de concept de m'appuyer sur des ensembles de données que j'ai pu trouver sur un Github en ligne publié par « Sampathrajapaksha » et qui met à disposition un espace de stockage Google où il est possible de retrouver des données de bus CAN. Les données sont envoyées via un programme qui joue le rôle du TCU, il enrichit chaque trame d'un identifiant de véhicule (numéro VIN), applique un double horodatage (date à laquelle sont envoyées les données dans la solution et date de la donnée en elle-même) et transmet les journaux par lots vers le l'agrégateur (Logstash dans l'environnement Elasticsearch). L'agrégateur assure ensuite la normalisation vers un schéma commun, fait une classification fonctionnelle

par domaine selon la plage d'identifiant CAN et indexe quotidiennement dans le SIEM Elasticsearch sous le pattern « autosiem-can-YYYY.MM.DD ».

Avant de pouvoir créer des règles de détection, il a été nécessaire de procéder à une phase de profilage du trafic par analyse comparative entre le fichier bénin et le fichier d'attaque. Cette étape correspond exactement à ce qui a été décrit dans ma partie sur la mise en forme et la corrélation concernant la nécessité d'établir une fondation avant tout enrichissement ou toute corrélation. Cette analyse a permis d'identifier que l'identifiant CAN 0x372 atteignait un pic de 2 412 trames par seconde sur le trafic d'attaque, contre un maximum de 1 237 trames par seconde sur le trafic bénin de référence, soit une augmentation de 95 %. Deux règles de détection ont été créées et validées sur ces données réelles.

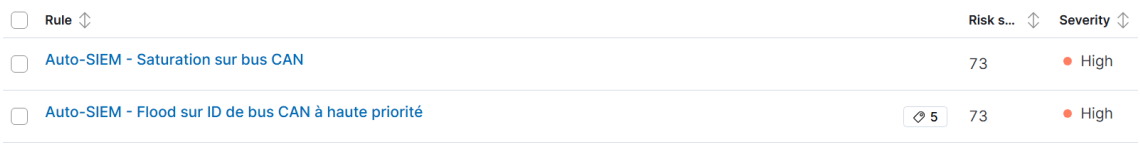

Figure 11 : Règles de détection dans Kibana

La première règle va cibler les attaques par saturation du bus CAN sur les identifiants à haute priorité, correspondant à la menace 24.1 de l'annexe 5 du règlement UNECE R155. Comme évoqué dans ma partie sur la détection des évènements anormaux, un attaquant qui envoie un nombre anormal de flux sur les identifiants bas du bus CAN peut amener à un déni de service ce qui fait que les ECU critiques ne peuvent plus transmettre leurs commandes cela peut alors entraîner une indisponibilité des systèmes de freinage ou de direction. La seconde règle cible les attaques par injection de trames CAN sur l'identifiant 0x372 dont la signature avait été identifiée lors du profilage, correspondant à la menace 11.1 du même règlement.

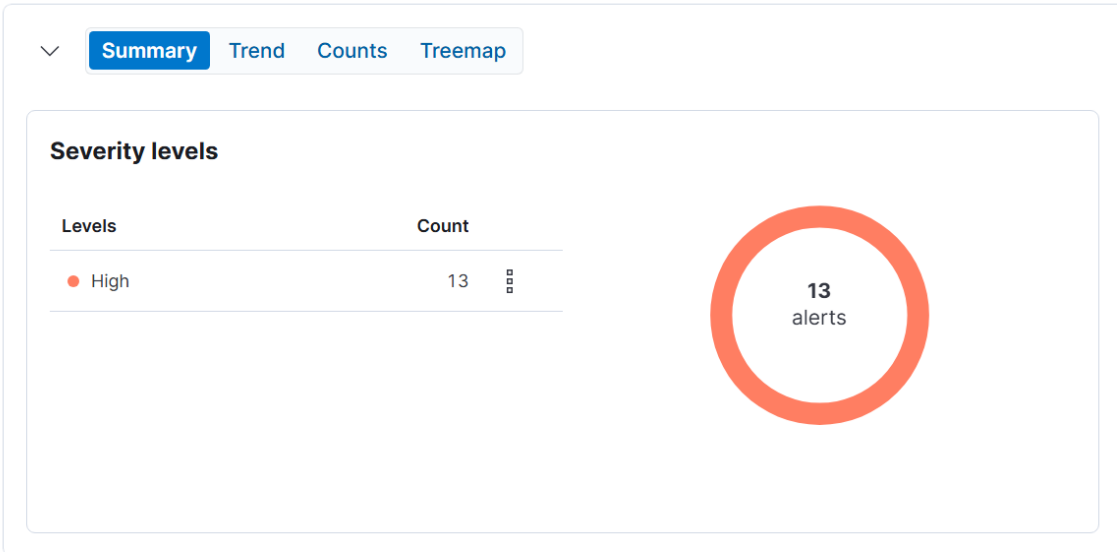

Figure 12 : Alertes générées

Sur les 11 672 671 journaux ingérés via une sonde écrite en Python, pour tenter de simuler au mieux le débit d'une voiture, le taux d'erreur d'ingestion est nul et les 12 alertes générées concernent exclusivement le VIN compromis, sans aucun faux positif sur l'identifiant de référence bénin.

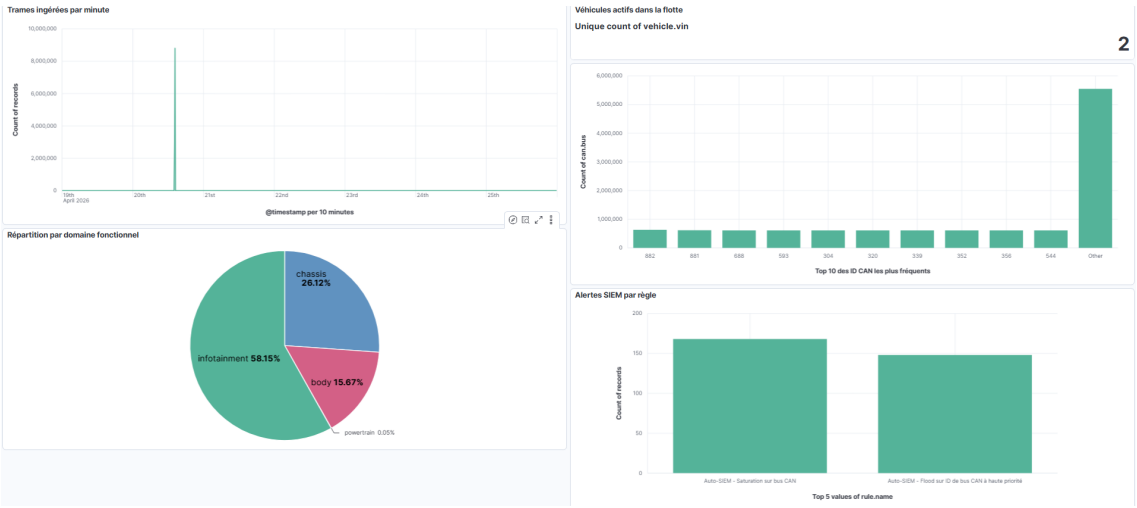

Figure 13 : Tableau de bord pour automobile

J'ai par la suite créé un tableau de bord dans l'interface Sécurité de Kibana ce qui m'a permis de visualiser en temps réel le débit d'ingestion, la répartition du trafic par domaine fonctionnel, le nombre de VIN actifs dans la flotte et les dernières

alertes avec leur sévérité. Ce tableau de bord regroupe cinq panneaux avec un graphique temporel du débit d'ingestion des trames (dans mon schéma ce n'est pas très représentatif puisque j'ai fait ingéré au SIEM l'ensemble des données en quelques minutes) ainsi qu'un classement des dix identifiants CAN les plus fréquents, une répartition du trafic par domaine fonctionnel (j'observe que l'infodivertissement monopolise les journaux à 58,15%, le chassis à 26,12% et la carrosserie à 15,67%) puis un autre panneau pour le nombre unique d'identifiants VIN présents dans les journaux (ici au nombre de deux puisque dans les deux ensembles de données importés il n'y avait qu'une voiture chacun) et enfin un panneau pour visualiser le nombre d'alertes par règles de détection. Ce tableau de bord illustre concrètement ce qu'un analyste pourrait utiliser au quotidien pour surveiller sa flotte automobile.

Il convient de noter que pour cette preuve de concept je n'ai pas pu avoir accès aux bases de données des constructeurs qui définissent clairement la sémantique et donc ce que représentent les signaux CAN. En effet, ces données ne sont pas publiques puisqu'elles permettraient aux acteurs malveillants de pouvoir les décoder facilement et ainsi de pouvoir les exploiter à leur avantage. J'ai été donc contraint à travailler sur les identifiants bruts plutôt que sur les valeurs physiques décodées empêchant la création de règles fondées sur une valeur fonctionnelle comme une pression de freinage anormale ou une vitesse incohérente. Enfin, l'architecture déployée n'avait que pour intérêt d'en démontrer sa faisabilité pour mon mémoire de recherche et n'ai donc pas de réplication ni de chiffrement entre les composants, ce qui serait incompatibles pour un déploiement industriel mais qui n'invalide pas la démonstration.

Conclusion

J'ai souhaité construire mon mémoire autour d'une question d'actualité qui est celle de la sécurité autour du secteur automobile. Pour répondre à la faisabilité d'un système de collecte et d'analyse de journaux appliqué à l'automobile, il a fallu d'abord poser les bases de ce qu'est l'Internet des Objets et comprendre pourquoi les véhicules connectés en font pleinement partie. La voiture moderne est un objet connecté à part entière embarquant des centaines de calculateurs qui communiquent en permanence via des bus de données internes et des interfaces sans-fil avec le monde extérieur. La deuxième partie de mon travail a permis de confirmer que cette surface d'attaque était non seulement réelle et déjà exploitée mais encore sous-estimée par les constructeurs automobiles comme ce qui m'avait été présenté pendant l'atelier "Car Hacking" à laquelle j'ai pu assister pendant "leHACK 2025". Le règlement UNECE R155 et la norme ISO 21434 ont commencé à poser un cadre réglementaire mais en réalité les acteurs du secteur automobile et les éditeurs de solutions de sécurité sont encore en train de définir les standards et les architectures qui permettront d'y répondre clairement. La troisième partie consacrée au fonctionnement d'un SIEM a permis de comprendre qu'un SIEM n'est pas seulement un outil de collecte de journaux, c'est aussi un moteur de corrélation capable de mettre en relation des signaux issus de sources hétérogènes pour identifier des comportements anormaux. Appliqué au contexte automobile, cette solution présente des contraintes comme l'hétérogénéité des sources et des formats des données, la connectivité qui peut s'avérer compliquée dans les voitures puisqu'elles peuvent être soumises à des pertes de connexion. Ces contraintes ont été confirmées par Aurélien BOUVARD, RSSI du groupe Kuhn, que j'ai eu la chance de pouvoir interroger dans le cadre de ce mémoire qui soulignait également que rares étaient les solutions proposées aujourd'hui pouvant ingérer simultanément des journaux IT classiques et les données embarquées des véhicules dans un SIEM. C'est dans la quatrième partie de ma réponse que j'ai pu définir les données exploitables, leur mise en forme et leur organisation dans un SIEM. Pour valider la faisabilité de

ma solution, j'ai choisi d'exploiter une solution ELK (Elasticsearch, Logstash et Kibana) pour ma preuve de concept ce qui m'a permis d'obtenir des résultats concrets sur l'exploitation de journaux automobiles. Sur plus de onze millions de journaux ingérés, deux règles de détection ont généré treize alertes exclusivement sur l'ensemble de données compromis. Ces résultats doivent cependant être nuancés puisqu'ils valident la faisabilité technique dans la démarche mais plusieurs conditions nécessaires à un déploiement industriel n'étaient pas réunies comme l'absence des fichiers constructeurs permettant de déchiffrer la sémantique réelle des signaux CAN et ainsi améliorer les règles de détection, puisque dans le cadre de ma validation de la solution les règles ont été définies avec des seuils statiques.

La validation de cette solution s'inscrit donc dans un contexte où la question de pouvoir visualiser ses journaux IT et ses journaux générés par les différents équipements automobiles dans une même plateforme reste largement ouverte et est encore en phase de laboratoire pour la plupart des éditeurs de solution de sécurité proposant des services de journalisation. La preuve de concept réalisé démontre que ce regroupement de journaux est techniquement réalisable dans une solution tel que celle d'Elasticsearch qui est open-source et sans couche intermédiaire propriétaire. J'estime ainsi que les résultats obtenus constituent une réponse concrète à la problématique posée puisque l'ingestion de journaux automobiles est possible dans cette solution, tout autant que des journaux IT classiques ainsi le mélange des deux, avec quelques spécificités l'est aussi. Enfin, le Cyber Resilience Act, dont l'application est progressive jusqu'en 2027, impose aux fabricants de produits connectés une surveillance continue et un signalement des incidents. La solution démontrée répond directement à cette exigence dans sa propre dimension, les alertes horodatées et les journaux conservés constituant précisément les preuves documentaires que le règlement exige.

Postface

Ce mémoire, dont les consignes nous ont été présentées en octobre 2025, m'a permis de développer une connaissance et de faire mûrir mes deux passions que sont la cybersécurité et l'automobile. Le thème que je devais choisir pour ce mémoire m'est apparu comme une évidence pour avoir la motivation de pouvoir écrire ce document d'une centaine de pages. Depuis octobre, j'ai pensé à cet exercice quotidiennement, programmant mes journées tout au long de l'année afin de dégager le plus de temps possible pour travailler ce mémoire. Les premières pages étaient les plus dures et j'espère que vous pourrez à travers l'ensemble de mon travail, percevoir mon évolution tout du long de ma dernière année d'études, ce qui me fait enfin rentrer dans la cour des grands.

Ce mémoire bien qu'éprouvant m'a fait prendre goût au travail, m'a fait apprendre à m'organiser pour rendre ce travail dans les temps mais surtout m'a fait apprendre à apprendre et m'a rendu encore plus curieux que je ne l'était en particulier dans mes domaines de passion. De mon point de vue le travail passionné est toujours meilleur que le travail qui n’est pas choisi et qui est subi. Je peux donc affirmer que ce travail était passionnant à produire m'en apprenant plus sur de multiples sujets et notamment sur des domaines qui me passionnent. Je pense continuer après le rendu de ce mémoire à explorer cette voie de la cybersécurité automobile pour aider, je l'espère, les plus grands constructeurs dans leur démarche de sécurité dès la conception. J'ai pu comprendre que je n'étais pas le seul à m'y intéresser notamment avec la revue du MISC Hors série n°32 qui présente beaucoup de sujets de cybersécurité automobile et qui a été très instructif mais aussi avec l'atelier du HACK 2025 qui m'a poussé à produire ce travail.

J'aurai souhaité avec plus de temps, mieux développer ma preuve de concept avec l'ingestion de journaux IT classiques ainsi que les journaux de systèmes embarqués automobiles. J'aurai aussi souhaité aborder la question des voitures autonomes qui sont au coeur de l'actualité mais je pense que ce sujet mérite à lui seul un mémoire dédié, je ne me suis concentré que ce sur quoi j'étais en confiance.

Bibliographie

Introduction

[Vikidia] Vikidia. « Automobile ». Vikidia. Lien : https://fr.vikidia.org/wiki/Automobile#Fabrication_en_série_:_la_Ford_Modèle_T

[Wikipedia.2025i] Wikipedia. « Système embarqué ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Système_embarqué

[Wikipedia.2026f] Wikipedia. « Histoire de l'automobile ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Histoire_de_l'automobile

[Wikipedia.2026h] Wikipedia. « Soupape (moteur) ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Soupape_(moteur)

1.1.1. Le concept d'IoT

[RadioFrance.2026] Radio France. « « Ça m'a fait flipper » : un informaticien français pirate involontairement 7 000 aspirateurs robots ». France Inter. 26 février 2026 Lien : https://www.radiofrance.fr/franceinter/podcasts/l-info-de-france-inter/ca-m-a-fait-flipper-un-informaticien-francais-pirate-involontairement-7-000-aspirateurs-robots-6451110

[REQUEA] REQUEA. « Qu'est-ce que l'IOT ? ». REQUEA. Lien : https://requea.com/qu-est-ce-que-l-iot.html

1.1.2. Aperçu technique de l'IoT

[ITUT.2012] ITU-T. « Recommendation ITU-T Y.2060 - Overview of the Internet of things and its requirements ». ITU. juin 2012. Lien : https://www.itu.int/rec/T-REC-Y.2060

[ScienceDirect.2013] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic et Marimuthu Palaniswami. « Internet of Things (IoT): A vision, architectural elements, and future directions ». Future Generation Computer Systems. septembre 2013. Lien : https://www.sciencedirect.com/science/article/abs/pii/S0167739X13000241

[Wikipedia.2025j] Wikipedia. « Technologies de l'information et de la communication ». Wikipedia. 20 septembre 2025. Lien : https://fr.wikipedia.org/wiki/Technologies_de_l'information_et_de_la_communication

1.1.3. Caractéristiques fondamentales de l'IoT

[IEEExplore.2015] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari et Moussa Ayyash. « Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications ». IEEE Communications Surveys & Tutorials. 15 juin 2015. Lien : https://doi.org/10.1109/COMST.2015.2444095

[OASISOpen.2019] Andrew Banks, Ed Briggs, Ken Borgendale, Rahul Gupta. « MQTT Version 5.0 ». OASIS Open. 7 mars 2019. Lien : https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

[RFC7452.2015] Hannes Tschofenig, Jari Arkko, Dave Thaler et Dan McPherson. « Architectural Considerations in Smart Object Networking ». RFC Editor / IETF. mars 2015. Lien : https://www.rfc-editor.org/rfc/rfc7452.html

1.1.4. Modèle de référence de l'IoT

[CNIL.2026] CNIL. « Modèle OSI ». CNIL. Lien : https://www.cnil.fr/fr/definition/modele-osi

[IoTIndustriel.2026] Mehdi Ben Nasser. « IoT industriel Blog - Votre référence en IIoT ». IoT industriel. Lien : https://iotindustriel.com/

1.2.1. Gestion de l'énergie

[CegedimCloud.2026] Cegedim.cloud / ITCare. « Carbon footprint ». Cegedim.cloud. Lien : https://academy.cegedim.cloud/itcare/enercare/carbon-footprint

[EcologieGouv.2019] Ministères de l'Aménagement du territoire et de la Transition écologique. « La responsabilité sociétale des entreprises ». 7 février 2019. Lien : https://www.ecologie.gouv.fr/politiques-publiques/responsabilite-societale-entreprises

[EnergyBots.2024] Arunima S. « How is Energy Monitoring Reshaping the Future of Automotive Industry? ». Energy Bots. 31 décembre 2024. Lien : https://www.energy-bots.com/blog/how-is-energy-monitoring-reshaping-the-future-of-automotive-industry/

[ISO50001] ISO. « ISO 50001 — Management de l'énergie ». ISO. Lien : https://www.iso.org/fr/iso-50001-energy-management.html

[LaFinancePourTous.2025] Nicolas. « Qu'est-ce que le greenwashing ? ». La finance pour tous. 19 juin 2025. Lien : https://www.lafinancepourtous.com/outils/questions-reponses/quest-ce-que-le-greenwashing/

1.2.2. Confort et productivité

[Matics.2024] Meirav Nachmanovitch Lazar. « How the Benefits of IIoT Are Transforming the Automotive Industry ». Matics. 29 juillet 2024. Lien : https://matics.live/blog/how-the-benefits-of-iiot-are-transforming-the-automotive-industry/

[OcellisEnergies.2024] Tony Bernardo. « L'intégration des solutions de climatisation et ventilation dans les bâtiments intelligents ». Ocellis Energies. 6 septembre 2024. Lien : https://ocellis-energies.fr/actualites/news/lintegration-des-solutions-de-climatisation-et-ventilation-dans-les-batiments-intelligents

[SafetyCulture.2025] SafetyCulture Staff. « Systèmes CVC ». SafetyCulture. 11 juillet 2025. Lien : https://safetyculture.com/fr/themes/systemes-cvc

[SmartDev.2024] Phuong Anh Ta. « The Future of IoT in Office Workspaces ». SmartDev. 5 décembre 2024. Lien : https://smartdev.com/fr/the-future-of-iot-in-office-workspaces/

1.2.3. Sécurité et contrôle d'accès

[AlgoSecure] AlgoSecure. « Audit Red Team ». AlgoSecure. Lien : https://www.algosecure.fr/audit/red-team

[KoreLock.2025] KoreLock. « How IoT Smart Lock Technology is Transforming Security ». KoreLock. Lien : https://www.korelock.com/post/how-iot-smart-lock-technology-is-transforming-security

[LabKey] LabKey. « IoT and Access Control: How Technology Is Revolutionizing Access Management ». LabKey. Lien : https://www.labkey.io/en/iot-access-control-security/

[MakeLocks.2025] Eliza. « How IoT Locks Are Reshaping Modern Security and Access Management ». MakeLocks. 26 décembre 2025. Lien : https://www.makelocks.com/news/how-iot-locks-are-reshaping-modern-security-and-access-management.html

[MercurySecurity] Mercury Security. « Beyond the Door: Why Access Control Is Becoming a Hub for IoT and Security Systems ». Mercury Security. Lien : https://www.mercury-security.com/beyond-the-door-why-access-control-is-becoming-a-hub-for-iot-and-security-systems/

[RobustelStore.2025] Robert Liao. « A Guide to Access Control IoT Devices: Secure, Scalable, and Remotely Managed ». Robustel Store. 19 septembre 2025. Lien : https://www.robustel.store/blogs/industrial-iot-blog/a-guide-to-access-control-iot-devices-secure-scalable-and-remotely-managed

1.3.1. Transport agricole

[LeRobert] LeRobert. « Définition de GPS ». LeRobert. Lien : https://dictionnaire.lerobert.com/definition/gps

[SIAPartners.2020] SIA Partners. « L'essor des objets connectés dans l'Agriculture 4.0 ». SIA Partners. 27 février 2020 Lien : https://www.sia-partners.com/fr/publications/publications-de-nos-experts/lessor-des-objets-connectes-dans-lagriculture-40

[Wattsense.2025] Cyril Mathé. « LoRaWAN : qu'est-ce que c'est ? ». Wattsense. 19 décembre 2025. Lien : https://www.wattsense.com/fr-fr/blog/protocoles-de-communication/quest-ce-que-le-protocole-lorawan/

[Wikipedia.2025e] Wikipedia. « Global Positioning System ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Global_Positioning_System

1.3.2. Transport routier de marchandises

[ELAInnovation.2022] Fanny WATERLOT. « Comment l'IoT sécurise le transport de marchandises ? ». ELA Innovation. 31 mars 2021. Lien : https://elainnovation.com/comment-liot-securise-le-transport-de-marchandises/

[FlotAuto.2022] La rédaction. « Télématique et IoT : des poids lourds connectés ». FlotAuto. 28 septembre 2022. Lien : https://www.flotauto.com/poids-lourds-telematique-20200928.html

[Kuzzle] Kuzzle. « The cold chain ». Kuzzle IoT. Lien : https://kuzzle.io/break-cold-chain/

[TargaTelematics] Targa Telematics. « Targa Telematics : Gestion de flotte, Smart Mobility et IoT ». Targa Telematics. Lien : https://targatelematics.com/fr-fr/

1.3.3. Transports en commun

[IRISSensing] IRIS Intelligent Sensing. « Systèmes de transport public intelligents: L'avenir des transports en commun ». IRIS Intelligent Sensing. Lien : https://www.iris-sensing.com/fr/actualites/article/systemes-de-transport-public-intelligents-lavenir-des-transports-en-commun/

[ISO] ISO. « Systèmes de transport intelligents : transformer la mobilité moderne ». Lien : https://www.iso.org/fr/transport/sti-systemes-transport-intelligents

[YouTube.2017] Groupe Keolis. « [Innovation] : IoT on TBM public transport network by Keolis Bordeaux (France) ». YouTube. 15 novembre 2017. Lien : https://www.youtube.com/watch?v=QZ9lfFoM9X0

2.1.1. Évolution de la sécurité routière

[ONISR] Observatoire national interministériel de la sécurité routière. « Historique de la sécurité routière et perspectives ». ONISR. Lien : https://www.onisr.securite-routiere.gouv.fr/politique-de-securite-routiere/historique-de-la-securite-routiere-et-perspectives

[PointsDeVue.2015] Points de Vue. « Evolution de la mortalité routière en France ». Points de Vue. 2 août 2015. Lien : https://www.stage-pointsdevue.fr/donnees-chiffrees/historique-de-la-mortalite-routiere

2.1.2. Types de sécurité routière

[DeviceAuthority] Device Authority. « Connected Car Security: Automotive IoT Threats and Protection ». Device Authority. Lien : https://deviceauthority.com/connected-car-security-automotive-iot-threats-and-protection/

[Ornikar.2026a] Curtis Bassy. « La cellule de survie des automobiles ». Ornikar. Lien : https://www.ornikar.com/code/cours/mecanique-vehicule/habitacle/cellule-survie

[Ornikar.2026b] Curtis Bassy. « Sécurité active et passive : quelles différences ? ». Ornikar. Lien : https://www.ornikar.com/code/cours/securite/dispositif/differences-active-passive

[RooleMedia.2025] Roole Média. « Système ESP : fonctionnement, utilité et limites pour votre sécurité ». Roole Média. 16 mai 2025. Lien : https://media.roole.fr/quotidien/equipement/a-quoi-sert-le-systeme-esp

[Wikipedia.2025a] Wikipedia. « Assistance au freinage d'urgence ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Assistance_au_freinage_d'urgence

[Wikipedia.2025l] Wikipedia. « eCall ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/ECall

[Wikipedia.2026i] Wikipedia. « Système anti-blocage des roues ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Système_anti-blocage_des_roues

2.1.3. Normes et référentiels

[EuroNCAP] Euro NCAP. « Euro NCAP - YouTube ». YouTube. Lien : https://www.youtube.com/@EuroNCAP_forsafercars/videos

[ISO.2012] ISO. « ISO 39001:2012 - Systèmes de management de la sécurité routière — Exigences et recommandations de bonnes pratiques ». ISO. octobre 2012. Lien : https://www.iso.org/fr/standard/44958.html

[LArgus.2022] Johann Leblanc. « Boîtes noires automobiles. Comment ça marche et à quoi ça sert ? ». L'argus. 6 mai 2022. Lien : https://www.largus.fr/actualite-automobile/boites-noires-automobiles-comment-ca-marche-et-a-quoi-ca-sert-20000407.html

[LArgus.2024] Johann Leblanc. « GSR 2. Les nouvelles règles de sécurité pour les véhicules en Europe ». L'argus. 1 mars 2024. Lien : https://www.largus.fr/actualite-automobile/gsr-2-les-nouvelles-regles-de-securite-pour-les-vehicules-en-europe-30032438.html

[Wikipedia.2026d] Wikipedia. « Code de la route ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Code_de_la_route

[Wikipedia.2026e] Wikipedia. « Euro NCAP ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Euro_NCAP

2.2.1. Réseau cellulaire

[Cisco] Cisco. « Qu'est-ce que la 5G ? ». Cisco. Lien : https://www.cisco.com/c/fr_fr/solutions/what-is-5g.html

[HubOne] HubOne. « Réseau Mobile : Comment fonctionne un réseau de téléphonie mobile ? ». HubOne. Lien : https://www.hubone.fr/oneblog/comment-fonctionne-un-reseau-de-telephonie-mobile/

[OracleFrance.2022] Oracle. « Qu'est-ce que le deep learning ? ». Oracle. 20 août 2022. Lien : https://www.oracle.com/fr/artificial-intelligence/machine-learning/what-is-deep-learning/

[StudySmarter.2024] Lily Hulatt. « 2G, 3G, 4G, 5G ». StudySmarter. 13 septembre 2024. Lien : https://www.studysmarter.fr/resumes/ingenierie/ingenierie-des-telecommunications/2g-3g-4g-5g/

[Wikipedia.2026a] Wikipedia. « 5G ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/5G

[Wikipedia.2026g] Wikipedia. « Réseau de téléphonie mobile ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Réseau_de_téléphonie_mobile

2.2.2. Technologie Wi-Fi

[BouyguesTelecomEntreprises.2026] Bouygues Telecom. « Wifi ». Le Mag Business. Lien : https://www.bouyguestelecom-pro.fr/mag-business/lexique/wifi/?srsltid=AfmBOoorjY1zBzsyVRwAB5S3dtS9Md3VDovrOvydN676zyFg4MmcEkRe

[Proofpoint] Proofpoint. « Qu'est-ce que le Wi-Fi ? ». Proofpoint. Lien : https://www.proofpoint.com/fr/threat-reference/wifi

[Wikipedia.2021] Wikipedia. « Temporal Key Integrity Protocol ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol

[Wikipedia.2025b] Wikipedia. « Attaque de l'homme du milieu ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu

[Wikipedia.2025g] Wikipedia. « RC4 ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/RC4

[Wikipedia.2026b] Wikipedia. « Advanced Encryption Standard ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard

[Wikipedia.2026c] Wikipedia. « Carrier Sense Multiple Access with Collision Avoidance ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Carrier_Sense_Multiple_Access_with_Collision_Avoidance

[Wikipedia.2026j] Wikipedia. « Wi-Fi ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Wi-Fi

[Wikipedia.2026k] Wikipedia. « Wi-Fi Alliance ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Wi-Fi_Alliance

2.2.3. Bluetooth

[CapCar] CapCar. « Bluetooth automobile ». CapCar. Lien : https://www.capcar.fr/lexique-auto/bluetooth-automobile

[IPSystemes.2025] IP Systèmes. « Communication Bluetooth, comment ça marche ? ». IP Systèmes. 28 avril 2025. Lien : https://www.ip-systemes.com/communication-bluetooth-comment-a-marche.html

[Intel] Intel. « Qu'est-ce que la technologie Bluetooth® ? ». Intel. Lien : https://www.intel.fr/content/www/fr/fr/products/docs/wireless/what-is-bluetooth.html

[MDPI.2019] Dong-Kyu Choi, Joong-Hwa Jung, Ji-In Kim, Moneeb Gohar, Seok-Joo Koh. « IoT-Based Resource Control for In-Vehicle Infotainment Services: Design and Experimentation ». Sensors. 1 février 2019. Lien : https://www.mdpi.com/1424-8220/19/3/620

[Vroomly.2022] Ariane. « Kit main-libre : ce qui est autorisé et ce qui ne l'est pas ». Vroomly. 8 août 2022. Lien : https://www.vroomly.com/blog/kit-main-libre/#titre-2

[Wikipedia.2025c] Wikipedia. « Bluetooth Special Interest Group ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Bluetooth_Special_Interest_Group

[Wikipedia.2025f] Wikipedia. « Harald à la Dent bleue ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Harald_à_la_Dent_bleue

2.3.1. Electronic Control Unit (ECU)

[ECUAUTO21.2025] ECU AUTO 21. « Le Stage 1 passe-t-il au contrôle technique ? ». ECU AUTO 21. Lien : https://ecuauto21.fr/stage-1-controle-technique/

[Lembarque.2022] Carmelo De Mola. « L'Ethernet automobile, oui, mais pas tout seul... ». L'Embarqué. Février 2020. Lien : https://www.lembarque.com/fichiers/cms/file/002_005_MCA813%20APPLICATION_MICROCHIP%20DEF.pdf

[Wikipedia.2025k] Wikipedia. « Unité de commande électronique ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Unité_de_commande_électronique

2.3.2. Types de BUS

[FlexiHub.2024] Olga Weis. « Comprendre les systèmes de bus CAN : Guide complet sur le bus CAN ». FlexiHub. 16 juillet 2024. Lien : https://www.flexihub.com/fr/can-bus/

[PCM.2024] PCM. « 4 types de bus de voitures ». PCM. 30 septembre 2024. Lien : https://fr.pcm-cable.com/info/4-kinds-of-car-bus-80286654.html

[ParlezVousTech.2024] N. Samba. « Le bus LIN : Une révolution dans la connectivité automobile, hier et aujourd'hui ». Parlez-vous Tech. 26 mars 2024. Lien : https://

www.parlezvoustech.com/le-bus-lin-une-revolution-dans-la-connectivite-automobile-hier-et-aujourdhui/

[Tektronix] Tektronix. « Ethernet automobile ». Tektronix. Lien : https://www.tek.com/fr/solutions/industry/automotive-test-solutions/in-vehicle-networks/automotive-ethernet

[Wikipedia.2024a] Wikipedia. « Bus LIN ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Bus_LIN

[Wikipedia.2024b] Wikipedia. « MOST ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/MOST

[Wikipedia.2025d] Wikipedia. « Bus de données CAN ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Bus_de_données_CAN

2.3.3. OBD (on-board diagnostics)

[CarElectroDiag.2024] Frantz. « Systèmes OBD-I, OBD-II/EOBD (ou OBD2) ». Car Electro Diag. 4 novembre 2024. Lien : https://carelectrodiag.com/2024/11/04/systemes-obd-et-eobd/

[DUNASYS.2024] DUNASYS. « On-Board Diagnostic : Comprendre le Diagnostic Embarqué ». DUNASYS. Lien : https://www.dunasys.com/article/on-board-diagnostic-comprendre-le-diagnostic-embarque/

[Frandroid.2015] Romain. « Des hackers américains piratent une Corvette grâce à un dongle OBD français ». Frandroid. 12 août 2015. Lien : https://www.frandroid.com/culture-tech/securite-applications/302578_hackers-americains-piratent-corvette-grace-a-port-obd-francais

[KLAVKARR.2026] KLAVKARR. « Mode OBD ou constructeur : Quelle est vraiment la différence ? ». KLAVKARR. 2 avril 2026. Lien : https://www.outilsobdfacile.fr/blog/difference-mode-obd-constructeur-p127.html

[OBDAUTOALB.2025] Loic. « C'est quoi le système OBD ? ». OBD AUTO. 4 août 2025. Lien : https://www.obdauto.fr/blog/cest-quoi-le-systeme-obd/

[OutilsOBDFacile.2026] Outils OBD Facile. « OBD2 Bluetooth : guide complet du diagnostic auto sans fil ». Outils OBD Facile. 2 avril 2026. Lien : https://www.outilsobdfacile.fr/blog/boitier-obd2-bluetooth-p113.html

3.1.1. Collecteurs de données

[InformaticaEconomica.2024] Cosmin MĂCĂNEAȚĂ. « Overview of Security Information and Event Management Systems ». revistaie.ase.ro. 2024. Lien : https://www.revistaie.ase.ro/content/109/02 - macaneata.pdf

[Microsoft] Microsoft. « Qu'est-ce que la SIEM ? ». Sécurité Microsoft. Lien : https://www.microsoft.com/fr-fr/security/business/security-101/what-is-siem

[Wikipedia.2025h] Wikipedia. « Security information and event management ». Wikipedia. Lien : https://fr.wikipedia.org/wiki/Security_information_and_event_management

3.1.2. Traitement / agrégation

[ArXiv.2017] Mario Di Mauro; Cesario Di Sarno. « Improving SIEM capabilities through an enhanced probe for encrypted Skype traffic detection ». arXiv. 1 novembre 2017. Lien : https://arxiv.org/pdf/1711.00524

[Varonis.2025] Michael Buckbee. « IDS et IPS : en quoi sont-ils différents ? ». Varonis. 20 mars 2025. Lien : https://www.varonis.com/fr/blog/ids-et-ips-en-quoi-sont-ils-differents

3.1.3. Stockage / Restitution

[AFNORCertification] AFNOR Certification. « Certification HDS - Hébergeurs de données de santé ». AFNOR Certification. Lien : https://certification.afnor.org/numerique/hebergement-des-donnees-de-sante-hds

[Inkivari] Inkivari. « Ai-je le droit de conserver les données de connexion des utilisateurs de mon site web pendant 5 ans ? ». Inkivari. Lien : https://www.inkivari.com/blog/le-quizz-hebdomadaire-d-inkivari-7/rgpd-conservation-logs-connexion-cpce-cnil-1-an-34

[PureStorage.2026] Pure Storage. « Qu'est-ce que le stockage de données à froid ? ». Pure Storage. Lien : https://www.purestorage.com/fr/knowledge/what-is-cold-storage.html

3.2.1. Cycle de vie d'un évènement

[CNIL.2024] CNIL. « Sécurité : Tracer les opérations ». CNIL. 14 mars 2024. Lien : https://www.cnil.fr/fr/securite-tracer-les-operations

[Vizee] Vizee. « La centralisation des logs : qu'est-ce que c'est, comment la mettre en place ? ». Vizee. Lien : https://www.vizee.io/centralisation-logs/

[Wescale.2023] Antoine Mayer. « Comment mettre en place une solution de centralisation de logs ? ». Wescale. 28 juin 2023. Lien : https://blog.wescale.fr/comment-mettre-en-place-une-solution-de-centralisation-de-logs

3.2.2. Détection et corrélation

[FeelAgile.2026] FeelAgile. « Qu'est-ce qu'un Système de Management de Sécurité de l'Information ? ». FeelAgile. Lien : https://www.feelagile.com/blog/quest-ce-quun-smsi

[KTnS.2024] K TnS. « L'importance du SIEM dans la gestion des événements de sécurité ». K TnS. 4 mars 2024. Lien : https://www.k-tns.com/limportance-du-siem-dans-la-gestion-des-evenements-de-securite/

[Napsis] Napsis. « Le SIEM, tour de contrôle de la cybersécurité de votre entreprise ». Napsis. Lien : https://www.napsis.fr/cybersecurite/siem/

[SNSSecurity.2025] SNS Security. « SIEM : Comprendre la gestion de l'information et des événements de sécurité ». SNS Security. 25 mars 2025. Lien : https://sns-security.fr/siem-comprendre-gestion-information-evenements-securite/

[StellarCyberb] Stellar Cyber. « SIEM Règles de corrélation : Améliorer votre détection des menaces ». Stellar Cyber. Lien : https://stellarcyber.ai/fr/learn/règles-de-corrélation-de-siem/

3.2.3. Exploitation

[IBM] IBM. « Qu'est-ce que SOAR (l'orchestration, l'automatisation et la réponse à la sécurité) ? ». IBM.com. Lien : https://www.ibm.com/fr-fr/think/topics/security-orchestration-automation-response

[WAYDEN.2026] WAYDEN. « Security Information & Event Management (SIEM) : rôles, enjeux et déploiement en entreprise ». WAYDEN. 26 janvier 2026. Lien : https://www.wayden.fr/security-information-event-management-siem-roles-enjeux-et-deploiement-en-entreprise/

3.3.1. Détection d'intrusions

[DanielCraft.2026] DanielCraft. « SIEM : logs, corrélation et détection ». DanielCraft. 11 novembre 2025. Lien : https://danielcraft.fr/blog/articles/siem-log-management-detection

[ITConnect.2024] Mickael Dorigny. « Sécurité Active Directory - Comment détecter les attaques par brute force dans un domaine ? ». IT-Connect. 19 juin 2024. Lien : https://www.it-connect.fr/securite-active-directory-detecter-attaques-par-brute-force/

[StellarCyber.2026b] Stellar Cyber. « SIEM Règles de corrélation : Améliorer votre détection des menaces ». Stellar Cyber. Lien : https://stellarcyber.ai/fr/learn/siem-correlation-rules/

3.3.2. Conformité

[LOGIQE.2025] LOGIQE. « Conservation des logs : traçabilité, conformité et sécurité des systèmes ». LOGIQE. 19 septembre 2025. Lien : https://logiqe.fr/cybersecurite-managee/conservation-des-logs/

[SentinelOne.2025a] SentinelOne. « Conformité SIEM : composants clés et cas d'utilisation ». SentinelOne. 19 août 2025. Lien : https://www.sentinelone.com/fr/cybersecurity-101/data-and-ai/siem-compliance/

[StellarCyberc] Stellar Cyber. «Top SIEM Cas d'utilisation en matière de conformité : RGPD, PCI DSS, ISO et plus encore ». Stellar Cyber. Lien : https://stellarcyber.ai/fr/learn/siem-compliance-use-cases/

[WEDOSProtection.2025] WEDOS Protection. « Rétention des journaux selon NIS2 (6, 18 mois ou personnalisé) ». WEDOS Protection. Lien : https://wedos.protection/fr/log-retention-as-per-nis2-6-18-months-or-custom/

3.3.3. Réponse aux incidents

[IMSNetworks] IMS Networks. « Cyber-SOC Détection & Réponse à incident ». IMS Networks. Lien : https://www.imsnetworks.com/service/cyber-soc-detection-reponse-a-incident/

[OrangeCyberdefense] Orange Cyberdefense. « Incident Response ». Orange Cyberdefense. Lien : https://www.orangecyberdefense.com/fr/solutions/offres-detection-reaction/incident-response

[PaloAltoNetworks.2026] Palo Alto Networks. « Opérations DFIR (analyse forensique et réponse à incident) ». Palo Alto Networks. Lien : https://www.paloaltonetworks.fr/cyberpedia/digital-forensics-and-incident-response

[Wiz.2026] Équipe d'experts Wiz. « Qu'est-ce que la réponse aux incidents ? Le guide accéléré pour les SOC ». Wiz. 20 janvier 2026. Lien : https://www.wiz.io/fr-fr/academy/detection-and-response/incident-response-fast-track-guide

4.1.1. Nature des données collectées

[MDPI.2022] Jay Johnson, Timothy Berg, Benjamin Anderson et al.. « Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses ». MDPI / Energies. 26 mai 2022. Lien : https://www.mdpi.com/1996-1073/15/11/3931

[MISC.2025a] Bogdan G. « Cybersécurité automobile, brève introduction ». MISC hors série n°32. Juin-juillet 2025. Lien : https://boutique.ed-diamond.com/home/1779-misc-hs-32.html

[MISC.2025b] Philippe AZALBERT. « Introduction au reverse-engineering d'ECU ». MISC hors série n°32. Juin-juillet 2025. Lien : https://boutique.ed-diamond.com/home/1779-misc-hs-32.html

[PMPStrategy.2019] Cyril Rousset et Lionel Chapelet. « La télématique automobile, source d'opportunités ou écran de fumée ? ». PMP Strategy. 30 juillet 2019. Lien : https://pmpstrategy.com/2019/07/30/la-telematique-automobile-source-d-opportunites-ou-ecran-de-fumee/

[ResearchNester.2026] Research Nester. « Taille et part de marché de la télématique embarquée, par type de véhicule... ». Research Nester. 5 février 2026. Lien : https://www.researchnester.com/fr/reports/vehicle-telematics-market/4462

[SensorsMDPI.2024] Claudiu Vasile Kifor et Aurelian Popescu. « Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies ». MDPI. 23 septembre 2024. Lien : https://www.mdpi.com/1424-8220/24/18/6139

[Wavestone.2020] Anthony di Prima. « Saga 3/3 : La sécurité des véhicules connectés, les réponses pour une transformation nécessaire ! ». RiskInsight. 2020. Lien : https://www.riskinsight-wavestone.com/2019/10/saga-33-voiture-connectee/

4.1.2. Modes de transit des données

[BoschRexroth.2022] Christian Grabe. « Transfert des données télématiques dans le cloud de manière efficace et sécurisée ». Bosch Rexroth. 12 décembre 2022. Lien : https://www.boschrexroth.com/fr/ch/blog/transfert-des-donnees-telematiques-dans-le-cloud/

[CleanMob.2025] Sarah. « Qu'est-ce qu'un boîtier télématique et comment bien le choisir ? ». CleanMob. 7 mai 2025. Lien : https://www.cleanmob.eu/article/quest-ce-quun-boitier-telematique-et-comment-bien-le-choisir-cleanmob

[FARECO.2019] FARECO. « Système de communication V2X - Véhicules autonomes avec l'infrastructure routière ». France Mobilités. 24 juillet 2019. Lien : https://www.francemobilites.fr/solutions/systeme-communication-v2x-vehicules-autonomes-avec-linfrastructure-routiere

[Fortinet] Fortinet. « Qu'est-ce que le protocole DHCP (Dynamic Host Configuration Protocol) ? ». Fortinet. Lien : https://www.fortinet.com/fr/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp

[Geotab.2025] Christoph Ludewig. « La flotte du futur : les véhicules connectés, la télématique et l'importance croissante des données ». Geotab. 13 février 2025. Lien : https://www.geotab.com/fr/blog/vehicules-connectes-telematique-et-oem/

[MISC.2025c] David BERARD. « Modèle de sécurité des véhicules Tesla ». MISC hors série n°32. Juin-juillet 2025. Lien : https://boutique.ed-diamond.com/home/1779-misc-hs-32.html

[Navixy.2025] Benjamin Hayes. « Télématique OEM : intégrer la télématique véhicule intégrée dans vos opérations ». Navixy. 3 décembre 2025. Lien : https://www.navixy.com/fr/blog/telematique-oem-integrer-la-telematique-vehicule-integree-dans-vos-operations/

[TruGem] TruGem. « Qu'est-ce que l'unité de contrôle télématique et comment fonctionne-t-elle ? ». TruGem. Lien : https://www.trugemtech.com/fr/quest-ce-que-lunite-de-controle-telematique/

4.1.3. Contraintes de collecte

[ANSSI.2024] Lucas HASSAN. « Cyber Resilience Act (CRA) : ce qui change pour les entreprises et comment s'y préparer ». cyber-gouv. 12 mars 2026. Lien : https://www.entreprises.gouv.fr/decryptages-de-nos-experts/cyber-resilience-act-cra-ce-qui-change-pour-les-entreprises-et-comment

[CNIL.2025] CNIL. « [Clôturée] Véhicules connectés et localisation : la CNIL lance une consultation publique sur son projet de recommandation ». CNIL. 25 mars 2025. Lien : https://www.cnil.fr/fr/vehicules-connectes-et-localisation-consultation-publique-projet-de-recommandation

[ETAS.2025] ETAS. « De la cybersécurité automobile à l'ensemble du domaine de la mobilité ». ETAS. Lien : https://www.etas.com/ww/fr/a-propos-detas/newsroom/vue-densemble/de-la-cybersecurite-automobile-a-lensemble-du-domaine-de-la-mobilite/

[EvolutioAvocats.2025] Evolutio Avocats. « Véhicules connectés : la CNIL lance une consultation sur les données de localisation ». Evolutio Avocats. 6 mai 2025. Lien : https://evolutio-avocats.com/it/vehicules-connectes-la-cnil-lance-une-consultation-sur-les-donnees-de-localisation

4.2.1. Centralisation des données

[ANSSI.2025] ANSSI. « Approche SSI pour l'Internet des objets industriels ». cyber.gouv.fr. 30 mai 2025. Lien : https://messervices.cyber.gouv.fr/documents-guides/approche_ssi_pour_l_internet_des_objets_industriels_2025.pdf

[SOCPrime.2026] Steven Edwards. « SIEM vs Gestion des Logs : Observabilité, Télémétrie et Détection ». SOC Prime. 5 mars 2026. Lien : https://socprime.com/fr/blog/siem-vs-gestion-des-logs/

[SentinelOne.2025b] SentinelOne. « Qu'est-ce que l'architecture SIEM ? Composants et meilleures pratiques ». SentinelOne. 11 août 2025. Lien : https://www.sentinelone.com/fr/cybersecurity-101/data-and-ai/siem-architecture/

[StellarCybera] Stellar Cyber. « SIEM Journalisation : aperçu et meilleures pratiques ». Stellar Cyber. Lien : https://stellarcyber.ai/fr/learn/siem-logging-overview-best-practices/

[UNECE.2020] UNECE. « Les Nations unies adoptent deux règlements clés pour le déploiement des véhicules connectés, sur la cybersécurité et les mises à jour de logiciels ». UNECE. 24 juin 2020. Lien : https://unece.org/fr/press/les-nations-unies-adoptent-deux-reglements-cles-pour-le-deploiement-des-vehicules-connectes

4.2.2. Mise en forme et corrélation

[AzurSecure] Azur Secure. « Introduction à NXLOG ». Azur Secure. Lien : https://www.azursecure.com/cours/administration-securite/introduction-a-nxlog/

[Microsoft.2019] Nicholas DiCola; Cristhofer Romeo Munoz. « Best Practices for Common Event Format (CEF) collection in Azure Sentinel ». Microsoft Community Hub. 19 novembre 2019. Lien : https://techcommunity.microsoft.com/blog/microsoftsentinelblog/best-practices-for-common-event-format-cef-collection-in-azure-sentinel/969990

[Splunk.2023] Stephen Watts. « Common Event Format (CEF): An Introduction ». Splunk. 3 mars 2023. Lien : https://www.splunk.com/en_us/blog/learn/common-event-format-cef.html

[StellarCyber.2026a] Stellar Cyber. « Common Log Formats ». Stellar Cyber Docs. Lien : https://docs.stellarcyber.ai/5.4.x/Configure/LogParser/common-data-log-formats.htm

4.2.3. Organisation et stockage

[Actian] Actian. « analyse des logs expliquée - Importance, exemples et avantages ». Actian. Lien : https://www.actian.com/fr/glossary/log-analytics/

[CIO.2021] Bertrand Lemaire. « La CNIL recadre la conservation des logs ». CIO Online. 28 novembre 2021. Lien : https://www.cio-online.com/actualites/lire-la-cnil-recadre-la-conservation-des-logs-13687.html

[CNIL.2017] CNIL. « VÉHICULES CONNECTÉS ET DONNÉES PERSONNELLES ». CNIL. octobre 2017. Lien : https://www.cnil.fr/sites/cnil/files/atoms/files/pack_vehicules_connectes_web.pdf

[CNIL.2021] CNIL. « La CNIL publie une recommandation relative aux mesures de journalisation ». CNIL. 18 novembre 2021. Lien : https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-relative-aux-mesures-de-journalisation

[DFIS.2024] Alain Mutrelle. « Quelle est la bonne durée de conservation des logs ? ». DFIS. 26 septembre 2024. Lien : https://www.dfis.fr/2024/09/26/quelle-est-la-bonne-duree-de-conservation-des-logs/

[FacemWeb] Xavier Deloffre. « SIEM : Comment centraliser et exploiter les journaux de sécurité ». Facem Web. Lien : https://facemweb.com/blog/creation-site/siem-journaux-de-securite/

[Microsoft.2026] Microsoft. « Benchmark de sécurité cloud Microsoft - Journalisation et détection des menaces ». Microsoft Learn. 3 février 2026. Lien : https://learn.microsoft.com/fr-fr/security/benchmark/azure/mcsb-logging-threat-detection

[RedHat.2023] Red Hat. « La gestion des informations et des événements de sécurité, qu'est-ce que c'est ? ». Red Hat. 21 septembre 2023. Lien : https://www.redhat.com/fr/topics/security/what-is-SIEM

4.3.1. Détection d'événements anormaux

[AutomobilePropre.2018] Philippe SCHWOERER. « Les bornes de recharge pour voitures électriques vulnérables aux hackers ? ». Automobile Propre. 26 décembre 2018. Lien : https://www.automobile-propre.com/articles/bornes-recharge-voitures-electriques-vulnerables-hackers/

[MISC.2025d] Etienne CHARRON, Khadim DIENG. « Retour d'expérience sur la recherche de vulnérabilités sur un service d'un boîtier multimédia : Carplay ». MISC hors série n°32. Juin-juillet 2025. Lien : https://boutique.ed-diamond.com/home/1779-misc-hs-32.html

[MISC.2025e] Aymeric PALHIERE. « Compromission d'un chargeur de véhicules électriques lors de Pwn2Own 2024 ». MISC hors série n°32. Juin-juillet 2025. Lien : https://boutique.ed-diamond.com/home/1779-misc-hs-32.html

[Parasoft.2025] Ricardo Camacho. « Pourquoi la cybersécurité automobile est importante ». Parasoft. 30 janvier 2025. Lien : https://fr.parasoft.com/blog/why-automotive-cybersecurity-is-important/

[SERMASafetyAndSecurity.2025] SERMA Safety and Security. « La révolution Flipper Zero : Parlez avec votre voiture ! ». SERMA Safety and Security. 9 janvier 2025. Lien : https://www.serma-safety-security.com/blog/flipper-zero-communiquez-avec-votre-voiture/

[TechniquesDeLIngenieur.2025] Nicolas LOUIS. « Stations de recharge électrique : la nouvelle cible des cyberattaques ». Techniques de l'Ingénieur. 26 décembre 2025. Lien : https://www.techniques-ingenieur.fr/actualite/articles/stations-de-recharge-electrique-la-nouvelle-cible-des-cyberattaques-154476/

[TechnoCar.2023] Mickael Duros. « Détournement de bornes de recharge de véhicules électriques et risque de DoS ». Techno-Car. 24 février 2023. Lien : https://www.techno-car.fr/detournement-de-bornes-de-recharge-de-vehicules-electriques/

[VoitureConnecteeCom] Aline Marchand. « Pirater une voiture connectée ». Voiture-connectee.com. novembre 2025. Lien : https://www.voiture-connectee.com/pirater-voiture-connectee/

4.3.2. Gestion et analyse des incidents

[CapgeminiFrance.2023] Thomas Chasles. « Quelle cybersécurité pour les véhicules connectés ? ». Capgemini France. 23 mars 2023. Lien : https://www.capgemini.com/fr-fr/perspectives/blog/cybersecurite-vehicules-connectes/

[IntervalleTechnologies.2025] Marketing Intervalle. « SOC : Le Guide Complet du Security Operations Center 24/7 ». Intervalle Technologies. 28 juin 2025. Lien : https://intervalle-technologies.com/blog/soc-guide-complet-security-operations-center-24-7/

[ScopeCyber] Scope Cyber. « SIEM : définition, fonctionnalités et gestion des événements de sécurité ». Scope Cyber. 26 février 2026. Lien : https://scopecyber.fr/blog/siem-comprendre-et-implementer-un-systeme-de-gestion-des-evenements

[TSystemsInternationalGmbH] T-Systems International GmbH. « Un détective pour le logiciel des réseaux embarqués ». T-Systems. Lien : https://www.t-systems.com/fr/fr/industries/automotive/solutions/intrusion-detection-system

[UNECE.2021] UNECE. « UN Regulation No. 155 - Cyber security and cyber security management system ». UNECE. 4 mars 2021. Lien : https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

4.3.3. Validation de la solution proposée

[Elasticsearch] Elastic. « Install Elasticsearch ». Elasticsearch. Lien : https://www.elastic.co/docs/deploy-manage/deploy/self-managed/installing-elasticsearch

[GitHub.2023] sampathrajapaksha. « CAN-MIRGU: A Comprehensive CAN Bus Attack Dataset from Moving Vehicles for Intrusion Detection System Evaluation ». GitHub. 28 décembre 2023. Lien : https://github.com/sampathrajapaksha/CAN-MIRGU/tree/main

[UpstreamSecurity] Upstream Security. « Meet the Expert: Enhancing SIEM solutions ». Upstream Security. Lien : https://upstream.auto/resources/meet-the-expert-enhancing-siem-solutions/