IUT d'Aix-Marseille Département Informatique
Ortec Service
413 Av. Gaston Berger
13100 Aix-en-Provence

550 Rue Pierre Berthier
13090 Aix-en-Provence

RAPPORT DE STAGE

Nils SAADI

Exemplaire pour Ortec – version 1.1

Maitre de stage : Jean-Marc Roussel

Tuteur : Safa Yahi

Remerciements

Avant tout, je voudrais commencer mon rapport de stage avec les remerciements, à ceux qui m'ont accompagné tout au long de ce stage.

Je remercie M. Jean-Marc Roussel, RSSI[1] d'Ortec, pour m'avoir offert l'opportunité de rejoindre cette entreprise et de participer à des projets passionnants dans le domaine de la cybersécurité.

Je tiens également à remercier mes collègues de l'équipe cybersécurité, M. Clément Barcenilla, M. Orlando Ducamp et M. Tristan Leleu, pour leur aide tout au long de mon stage.

Je suis reconnaissant pour cette opportunité de stage qui m'a permis d'acquérir de nouvelles compétences et de découvrir le monde de la cybersécurité et celui de l'entreprise. Votre soutien et votre collaboration ont été essentiels pour la réussite de mon stage.

Je tiens également à remercier Madame Safa Yahi qui a été ma tutrice et qui m'a accompagné durant toute la période du stage et à Madame Christine Makssoud pour avoir pris en considération mes différentes requêtes.

[1] RSSI : Responsable Sécurité du Système d'Information.

Fiche Technique	
Etudiant	Nils SAADI
Année	2023
Raison Sociale de l'entreprise	Ortec Services
Maître de stage Fonction	Jean-Marc Roussel RSSI
Mission	Dans le cadre de l'utilisation partagée d'ordinateurs qui fonctionnent sous Windows 10, il sera demandé l'étude et la mise en place complète du mode kiosque Windows
Plateforme informatique et systèmes	Windows 10
Outils logiciels et langages	Azure Active Directory, Windows 10
Mots clés	Mode kiosque, Windows, Cybersécurité, Active Directory, GPO Stratégie de Groupe, Log, Cloud

Versionnage

Date	Version	Modification
05/05/2023	0.1	Remerciement – Fiche technique – Sommaire – Introduction - Présentation d'Ortec - Bilan de la formation – Conclusion (à compléter)
26/05/2023	0.2	Travail réaliser (à compléter) - versionnage
01/06/2023	0.3	Travail réaliser (à compléter) - Bilan de l'expérience en entreprise
07/06/2023	0.4	Travail réaliser (à compléter) - Mise en Page - Conclusion
16/06/2023	0.5	Ajout du journal de stage
16/06/2023	1.1	Rapport complet

Sommaire

1 - Introduction

1.1 - Introduction en Français

Mon stage se déroule au sien de l'équipe cybersécurité de la DSI[2] de Ortec. C'est une petite équipe composée de Jean-Marc Roussel, le RSSI et de trois alternants, Clément Barcenilla, Orlando Ducamp et Tristan Leleu. Cette équipe s'occupe de la sécurité informatique au sein du groupe Ortec. Le Groupe Ortec, est une grande entreprise française dans les secteurs, de l'industrie, l'énergie, l'environnement, l'aéronautique, et le spatial. Elle est présente dans 28 pays, répartis sur 4 continents, et emploie plus 11 000 personnes. Son siège est situé à Aix-en-Provence, là où j'effectue mon stage.

La mission, qui m'a été confiée, est la sécurisation des ordinateurs qui sont utilisés lors de la pesée des camions à l'entrée, et la sortie des différentes agences d'Ortec. Ces ordinateurs peuvent être libres d'accès et parfois connectés au réseau de l'entreprise. Mon rôle était donc de faire en sorte que ces ordinateurs ne soient plus une porte ouverte vers le réseau du groupe.

1.2 - Introduction in English

The internship happened in cybersecurity team of DSI Ortec's. It is a small team composed of Jean-Marc Roussel the RSSI and three people who are in cooperative training course Clément Barcenilla, Orlando Ducamp and Tristan Leleu. The role of this is to take care of IT in Ortec. Ortec Group is a big French company in the sector of industry, energy, environment, aeronautics, spatial. The company is in twenty-eight countries, and she has more than 11000 employees. And headquarter is in Aix-en-Provence, it is here where I do my internship.

My mission is to secure some computers which are used to weigh trucks. Their computers are free access and sometimes connected to the network of the company. My goal is to secure their computers for those who are not an open door to the network.

[2] DSI : Direction des Système d'Information.

2 - Présentation d'Ortec

2.1 - Son histoire

Le groupe Ortec est une grande entreprise française créée en 1992 par André EINAUDI, qui est l'actuelle PDG[3] de Ortec Expansion qui détient toutes les filiales d'Ortec. André EINAUDI était dans un premier temps à la tête de la branche industrie du groupe Onet, qui au début du 20ème siècle souhaite se séparer de cette branche. Il rachète et crée Ortec en 1992.

En 1993, Ortec s'occupe des grands sites industriels français, comme l'usine de Grande Paroisse à Toulouse, où elle s'occupe de la dépollution, et de la gestion des déchets. L'année d'après, Ortec est chargé par le Centre d'Ingénierie du Parc Nucléaire, d'évacuer les couvercles de toutes les centrales nucléaires en France. Le système mis en place pour cette mission, par Ortec servira pendant les 10 ans après sa mise en place. Le groupe décide de lancer en 1995 les contrats "Usine propre", qui proposent à ces clients la délégation totale de la gestion des déchets issue de leurs industries.

1996, marque l'année où le siège social déménage de Vitrolles, à Aix-en-Provence. Mais surtout l'acquisition de Friedlander. Friedlander est une entreprise créée en 1936 en France, et devient rapidement le premier fournisseur de service pour les compagnies pétrochimique sur tout le continent africain. En 1978 Friedlander, travaille déjà avec plus de 60 entreprises en Afrique. Et quand elle rejoint le groupe Ortec en 1996, cela permet à Ortec d'augmenter considérablement sa capacité d'intervention, et de renforcer son réseau en dehors de l'hexagone.

À la veille du nouveau millénaire, Ortec est choisi par l'entreprise britannique BP pour assurer la gestion de maintenance, de sa raffinerie toutes activités confondues (montage, levages, mécanique, tuyauterie, déchets, nettoyage industriel électricité, génie civil, peinture, espace vert). Ce nouveau type de contrat, est aujourd'hui la principale offre que propose Ortec Services[4].

En 2000, Ortec lance O'Forum, une convention pour échanger sur les problématiques rencontrées, où est convié des entreprises présentes en France et clients du groupe. Cette convention est aujourd'hui un rendez-vous majeur pour les professionnels. En 2002 et 2003 Ortec se concentre sur la sécurité de leurs collaborateurs en créant une nouvelle filiale, Ortec Vigilance, et en créant des plans d'actions visant à garantir une meilleure sécurité pour ces collaborateurs.

En 2006 ValOrtec est créé, c'est le premier centre de traitement pour traiter les terres polluées, via la technique biopile[5]. Deux ans plus tard, le groupe lance "Casque d'Or", une récompense qui vise à valoriser les savoirs, des hommes et femmes qui travaillent au sein du groupe. Elle

[3] PDG : Président-Directeur Général.
[4] Ortec Services : filiales du groupe Ortec.
[5] Biopile : technique de dégradation des déchets à l'aide de bactéries.

lance l'année d'après, O'Metier un plan destiné à former les collaborateurs et à renforcer leur compétence.

Entre 2013 et 2017 Ortec, achète cinq entreprises dans plusieurs secteurs, Ducamp dans les domaines de l'environnement et la valorisation des déchets, Sonovision dans le secteur de l'aéronautique, Cico Centre et VDLS pour les secteurs des travaux industriels et nucléaires, et Brunet pour le domaine du génie électrique et thermique.

En 2018 Ortec, est présent sur 38 des 58 réacteurs français pour le programme d'installations des DUS[6], et finie tous ces chantiers avant la fin de l'année. La même année SOM[7], assure le raccordement d'un parc d'éoliennes offshore. De plus, Sonovision emploie plus de 450 personnes en Inde, et renforce donc sa part de marché dans la zone Asie-Pacifique. La même année, le bureau d'étude du groupe crée une nouvelle méthode de soudure des Tokamak[8] Iter. En même temps, Ortec est chargé de la maintenance du réseau hydraulique, et des bassins du Château de Versailles. De plus à quelques kilomètres du château, à l'ancien site industriel de Boulogne-Billancourt, Ortec s'occupe de l'opération METAL-57, et dépollue 78 000 mètres cube de terre polluée. L'année d'après Brunet, une des nombreuses filiales du groupe, à obtenue un contrat avec Nantes Métropole, pour s'occuper de tout son parc immobilier.

Ortec achète Soléo[9] est devient un des leaders du secteur en 2021. Un an plus tard, Ortec rachète les activités de Véolia Canada, et crée une nouvelle entité au Canada avec plus de 20 agences et plus de 550 personnes. En plus de cet achat au Canada Ortec, achète la société ATMNI.

Durant plus de 30 ans, Ortec, c'est agrandi et a élargi son offre de service dans divers secteurs, et pendant tout ce temps Ortec est resté détenue à 100 % par M. André Einaudi.

2.2 - Aujourd'hui

Aujourd'hui Ortec, c'est 1.2 milliard d'euro de chiffre d'affaires, 12 500 collaborateurs dans 249 agences, dont 62 à l'international reparti sur 24 pays sur 4 continents, l'Afrique, l'Amérique du Nord, l'Asie, l'Europe.

Grâce à ces nombreuses acquisitions Ortec Groupe est présent dans de nombreux secteurs, dont la pétrochimie, les énergies, les mines et l'industrie lourdes, l'automobile, le tertiaire, les collectivités et l'aménagement de territoire, le ferroviaire, le secteur pharmaceutique, la chimie, l'aéronautique et la défense, et le spatial. Grâce à toutes ces filiales, Ortec peut proposer un grand catalogue d'offre et de service dans chacun de ces domaines.

Aujourd'hui Ortec est conscient des problématiques sociales et environnementales, et met un point d'honneur sur l'environnement et la formation de ces collaborateurs pour leur permettre

[6] DUS : Diesels d'Ultime Secours.
[7] SOM : filiale spécialisée dans l'ingénierie dans les secteurs de l'énergie et des transports.
[8] Tokamak : est un dispositif de confinement magnétique expérimental explorant la physique des plasmas et les possibilités de produire de l'énergie par fusion nucléaire.
[9] Soléo : entreprise spécialisée dans l'étude des sols, la gestion des eaux pluviales et l'environnement.

d'évoluer et de valoriser leurs savoirs. Sur l'environnement, Ortec a pris en charge plus de 390 000 tonnes de déchet en France et à l'étranger. Elle valorise 68 % et 82 % des déchets qu'elle récupère dans leurs centres de traitement, respectivement en France et à l'international, de plus le groupe récence zéro déversement accidentel dans la nature. L'année dernière le 21 juin, Ortec lance la journée O'Climat, toutes les agences du groupe doivent proposer des animations autour du climat pour sensibiliser les collaborateurs. Sur le plan de la formation des collaborateurs, Ortec investit 5 % de la masse salariale à la formation. Ces 5 % forment 75 % des collaborateurs par an. Du côté de la sécurité de ces collaborateurs Ortec à réduit de 20 % les accidents de travail en trois ans et mettant en place des semaines de sensibilisation de la sécurité au travail. Ortec a mis en place des initiatives comme "Casque d'Or" qui met en avant les savoirs des collaborateurs.

2.3 - L'équipe

Le service dans lequel j'ai évolué est rattaché à Ortec Service. J'ai donc intégré l'équipe cybersécurité de la DSI. L'équipe est composée de quatre personnes, Jean-Marc Roussel, le RSSI, et de trois alternants comme dit plus tôt. La DSI est composée de trois grandes équipes, les Opérations qui s'occupent des achats, de l'architecture et infrastructure, l'équipe Études et Solutions qui s'occupe du support applicatif, le développement et l'architecture logicielle, et l'équipe Sécurité du Numérique.

Les missions de l'équipe sont sur 3 axes :

- Documentation : se documenter sur les politiques de sécurité du SI[10]. Mais aussi rédiger les plans de sensibilisation et les communiquer aux collaborateurs.
- Architecture & Veille : conseiller sur les solutions logicielles et le matériel en lien avec la sécurité du système d'information, valider les règles d'usage DMZ[11] et les architectures matérielles et logicielles dans le cadre de tous les projets liés aux nouvelles technologies. Assurer la veille technique et réglementaire. Rester à l'affût des failles et CVE[12] qui sortent, pour garantir un haut niveau de sécurité.
- Réalisation : analyser et cartographier des risques liés aux nouvelles technologies, réaliser des audits et piloter des plans de remédiations.

Les missions d'implémentation des systèmes ou de configuration sont effectuées par les équipes Opérations ou Solutions. L'équipe cybersécurité n'intervient pas sur les changements de configuration, elle analyse, définit, conseille, et vérifie.

L'équipe Sécurité numérique et qualité du SI travaille directement avec tous les collaborateurs, qui peuvent demander des conseils sur la sécurité du système d'information et qui sont sensibilisés par l'équipe sur le risque du SI.

[10] SI : Système d'Information.

[11] DMZ : zone démilitarisée, est un sous-réseau qui héberge les services exposés et accessibles de l'extérieur d'une entreprise.

[12] CVE : Common Vulnerabilities and Exposures ou Vulnérabilités et expositions communes.

3 - Travail réalisé

Avant de commencer mes tâches, j'ai dû prendre connaissance de la documentation d'Ortec. De plus j'ai pris connaissance du fonctionnement de la direction du système d'information et celui de l'équipe cybersécurité.

Cela m'a permis d'en savoir plus sur, comment fonctionne une entreprise, mais surtout comment l'équipe dans laquelle j'évolue. J'ai pu aussi voir, les différentes architectures réseau des agences Ortec qui sont reparties sur quatre continents. Mais aussi, ce qui est mis en place par Ortec, lorsque qu'il y a des informations sensibles qui sont dans le réseau d'une agence. J'ai pu aussi découvrir l'architecture des différents logiciels développés par Ortec comme leur ERP ou leur logiciel de gestion des déchets.

3.1 - Le mode Kiosque

La première partie de mon stage, est l'étude, et la mise en place de l'implémentation du mode kiosque sur les ponts-bascules. Un pont bascule, est une structure spécialement conçue pour peser des charges lourdes, telles que des véhicules ou des marchandises. Il est utilisé dans divers domaines, tels que la logistique, le transport, l'industrie.

Les étapes de ma mission ont été, de réaliser une analyse des risques, l'établissement des règles de sécurité GPO[13], la construction de la maquette, réaliser des tests avec les métiers, rédiger la documentation et le déployer en Agence.

Pour réaliser cette première étape, l'analyse des risques, j'ai utilisé le modèle AMDEC[14]. C'est la première fois que je rédigeais une analyse de risque. La principale difficulté à laquelle j'ai dû faire face, a été de bien définir le périmètre et à faire ressortir les différents risques. Puis, j'ai dû classer ces risques en 6 familles :

- Economique
- Environnementale
- Juridique
- Opérationnel
- Organisationnel
- Stratégique

Pour cela, j'ai dans un premier temps effectué quelques recherches sur les ponts-bascules, pour compléter celle que j'ai pu faire avant le début du stage. Une fois que je savais le

[13] GPO : Group Policy Object ou stratégie de groupe en français.
[14] AMEDEC : est une méthode d'analyse des modes de défaillances, de leurs effets et de leurs criticités.

fonctionnement d'un pont-bascule, j'ai commencé à rédiger une première liste de risques. J'ai ensuite échangé avec l'équipe, et la principale remarque que j'ai reçue, a été de regrouper les risques par type. Pour ce premier essai, j'ai eu tendance à lister trop de risques qui dans le fond étaient similaires, je me concentrais trop sur les détails.

Dans un second temps, j'ai eu une réunion avec les responsables métier. Cette réunion, m'a permis d'avoir plus d'informations sur le fonctionnement des ponts-bascules, et leurs potentielles failles. Les participants de cette réunion m'ont aussi donné des nouveaux documents, mais qui ne traitent pas des ponts-bascules mais des projets qui les utilisent, (comme le logiciel de gestion des déchets) et même si ces documents ne m'ont pas donné beaucoup d'information j'ai pu visualiser l'ensemble de la chaine d'utilisation métier.

Avec cette réunion et les retours, j'ai amélioré ma liste de risques. Cette liste était complète et j'ai supprimé les répétitions.

Puis, j'ai noté à chaque risque de 1 à 4 sur ces 3 critères, la gravité, la fréquence, et la détectabilité. Concernant la gravité, plus la note est grande, plus les conséquences du risque sont importantes. Par exemple, le risque d'une grosse cyber-attaque sera à 4. La fréquence, plus la note est élevée, plus la probabilité que le risque arrive est élevée. Un utilisateur qui oublie son mot de passe, et qui bloque son compte aura une note de 4, car cela peut arriver très souvent. La détectabilité, plus la note est haute plus il est difficile de détecter le risque. Une intrusion dans le système, qui est mal réalisée, et qui est automatiquement remontée par un logiciel de surveillance aura une note de 1.

Puis, en multipliant les notes de ces trois critères j'obtiens la note finale du risque, la criticité. Une criticité, peut aller de 1 à 64. Un risque avec une criticité de 1 à 8 est considéré comme minime, de 9 à 18 est un risque moyen, de 19 à 36 est un risque élevé et un risque critique est un risque de 37 à 64.

J'ai ensuite rédigé pour chaque risque un plan d'action, visant à réduire la criticité du risque. Le plan d'action doit réduire un ou plusieurs des trois critères. Cela va permettre de faire baisser la criticité.

Ensuite, j'ai renoté les risques après des plans d'action mise en place. Puis, on fait un graphique en radar, qui nous donne l'évolution pour chaque risque. Après cette étape, j'ai demandé un retour sur l'analyse de risque. J'ai eu comme remarque, que je devrais ajouter un scénario pour chaque risque pour décrire le risque, et dans quels principes de la triade CIA[15] le risque fait partie. Le but d'avoir décrit un scénario, est de montrer que le risque est concret aux personnes qui ne sont pas initié aux différents risques liés au SI.

La deuxième étape, est de rédiger les règles de sécurité. Pour cela, les documents, que j'ai lus au début de mon stage m'ont bien aidé. J'ai donc pris connaissance des normes de règles de sécurité et de conformité qui sont obligatoires et conseillées par la DSI d'Ortec.

[15] CIA : la triade CIA est model de cybersécurité qui aide à assurer la sécurité des données. Ces 3 principes sont la confidentialité, l'intégrité et la disponibilité (Confidentiality, Integrity, Availability en anglais).

Une fois les règles acquises, j'ai commencé à rédiger toutes les règles que je voulais mettre en place. Je les ai rédigées sous forme de texte pour les décrire, ensuite je les ai mises sous forme de tableau. Le texte me permet d'être plus précis sur l'ensemble des règles. Le tableau permet de voir plus rapidement les règles et la configuration que je veux mettre en place.

L'ensemble des règles obligatoires chez Ortec a été inclus, comme la stratégie sur le mot de passe, ou la mise en veille. De nouvelles règles ont été inclues sur les protocoles utilisés comme le 802.1x qui permet de restreindre les connexions des appareils inconnus au réseau. Ou encore bloquer l'accès au périphérique de stockage, comme des clés USB, pour éviter l'injection de code malveillant.

Après cela, j'ai pu commencer une autre étape importante de ma mission, la création de la maquette, c'est aussi l'étape ou j'ai eu le plus de difficulté.

Pour réaliser la maquette, j'ai dû créer mon environnement de test. J'ai créé une machine virtuelle, qui est mon Windows Serveur qui hébergera le serveur Active Directory[16] et une machine virtuelle, qui est la machine qui hébergera le mode kiosque. Le serveur Active Directory est utilisé par Ortec pour administrer tous les utilisateurs et les machines qui sont dans le réseau de l'entreprise. Cela permet principalement de gérer les droits et les configurations des objets (ordinateurs et utilisateurs) qui sont dans le réseau.

Avant la création du serveur Active directory, il faut configurer les machines que l'on va utiliser. Il faut donc modifier les paramètres réseau. Il faut passer le serveur du DHCP[17] à une IP[18] statique[19], pour cela il faut aller dans les paramètres. De plus il faut faire de même avec l'ordinateur que l'on veut enrôler dans le serveur. Sur l'ordinateur, il ne faut pas oublier de spécifier l'adresse du serveur en tant que DNS[20]. J'ai été bloqué un petit moment, car je ne savais pas qu'il fallait changer les configurations des cartes réseau des machines.

La création du serveur Active Directory et d'un domaine n'était pas compliquée. Il suffit de suivre la documentation disponible gratuitement sur Internet. Il faut avoir Windows Serveur comme système d'exploitation. Il faut commencer par installer un ADDS[21], ajouter le rôle (ADDS) à notre serveur. Puis le serveur installe l'ADDS et redémarre. Une fois installé, je dois promouvoir le serveur en Contrôleur de domaine. C'est le grade le plus haut dans l'Active Directory celui qui permet de tout contrôler. Puis j'ajoute une forêt. Une forêt représente une organisation dans l'Active Directory. Je donne un nom de domaine à cette forêt, pour mes tests

[16] Active Directory : ou AD est un service développé par Microsoft de gestion des utilisateurs et des ordinateurs d'un réseau.

[17] DHCP : Dynamic Host Configuration Protocol est un protocole qui attribue une adresse IP automatiquement.

[18] IP : Internet Protocol adresse est une suite de chiffres attribuée à chaque appareil connecté à un réseau informatique ou à Internet.

[19] IP statique : une machine garde sont IP définie par l'utilisateur.

[20] DNS : Domain Name System est un service qui associe un nom de domaine à une adresse IP.

[21] ADDS : Active Directory Domain Services est utiliser pour l'implémentation d'un domaine Active Directory.

je l'ai nommé MONAD et j'ai mis l'extension .local, pour préciser que le serveur est bien en local. Puis après avoir définie un mot de passe pour l'Active Directory, le serveur redémarre et après le serveur active Directory sera installé.

Maintenant, il faut modifier le mot de passe du compte administrateur. Pour ce faire il faut aller dans un outil qui se nomme "Utilisateur et ordinateur Active Directory". Cet outil va nous permettre de gérer toutes les machines, et compte qui sont sur l'Active Directory. Dans cet outil, on ouvre le dossier "Users" puis, on clique sur le compte qui se nomme Administrateur, et on modifie son mot de passe.

Puis, pour associer l'ordinateur au serveur, il faut aller dans ses paramètres et plus précisément dans les propriétés du système. Ensuite spécifier le nom du domaine que l'on vient de créer. Cette fois-ci, on redémarre l'ordinateur, et le tour est joué, l'ordinateur a rejoint le serveur Active Directory.

Maintenant, mon plan est de créer des GPO pour répondre à mes besoins, et d'utiliser Intune[22] pour mettre en place le mode kiosque. Mais Intune ne peut pas s'utiliser en local, car celui-ci utilise le cloud. Ortec n'ayant pas d'espace de test dans Intune, j'ai donc cherché un autre moyen de réaliser le mode kiosque. La solution que j'ai trouvée est de le faire à l'aide des GPO, cela est plus complexe car il faut configurer une par une toutes les règles que l'on souhaite pour copier le mode kiosque de Windows.

Durant cette étape j'ai eu la chance d'aller voir au site de ValOrtec Rognac, le fonctionnement d'un pont-bascule. Cela était très intéressant, mais cette visite nous a permis de voir que la mise en place du mode kiosque est impossible, sur les ordinateurs utiliser pour les ponts-bascules. Ces ordinateurs ne sont pas en libre-service mais utilisés par les collaborateurs toute la journée pour réaliser leurs missions. Je continue quand même mon projet car cette visite, nous avons pu constater que les ordinateurs qui ne sont pas dans le réseau d'Ortec et qui étaient utilisés pour une seule tache (gestion et affichage des caméras de vidéosurveillance). Il est donc nécessaire de les sécuriser par la mise en place de ma configuration. Ma tâche reste identique, il y a juste l'utilisation finale qui a été modifié, mais cela ne m'impacte pas.

Avant de créer les GPO, j'ai utilisé l'outil utilisateur et ordinateur Active Directory pour créer un utilisateur qui servira à la connexion automatique. J'ai aussi créé un groupe, dans lequel j'ai mis l'ordinateur et l'utilisateur que je viens de créer pour pouvoir lier mes GPO au groupe et pas à tous les objets (ordinateur et utilisateur) qui sont dans le serveur Active Directory.

[22] Intune : selon Microsoft Intune est : Intune est une solution de gestion des points de terminaison basée sur le cloud. Il gère l'accès utilisateur et simplifie la gestion des applications et des appareils sur vos nombreux appareils, notamment les appareils mobiles, les ordinateurs de bureau et les points de terminaison virtuels.

Pour créer les GPO, on utilise l'outil "Gestion des stratégies de groupe", qui est un outil qui permet de créer, modifier, supprimer et lié des GPO. J'ai donc faire une GPO qui regroupe toutes les règles pour commencer et par la suite une fois que je suis satisfait de la configuration, je sépare celle qui concerne l'utilisateur et celle qui concerne l'ordinateur.

Donc, dans un premier temps, j'ai voulu faire en premier la connexion automatique. Après quelques recherches sur Internet, j'ai trouvé quels sont les paramètres à configurer. Ces paramètres modifient Winlogon[23] qui est un composant Windows qui gère l'ouverture et la fermeture des sessions. En spécifiant les identifiants de l'utilisateur que je viens de créer et en précisant le nom du domaine, cela va modifier des variables dans Winlogon pour activer la connexion automatique. Pour que ce paramètre soit activé il faut redémarrer deux fois l'ordinateur. Une première fois, pour que les variables soient modifiées et une seconde fois pour que la connexion automatique soit effectuée.

La deuxième règle que je voulais mettre en place est l'installation automatique d'un logiciel. Pour ce faire j'ai aussi effectué des recherches sur Internet. Au bout de quelques minutes de recherche j'ai trouvé ce qu'il fallait faire pour configurer cette règle. Dans un premier temps j'ai pris sur le fichier .msi d'un logiciel, pour mes tests j'ai choisi Google Chrome. Le format MSI[24] est le seul format accepté par la règle. Puis j'ai déplacé le fichier .msi dans un dossier partagé.

Pour créer un dossier partagé dans le serveur Active Directory, il faut suivre quelques étapes. Il faut activer le partage dans les propriétés du dossier. Puis il faut lui donner un nom, moi j'ai décidé de cacher tous les dossiers partagés que je vais créer, donc à la fin de chaque nom je rajoute un caractère '$'. Puis, on doit gérer les droits pour tous les dossiers, je vais donner seulement un droit de lecture aux utilisateurs qui ne sont pas « administrateur » (on ne donne pas les droits un par un aux utilisateurs même si on peut le faire, on utilise les groupes qui sont déjà configurés dans le serveur Active Directory), et je vais donner tous les droits à mon compte administrateur.

Donc, revenons sur notre règle. Après avoir déplacé le fichier servant à l'installation dans un dossier partagé, il suffit d'indiquer le chemin vers ce dernier. Attention, quand on utilise un dossier partagé on ne doit pas utiliser celui qui commence par "C: ", car celui-ci correspond au disque dur local. Il faut utiliser celui commençant par "\\" , ce pattern permet d'accéder au partage sur le réseau.

[23] Winlogon : est un composant de Windows qui s'occupe de l'ouverture et la fermeture de session.

[24] MSI : Microsoft Système Installer est un format pour installer des logiciels dans des environnements Microsoft.

La règle suivante, que j'ai mise en place, est le lancement automatique de Google Chrome, l'application que j'ai décidé d'utiliser dans la règle précédente. Pour ce faire, même procédé, je vais chercher toutes les informations dont j'ai besoin sur Internet. Au bout d'une dizaine de minutes de recherche je trouve toutes les informations qu'il me faut.

Mais avant de configurer la règle, je dois faire un script Batch[25]. Pour ce faire rien de compliqué, je dois juste trouver la commande qui permet de lancer un logiciel. Je me dis simplement quelle serait le nom de commande le plus logique, donc j'essaie avec « start » et ça marche je vais juste faire une petite recherche pour trouver comment lancer le logiciel en plein écran. Cela s'effectue en rejoutant « /max » à la commande.

Donc, maintenant que j'ai mon petit script, je crée un nouveau dossier partagé, et je le déplace à l'intérieur. Je configure la règle qui permet d'exécuter des scripts au démarrage, je pense que celle-ci est bien configurée, mais elle ne l'est pas. Il y a deux règles qui se ressemblent avec une seule différence, le moment de l'exécution du script. Je venais de configurer la règle qui lance le script lorsque que mon ordinateur venait de s'allumer et qu'il n'y avait pas de session utilisateur lancée. Donc cela ne marchait pas, j'ai donc configuré la règle qui lance le script une fois la session utilisateur lancée.

Maintenant, je souhaitais que l'utilisateur soit bloqué, qu'il ne puisse plus rien faire, qu'interagir avec l'application que j'avais choisie. Pour ce faire, j'ai dû rechercher une seule règle qui faisait ça, mais cela n'existe pas. J'ai donc dû chercher un ensemble de règles pour faire ce que je voulais. Cela a été très long, car je n'ai pas trouvé de documentation qui répertorie toutes les règles. J'ai donc cherché pour chaque élément, la règle qui lui correspond puis comment la configurer. Les éléments principaux sur lesquels je voulais agir étaient :

- Supprimer tous les éléments du bureau et bloquer celui-ci
- Désactiver les notifications
- Supprimer la barre des taches
- Supprimer le menu Démarrer
- Supprimer l'accès au paramètre de l'ordinateur
- Supprimer l'accès au paramètre de l'utilisateur
- Supprimer l'accès à tous les fichiers

Pour ce faire, j'ai dû activer plus d'une vingtaine de règles différentes. J'ai aussi dû créer un dossier partagé pour stocker une mise en page, personnaliser du menu démarrer. La mise en page est faite avec un fichier .xml[26].

Comme je viens de le dire c'était très long, car il fallait effectuer des recherches pour chaque élément pour trouver quelles sont les règles à configurer. De plus, certaines règles ne marchaient pas pour diverses raisons. Cela était la partie la plus frustrante pour moi car je

[25] Batch : langage utilisé pour exécuter des commander Windows. L'extension des fichiers est .bat.
[26] XML : Extensible Markup Language est un langage de balisage. L'extension est .xml.

n'arrivais pas à avancer comme je le voulais. Une étape que je pensais être simple, m'a finalement pris beaucoup de temps.

Une fois cette étape finie, j'avais une maquette qui correspondait à ce que je voulais. C'est-à-dire, lorsque l'on démarre l'ordinateur on est automatiquement connecté au compte que j'ai créé. Puis, le ou les logiciels qui sont définis se lancent. L'utilisateur est bloqué, il ne peut rien faire d'autres que ce que j'ai prévu. Mais la configuration n'était pas optimisée. J'ai donc séparé la configuration en deux, une qui va concerner l'utilisateur et une autre qui va concerner l'ordinateur. De plus cette séparation va permettre de pouvoir plus facilement administrer l'ordinateur et / ou la configuration.

Dans la configuration de l'ordinateur, j'ai mis la connexion automatique, le téléchargement du ou des logiciels. Cela va permettre d'être sûr que sur tous les ordinateurs le ou les logiciels présents sur l'ordinateur, et aussi d'être sûr qu'il se connecte automatiquement sur le compte que j'ai créé.

Dans la configuration de l'utilisateur, il y a toutes les règles qui bloquent les actions de l'utilisateur. Cette GPO sera active seulement sur l'utilisateur que j'ai créé et cela va permettre de pouvoir se connecter avec un compte administrateur sur l'ordinateur pour l'administrer.

Lors de cette séparation des règles, il y a eu des problèmes qui sont apparus. Les configurations ne fonctionnaient plus normalement.

Pour pallier cet incident, j'ai simplement recréé une nouvelle GPO qui reprend les mêmes règles. Cette action a parfaitement joué son rôle, j'avais donc dû commettre une erreur en séparant la configuration de base.

Une fois la maquette finie, je l'ai présentée à mon tuteur pour qu'il la valide, ce qu'il a fait. Ensuite, j'ai entamé la rédaction de la documentation.

Afin d'accomplir cette tâche, j'ai utilisé un modèle fourni par Ortec pour les documents. J'y ai décrit l'objectif de la configuration, expliqué mon choix de séparer la configuration en deux parties. Puis j'ai listé des règles de chaque partie, tout en expliquant qu'elle est le rôle de la règle qui est configuré et comment la configurer.

Ce document a été conçu dans un souci de clarté et de concision, en utilisant un langage accessible et en fournissant des captures d'écran illustratives pour faciliter la compréhension. J'ai rédigé chaque règle pour qu'elle soit expliquée le mieux possible, afin de permettre aux administrateurs système d'implémenter et d'administrer la configuration de manière la plus efficace possible.

Après la validation de mon tuteur, on a organisé une réunion avec d'autres services de la DSI pour voir la faisabilité de ma configuration.

Durant cette réunion j'ai fait une démonstration des configurations. On a pu voir qu'il y avait des éléments de la configuration à modifier avant de déployer la configuration en agence.

J'ai donc fait les modifications nécessaires. Dans un premier temps je les ai testées sur la maquette. Puis j'ai modifié le document que j'avais rédigé.

Désormais la DSI doit intégrer les GPO et créer les groupes correspondants dans l'AD de production Ortec, ainsi la configuration sera opérationnelle et pourra être testée sur l'agence Valortec Rognac, en conditions réelles.

Malheureusement, je n'ai pas pu déployer ma configuration en agence par manque de temps.

3.2 - Autres missions

3.2.1 - Recherche sur le cloud

Mon tuteur m'a donné la mission d'effectuer des recherches sur quels sont les critères de sécurité pour le cloud[27] pour qu'Ortec puisse se mettre aux normes.

Lorsque j'ai eu cette mission, on m'a transmis le nom de deux organismes qui travaillent sur le cloud. Le CSA pour Cloud Security Alliance et le BSI pour Bundesamt für Sicherheit in der Informationstechnik. Le CSA est une organisation américaine à but non-lucratif qui est spécialiste dans la sécurité du cloud. Le BSI est l'agence gouvernementale allemande de la sécurité des technologies de l'informatique, c'est l'équivalent de ANSSI[28] en France.

Le CSA à un document qui se nomme Cloud Contrôle Matrix (CCM), est une matrice[29] de plus de 250 points répartis en plusieurs groupes. Chaque point décrit un élément de la sécurité du cloud. Le BSI a publié le C5, un document qui comme le CCM est une matrice d'environ 75 points qui concernent la sécurité du cloud. Ces deux documents sont utilisés comme référence en Europe pour le BSI, et à l'internationale pour le CCM. En plus de ces deux documents, j'ai trouvé un document de l'ANSSI sur le cloud qui ne nomme SecNumCloud qui décrit quelques règles de sécurité pour le cloud. Puis j'ai rédigé un document qui décrit ces trois documents.

Une fois cela effectué, j'ai fait le lien entre ces documents et une grille de sécurité rédigée par un client majeur d'Ortec, une grande société d'aéronautique. C'était une tache très longue, car

[27] Cloud : ou l'informatique en nuage, est un mode de stockage qui consiste à utiliser des serveurs à distance pour stocker, gérer et traite des données au lieu de le faire d'un serveur local.

[28] ANSSI : Agence National de la Sécurité des Système d'Information est l'agence gouvernementale française qui s'occupe comme son nom l'indique de la sécurité des SI.

[29] Une matrice : est un document sous forme de point qui permet d'évaluer ce pourquoi elle est faite.

pour chaque point qu'il y avait dans la grille, je devais trouver quels étaient les points des autres documents qui ont servi de référence.

Ainsi pour chaque point, la DSI Ortec peut vérifier si elle est conforme aux exigences de son client, selon la situation actuelle de ses installations dans le cloud. Certaines configurations devront être améliorées pour être conformes.

3.2.2 - Travail sur les normes

Au début de mon stage, j'ai participé à des réunions pour le framework NIST[30]. Le but de ce framework, est de permettre aux entreprises de s'évaluer en matière de cybersécurité. Il y avait des réunions toutes les semaines pour évaluer Ortec, et je suis arrivé à l'avant-dernière réunion dessus. Une fois les réunions finies, je me suis occupé de résumer la matrice sous forme de tableau pour que cela soit plus lisible. Cela m'a permis de voir quelles sont les normes en termes de cybersécurité aujourd'hui.

Puis on a refait ce même travail, d'auto-évaluation, mais avec la norme ISO 27002:2022. Le but de refaire ce travail est de pouvoir répondre au besoin des clients, qui souhait en fonction de leur localisation (le NIST pour le continent américain et l'ISO pour l'europe) ou juste par préférence, un organisme plutôt qu'un autre.

Pour chaque point de la norme, on a donné le point équivalent du framework du NIST. Ensuite, on m'a mis une note, sur ce qui ait mis en place par Ortec par rapport à ce point. Et pour finir, on donne des preuves pour garantir que le point est bien respecté.

Ce travail sert la DSI, pour savoir quelle sont les axes d'amélioration, mais aussi au client pour qu'ils peuvent voir ce qui est mise en place par Ortec au niveau de la sécurité.

3.2.3 - Recherche sur un DLP[31]

J'ai également effectué des recherches sur un moyen d'éviter la fuite des fichiers sensibles. Chez Ortec, de nombreux fichiers sensibles, comme des bases de données de mots de passe, sont stockés dans des dossiers partagés et personne ne peut savoir si un fichier à fuité. C'est pour répondre à cette problématique, que je suis allé chercher une solution pour tracer les activités effectuées sur ces fichiers.

Sur mon réseau de machines virtuelles, que j'avais créé pour ma mission sur la configuration "mode kiosque", j'ai installé un des gestionnaires de mot de passe qui est utilisé par Ortec. Puis

[30] NIST : National Institute of Standards and Technology est une agence américaine qui a pour développer les technologies, la métrologie et l'industrie. Pour ce faire le NIST publie des normes pour aider les entreprises à se développer.

[31] DLP : Data Loss Provention est un ensemble de techniques qui permettent d'identifier, de contrôler et de protéger les informations.

sur le serveur, j'ai créé un dossier partagé pour y stocker ma base de données qui contient des mots de passe.

Ma première idée a été d'utiliser le gestionnaire de log[32] qui est intégré au gestionnaire de serveur Windows. Pour ce faire, j'ai dû activer crée une GPO et activer une règle qui permet d'activer la récolte des logs. Puis je suis allé sur le gestionnaire de log qui se nomme "Observateur d'événements" puis je suis allé dans le dossier où sont stockés tous les logs de Windows. Chaque événement a un numéro unique qui lui est attribué, par exemple le fait d'ouvrir un fichier aura le numéro 4663, quel que soit le fichier ouvert. J'ai donc cherché à trier ces numéros pour garder seulement ce qui est lié à une éventuelle fuite de donnée. Mais cela n'a pas été fructifiant, après des heures de recherche, j'ai appris que Windows ne stockent pas les logs liés au transfert de fichier.

Je dois donc trouver une autre solution.

Je me mets à chercher des logiciels qui permettent de voir la fuite de donnée, un DLP.

Ma première piste, est un logiciel, open-source[33], français sur GitHub[34]. Malheureusement, il n'avait pas de documentation. J'essaie donc de faire fonctionner le logiciel mais je n'arrive pas à faire ce que je veux. En fouillant la page GitHub, je trouve un serveur discord que je rejoins. J'explique ma situation, et pose mes questions dans un salon. Le créateur du logiciel me répond, nous échangeons rapidement, puis me dit que son logiciel ne peut pas faire ce type de tache.

Je me remets à chercher des logiciels. J'en trouve un autre, qui n'est pas open-source. Il y a une version d'essai, que j'implémente sur le serveur (qui est une machine virtuelle). Mais je dois avoir un serveur SQL[35], j'implémente donc sur mon serveur un serveur SQL, qui me permet de finir de configurer le logiciel. Une fois la configuration terminée, je regarde si on peut récupérer toutes les actions réaliser sur un fichier (copier, modifier, lecture, déplacer, etc). Mais je n'ai pas réussi à avoir ce que je voulais.

Je continue mes recherches et je trouve un autre logiciel. Celui-ci est facile à implémenter et à utiliser, car il y a une bonne documentation. Ce logiciel permet de créer des filtres pour n'avoir que les logs qui nous intéressent et envoi un mail périodiquement avec un rapport.

Celui-ci fait exactement ce dont j'ai besoin. Je rédige donc un document, dans lequel j'explique à quoi ce logiciel servirait et comment l'utiliser. Comme tous les documents que j'ai réalisés chez Ortec j'illustre un maximum, je fais en sorte d'être le plus compréhensible possible.

Si la solution que j'ai trouvée est implémentée, cela va permettre de protéger les données qui sont dans des serveurs de fichier. On pourrait savoir si une personne sort des fichiers, mais aussi bloquer cette fuite de donnée.

[32] Log : est une trace générée automatiquement d'un événement qui a eu lieu dans le système.
[33] Open-source : libre de droit.
[34] GitHub : est un site qui permet au développeur de stocker, gérer plus facilement leurs projets.
[35] SQL : Structured Query Language ou langage de requête structurée est un langage utilisé en informatique pour exploiter des bases de données relationnelles.

4 - Bilans

4.1 - Bilan de l'expérience professionnelle en entreprise

Pour faire le bilan, de cette première expérience professionnelle dans le monde du travail.

D'un point de vue organisationnel, déjà je ne pensais pas que l'équipe chargée de la cybersécurité d'une grande entreprise comme Ortec, soit composée de 4 personnes et quasiment exclusivement d'alternants. De plus même, si nous avons eu un programme sur la communication, je ne pensais pas que celle-ci est si complexe.

D'un point de vue technique, je me suis pris une claque par l'écart de niveau qu'il y a entre en les alternants et moi. Je ne pense pas être un élève avec un niveau mauvais, mais cela m'a donné l'envie de m'améliorer pour réduire cet écart qui me semble plutôt important.

En termes de compétences, j'ai pu travailler avec l'Active Directory, et par conséquent avoir des compétences dans ce domaine. J'ai évolué au sien de l'équipe ce qui m'a permis aussi de suivre leurs différentes tâches durant mon stage et donc je ne dirais pas que j'ai pris des connaissances, mais des notions de cybersécurité que je pourrais faire évoluer en compétence dans le futur.

Pour ce qui ai de mon travail réalisé, je suis mitigé. D'un côté, je suis content du travail que j'ai réalisé, mais d'un autre, je me dis qu'il y a des difficultés que j'aurais pu éviter. Je pense que je ne suis pas assez méticuleux dans mon travail, et cela me pose des problèmes, car je commets des erreurs qui pourraient être évitées.

Pour ce qui est d'un point de vue humain, je suis content d'avoir fait partie de cette équipe. Clément, Orlando et Tristan ont toujours été là quand j'en avais besoin. Jean-Marc Roussel, mon tuteur lui aussi était présent pour moi lorsque j'en avais besoin malgré ses responsabilités de RSSI. J'ai bien été intégré à l'équipe.

Pour conclure, ce premier contact avec le monde du travail a été très positif, cela m'a permis de monter en compétences, mais surtout de voir les axes d'amélioration sur lesquels je dois travailler.

4.2 - Bilan de la formation

Si je devais résumer ma formation BUT informatique je suis satisfait mais il y a des points sur lesquels il faudrait effectuer des changements.

Les premiers cours que nous avons eu en BUT, étaient de la communication, et de l'économie durable et numérique. Je n'ai pas de soucis sur le fait qu'il y ait des matières plus génériques mais le souci c'est qu'elles soient utilisées pour faire nos SAE, je ne vois pas l'utilité et la plus-value que cela nous apporte d'organiser un événement ou de connaître les mesures environnementales mises en place par des communes.

Durant la seconde année, il y a des couacs logistiques aux niveaux des matières. On nous demande d'utiliser des technologies pour les SAE sans y avoir était introduit, et ce n'est qu'une fois le projet fini, qu'on nous introduit la technologie.

Concernant le parcours Déploiement d'application communicante et sécurisée, les enseignants nous ont décrit ce parcours comme étant un parcours orienté cybersécurité, réseaux. Mais de mon point de vue le module cybersécurité est bien trop court. Je pense qu'il devrait être plus approfondi, pour pouvoir appréhender tous les aspects de la cybersécurité. On pourrait prendre du temps sur des matières plus génériques ou sur des matières orientées développement.

Si je devais résumer les compétences que j'ai acquises et leur utilité. Je suis mitigé quant à leur profondeur. J'ai acquis des compétences, mais nous n'avons pas approfondi suffisamment le sujet, pour quelles soit réellement utiles dans le monde professionnel. Je pense qu'il devrait y avoir une véritable distinction entre les différents parcours, car actuellement, les personnes du parcours B sont impliquées dans divers domaines. Ce qui est bien, mais cela signifie que nous ne pouvons pas aller en profondeur dans les domaines de notre parcours. Je trouve cela dommage, dans des domaines comme la cybersécurité et le réseau ou il y tellement de chose à apprendre et découvrir. Puis faire des groupes aléatoires, pour nous apprendre à travailler avec des gens que nous n'avons pas choisis, pour faire comme en entreprise n'est pas une bonne chose, de mon point de vue. Les élèves ne travaillent pas comme des employés. Je pense que ces groupes ont freiné l'apprentissage et impacté la qualité du rendu. Cela nous oblige à faire les taches des membres du groupe qui ne sont pas à l'aise avec les technologies utilisées pendant la SAE ou que simplement les taches qu'ils n'ont pas réalisées. Avec la charge de travail d'une SAE, on ne peut pas prendre trop de temps à expliquer, et accompagner une personne pour la faire monter en compétence.

De mon côté pour mon stage je n'ai pas eu l'impression que les compétences que j'ai acquises m'ont réellement servi car j'ai fait quelque chose que je n'ai pas eu l'impression d'avoir vu durant ma formation.

4.3 - Conclusion

Ce stage m'a permis de découvrir le monde du travail et le secteur de la cybersécurité.

Durant ce stage, j'ai pu apprendre comment on gère un projet dans une entreprise comme Ortec. Cela m'a permis de monter en compétences, de découvrir les domaines sur lesquelles je dois m'améliorer, mais surtout d'en apprendre plus sur moi-même, de savoir quelle sont mes défauts et mes qualités. Je suis un peu déçu de ne pas avoir pu implémenter ma configuration en agence, mais je suis content d'avoir réussi à faire un truc pas trop mal alors que je partais sans connaître la technologie.

J'ai intégré et évolué au sein de l'équipe cybersécurité et appris son fonctionnement.

De plus, j'ai pu travailler sur divers sujets, comme le cloud. Toutes mes missions et toutes celles que mes collègues on effectuer, m'ont permis de voir une grande partie de ce qui ait possible de faire dans une équipe cybersécurité dans un groupe comme Ortec.

Pour ce qui est de mon projet professionnel. À court terme, je suis à la recherche une entreprise pour une alternance pour la rentrée prochaine. J'aimerai intégrer une alternance durant laquelle je peux voir plusieurs aspects de l'informatique donc du développement au réseau en passant par les bases de données. Cela me permettrait donc découvrir des aspects que je n'aurais pas appréhendé durant mon stage de fin d'année et donc m'aider pour mes choix futurs. Ou sinon une alternance dans le domaine de la cybersécurité pour continuer sur la lancée du stage que je viens de réaliser ou dans un autre secteur comme le développement applicatif ou la gestion de bases de données, car ces sont des secteurs que j'aimerai bien approfondir.

Pour le moyen terme, j'aimerai poursuivre mes études en continuant l'alternance. Les domaines cités plus haut m'attirent, je m'orienterai vers eux. Pourquoi pas continuer mes études à l'étranger car je pense que cela pourrait être une bonne expérience personnelle, culturelle, et professionnelle.

Quant à long terme, mon futur scolaire et professionnel est encore bien trop flou pour avoir une idée. J'aimerai fortement travailler dans des secteurs que j'apprécie comme l'automobile, l'aéronautique, le spatial et la défense, car je ne veux pas faire un travail "alimentaire", mais effectuer un travail qui me passionne. Je ne veux pas être esclave de mon travail, mais prendre du plaisir chaque jour, car comme le dit un proverbe chinois "Choisissez un travail que vous aimez et vous n'aurez pas à travailler un seul jour de votre vie".

5 - Journal de Stage

17 avril / 21 avril - Semaine 1 - L'installation

Cette première semaine a marqué pour moi les premiers contacts avec le monde professionnel, ainsi que la découverte de l'environnement dans lequel je vais évoluer tout au long de mon stage chez Ortec.

Les objectifs de la semaine étaient pour moi : découvrir et m'installer dans cet environnement qui est nouveau pour moi. Mais aussi commencer la mission qui m'est confiée.

Le premier jour a été assez spécial, puisque j'ai intégré une équipe qui était en train de changer de bureau. J'ai naturellement suivi l'équipe dans ce déménagement, ce qui m'a permis de découvrir les locaux d'Ortec. Une fois le déménagement terminé, j'ai pu prendre possession de mon poste de travail.

Les premiers jours ont été consacrés à la prise de connaissance du fonctionnement de la DSI et des différentes procédures mises en place par l'équipe cybersécurité qui est compose de 4 personnes 3 alternants et le RSSI mon tuteur. J'ai également commencé à travailler sur le projet qui m'a été confié : la sécurisation des ordinateurs utilisés pour les ponts bascule. Ces grosses balances sont utilisées pour peser les camions qui entrent et sortent des sites. Mon rôle est donc de mettre en place des mesures qui serviront à sécuriser ces ordinateurs. J'ai ainsi appris à faire une analyse de risque et à en effectuer une sur les ordinateurs.

Je n'ai pas rencontré de difficulté particulière durant cette semaine, car je n'ai pas eu de tâche réelle à effectuer. Si je devais en citer une, je dirais que cela a été de trouver les bons coefficients pour chaque risque, car j'ai eu tendance à les sous-estimer.

Pour la semaine prochaine, j'aimerais améliorer mon analyse de risque en prenant en compte les nouveaux risques que je vais découvrir dans le métier. J'espère également commencer à élaborer une première maquette de ce que je vais devoir mettre en place.

Cette première semaine a été l'occasion de découvrir l'équipe et le milieu dans lequel je vais travailler, mais également de commencer à apprendre comment fonctionne une grande entreprise comme Ortec

24 avril / 28 avril - Semaine 2 – Le commencement

Durant cette semaine dans l'équipe cybersécurité du groupe Ortec j'ai continué la mission qui m'a été confiée.

Mes objectifs de la semaine ont été de rencontrer les responsables métiers d'Ortec pour compléter mon analyse de risque et de rédiger les règles de sécurité, GPO (Group Policy Object ou stratégie de groupe en français)

Cette semaine a été un peu longue. J'ai dans un premier temps dû organiser une réunion avec les responsables métier pour qu'il m'explique ce que c'est un pont-bascule et comment il fonctionne chez Ortec parce que jusqu'ici les seules connaissances que j'avais étaient celles que j'ai pu trouver sur l'intranet et sur les documents que j'ai trouvés dans l'intranet du groupe. Souvent ces documents ne traitent pas des ponts bascule et donc il fallait essayer de réunir les petites informations qui se trouvait dans tous les documents pour avoir une réelle information utile. À la fin de cette réunion je n'avais pas à toutes les réponses à mes questions. On a donc décidé de prévoir d'aller voir sur le terrain le fonctionnement des ponts-bascules et on profitera de cette sortie pour faire un audit sur toute l'agence pour trouver des failles de sécurité.

Durant la semaine j'ai commencé et fini la rédaction des règles de sécurité qui seront sur l'ordinateur. Pour cela j'ai dû trouver quelle sont les normes de conformité et de sécurité d'Ortec afin que la configuration de l'ordinateur respect les règles déjà mises en place. J'ai dû ajouter les règles de sécurité que j'ai jugées utiles et nécessaires dans le cadre de la mise en place du mode kiosque.

Durant ces deux premières semaines j'ai pu voir des petits problèmes de communication d'Ortec à cause de la grande taille du groupe. Les informations se transmettent lentement et que des informations du message "ne sont pas prises en compte ou oubliées". Par exemple la semaine dernière durant le déménagement, l'équipe cybersécurité avait besoin d'avoir des prises Rj45 pour pouvoir travailler et on nous a mis dans une salle sans prise. Donc pour résoudre ses soucis ils sont en train d'installer des prises dans lieux où je suis.

Je n'ai pas pu commencer la maquette car je n'avais pas un compte avec des droits suffisants je devrais les avoir la semaine prochaine.

Pour résumer la semaine en quelques mot, je dirais que la semaine a été longue mais que dans un projet il n'y a pas que les moments où on doit réaliser la tâche mais aussi une grande partie de gestion de projets où on doit rédiger des documents pour une partie montrée que la mission est justifiée et documenté cette dernière pour qu'elle puisse être reprise par d'autres dans le futur.

2 mai / 5 mai - Semaine 3 - Les Difficultés

Durant cette semaine, j'ai eu mes premières grosses difficultés.

Durant cette semaine, j'ai commencé à faire une maquette. J'ai donc créé un Active Directory dans lequel il y a une machine sur laquelle il y aura le mode kiosque de configurer.

Un Active Directory ou AD est un service de gestion des utilisateurs et des machines qui sont sur un réseau. Avec un Active Directory, les administrateurs peuvent facilement donner et restreindre les droits des utilisateurs. Cela est souvent utilisé pour gérer de grands groupes tout en garantissant la sécurité du réseau.

J'ai utilisé VMware pour créer mon écosystème. J'ai commencé par créer un serveur Windows qui hébergera mon serveur AD (on va l'appeler S-01). Puis j'ai une autre machine virtuelle (M-01) qui sera celle qui recevra la configuration que je fais faire.

Créer et configurer le serveur Windows n'est pas très compliqué. Il y a beaucoup de documentation non-officielle qui nous guide dans la configuration. Mais le principal défi a été d'associer l'autre machine sur le domaine que j'ai créé. Dans un premier temps, la VM était reliée sur le domaine d'Ortec et pas le mien. Il fallait donc le retirer du domaine, mais cela n'était pas aussi simple que prévu. J'ai donc tout simplement créé une nouvelle machine (M-02) sans connexion. Et une fois la machine lancée, activer la connexion et faire rejoindre mon domaine.

Mais je n'étais pas sortie d'affaire, car il fallait modifier la configuration de la carte réseau de M-02 en lui mettant un IP fixe en changer l'adresse IP du DNS et en ajoutant S-01 dans la liste des hôtes de confiance de M-02 et inversement.

Une fois que M-02 a rejoint l'active directory, il a fallu créer la GPO. Les GPO sont les stratégies de groupe qui sont des fonctions de gestion des utilisateurs et des machines. La difficulté pour moi a été de trouver les bonnes fonctions à activer et à configurer. Et de lier les GPO aux ordinateurs et aux utilisateurs. Là aussi, il y a une grande difficulté pour trouver les bonnes stratégies, car je n'ai pas trouvé de documentation qui les décrivent, et aussi de lier les GPO aux objets (ordinateurs et utilisateurs) qui sont dans l'AD.

Ces difficultés m'ont permis pour une fois depuis le début du stage de sortir de ma zone de confort. Pour la semaine prochaine, j'espère réussir à finir ce qu'est commencé cette semaine.

9 mai / 12 mai - Semaine 4 - De nouvelles choses

Au cours de cette semaine, j'ai pu faire de nouvelles choses en parallèle de ma mission principale.

J'ai commencé la semaine avec une nouvelle tâche, Ortec stocke toutes ses données et application en On-Premise et souhaite commencer à utiliser le cloud. Je dois donc voir quelles sont les normes qu'Ortec doit mettre en place. J'ai donc recherché quelle sont les organismes qui sont spécialisés dans la sécurité du cloud. J'ai trouvé des documents de l'ANSSI1, du BSI2 et du CSA3. Les plus intéressants sont ceux de l'ANSSI et du CSA, l'ANSSI car Ortec est une entreprise française qui travaille avec des acteurs français dans des secteur sensibles comme la défense ou le nucléaire par exemple, et donc l'ANSSI est la référence en France. Et aussi les recommandations du CSA qui est spécialisé dans le domaine et qui a une portée plus internationale et qui propose des certifications reconnues. Pour ce qui ait du BSI, je n'ai pas gardé leurs recommandations, car même s'ils ont de bonnes recommandations, celles-ci sont déjà dans le CSA et dans l'ANSSI, et Ortec ne travaille pas avec le gouvernement allemand donc il n'y a pas besoin de s'y plier. Cette mission m'a accompagné toute la semaine.

Mercredi, j'ai pu assister à une réunion avec EDF. Cette réunion avait pour but de faire une revue du PAS4. La réunion a été très intéressante parce que j'ai pu voir ce que demande et comment travaille un grand groupe comme EDF en matière de sécurité. Les choses que j'ai retenues c'est qu'EDF est un groupe qui fait très attention aux conséquences que peux avoir une cyber-attaque et qu'aujourd'hui le fait de travailler avec EDF expose Ortec et les autres collaborateurs à des attaques par des groupes étatiques. Et avoir les procédures est vital dans l'informatique, on ne peut pas se permettre de ne pas les suivre ou de ne pas en avoir pour des choses qui touchent à la sécurité ou aux données.

Jeudi, j'ai pu visiter un site ValOrtec et donc voir sur place le fonctionnement des ponts-bascules. C'était intéressant d'aller voir directement sur place comment le fonctionnement. Mais malheureusement, on ne peut pas implémenter un mode kiosque, car cela compliquerait trop le métier des gens sur place. Mais je continue à travailler dessus, car on a vu sur place un moyen de l'implémenter.

Et pour finir la semaine, j'ai essayé de reprendre la création de la maquette, mais sans succès.

Pour la semaine prochaine, je veux finir mes recherches sur le cloud, mais surtout finir la maquette je sais que je peux le faire donc je pense que lundi, je vais repartir de zéro.

15 mai / 19 mai - Semaine 5 - La maquette

Durant cette semaine, je me suis focalisé sur la création de la maquette.

Lundi, avant de commencer la maquette, j'ai fini mes recherches cloud et j'ai rédigé un document pour pouvoir résumer ce que j'ai trouvé et ce que je recommande à Ortec pour son cloud. Cela m'a pris de voir quelles sont les grands acteurs en matière de cloud, quelles sont les certifications qui sont intéressantes à passer pour une organisation et pour une personne a passer pour garantir la sécurité d'un cloud.

Puis je voulais finir la maquette, j'ai donc tout recommencé à zéro. J'ai recréé un serveur Active Directory ou AD. Je l'ai configuré, j'ai passé son IP en une IP statique. Puis j'ai recréé une machine, que je lui aie donnée une IP statique, je l'ai fait rejoindre le serveur AD. Puis sur le serveur, j'ai créé un contrôler de domaine, j'ai fait rejoindre la machine à ce domaine. J'ai créé un utilisateur dans le domaine. À cette étape tout-va bien, j'avance à une bonne allure.

Je commence par créer la GPO1 de la configuration de l'ordinateur. Je fais en sorte que dès qu'on allume l'ordinateur, l'utilisateur est automatiquement connecté. Je recrée un dossier partagé sur le réseau qui va contenir tout ce dont l'ordinateur a besoin. Cela étant, je mets dans le dossier l'installer d'une application (ici chrome) pour qu'elle soit de base installée dans la machine. Et je crée la GPO pour exécuter le .msi de Chrome s'il n'est pas déjà installé. Puis je teste si tout marche bien. Et tout fonctionne, la connexion automatique marche et chrome est bien installé s'il est absent sur la machine.

Je passe donc à la GPO de la configuration de l'utilisateur. Je fais en sort que chrome se lance au démarrage de la session. Puis il faut bloquer toutes les actions de l'utilisateur, c'est là que cela se complique, car je ne peux pas utiliser Intune, car Ortec n'a pas de serveur de test. Intune est un outil de Microsoft qui sert à gérer la configuration des ordinateurs. Je cherche donc toutes les règles à activer et à configurer pour faire un mode kiosque fait maison (qui n'est pas le mode officiel de Windows). Et là il n'y a pas tout qui marche du premier coup, je dois faire beaucoup de retours en arrière ce qui franchement m'agace sur le moment, car j'ai l'impression de reculer dès que j'arrive à trouver une piste pour avancer. Vendredi matin plus rien ne fonctionne comme je le veux, mais je continue à essai d'avancer et vendredi après-midi, j'arrive à tout faire fonctionner. Je n'ai pas eu le temps de faire de vrais tests, la journée était finie, mais je les ferai lundi matin.

La semaine prochaine, j'accompagnerai l'équipe lors d'un audit d'une agence et donc je ferai les tests de ma maquette est espérant que tout fonctionne bien comme prévu.

22 mai / 26 mai - Semaine 6 - Avancées tranquilles

Cette semaine a été plutôt tranquille, j'ai fini la maquette et les tests et j'ai reçu des retours sur mon travail sur le cloud.

Donc, dans un premier temps, j'ai fini la rédaction des GPO de la maquette. Il manquait des règles qui étaient mal configurées. Puis j'ai fait des tests à la main si les actions de l'utilisateur sont bien restreintes a ceux que je voulais. Je n'ai pas trouvé un moyen de faire les tests automatiquement, un peu comme ceux qu'on peut faire en développement.

Puis j'ai reçu des retours sur mes recherches sur le cloud. On m'a demandé de regarder quelle sont les règles utiliser par notre client pour la sécurité de son cloud en plus des organismes que j'avais déjà fait. C'est un travail plutôt long, mais cela me permet de voir quel est le contenu des normes que j'avais relevé plus tôt.

Au début de mon stage avec mes collègues, on a fini d'appliquer la matrice du NIST sur la cybersécurité. La matrice est un document présenté sous forme de points répartis par thème, et pour chaque point on doit mettre une note par rapport si on est conforme à ce qui est dit dans le point. Cette semaine, j'ai résumé le niveau de chaque thème de la matrice. Cette tache m'a permis de voir l'ensemble des points qui sont dans la matrice, car je n'étais présent que sur la fin de cette évaluation.

Puis j'ai commencé la rédaction de la documentation de la configuration que j'ai créée. La maquette a été validée par mon tuteur, j'ai donc commencé la rédaction de documentation. Dans celle-ci, j'explique quel est le but de la configuration et je liste les règles que j'ai configurées et quelle est leurs rôles. J'ai également mis en annexe un exemple de script Batch pour lancer un logiciel, mais aussi le modèle de fichier XML pour la mise en page du menu démarrer.

Cette semaine a été plutôt calme, j'ai pu avancer tranquillement sur mes taches sans grande difficulté. La semaine prochaine, je pense que je vais relire la documentation que j'ai rédigée puis continuer mon travail sur le cloud.

29 mai / 2 juin - Semaine 7 - Documentation et Incident Perturbateur

Durant cette semaine, j'ai fini la documentation de ma configuration.

Durant cette semaine, j'ai fini la documentation de la configuration que j'avais finie la semaine dernière. Je suis reparti de zéro car je n'aime pas la façon dont j'avais commencé la documentation. Elle était trop dispersée, mal organisée et mal rédigée, le modèle de documentation n'était pas celui qui était le plus adapté. Donc cela rendait bizarrement, et j'avais du mal à écrire la suite de la doc.

Je suis donc reparti d'un modèle qui me semble plus adapté, ce mode m'a facilité la mise en page et l'organisation du document. Dans ce document, j'explique mes différents choix, comme celui de séparer la configuration en deux, je liste et je justifie les différentes règles que j'ai activées et comment les configurer. Et bien sûr, j'essaie d'être le plus clair possible. Sur ce point, Clément l'un de mes collègues me conseille d'ajouter des images au maximum pour illustrer ce que je dis. Bien sûr, je l'écoute et je rajoute des captures d'écran pour aider les personnes qui vont lire ou refaire la configuration.

Dans la nuit du mardi au mercredi, dans le datacenter de Jaguar Network (un hébergeur), il y a eu une surchauffe dans l'une des salles. La température de la salle est montée jusqu'à plus de 70 degrés Celsius (petit rappel une salle serveur doit être vers les 20 °C).

Mais quel est le rapport avec mon stage, et bien, je vais vous le dire. Mercredi matin, une grande partie des services utilisés par Ortec ne fonctionnaient plus. Parmi ces services, on peut citer la boite mail mais aussi le logiciel pour les réunions etc. Et donc c'était un peu la panique, vu que plus personne ne pouvait travailler. On nous avait dit que les services allaient revenir en début d'après-midi, mais malheureusement avec ces grandes chaleurs dans la salle, certains équipements n'ont pas tenu le coup et sont tombés hors service. Alors je n'ai pas participé aux réunions de gestion de l'incident, mais Tristan un de mes collègues lui y a participer. Et c'était intéressant de suivre de manière partielle la gestion d'un incident qui touche la DSI, et qui a d'aussi grandes conséquences.

J'ai aussi reçu de nouvelle tâche de j'ai commencé vendredi, donc je vais vraiment m'y mettre la semaine prochaine. Cette tache concerne les logs sur les fichiers qui contiennent des mots de passe.

5 juin / 9 juin - Semaine 8 - Les Logs

Durant cette semaine je me suis concentré sur la nouvelle mission.

Ma mission consiste à trouver des solutions pour prévenir la fuite de fichiers sensibles chez Ortec. Les fichiers sensibles, tels que les bases de données de mots de passe, sont stockées dans des dossiers partagés sans qu'il ne soit possible de détecter les fuites. Ainsi, on m'a confié la tâche de trouver une solution permettant de surveiller les activités effectuées sur ces fichiers.

Dans un premier temps, j'ai utilisé mon réseau de machines virtuelles. J'ai installé un des gestionnaires de mots de passe utilisé par Ortec, et j'ai établi un dossier partagé sur le serveur pour y stocker la base de données des mots de passe.

Pour commencer, j'ai exploré l'utilisation du gestionnaire de logs intégré au gestionnaire de serveur Windows. J'ai configuré une GPO (Objet de stratégie de groupe) pour activer la collecte des logs, puis j'ai consulté l'"Observateur d'événements" où les logs de Windows sont enregistrés. Chaque événement est identifié par un numéro unique, par exemple le numéro 4663 correspond à l'ouverture d'un fichier, quelle que soit sa nature. J'ai tenté de filtrer ces numéros afin de ne conserver que ceux liés à d'éventuelles fuites de données, mais malheureusement cette approche n'a pas fonctionné. Après des recherches approfondies, j'ai découvert que Windows ne stocke pas les logs relatifs au transfert de fichiers.

J'ai donc effectué des recherches et j'ai trouvé un logiciel, qui s'est avéré simple à mettre en place et à utiliser grâce à sa documentation complète. Ce logiciel permet de créer des filtres afin de sélectionner les logs qui nous intéressent et envoie régulièrement des rapports par e-mail.

Ce logiciel répond parfaitement à mes besoins. J'ai rédigé une preuve de concept (POC) décrivant son utilité et les instructions pour son utilisation. Tout comme pour tous les documents que j'ai produits chez Ortec, j'ai inclus un maximum d'illustrations afin d'assurer une compréhension claire.

De plus j'ai bien avancé mon rapport de stage.

12 juin / 16 juin - Semaine 9 - La fin

Durant cette semaine, avec l'équipe on a eu une nouvelle mission.

Mais dans un premier temps, j'ai réalisé des tests supplémentaires sur le logiciel que j'ai découvert la semaine dernière. J'ai effectué des essais afin d'évaluer les différentes fonctionnalités.

En parallèle, j'ai également poursuivi la rédaction du document entamé précédemment. J'ai veillé à fournir des informations claires et concises.

Maintenant, abordons la mission principale qui nous a été assignée : réaliser un travail d'auto-évaluation. Notre objectif est d'évaluer les lacunes et les points forts du système de sécurité en nous appuyant sur la norme ISO 27002:2022. Cette norme internationale fournit un cadre solide et reconnu mondialement pour évaluer et améliorer la sécurité de l'information dans les organisations.

Dans le cadre de cette évaluation, nous avons établi une correspondance entre chaque point de la norme ISO et les recommandations du framework du NIST. Pour chaque point de la norme, par nous avons évalué et noté les mesures mises en place Ortec. Cette évaluation comprend non seulement les politiques et les procédures documentées, mais aussi la mise en œuvre concrète de ces mesures dans notre environnement opérationnel.

Pour garantir l'objectivité de notre évaluation, nous avons recueilli des preuves tangibles pour chaque point évalué. En fournissant ces preuves, nous démontrons notre engagement envers la conformité aux normes de sécurité et nous apportons une assurance supplémentaire à nos clients quant à la fiabilité de nos pratiques de sécurité.

Ce travail d'auto-évaluation a une double finalité. D'une part, il sert la DSI pour savoir ce qu'elle doit améliorer. D'autre part, elle sert pour garantir un bon niveau de sécurité au client.