



Rapport de stage technicien

STAGE REALISE DANS L'ENTREPRISE SII DU 24 JUIN AU
30 AOUT 2019



Encadreur professionnel :

Monsieur **Sylvain GAUDEL** | Responsable
informatique local

Etudiant :

Franck-Olivier Cyrille NGOUNOU |
Dominante **ASR** (Architecture et
Sécurité des Réseaux)

REMERCIEMENTS

Avant d'entamer tout développement sur cette expérience professionnelle, il me semble opportun de remercier tous ceux qui de près ou de loin ont contribué à la réussite de mon stage et m'ont aidé dans l'élaboration de ce rapport.

Je tiens tout d'abord à remercier le groupe **SII** (Société pour l'informatique industrielle) et le directeur de son agence Rhône-Alpes, madame Marilyn **MONTON**, qui ont cru en moi et m'ont donné l'opportunité d'effectuer ce stage de 9 semaines au sein de leurs locaux.

Mes remerciements vont également à l'endroit de mon encadreur professionnel monsieur Sylvain **GAUDEL** pour son accompagnement et sa disponibilité pour répondre à mes différentes questions.

Je n'oublie pas de remercier les autres membres du service IT, Justin **LAJARTIER** et Emmanuel **SABUGUEIRO** pour les savoir-faire qu'ils m'ont communiqués et aussi pour la bonne ambiance qu'ils entretenaient au sein du service.

Je remercie enfin l'**ESIGELEC** pour la mise en place d'un stage technicien dans la formation de ses étudiants.

Que tous ceux qui ont contribué à mener à bien ce stage trouvent ici l'expression de ma parfaite considération.

SOMMAIRE

REMERCIEMENTS	II
SOMMAIRE.....	1
INTRODUCTION	2
PRESENTATION DE L'ENTREPRISE	3
Historique.....	3
Métiers et solutions.....	4
Secteurs d'activité et clients	6
Déroulement du STAGE	7
Journée d'intégration	7
Cadre de travail	7
Missions	8
Traitement des alertes de vulnérabilité.....	8
Durcissement du système d'exploitation Ubuntu version 18.04.....	11
Réalisation d'une bannière d'information de connexion	12
Mise à jour de la matrice de Flux	13
Déploiement APT-MIRROR pour UBUNTU 18.04	14
Difficultés rencontrées et solutions	15
BILAN	16
CONCLUSION.....	17
LISTE DE FIGURES	18
ANNEXE	19
SITOGRAFIE.....	22
GLOSSAIRE.....	23

INTRODUCTION

Espionnage, vol de données sensibles, fraude, sabotage, malveillance.... Le nombre de cyberattaques est de plus en plus important au fil des années. Ceci s'explique par l'apparition de nouvelles technologies telles que le Cloud, l'IoT, l'intelligence artificielle, qui rendent les systèmes d'information plus ouverts qu'auparavant. Face à cette recrudescence des menaces informatiques, il est important et même vital de se protéger efficacement.

C'est pour répondre à ces enjeux qu'a été rédigée et publiée en octobre 2005 la **norme ISO/CEI 27001** qui définit les exigences pour la mise en place d'un système de management du système d'information, celui-ci étant en charge de recenser les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs de l'organisme. L'objectif est de protéger les fonctions et informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique.

Le groupe SII soucieux de la **protection de ses données et de celles de ses clients** s'est donnée comme projet de faire passer la certification sus-citée à son agence de Rhône-Alpes au premier semestre 2020. Ceci nécessite un travail préalable qui consiste en l'application de règles telles que la réalisation régulière d'audits de sécurité, la mise en place de procédures de sécurité physique et l'évaluation et la gestion des risques menaçant l'entreprise.

C'est cette dernière tâche qui, du 24 Juin au 30 Août 2019, a meublé mon temps au sein du service IT.

En vue de retranscrire fidèlement cette expérience de 9 semaines chez SII, il sera question en amont de présenter l'entreprise, son secteur d'activité, puis suivront les différentes tâches effectuées durant le stage, les difficultés rencontrées, les solutions apportées et in fine un bilan technique et humain sera dressé.

PRESENTATION DE L'ENTREPRISE

HISTORIQUE

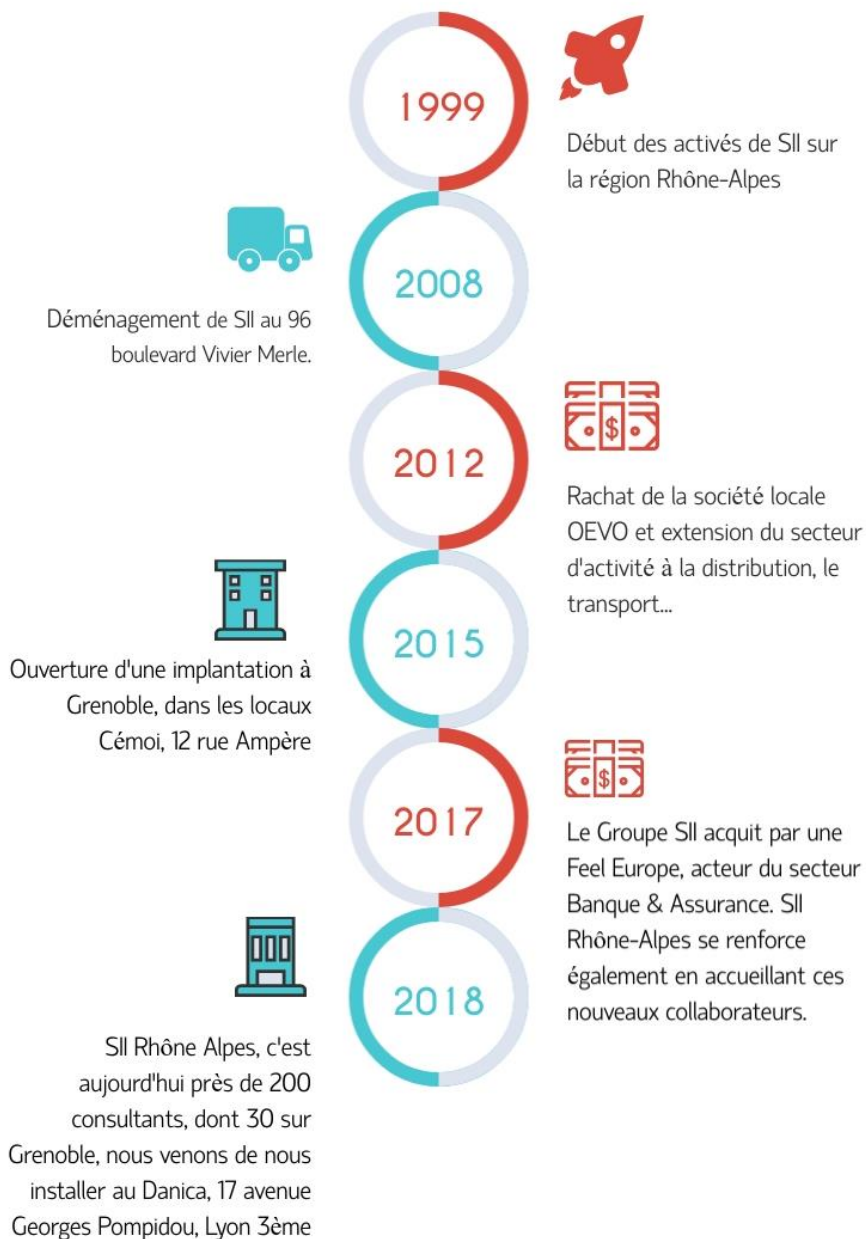


Figure 1 : Historique de l'entreprise

METIERS ET SOLUTIONS

Le Groupe SII est une société de conseil en technologies dans 18 pays au travers de 66 implantations. 7000 ingénieurs interviennent quotidiennement sur les problématiques de transformation numérique des grands-comptes. Fort de plus de 30 ans d'expertise dans le conseil en technologies et l'intégration de systèmes, le groupe SII possède l'ensemble des compétences nécessaires à l'accompagnement de ses clients dans leurs besoins d'évolution technologique. La société propose ainsi différents types d'interventions pour couvrir l'intégralité du cycle d'un projet :

- Le conseil et les études en amont
- L'ingénierie de développement
- Les tests, le déploiement et la maintenance

Dans les métiers suivants :

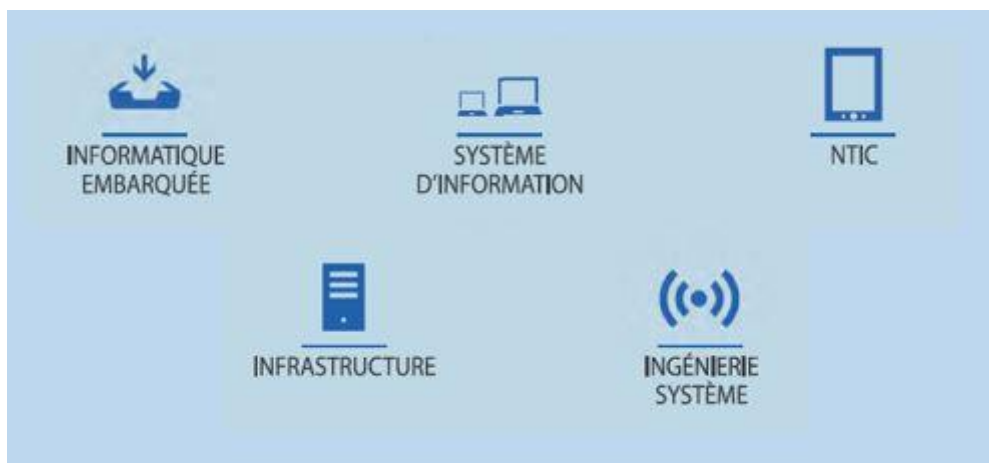


Figure 2 : Métiers traités par SII

✓ Informatique embarquée :

Logiciel embarqué et temps réel, applicatifs de traitement de données scientifiques, bancs de test, logiciel de contrôle commande, électronique, télécommunications, logiciel de supervision : SII propose des solutions innovantes sur l'ensemble de ces domaines. Des bureaux d'études à la conception jusqu'au maintien en condition opérationnelle des produits et systèmes mis en œuvre, notre intervention se fonde sur une méthodologie projet éprouvée.

✓ Systèmes d'information :

Dans ce domaine, SII élabore des solutions à forte valeur ajoutée pour permettre à ses clients d'optimiser leurs performances et de soutenir leur stratégie métier. Parmi ces solutions nous avons :

- Développement d'application
- Informatique décisionnelle
- Informatique financière
- ERP (Enterprise Resource Planning)
- Sécurité des systèmes d'information

✓ **NTIC :**

SII est depuis plusieurs années un acteur reconnu du secteur des nouvelles technologies de l'information et de la communication. Son offre se décline en prestations de haute technicité :

- Convergence IP ;
- Web ;
- Mobilité ;
- Infrastructures.

✓ **Infrastructures :**

SII, intervient dans les domaines de l'architecture réseau, de la sécurité, du stockage, des bases de données, de l'hébergement et des télécoms. L'offre proposée se décline en trois types d'interventions :

- Expertise, évaluation et conseil ;
- Ingénierie et mise en œuvre de solutions de sécurité ;
- Infogérance des systèmes de sécurité et des systèmes critiques ;

✓ **Ingénierie systèmes :**

L'offre en ingénierie système de SII s'adresse aux clients issus des secteurs aéronautique, spatial, naval, nucléaire mais aussi des industries de pointe. Cette activité répond à un besoin de collecte et de traitement de données scientifiques et/ou techniques.

Dans ce cadre, le groupe assure le développement de systèmes temps réel ainsi que de logiciels embarqués et de supervision.

SECTEURS D'ACTIVITE ET CLIENTS

SII réalise son chiffre d'affaires sur des segments de marché très diversifiés :



Figure 3 : Secteurs d'activité couverts par SII

Et fournit ses services à de nombreux grands comptes :



Figure 4 : Liste des clients du groupe SII

DEROULEMENT DU STAGE

JOURNEE D'INTEGRATION

Mon arrivée chez SII a eu lieu le 24 Juin 2019 et j'ai eu droit ce jour à la traditionnelle journée d'intégration organisée par l'agence. En effet elle est organisée chaque mois à l'agence et a pour but d'accompagner les nouveaux collaborateurs lors de leur arrivée en reprenant différents points :

- Présentation de l'organisation et de la vie de salarié SII ;
- Formation aux outils internes comme l'extranet et la qualité ;
- Présentation de l'IT et paramétrage des accès ;
- Sensibilisation sécurité.

Tous ces éléments sont articulés autour de moments de partage et de convivialité.

CADRE DE TRAVAIL

Lors de mon stage, j'ai intégré le service IT (Information and Technology) au sein duquel j'occupais le poste d'Administrateur système et sécurité. Le service est constitué de 3 personnes :

- Monsieur Sylvain GAUDEL : Responsable informatique local
- Monsieur Justin LAJARTIER : Administrateur système et réseau
- Monsieur Emmanuel SABUGUEIRO : Technicien informatique

C'est sous la responsabilité de Sylvain GAUDEL que j'ai effectué mes missions tout au long de mon séjour dans l'entreprise.

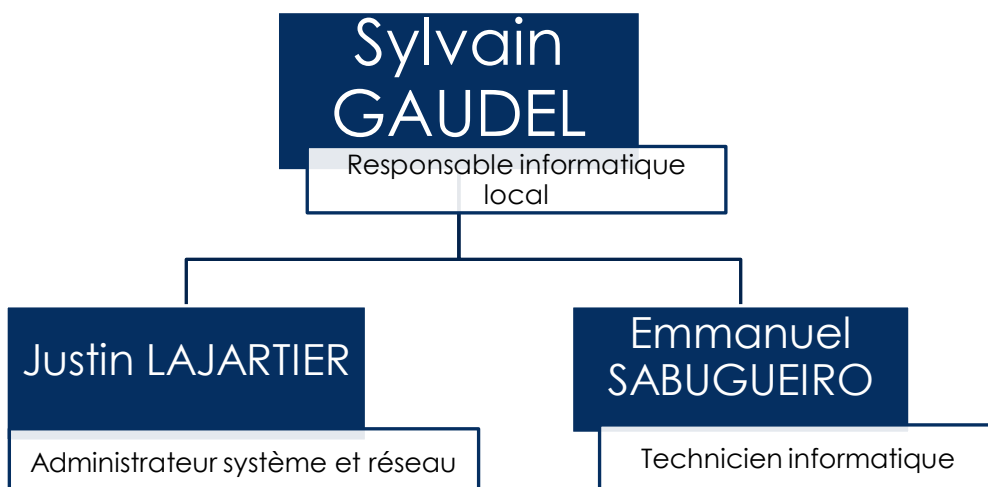


Figure 5 : Organisation du service IT

MISSIONS

Ma mission principale consistait à traiter les alertes de vulnérabilités remontées au travers d'un abonnement aux services de XMCO ainsi que les tickets ouverts par le **SOC** (Security Operation Center) en cas de suspicion d'attaque détectée par le **SIEM** (Security Information and Event Management). Ceci était fait dans le but de se conformer à la réglementation **ISO 27001** qui préconise la gestion des vulnérabilités qui pèsent sur le système d'information de l'entreprise.

D'autres tâches ponctuelles m'ont été assignées, celles-ci seront développées de manière chronologique dans la suite de ce document.

TRAITEMENT DES ALERTES DE VULNERABILITE

Cette tâche représentait mon activité principale tout au long de mon stage. Dès mon deuxième jour de stage il m'a été présenté les différents outils et logiciels dont j'aurais besoin pour la réalisation de mon travail :

- **GLPI** (Gestion libre de parc informatique) : Il s'agit d'un logiciel qui permet de faire un inventaire de tout le parc informatique de l'entreprise. Y sont consignés tous les ordinateurs, téléphones portables présent dans l'organisation ainsi que les logiciels qui y sont installés.

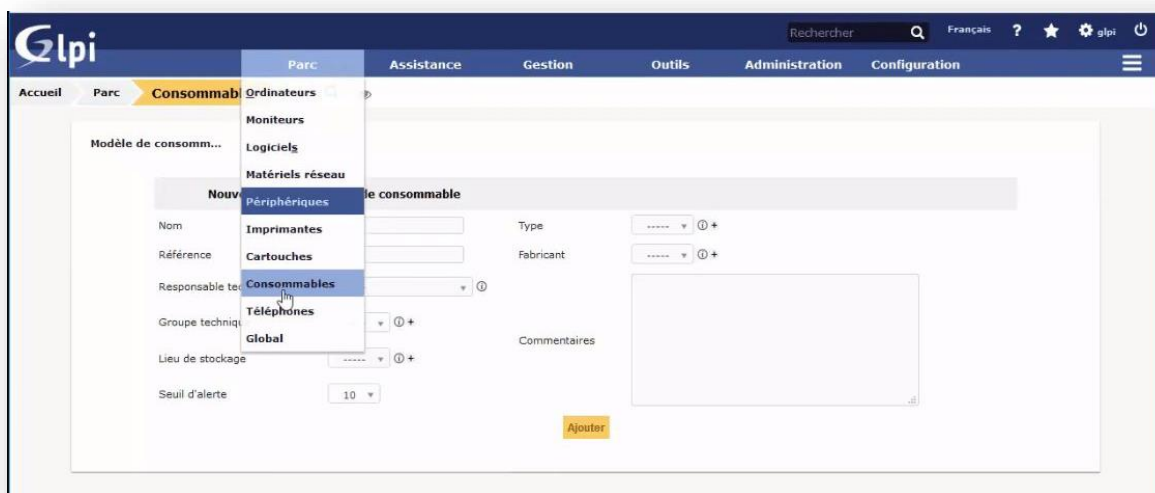


Figure 6 : Interface du logiciel GLPI

- **GIS** : c'est l'outil de Gestion des Incidents de Sécurité dont l'interface s'appuie sur GLPI.

ID	Titre	Statut	Date d'ouverture	Impact	Demandeur	Attribué à	Catégorie	Dernière modification
4 694	[EXTERNAL] [PATCH][GOOGLE] Manipulation de données et divulgation d'informations via une vulnérabilité au sein de Google Chrome Criticité : Moyenne	En cours (attribué)	27-08-2019 14:57	Moyen	Mail2 GIS		Vulnérabilité	29-08-2019 09:38
4 646	[EXTERNAL] [PATCH][MOZILLA] Contournement de sécurité et divulgation d'informations via une vulnérabilité au sein de Firefox et Firefox ESR (mfsa2019-24) Criticité : Moyenne	En cours (attribué)	19-08-2019 16:38	Moyen	Mail2 GIS		Vulnérabilité	28-08-2019 16:16
4 288	[EXTERNAL] [PATCH][WINSCP] Prise de contrôle du système et divulgation d'informations via 3 vulnérabilités au sein de WinSCP Criticité : Moyenne	En cours (attribué)	24-07-2019 16:23	Moyen	Mail2 GIS		Vulnérabilité	28-08-2019 14:50
4 693	[EXTERNAL] [PATCH][APPLE] Prise de contrôle du système via une vulnérabilité au sein d'Apple iOS (HT210549) Criticité : Élevée	En cours (attribué)	27-08-2019 14:57	Haut	Mail2 GIS		Vulnérabilité	27-08-2019 16:18
3 297	[VULN][MICROSOFT] Prise de contrôle du système via une vulnérabilité dans Microsoft Windows Criticité : Élevée	En cours (attribué)	12-04-2019 10:22	Haut	Mail2 GIS		Vulnérabilité	26-08-2019 17:03
4 645	[EXTERNAL] [PATCH][APACHE] Manipulation de données et divulgation d'informations via 6 vulnérabilités au sein d'Apache Criticité : Moyenne	En cours (attribué)	19-08-2019 16:38	Moyen	Mail2 GIS		Vulnérabilité	19-08-2019 16:38
4 619	[EXTERNAL] [VULN][MICROSOFT] Élévation de privilèges et manipulation de données via une vulnérabilité au sein de Windows 10 Criticité : Moyenne	En cours (attribué)	16-08-2019 17:33	Moyen	Mail2 GIS		Vulnérabilité	16-08-2019 17:33
4 584	[EXTERNAL] [PATCH][MICROSOFT] Prise de contrôle du système et élévation de privilèges via 65 vulnérabilités au sein de Windows 10 (2019-Aug) Criticité : Élevée	Nouveau	16-08-2019 09:18	Haut	Mail2 GIS		Vulnérabilité	16-08-2019 15:57
4 460	[EXTERNAL] [PATCH][GLPI-PROJECT] Manipulation de données et divulgation d'informations via 2 vulnérabilités au sein de GLPI Criticité : Moyenne	En cours (attribué)	06-08-2019 22:05	Moyen	Mail2 GIS		Vulnérabilité	16-08-2019 15:00
4 587	[EXTERNAL] [PATCH][MICROSOFT] Prise de contrôle du système et contournement de sécurité via 10 vulnérabilités au sein de Microsoft Edge (2019-Aug) Criticité : Moyenne	En cours (attribué)	16-08-2019 09:18	Moyen	Mail2 GIS		Vulnérabilité	16-08-2019 14:53
4 586	[EXTERNAL] [PATCH][UBUNTU] Linux kernel (Xenial HWE), Linux kernel, PHP, MariaDB, Linux kernel (AWS) Criticité : Moyenne	En cours (attribué)	16-08-2019 09:18	Moyen	Mail2 GIS		Vulnérabilité	16-08-2019 14:51
4 588	[EXTERNAL] [PATCH][MICROSOFT] Prise de contrôle du système et élévation de privilèges via 49 vulnérabilités au sein de Windows Server 2016 (2019-Aug) Criticité : Élevée	En cours (attribué)	16-08-2019 09:19	Haut	Mail2 GIS		Vulnérabilité	16-08-2019 14:11
3 169	Veille incomplète sur les vulnérabilités logicielles	En cours (attribué)	10-04-2019 17:46	Haut	LERONDEAU Julien	SABUQUERO Emmanuel	Non respect d'une directive sécurité	12-08-2019 14:41
2 600	Perte de clé du local de Grenoble	En cours (attribué)	06-02-2019 10:28	Moyen	LERONDEAU Julien	SAUVAGEAU Romain	Vol / Perte de matériel	12-08-2019 14:35

Figure 7 : Interface du GIS

ID	Titre
4 694	[EXTERNAL] [PATCH][GOOGLE] Manipulation de données et divulgation d'informations via une vulnérabilité au sein de Google Chrome Criticité : Moyenne
4 646	[EXTERNAL] [PATCH][MOZILLA] Contournement de sécurité et divulgation d'informations via une vulnérabilité au sein de Firefox et Firefox ESR (mfsa2019-24) Criticité : Moyenne
4 288	[EXTERNAL] [PATCH][WINSCP] Prise de contrôle du système et divulgation d'informations via 3 vulnérabilités au sein de WinSCP Criticité : Moyenne
4 693	[EXTERNAL] [PATCH][APPLE] Prise de contrôle du système via une vulnérabilité au sein d'Apple iOS (HT210549) Criticité : Élevée
3 297	[VULN][MICROSOFT] Prise de contrôle du système via une vulnérabilité dans Microsoft Windows Criticité : Élevée

Figure 8 : Extrait de la liste des alertes de vulnérabilité

Il était en effet question pour moi de consulter chacun de ces tickets, de vérifier quels sont les logiciels ou système d'exploitation concernés et leurs versions, et d'ensuite aller vérifier dans l'inventaire GLPI si ces différentes entités sont présentes dans le parc informatique de l'entreprise.

Ticket# 1115 description

[PATCH][JENKINS] Contournement de sécurité via une vulnérabilité au sein de plugins Jenkins

* [PATCH][JENKINS] Contournement de sécurité via une vulnérabilité au sein de plugins Jenkins

* Jenkins Security Advisory 2018-10-29

- Date: 30-10-2018
- Criticité: Élevée
- Plateformes: Toutes
- Exploitation: Locale
- Dommages: Contournement de sécurité

Description de la vulnérabilité

- Description:
Une vulnérabilité a été corrigée au sein des plugins Pipeline: Groovy et Script Security de Jenkins. Son exploitation permettait à un attaquant de contourner des restrictions de sécurité.

La faille de sécurité non référencée provenait d'un manque d'application des restrictions de Sandbox. Cela permettait à un attaquant d'invoquer des constructeurs et des méthodes arbitraires permettant de s'échapper de la Sandbox.

- Vulnérables:
* Pipeline: Groovy Plugin <= 2.59
* Script Security Plugin <= 1.47

Identification des paquets et des versions impactés

Correctifs à apporter

- Recommandation:
Le CERT-XMCO recommande l'installation de la version 2.60 de Pipeline: Groovy Plugin et de la version 1.48 de Script Security Plugin.

- Référence CERT-XMCO:
<https://leportail.xmco.fr/watch/advisory/CXA-2018-4430>

Pour toute question concernant ce bulletin, vous pouvez contacter le CERT-XMCO à l'adresse suivante : cert@xmco.fr
Fin de l'avis CXA-2018-4430

CERT-XMCO
Service Veille Sécurité

cert@xmco.fr
Tel : +33 1 47 34 30 38
Web : <http://cert.xmco.fr>

Figure 9 : Présentation d'un ticket de vulnérabilité

Une fois la vérification effectuée, deux situations pouvaient se présenter, soit la vulnérabilité concernait bien notre parc et il fallait la traiter, soit elle ne nous concernait pas et il fallait clôturer le ticket. Dans les deux cas, l'ajout d'un commentaire de suivi du ticket devait être effectué afin que le CSSI (Correspondant Sécurité du Système d'Information) puisse apprécier la manière dont a été traitée la vulnérabilité ainsi que démontrer à un auditeur le bon déroulement du traitement d'un tel incident.

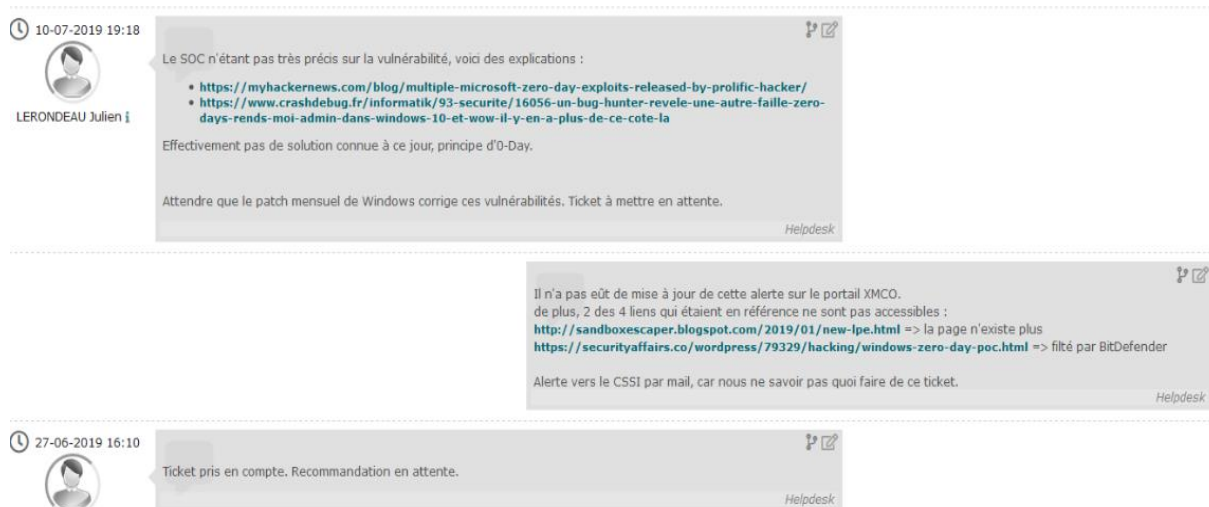


Figure 10 : Suivi d'un ticket de vulnérabilité

DURCISSEMENT DU SYSTEME D'EXPLOITATION UBUNTU VERSION 18.04

A mon arrivée chez SII, les serveurs de l'organisation avaient comme système d'exploitation Windows Server et Ubuntu dans sa version 16.04. Une nouvelle version **LTS** (Long Time Support) d'Ubuntu étant disponible, il était question de déployer cette version plus récente sur l'ensemble des serveurs concernés. Ce déploiement s'accompagne d'une opération de **durcissement du système d'exploitation** qui s'appuie sur les préconisations du **CIS** (Center for Internet Security). Il s'agit plus précisément de rendre le système plus résistant et mieux protégé face aux attaques ou aux mauvaises manipulations. Le durcissement peut passer entre autres par :

- La restriction des accès à la machine ;
- Le durcissement de la couche réseau ;
- Le durcissement des applications installées

Du fait du grand nombre de serveurs présents dans le parc, il serait alors fastidieux de réaliser cette tâche à tour de rôle sur chacun des serveurs. C'est pourquoi il était question d'utiliser un logiciel d'automatisation de tâches, **ANSIBLE** pour pouvoir déployer en une opération l'ensemble du travail effectué sur tous les serveurs.

Ansible est un outil en ligne de commande qui va lire une configuration, se connecter à un serveur, et exécuter les commandes nécessaires sur ce serveur afin d'appliquer la configuration. Dans le jargon Ansible, cette configuration se nomme **Playbook**. Il s'agit de la liste des opérations à exécuter afin de configurer le système.

```

ansible@lys-pic:/opt/ansible/hardening1804/roles/post_install/tasks$ ll
total 36
drwxr-xr-x 2 ansible ansible 4096 août 29 16:57 ./
drwxrwxr-x 5 ansible ansible 4096 août 20 14:27 ../
-rw-rw-r-- 1 ansible ansible 1202 août 29 16:28 00-IPTABLES.yml
-rw-rw-r-- 1 ansible ansible 239 août 26 10:55 02-APT.YML.old
-rw-rw-r-- 1 ansible ansible 161 août 26 10:53 03-PACKAGES.yml.old
-rw-rw-r-- 1 ansible ansible 2438 août 20 14:48 04-DOMAIN.yml.old
-rw-rw-r-- 1 ansible ansible 1042 août 26 11:06 05-NRPE.yml.old

```

Figure 11 : Liste des playbooks Ansible rédigés

```

# Define the role of specific IP/Hostname servers
# The all group is for all the machine \o/
[all:vars]
ansible_ssh_user=ansible
ansible_ssh_private_key_file=/home/ansible/.ssh/id_rsa

[update]
frrlyo-sap03
frrlyo-sap04
frrlyo-sap02
frrlyo-sap06
lys-blanc
lys-ducasse
lys-loiseau
lys-test

```

Figure 12 : Liste des serveurs à configurer

L'ensemble des serveurs à configurer est défini sous le nom de liste

```

- name: Effectuer les mises à jour
  hosts: update
  become: yes
  become_method: sudo
  gather_facts: no
  tasks:
    - name: Run the equivalent of "apt-get update" as a separate step
      apt:
        update_cache: yes

    - name: Update all packages to the latest version
      apt:
        upgrade: dist

```

Figure 13 : Contenu d'un playbook ansible d'automatisation

Nom de la liste de serveurs sur laquelle appliquer les playbooks

REALISATION D'UNE BANNIERE D'INFORMATION DE CONNEXION

En parallèle du durcissement des systèmes Ubuntu, j'ai eu à effectuer le déploiement du logiciel **BGinfo** sur les serveurs tournant sur Windows. Ce logiciel permettra d'afficher sur le bureau différentes informations sur la session de connexion en cours comme le nom de la machine serveur sur laquelle on est connecté, son adresse IP, l'identifiant de l'utilisateur connecté, etc. Il sera également possible de définir une couleur de fond particulière en fonction de l'environnement (production, pré-production ...) du serveur.

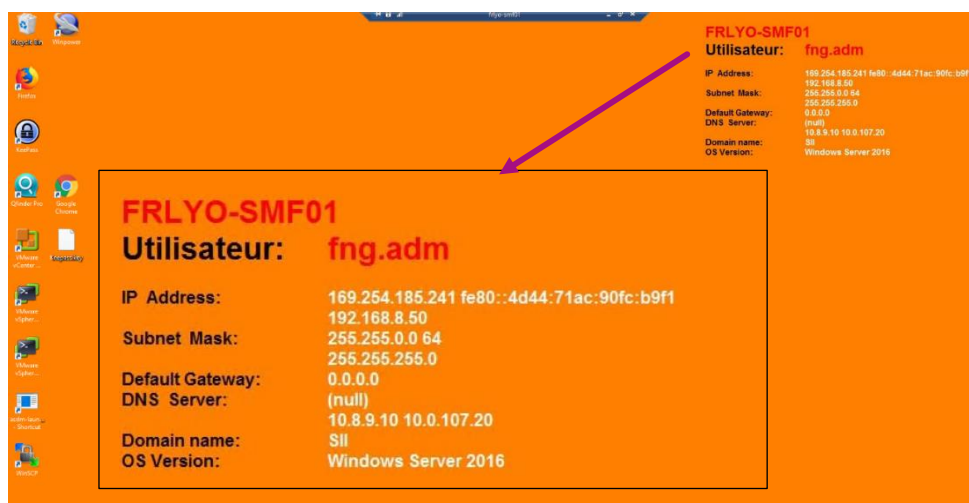


Figure 14 : Résultat de l'installation du programme BGinfo

MISE A JOUR DE LA MATRICE DE FLUX

Dans le souci de maintenir un niveau de sécurité élevé au sein du système d'information, des pare-feu ont été installés et configurés. Un pare-feu est un équipement physique ou logiciel qui permet de définir le type de communications autorisées sur le réseau, il surveille et contrôle les applications et les flux de données.

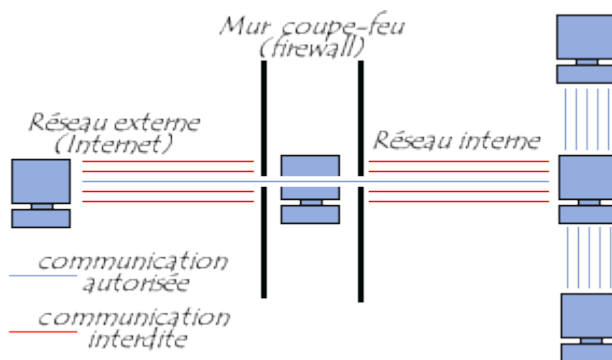
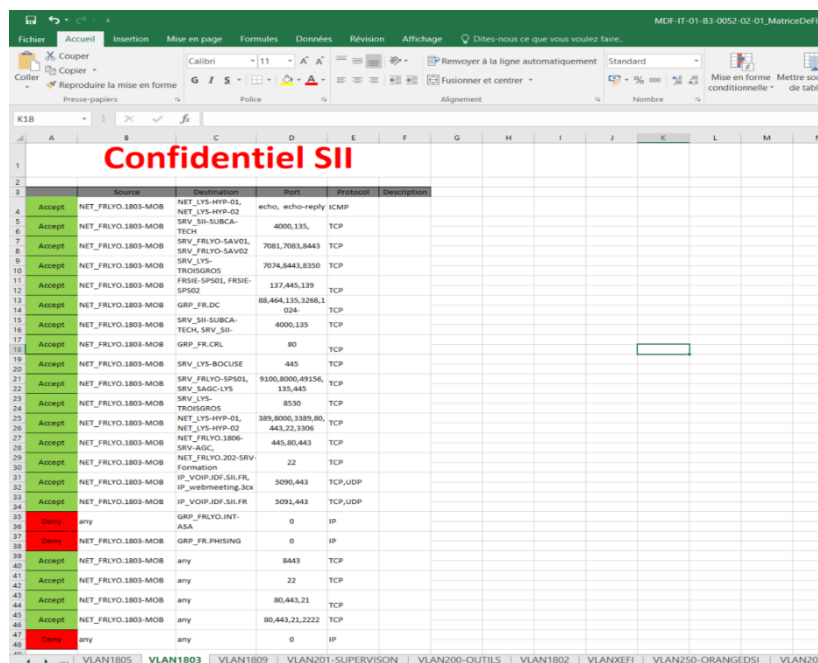


Figure 15 : Illustration d'un pare-feu

Afin de conserver une trace écrite des différents flux autorisés ou interdits sur le réseau et pour faciliter la mise à jour et la maintenance future, un fichier de suivi a été conçu. Celui-ci comportait l'ensemble des trafics de données circulant sur le réseau de l'entreprise. Son maintien à jour au fil des modifications est une obligation pour se conformer aux exigences de l'ISO27001.



	Action	Source	Destination	Port	Protocole	Description
4	Accept	NET_FRLYO.1803-MOB	NET_LYS-HYP-02	echo, echo-reply	ICMP	
5	Accept	NET_FRLYO.1803-MOB	SRV_SII-SUBCA-TECH	4000,135	TCP	
6	Accept	NET_FRLYO.1803-MOB	SRV_FRLYO-SAVEL	7081,7083,8443	TCP	
7	Accept	NET_FRLYO.1803-MOB	SRV_FRLYO-SAVEL	7074,8443,8350	TCP	
8	Accept	NET_FRLYO.1803-MOB	SRV_LYS-TRIOISGROS	137,445,139	TCP	
9	Accept	NET_FRLYO.1803-MOB	FRSIE-SP501, FRSIE-SP502	88,464,135,3268,1	TCP	
10	Accept	NET_FRLYO.1803-MOB	GRP_FRDC	4000,135	TCP	
11	Accept	NET_FRLYO.1803-MOB	SRV_SII-SUBCA-TECH, SRV_SII-	80	TCP	
12	Accept	NET_FRLYO.1803-MOB	GRP_FR.CRL	445	TCP	
13	Accept	NET_FRLYO.1803-MOB	SRV_LYS-BOCUSE	9100,8000,49156	TCP	
14	Accept	NET_FRLYO.1803-MOB	SRV_FRLYO-SP501, SRV_SAGC-LYS	135,445	TCP	
15	Accept	NET_FRLYO.1803-MOB	SRV_LYS-TRIOISGROS	8390	TCP	
16	Accept	NET_FRLYO.1803-MOB	NET_LYS-HYP-02	309,8000,3385,80	TCP	
17	Accept	NET_FRLYO.1803-MOB	NET_LYS-HYP-02	443,22,3306	TCP	
18	Accept	NET_FRLYO.1803-MOB	NET_FRLYO.1806-SRV-AGC	445,80,443	TCP	
19	Accept	NET_FRLYO.1803-MOB	NET_FRLYO.202-SRV-Formation	22	TCP	
20	Accept	NET_FRLYO.1803-MOB	IP_VOIP-GRF.SIL.FIL	5090,443	TCP,UDP	
21	Accept	NET_FRLYO.1803-MOB	IP_VOIP-GRF.SIL.FIL	5091,443	TCP,UDP	
22	Deny	any	GRP_FRLYO.INT-ASA	0	IP	
23	Deny	NET_FRLYO.1803-MOB	GRP_FR.PHESING	0	IP	
24	Accept	NET_FRLYO.1803-MOB	any	8443	TCP	
25	Accept	NET_FRLYO.1803-MOB	any	22	TCP	
26	Accept	NET_FRLYO.1803-MOB	any	80,443,21	TCP	
27	Accept	NET_FRLYO.1803-MOB	any	80,443,21,2222	TCP	
28	Deny	any	any	0	IP	

Figure 16 : Matrice de flux

DEPLOIEMENT APT-MIRROR POUR UBUNTU 18.04

L'installation des mises à jour sur les machines tournant sous le système Ubuntu est une opération qui demande de nombreuses ressources et consomme de cette faite beaucoup de **bande passante**. Pour pallier ce problème, il a été déployé un serveur de mise à jour, un **miroir APT**. Le rôle de ce serveur est de réaliser à fréquence programmée, **le téléchargement des ressources** dont auront besoin les différentes machines pour effectuer leurs mises à jour et de les stocker localement sur le réseau. Par conséquent lors des mises à jour les différents équipements feront les téléchargements directement à partir d'une machine présente sur le réseau de l'entreprise ce qui résultera en un gain conséquent de bande passante.

Etant déjà présent pour la **version 16.04 du système Ubuntu**, il était question pour moi de déployer un nouveau serveur qui sera utilisé pour la **version 18.04 d'Ubuntu**.

Réunion de service

Une réunion de service était programmée tous les mercredi matin afin que nous débâtions des projets en cours, de l'actualité et des éventuelles difficultés que nous avons rencontrées dans la semaine.

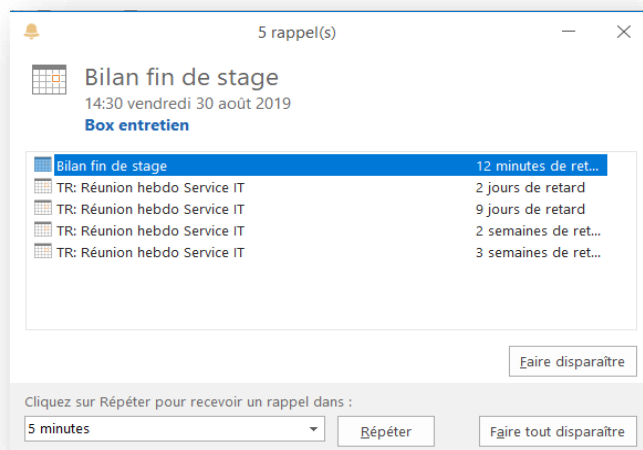


Figure 17 : Agenda présentant les différentes réunions de service

DIFFICULTES RENCONTREES ET SOLUTIONS

Durant cette expérience j'ai dû faire face à quelques difficultés auxquelles il a fallu apporter solution :

- **Difficulté d'adaptation** : Mes premières semaines furent assez compliquées. Il fallait se familiariser avec de nouveaux logiciels et également avec les noms des différents serveurs sur lesquels je devais travailler. Pour me faciliter la tâche je me suis constitué un petit document dans lequel figuraient les noms des différents serveurs et leurs rôles. Mes collègues m'ont par ailleurs été d'une grande aide en ce qui concerne l'utilisation des logiciels, ils étaient toujours disponibles pour répondre à mes questions.
- **Difficulté sur le plan technique** : les outils tels que Ansible et PowerShell étaient nouveaux pour moi. La réalisation de scripts était donc à chaque occasion un travail de recherche et modification car mes programmes ne marchaient pas toujours du premier coup. En me formant de manière autodidacte, j'ai pu braver cet obstacle et gagner en compétences et en connaissances.

BILAN

Ces 9 semaines passées chez SII ont été une expérience très enrichissante et une occasion de mettre en pratique les acquis de ma formation au sein de l'ESIGELEC. J'ai pu effectuer des travaux de natures différentes ce qui m'a permis de développer de nombreuses compétences.

L'autonomie qui m'a été conférée par mon responsable de stage et l'importance des tâches que j'avais à réaliser m'ont permis de grandir en termes de responsabilité et d'organisation. J'ai appris à réaliser des listes de tâches à effectuer et à les prioriser en fonction de leur importance. Bien que j'évoluais de manière autonome dans mes missions j'ai toujours eu l'appui de mes collègues qui ont été très pédagogues et disponibles pour répondre à toutes mes différentes interrogations.

Je regrette cependant le fait de ne pas avoir pu développer davantage mes compétences techniques en matière de cybersécurité. En effet bien qu'ayant eu à toucher du doigt ce domaine, les tâches qui m'étaient confiées n'avaient presque pas de connotation technique, par exemple le traitement des alertes de vulnérabilités qui n'était qu'un travail d'analyse de ticket. J'aurai également souhaité avoir un peu plus d'interactions avec le CSSI de la structure car il occupe un poste auquel j'aspire à la fin de ma formation.

De manière générale, je ressors de ce stage grandi. Cette expérience me sera très bénéfique en ceci qu'elle m'aura permis de me développer tant sur le plan personnel que professionnel. Ce stage a également été l'occasion de confirmer mon projet professionnel, celui étant d'occuper le poste de Responsable en Sécurité des Systèmes d'Information.

CONCLUSION

Pour conclure, j'ai effectué mon stage technicien en tant qu'Administrateur Système et sécurité au sein du groupe SII. Cette expérience de 9 semaines m'a permis de mettre en pratique mes connaissances théoriques acquises au cours de ma formation à l'ESIGELEC tout en me confrontant aux difficultés que représente le monde professionnel.

Cette expérience a été très enrichissante pour moi car elle m'a permis de voir comment est gérée la sécurité du système d'information dans un environnement réel d'entreprise et également de toucher du doigt le métier d'administrateur système. J'ai pu participer de manière concrète au maintien de la sécurité au sein de l'organisation et ceci a renforcé mon envie d'exercer dans ce domaine.

Ce stage a également été pour moi l'occasion de trouver réponses aux nombreuses questions que je me posais notamment par rapport à la gestion de projet en entreprise, la gestion des incidents de sécurité, la communication au sein de l'entreprise, etc....

Je peux affirmer à la fin de ce rapport que je ressors de cette expérience grandi, et ma vision du monde professionnel élargie.

LISTE DE FIGURES

Figure 1 : Historique de l'entreprise.....	3
Figure 2 : Métiers traités par SII.....	4
Figure 3 : Secteurs d'activité couverts par SII.....	6
Figure 4 : Liste des clients du groupe SII.....	6
Figure 5 : Organisation du service IT.....	7
Figure 6 : Interface du logiciel GLPI.....	8
Figure 7 : Interface du GIS.....	9
Figure 8 : Extrait de la liste des alertes de vulnérabilité.....	9
Figure 9 : Présentation d'un ticket de vulnérabilité.....	10
Figure 10 : Suivi d'un ticket de vulnérabilité.....	11
Figure 11 : Liste des scripts Ansible rédigés.....	12
Figure 12 : Liste des serveurs à configurer.....	12
Figure 13 : Contenu d'un script ansible d'automatisation.....	12
Figure 14 : Résultat de l'installation du programme BGInfo.....	12
Figure 15 : Illustration d'un pare-feu.....	13
Figure 16 : Matrice de flux.....	13
Figure 17 : Agenda présentant les différentes réunions de service.....	14
Figure 18 : Liste des tâches effectuées.....	19
Figure 19 : Extrait du bilan des tickets traités.....	20
Figure 20 : Procédure de traitement des tickets de vulnérabilité.....	21

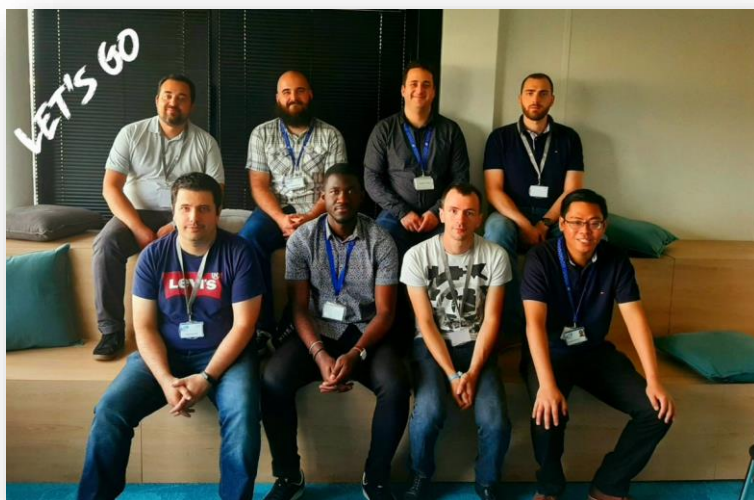
ANNEXES

Annexe n°1 : Liste des tâches effectuées

Quoi	En cours	Terminé	Reste à faire
Gestion des tickets Gis	X		Wiki : Méthodologie à utiliser pour traiter les GIS (Ubuntu et Windows) : Ajouter URL GIS/prendre exemple de ticket pour expliquer les différentes parties/Important le status ne doit jamais être clos/commande pour les mises à jours /URL GLPI/
Hardenning 18.04 (Ansible) Fichiers modifiés : IPTABLES.YML, Site.yml, SYSLOG.yml		X	Playbook : Site.yml
GPO BGInfo (Script)		X	
Bannière Warning Prod et Preprod (Ansible) Dossiers créés : - Banner-Warning 16.04 - Banner-warning18.04 Fichiers créés : - 99-banner-Prepod - 99-banner-prod - 96-banner-Prepod - 96-banner-prod		X	
Finaliser la communication en SSL sur la base de données de GLPI (FRLYO-SMF01 vers FRLYO-SPP04)	X		Documenter à mettre à jour avec la partie SSL : I:\Documentation IT\Validation docs\A valider\
Déploiement serveur apt-mirror 18.04	X		Voir avec sylvain si possibilité avant son départ
Mise en place des rôles pour le post_install		X	
Mise à jour de la doc Déploiement VM 18.04			

Figure 18 : Liste des tâches effectuées

Annexe n°2 : Journée d'intégration





Annexe n°3 : Bilan des traités

ID	Titre	Statut	Date d'ouverture	Impact	Catégorie	Suivis - Révisé	Dernière modification
4 717	[EXTERNAL][PATCH][UBUNTU] Dovecot, Ceph, Ghostscript Criticité Résolu	Résolu	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 288	[EXTERNAL][PATCH][WINSXP] Prise de contrôle du système et divulg En cours (A	En cours	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 316	[EXTERNAL][PATCH][APPLE] Prise de contrôle du système et manip. Résolu	Résolu	#####	Haut	Vulnérabilité NGOUNOU	#####	
4 289	[EXTERNAL][PATCH][APPLE] Prise de contrôle du système et contou. Résolu	Résolu	#####	Haut	Vulnérabilité NGOUNOU	#####	
3 237	[VULN][MICROSOFT] Prise de contrôle du système via une vulnérabilité En cours (A	En cours	#####	Haut	Vulnérabilité NGOUNOU	#####	
4 393	[EXTERNAL][PATCH][GOOGLE] Prise de contrôle du système et cont Résolu	Résolu	#####	Haut	Vulnérabilité NGOUNOU	#####	
4 584	[EXTERNAL][PATCH][MICROSOFT] Prise de contrôle du système et é Nouveau	Nouveau	#####	Haut	Vulnérabilité NGOUNOU	#####	
3 724	[EXTERNAL][PATCH][MICROSOFT] Prise de contrôle du système et é Clos	Clos	#####	Haut	Vulnérabilité NGOUNOU	#####	
3 611	[EXTERNAL][PATCH][APPLE] Prise de contrôle du système et élévati Clos	Clos	#####	Haut	Vulnérabilité NGOUNOU	#####	
3 866	[EXTERNAL][PATCH][GOOGLE] Prise de contrôle du système et cont Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
3 867	[EXTERNAL][VULN][MICROSOFT] Contournement d'une mesure de s Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 173	[EXTERNAL][PATCH][UBUNTU] Glib, ZeroMQ, Whoopsie, Docker, A Clos	Clos	#####	Haut	Vulnérabilité NGOUNOU	#####	
4 221	[EXTERNAL][PATCH][UBUNTU] Squid, Exiv2, Hightower, Bash, Zipios Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 266	[EXTERNAL][VULN][MICROSOFT] Divulgarion d'informations via une Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 267	[EXTERNAL][PATCH][UBUNTU] Linux kernel, Squid, Linux kernel (Hw Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 317	[EXTERNAL][PATCH][UBUNTU] Patch, Ansible, MySQL Criticité : Éle Clos	Clos	#####	Haut	Vulnérabilité NGOUNOU	#####	
4 339	[EXTERNAL][PATCH][UBUNTU] VLC, Linux kernel, Exim, Firefox Criti Clos	Clos	#####	Haut	Vulnérabilité NGOUNOU	#####	
4 369	[EXTERNAL][PATCH][UBUNTU] OpenJDK 8, OpenLDAP, SoX Critici Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 394	[EXTERNAL][PATCH][UBUNTU] Subversion, Linux kernel (HwE), Ope Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 434	[EXTERNAL][PATCH][UBUNTU] Subversion, Linux kernel (HwE), Ope Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 435	[EXTERNAL][PATCH][UBUNTU] Subversion, Linux kernel (HwE), Ope Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 435	[EXTERNAL][PATCH][UBUNTU] Subversion, Linux kernel (HwE), Ope Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 461	[EXTERNAL][PATCH][UBUNTU] Subversion, Linux kernel (HwE), Ope Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 513	[EXTERNAL][PATCH][UBUNTU] Subversion, Linux kernel (HwE), Ope Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 583	[EXTERNAL][PATCH][UBUNTU] Subversion, Linux kernel (HwE), Ope Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 585	[EXTERNAL][PATCH][UBUNTU] Subversion, Linux kernel (HwE), Ope Clos	Clos	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 460	[EXTERNAL][PATCH][GLPI-PROJECT] Manipulation de données et d En cours (A	En cours	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 587	[EXTERNAL][PATCH][MICROSOFT] Prise de contrôle du système et c En cours (A	En cours	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 586	[EXTERNAL][PATCH][UBUNTU] Linux kernel (Xenial HwE), Linux kern En cours (A	En cours	#####	Moyen	Vulnérabilité NGOUNOU	#####	
4 588	[EXTERNAL][PATCH][MICROSOFT] Prise de contrôle du système et é En cours (A	En cours	#####	Haut	Vulnérabilité NGOUNOU	#####	
1301	[VULN][MICROSOFT] Prise de contrôle du système via une vulnérabilité Clos	Clos	#####	Haut	Vulnérabilité NGOUNOU	#####	

Total des tickets traités : 118
Moyenne de temps de traitement pour un ticket : 10min

Légende :


 : Priorité élevée

 : Priorité moyenne

 : Ticket résolu

Figure 19 : Extrait du bilan des tickets traités

Annexe n°4 : Procédure de traitement des tickets de vulnérabilité rédigé à la fin du stage



Accueil

Rechercher

Liste des fichiers

Toutes les pages

Modifications récentes

Page au hasard

Liste des utilisateurs

Droits des utilisateurs

Aide

Outils

Pages liées

Suivi des pages liées

Importer un fichier

Pages spéciales

Vision imprimable

Lien permanent

Information sur la page

Page Discussion

Méthodologie de traitement des tickets Gis

Lien vers GIS : <https://gis.siienergy.net/>

Lien vers GLPI : <https://glpi-rha.sii.fr/>

Étape 1 : Tri et analyse des tickets

Ticket # 1115 description

[PATCH][JENKINS] Contournement de sécurité via une vulnérabilité au sein de plugins Jenkins

* [PATCH][JENKINS] Contournement de sécurité via une vulnérabilité au sein de plugins Jenkins

* Jenkins Security Advisory 2018-10-29

- Date: 30-10-2018

- Criticité: Élevée

- Plateformes: Toutes

- Exploitation: Locale

- Dommages: Contournement de sécurité

Description de la vulnérabilité

- Description: Une vulnérabilité a été corrigée au sein des plugins Pipeline: Groovy et Script Security de Jenkins. Son exploitation permettait à un attaquant de contourner des restrictions de sécurité.

La faille de sécurité non référencée provenait d'un manque d'application des restrictions de Sandbox. Cela permettait à un attaquant d'invoquer des constructeurs et des méthodes arbitraires permettant de s'échapper de la Sandbox.

- Vulnérables:

- * Pipeline: Groovy Plugin <= 2.59
- * Script Security Plugin <= 1.47

Identification des paquets et des versions impactés

- Références: <https://jenkins.io/security/advisory/2018-10-29/>

Correctifs à apporter

- Recommandation: Le CERT-XMCO recommande l'installation de la version 2.60 de Pipeline: Groovy Plugin et de la version 1.48 de Script Security Plugin.

- Référence CERT-XMCO: <https://leportail.xmco.fr/watch/advisory/CXA-2018-4430>

Pour toute question concernant ce bulletin, vous pouvez contacter le CERT-XMCO à l'adresse suivante : cert@xmco.fr
Fin de l'avis CXA-2018-4430

CERT-XMCO
Service Veille Sécurité
cert@xmco.fr
Tel : +33 1 47 34 30 38
Web : <http://cert.xmco.fr>

☐ Analyser les tickets.

☐ Vérifier si il n'existe pas de doublons du tickets et clôturer les doublons si oui.

☐ Vérifier dans GLPI si nous sommes concernés par la vulnérabilité mentionnée (Vérifier les paquets indiqués dans le cas des machines Ubuntu et vérifier les version de KB pour les machines Windows).

☐ Si aucune machine n'est concernée par cette vulnérabilité, Clôturer le ticket en précisant qu'il ne nous concerne pas.

☐ Si une ou plusieurs machines sont concernées, renseigner dans le suivi ces différentes machines.

Étape 2 : Traitement des vulnérabilités

☐ Vérifier le niveau de criticité de la vulnérabilité

Niveau Très haut

☐ Appliquer les correctifs immédiatement

Niveaux autres que Très haut

☐ Pour les machines Ubuntu attendre la date prévue pour effectuer les mises à jour et s'assurer de remplir la fiche de suivi de mise à jour qui se trouve dans I:\Preuves\Suivi MAJ

☐ Pour les mises à jour de logiciels sous Windows, vérifier dans GLPI les propriétaires des machines concernées et les contacter par mail pour qu'ils fassent le nécessaire











☐ Une fois le traitement effectué, Clôturer les tickets en apportant les preuves correspondantes

Figure 20 : Procédure de traitement des tickets de vulnérabilité

SITOGRAPHIE

- ✚ Groupe SII. (s. d.). Site web de l'entreprise. Consulté à l'adresse <http://lyon.groupe-sii.com/fr>
- ✚ Groupe SII. (s. d.-a). Mediatweets door SII_RhôneAlpes (@sii_rhonealpes) | Twitter. Consulté le 24 septembre 2019, à l'adresse https://twitter.com/sii_rhonealpes/media
- ✚ Pare-feu (informatique) — Wikipédia. (2019, septembre 8). Consulté le 24 septembre 2019, à l'adresse [https://fr.wikipedia.org/wiki/Pare-feu_\(informatique\)](https://fr.wikipedia.org/wiki/Pare-feu_(informatique))

GLOSSAIRE

-  **SII** : Société pour l'informatique industrielle
-  **ERP** : Enterprise Resource Planning
-  **IT** : Information and Technology
-  **SOC** : Security Operation Center
-  **SIEM** : Security Information and Event Management
-  **GIS** : Gestion des Incidents de Sécurité
-  **LTS** : Long Time Support
-  **CIS** : Center for Internet Security
-  **GLPI** : Gestion Libre du Parc Informatique
-  **CSSI** : Correspondant Sécurité du Système d'information

My internship at SII Rhône-Alpes was a very enriching experience on both a professional and personal level and allowed me to have a better vision of the professional world and its constraints. After a quick integration into the team, I was able to carry out several system administration and IT security assignments. The autonomy granted to me by my internship supervisor has allowed me to take more responsibility and learn to prioritize my tasks according to their importance. My success in carrying out the various tasks entrusted to me has increased my self-confidence and self-esteem. In a nutshell, I can say that these 9 weeks of internship were for me the opportunity to put into practice my knowledge acquired in class and reinforced the idea I had of practising later in the field of IT, particularly IT security.

Mon stage chez SII Rhône-Alpes a été une expérience très enrichissante tant sur le plan professionnel que personnel et m'a permis d'avoir une meilleure vision du monde professionnel et de ses contraintes. Après une intégration rapide au sein de l'équipe j'ai pu réaliser plusieurs missions d'administration système et de sécurité informatique. L'autonomie qui m'a été conférée par mon responsable de stage m'a permis de me responsabiliser davantage et d'apprendre à prioriser mes tâches en fonction de leur importance. Ma réussite dans la réalisation des différentes tâches qui m'étaient confiées ont eu pour résultat d'accroître ma confiance en moi et l'estime que j'avais pour moi. De manière brossée je peux dire que ces 9 semaines de stage ont été pour moi l'opportunité de mettre en pratique mes connaissances acquises en cours et ont conforté l'idée que j'avais d'exercer plus tard dans le domaine de l'informatique, en particulier de la sécurité informatique.

S'il fallait décrire ce stage en utilisant 5 mots clés, on pourrait citer :

-  Autonomie
-  Responsabilité
-  Communication
-  Initiative
-  Sécurité.