Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Mise en place d'une solution de supervision réseau Elastic Detector

Oriane DONADIO

Conseil Régional
Provence-Alpes-Côte d'Azur

Responsable entreprise : Jean-Michel Ruffin

Responsable académique : Jean-Luc Damoiseaux

2017

Remerciements

Mes remerciements vont tout d'abord à M. Didier VENTURINI, Directeur des Systèmes d'Information pour m'avoir permis de réaliser mon stage au Conseil Régional.

Je remercie particulièrement M. Jean Claude MELLET, responsable du service Architecture Technique, pour m'avoir accueilli dans son service et pour toute la sympathie et l'intérêt qu'il m'a montré durant ce stage.

Je remercie M. Jean-Michel RUFFIN, responsable de l'équipe Réseau et Télécom et mon tuteur, pour toutes les explications qu'il m'a fournies et l'excellent accueil qu'il m'a réservé au sein de son équipe.

Je souhaite faire part de ma reconnaissance au personnel des équipes Système et Exploitation pour leur bonne humeur et leur disponibilité, ainsi qu'à M. Thierry CAPUTI, ingénieur réseau, pour toutes ses explications.

Je tiens également à remercier M. Jérôme MURTAS, de l'équipe Réseau et Télécom, ainsi que Mme Emmanuelle ROME, qui m'ont accueilli dans leur bureau et m'ont aidé dans les tâches que j'avais à faire.

Enfin je voulais remercier aussi toutes les personnes du service pour leur bonne humeur et leur gentillesse envers moi.

Table des matières

Introduction

Actuellement en deuxième année de DUT Réseaux et Télécoms, j'ai eu l'opportunité de réaliser un stage au Service Architecture Technique du Conseil Régional. Ce dernier, d'une durée de dix semaines me permettra de valider mon diplôme.

Le sujet du stage qui m'a été confié porte sur l'amélioration et l'optimisation de la sécurité du réseau.

Jusqu'à présent, il n'y avait qu'un seul scan de la sécurité du réseau effectué une fois par an (généralement au cours des mois de juin-juillet). Durant ces quelques jours, des experts essayaient de pirater le réseau. Ils délivraient alors un rapport très complet et assez complexe sur l'état de la sécurité du réseau de la Région.

Le problème étant que s'il fallait modifier ou mettre à jour le réseau en ajoutant de nouveaux sites par exemple, il fallait attendre le prochain scan afin de voir si ces modifications ne réduisaient pas la sécurité globale du réseau.

Par exemple, un nouveau site web est lancé par la Région, mais il faudrait attendre juin pour tester sa fiabilité. Ce qui va entraîner une perte de temps importante.

Il était donc nécessaire de trouver une solution de supervision, qui permette de résoudre cette problématique. La mise en place de cette nouvelle solution de supervision réseau a été au cœur de mes activités durant mon stage.

1 Présentation du Conseil Régional

1.1 L'Hôtel de région et la Région PACA

1.1.1 L'historique

Si le découpage de la France en communes et en départements remonte à la Révolution, la création de régions est plus récente.
En 1961, vingt-et-une circonscriptions d'action régionale sont créées. C'est alors qu'apparaît la Région Provence-Alpes-Côte d'Azur, qui inclut alors la Corse (qui ne deviendra à son tour une Région qu'en 1970).

Mais c'est en 1982, par les lois de décentralisation, que la Région prend toute son ampleur. Elevée au rang de collectivité territoriale, elle est désormais administrée par un Conseil Régional élu au suffrage universel (la première élection eut lieu en 1986).

1.1.2 La disposition actuelle

La Région Provence-Alpes-Côte d'Azur comprend 6 départements : Vaucluse (84), Bouches-du-Rhône (13), Var (83), Alpes Maritimes (06), Hautes-Alpes (05) et Alpes de Haute-Provence (04). Elle s'étend sur 31 400 km² et abrite plus de 5 millions d'hommes et de femmes dont 20% ont moins de 20 ans. Elle est la troisième région la plus peuplé de France.

L'Hôtel de Région se situe à Marseille, avec des bureaux à la Porte d'Aix et à la Joliette. Elle possède aussi des antennes régionales dans chaque département, situées à Nice, Toulon, Avignon, Gap, Briançon, Digne-les-Bains et Arles.

A ce jour l'assemblée régionale est composée de 123 élus, présidée par M. Renaud Muselier. La Région a une organisation administrative assez classique ; elle est organisée autour de directions (au nombre de 18) et de services (45). Certaines directions sont regroupées sous la responsabilité d'un directeur général adjoint, le tout étant dirigé par un directeur général des services.

Organigramme général du réseau du Conseil Régional PACA

(Voir annexe 1)

1.2 La Direction des Services d'Informations (DSI)

Elle étudie et met en œuvre les systèmes d'information nécessaires au fonctionnement des services. Elle assure la mise à disposition des moyens informatiques matériels et logiciels.

1.2.1 L'organisation de la DSI

Elle est composée de 3 services, comme on peut le voir sur l'organigramme ci-dessous (Figure 1) ;

- Le service Poste de travail et Support assure la gestion du parc de la micro-informatique (matériel et logiciel). Il s'occupe aussi de l'assistance aux utilisateurs.

- Le service Applications et Données étudie les nouvelles procédures de traitement de l'information. Il fait aussi l'interface avec les prestataires qui sous-traitent une partie des développements de logiciel. Il porte assistance aux utilisateurs des applications informatiques, de manière à recenser, étudier et analyser leurs besoins.

- Le service Architecture et Technique est chargé d'assurer la bonne marche de l'informatique centrale (Serveurs, réseaux, systèmes, bases de données …). Il est divisé en plusieurs cellules.

  C'est précisément dans ce service que j'ai effectué mon stage.

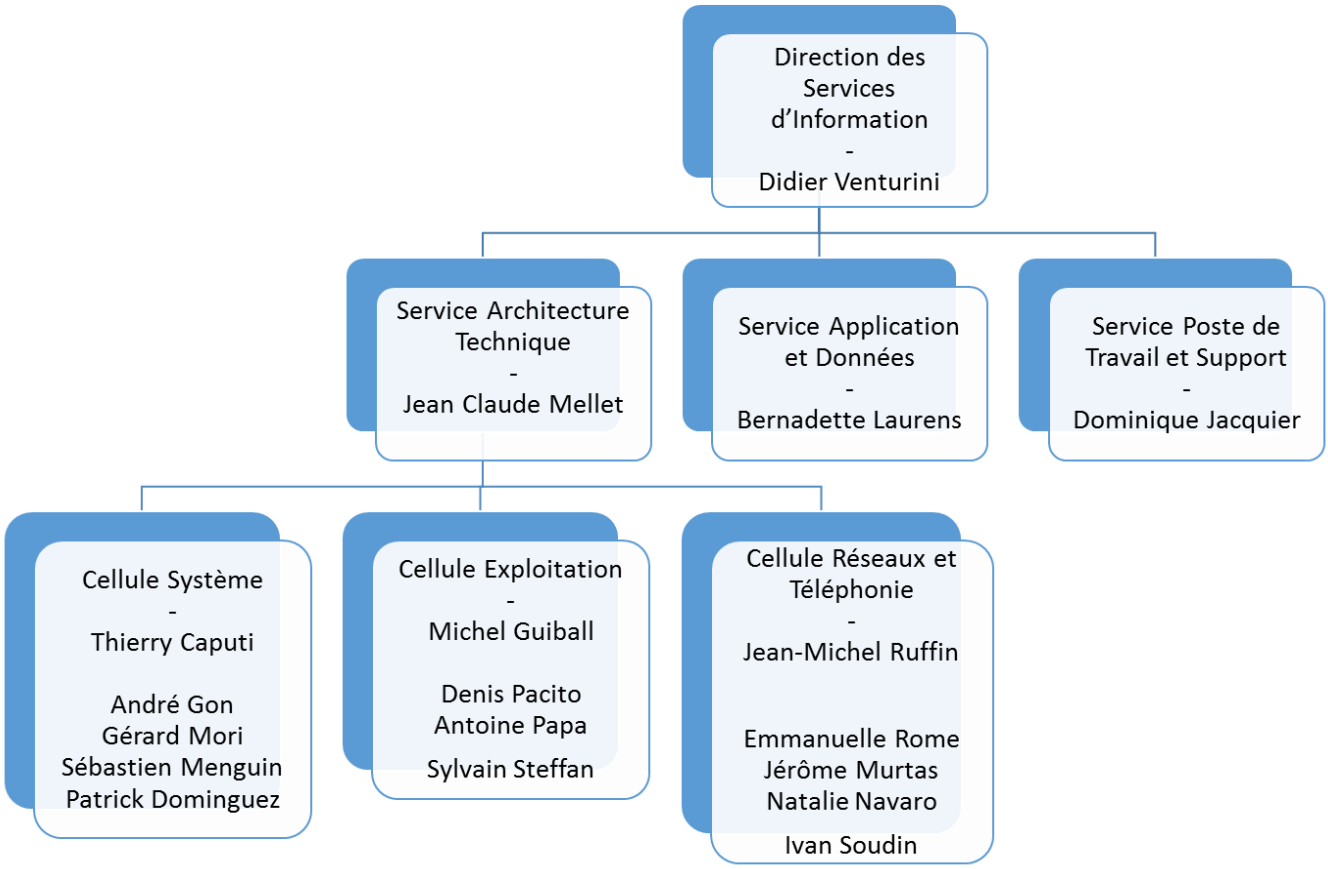


Figure 1 : Organigramme de la Direction des Services d'Information

1.2.2 L'organisation du service Architecture Technique

Ce service, sous la supervision de M. Jean-Claude Mellet, est constitué de 3 cellules ;

- La cellule Système, dont l'animateur est M. Thierry Caputi, est en charge de la surveillance des serveurs (Linux, Windows, Unix), de la gestion des bases de données (Oracle, SQL serveur) en liaison avec le service application et données. Elle s'occupe aussi de la surveillance des systèmes, et de l'élaboration d'un plan de sauvegarde des données et des programmes.

- La cellule Exploitation, dont l'animateur est M. Michel Guiball, est en charge de la gestion du plan de sauvegarde et de la gestion des sauvegardes des serveurs. Cette équipe s'occupe aussi de la surveillance, des visio-conférences et des salles informatiques.

- La cellule Réseaux et Téléphonie, dont l'animateur est Jean-Michel Ruffin, est le secteur où je réalise mon stage. Les missions principales de cette cellule sont la surveillance et la gestion de l'infrastructure réseau, l'élaboration et le suivi des évolutions de l'architecture réseaux. A ce titre, la cellule assure une veille technologique et effectue des études de faisabilité.
  Elle assure aussi l'administration des annuaires, informatique et téléphonique. Enfin cette équipe s'occupe également de la gestion de la sécurité du système d'information, en liaison avec la cellule Système.

  C'est une équipe de 5 personnes. Elles maitrisent chacune au moins une des missions du service. Par exemple, Mme Natalie Navarro et M. Ivan Soudin, sont plus spécialisés en téléphonie, et Mme Emmanuelle Rome et M. Jérôme Murtas sont plus spécialisés dans les réseaux. Cependant il est acquis que chacune d'entre elles maitrise un tronc commun de connaissances et de compétences afin de suppléer toutes absences.

2 La sécurité réseau, un domaine étendu

2.1 La sécurité réseau pour les Nuls

De nos jours, toutes les entreprises, associations et groupements ont besoin d'un réseau. C'est ce qui permet d'interconnecter des composants entre eux, comme des ordinateurs, des serveurs, des clients, des services, etc…
La communication de ces réseaux internes avec Internet est aujourd'hui indispensable. Là, ils s'exposent aux menaces de l'extérieur, même si parfois une attaque peut venir de l'intérieur du réseau.

C'est un des rôles de **l'administrateur réseau**, de veiller à mettre en place **la politique de sécurité** la plus étanche possible (par rapport aux menaces et attaques en tous genres). C'est aussi lui qui s'occupe de résoudre les problèmes qu'il peut y avoir sur le réseau. Il est toujours attentif aux **vulnérabilités** présentes, afin de pouvoir y remédier le plus vite possible avant qu'elles ne deviennent exploitables par des personnes mal intentionnées.

La sécurité d'un réseau peut se décliner en plusieurs aspects. Tout d'abord, il faut avoir une bonne sécurité physique, et donc restreindre l'accès à la salle des serveurs. Celles-ci doivent être constamment sous surveillance, avec de la vidéo par exemple.
Ensuite, il faut une sécurité technologie performante. Ce qui nécessite différents procédés, comme l'interdiction d'une connexion non authentifiée, ou la mise en place d'un pare-feu, pour n'en citer que quelques-uns. Nous allons voir cela plus en détails, en passant en revue ceux mis en œuvre au Conseil Régional.

2.2 Les politiques de sécurités mise en place

2.2.1 La sécurité physique

Le Conseil Régional est une structure très importante, et on peut le constater en voyant l'ampleur des solutions réseaux mises en œuvre. Comme je le disais précédemment, la sécurité technologique n'est rien, s'il n'y pas une sécurité physique efficace.

Celle du Conseil Régional se compose de plusieurs éléments.

Le cœur du réseau est constitué principalement de trois salles informatiques, dans les bâtiments les Présentines, Grand Horizon (tous les deux situés à la Porte d'Aix) et Thyrapolis (situé à la Joliette).

Les salles informatiques des bâtiments les Présentines et Grand Horizon fonctionnent de la même manière. Elles possèdent toutes les deux des baies de serveurs. Dans ces dernières on peut trouver deux sortes de disque dur, **SATA** et **SAS**. Je n'ai pu visiter que celle du bâtiment les Présentines, c'est donc celle-ci que j'évoquerai.

Premièrement, on doit d'abord passer par une salle avec authentification par carte ou par visiophone. A l'intérieur de cette dernière se trouvent les quatre personnes de la cellule Exploitation (voir Figure 1). Une de leurs missions est de surveiller la salle des serveurs ; un mur vitré entre les deux salles facilite amplement la tâche.

De plus, une authentification uniquement par carte est requise pour passer la porte de la salle informatique. Au milieu de la salle, trône un énorme extincteur et dans le cas où les multiples détecteurs de fumée repèreraient quelque chose de suspect, toute personne étant à l'intérieur a deux minutes pour sortir avant que l'extincteur ne se déclenche. Par ailleurs, plusieurs caméras de surveillances sont disposées dans les deux salles.

2.2.2 La sécurité technologique

La sécurité technologique est la plus grande partie de la sécurité informatique, elle résulte de différents composants. Il y a beaucoup de manières différentes de sécuriser un réseau, et elles se complètent souvent.

Sécurité au niveau de l'architecture réseau : Elle est constituée d'un ensemble de **VLAN**. Parmi ces derniers, il y a un Vlan pour les utilisateurs et un autre pour les serveurs. Ce qui permet d'empêcher un utilisateur non identifié d'accéder aux serveurs. En effet, des attaques pouvant venir de l'intérieur du réseau, il est indispensable de s'en protéger.

Le Conseil Régional utilise le **WAF** de DenyAll comme pare-feu. C'est premier pare-feu applicatif de nouvelle génération web français à être certifier par l'ANSSI.

Ce pare-feu propose plusieurs technologies comme par exemple, l'identification des requêtes SQL via analyse grammaticale des données transmises, ou encore la protection contre les blocs imbriqués en Java, PHP, SSI et Javascript, et d'autres comme la détection dynamique des injections de commande, et l'identification des éléments encodés en base64.

De plus il convient bien à la Région car il est basé sur des machines virtuelles, et donc il permet de surveiller le réseau virtuel.

2.2.3 La sauvegarde et la restauration de données

Un autre aspect de la sécurité est de faire face à une perte de données due à une panne technique.

Les systèmes de restauration des données sont là pour répondre à cette problématique. Ils sont présents dans les salles informatiques des bâtiments, les Présentines et Grand Horizon.

Actuellement le système utilisé est le « RAID 6 ». Il s'appuie sur le principe de la redondance des données afin de permettre une certaine protection s'il y a une perte de données. Voici un petit historique de cette technologie :

- Raid 1 est basé sur un système de disque en miroir. Il y a deux disques qui écrivent en même temps sur le disque dur. Si l'un des deux tombes en panne, l'autre peut prendre directement le relais. Par la suite quand on remplacera le disque endommagé, le plus ancien recopiera ses données sur le nouveau disque pour qu'il soit de nouveau disponible et que les deux soient à nouveau synchronisés (Cela peut prendre un temps variable selon les données). Le problème étant le coût d'achat, de l'entretien et d'avoir deux disques redondants.
- Raid 5 est basé sur un système de bit de parité. Tous les disques sauf un possèdent une valeur arbitraire qui leur est propre qu'on appelle le bit de parité. Le disque qui ne possède pas de bit de parité a la somme de tous les bits de parité des autres disques ; on appelle cette valeur, le bit de contrôle. Donc si un disque (excepté celui de contrôle) devient inactif, quand le disque de contrôle va vérifier la valeur actuelle avec la valeur du bit de contrôle, en faisant une opération simple, il peut savoir exactement ce qui manque. Le problème étant que ce système ne tolère qu'une panne à la fois.
- Raid 6 RDP (Raid with Double Parity), c'est une évolution de Raid 5 qui est basée sur un système de double parité. Comme son nom l'indique, les disques ont deux bits de parité différents. Ce qui permet de supporter la perte de deux disques simultanément. C'est le système utilisé aujourd'hui.

Enfin, ils utilisent de surcroit la technologie « Hot Spare » qui consiste à toujours avoir un disque de rechange, disponible. Lorsque qu'un disque tombe en panne, le disque de rechange prend directement et automatiquement le relais, il recopie alors les données des autres disques pour restaurer les données perdues. Cependant, il faut procéder physiquement à la mise en place d'un nouveau disque de rechange. Cette technique permet de réduire la vulnérabilité d'un Raid.

Avec ces technologies, leur système permet de supporter la perte de trois disques simultanément.

2.2.4 La sauvegarde de données

C'est le troisième bâtiment, Thyrapolis, qui sert prioritairement à la sauvegarde et au stockage des données. La sauvegarde se fait sur deux niveaux ;

- La sauvegarde classique, qui a pour but de restaurer les éléments perdus. Cette sauvegarde est versionnée. C'est-à-dire, qu'elle fait une copie du système à fréquence régulière, et elle peut varier selon le type de données. A la Région, les sauvegardes sont effectuées toutes les nuits et pour certaines données sensibles, toutes les trois heures.
- La réplication est le fait que les trois centres d'informations s'entre-copies entre eux, (ce qui s'appelle le snapshot miroir) afin que si l'un tombe en panne, les autres puissent le remplacer.

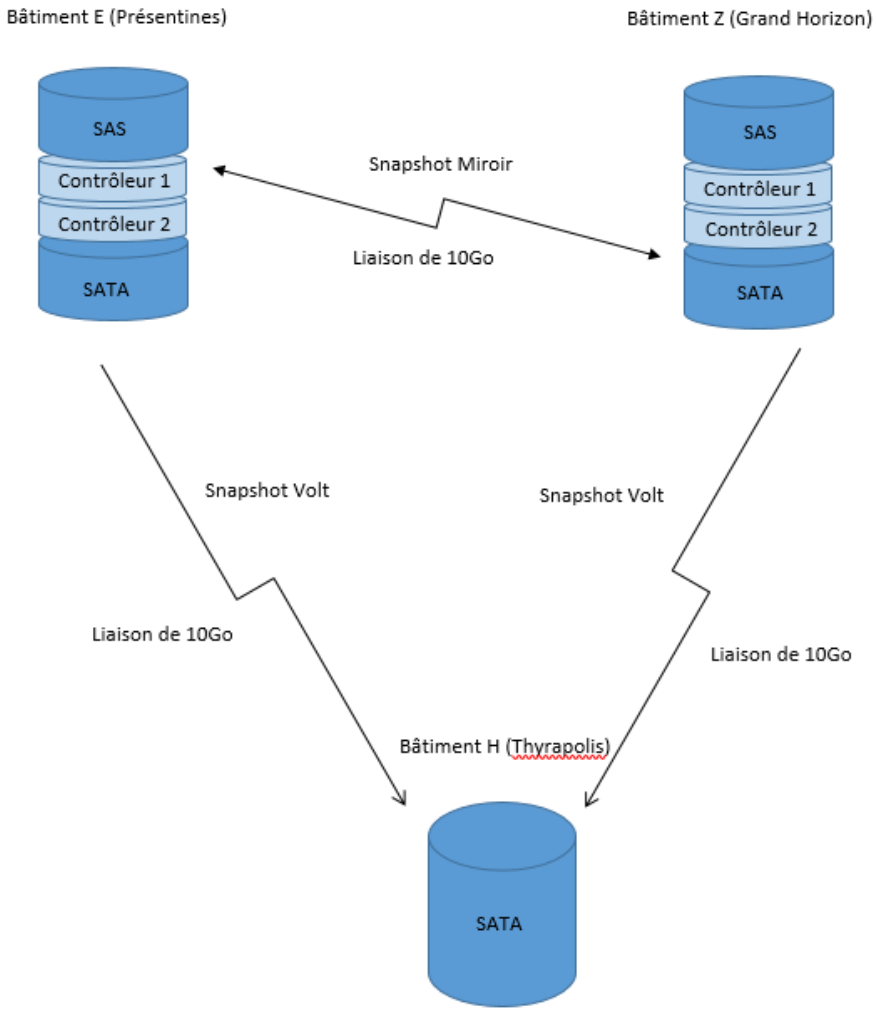


Figure 2 : Schéma résumant les procédés de sauvegarde des données

2.3 Les failles de sécurité résiduelles

Avoir le plus sûr des réseaux ne garantit pas qu'il puisse bloquer 100 % des attaques.
Il faut essayer de tendre vers ce 100 % et c'est d'ailleurs souvent pour cela que l'on voit des logiciels de sécurité informatique proposer des niveaux de 99,99% de fiabilité.

La difficulté avec la sécurité réseau ou la sécurité informatique en général, est que l'on ne pourra tester le niveau de sécurité qu'au moment où elle se trouve en défaut. Pour résumer, tant que tout se déroule comme prévu, il ne passe rien. Les pare-feu ou d'autre mesures de sécurité sont là pour alerter lorsqu'un problème arrive et non pas quand ils bloquent des tentatives d'accès malintentionnés.

Comme je l'ai évoqué au début de ce rapport, le seul moyen qu'avait la Région pour tester la sécurité de leur réseau était le passage d'experts pendant un mois (généralement en juin). Une batterie de test était réalisée, et un rapport complexe délivré. Cependant, aucun test n'était effectué durant le reste de l'année. D'où leur souhait de mettre en place une solution de supervision réseau qui permettrait une surveillance constante des réseaux et des systèmes. Ce qui donnerait lieu à plus de prévention, axe relativement absent de la sécurité informatique du Conseil Régional.

3 Le choix de la solution appropriée

3.1 Le cahier des charges

Toute demande de nouveaux systèmes (matériels ou logiciels) nécessite de remplir un dossier de consultation. Ce dossier comprend entre autres le Cahier des charges qui en constitue l'élément essentiel. En effet, c'est lui qui va définir les critères technico-économiques du choix de la solution.

Par rapport aux besoins exprimés, le Cahier des Charges de cette solution de supervision réseau avait comme principaux critères :

- Une détection des vulnérabilités pour au moins 40 sites + 15 **adresses IP ;**
- Une fréquence d'au moins 12 **audits**(scans)/an ;
- Une prestation d'installation + la formation des équipes de la DSI ;
- Une maintenance annuelle ;
- Une installation garantie des nouvelles versions ;
- Une maintenance préventive ;
- Un support téléphonique disponible de 8 – 18h ;
- Un prix abordable.

3.2 L'appel d'offres

Durant la phase d'appel d'offres, plusieurs entreprises proposent leurs services et le Conseil Régional fait son choix parmi les solutions proposées. Dans l'appel d'offres concerné, 2 entreprises ont répondu en proposant les solutions exposées ci-après.

3.2.1 Qualys

Figure 3 : Logo de Qualys

C'est une solution de supervision réseau américaine très connue. Leur solution est basée sur le **Cloud**, Il n'y a pas de logiciel à installer et la maintenance est directement assurée par l'éditeur dans le Cloud.

On peut voir ci-dessous, qu'ils proposent différents types d'abonnements. Ces derniers varient selon le nombre d'adresses IP à scanner, et selon le nombre de services.

Voici un bref résumé des différents services que propose Qualys ;

- AV pour Asset View fournit la visibilité nécessaire pour faire en sorte que les **Asset**, des ressources basiques pouvant être affichées dans un navigateur web, reste sécurisées.

- VM pour Vulnerability Management, détecte et protège en continu, afin de parer les attaques au moment précis où elles apparaissent.

- CM pour Continuous Monitoring, surveille en continu, afin d'obtenir des alertes en temps réel et accélère la réponse aux incidents

- TP, pour Thread Project, service spécifique à Qualys, permet de suivre l'évolution des menaces afin de savoir lesquelles prendre en charge en premier.

- PCI, pour Pci Compliance, service qui permet de sécuriser les transactions bancaires, en leur attribuant un certificat si elles sont dignes de confiance.

- WAS, pour Web Application Scanning, service qui permet d'analyser pour ensuite cataloguer toutes les vulnérabilités et les mauvaises configurations des sites Web.

- WAF, pour Web Application Firewall, service qui complète le WAS, il permet de remédier aux erreurs détectées par le WAS.

- MD, pour Malware Detection, permet d'identifier et d'éradiquer rapidement des **malwares** à l'aide de scan automatisé. De plus, met en place une **veille informatique** sur les nouvelles infections, comme les **infections zéro days.**

3.2.2 Elastic Detector

Figure 4 : Logo d'Elastic Detector

Cette solution de supervision française a été conçue par la société SecludIt à Sophia Antipolis. Cette startup se démarque des solutions traditionnelles avec son produit phare, Elastic Detector.

Ce dernier a comme particularité la possibilité de cloner des machines virtuelles, afin d'effectuer les scans sur les clones de la machine sans aucun impact sur la machine de base. Grâce ce système, la fréquence des scans peut grandement augmenter, passant d'un scan par mois à un scan par semaine.

Un autre de leurs atouts est de se focaliser sur la détection de vulnérabilité en continu.

Elastic Detector possède plusieurs fonctionnalités comme par exemple ;

- Auto-Découverte : les réseaux et les serveurs sont découverts automatiquement, sans risque d'erreur.

- Autotests : les tests de sécurité se mettent à jour et se lancent automatiquement, la base de tests est constamment renouvelée.

- Sans Agent : Aucun logiciel à installer sur les serveurs, par conséquence, il n'y a pas de ressource utilisée et pas de risque de Cheval-de-Troie.

- Clonage : Analyse approfondie de l'intérieur du serveur, en clonant les machines testées pour éviter d'affecter les performances de ces dernières. Les serveurs dormant sont aussi scannés. De plus ce système diminue le nombre de faux-positif.

- Interface intuitive : une présentation en tableaux de bord avec une vue décisionnelle, le détail des vulnérabilités, les tendances et les statiques ainsi que le niveau de cyber risque (**ANSII, OWASP, PCI Security**).

- Reporting : des rapports détaillés en temps réel que l'on peut configurer à sa guise pour qu'ils ciblent tel ou tel services. Les analyses ANSSI, OWASP et PCI-DSS, qui permettent de déduire des indicateurs de risque. De plus, des rapports dédiés listent des propositions de solutions contre les failles de sécurité.

Dernièrement, Elastic Detector s'est recentré autour d'un concept, la prévention. C'est pour cela qu'ils ont mis au point un nouveau modèle d'audit de sécurité breveté : la surveillance continue et adaptative.

Comme pour Qualys, les offres diffèrent selon le nombre d'adresses IP à surveiller, la maintenance et le support téléphonique.

3.3 La solution choisie

Le cahier des charges de la Région étant peu exigeant, une solution simple était de mise. C'est le prix qui a eu le plus de poids dans la balance. Comparé à Elastic Detector, Qualys était peut-être plus performant mais possédait beaucoup de fonctionnalités superflues pour l'usage que la Région allait en faire. De plus, la solution américaine était beaucoup plus chère, c'est donc ce qui les a poussés à choisir la française. En outre, le nouveau modèle d'audit sur la surveillance continue et adaptative d'Elastic Detector correspond tout à fait aux attentes du Conseil Régional. De plus, la Région a un partenariat avec cette solution, c'est en partie elle qui l'a financé lors de sa création.

4 Ma contribution à la mise en œuvre du logiciel

4.1 La découverte de la solution

4.1.1 Le fonctionnement global

Toute solution de supervision réseau est composée de deux parties distinctes :

- Le monitoring qui est une activité de surveillance et de mesure de ressource informatique,
- les audits qui sont des scans ponctuels qui analysent et évaluent en profondeur un serveur, un nom de domaine ou le réseau lui-même.

Sur Elastic Detector, ce clivage est très clair car il faut avoir deux comptes différents, un compte auditeur et un compte qui fait du monitoring. Le compte auditeur possède moins de droits que le compte moniteur.

L'interface graphique du logiciel se présente sous la forme d'une application web, c'est dans cette dernière que l'on pourra effectuer les scans, le monitoring et visualiser tous les rapports.

4.1.1.1 Les scans

Afin de commencer les scans, Elastic Detector permet d'accéder à plusieurs plateformes de virtualisations à surveiller, ou tout simplement de saisir des noms de domaines. Dans le cas de la Région où 90% des machines sont virtuelles, on peut saisir les différents serveurs disponibles sur **VMware vSphere**. La solution fait le reste, c'est-à-dire de découvrir toutes les machines et les ressources à scanner sur la plateforme **VCenter**.

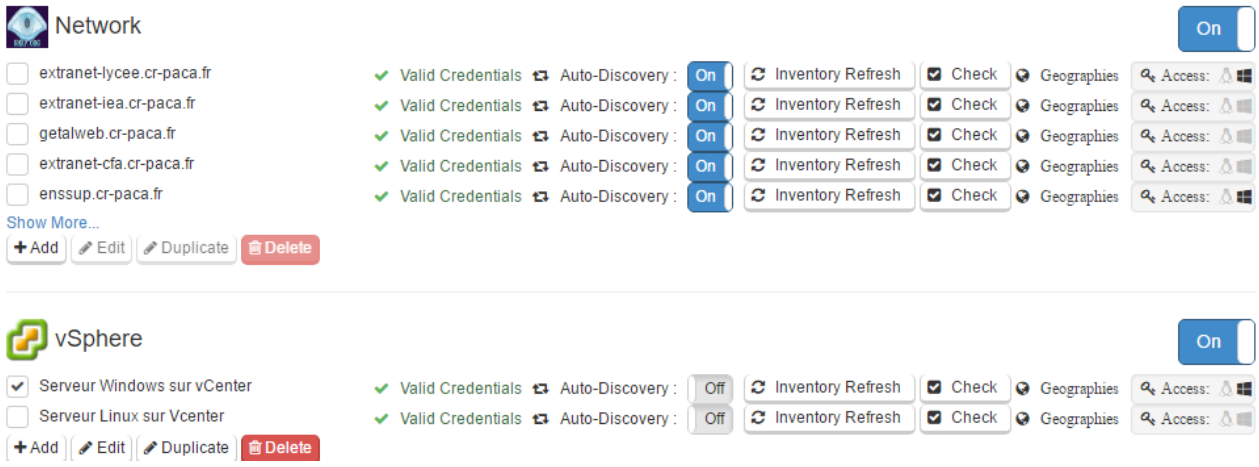


Figure 5 : Les deux façons de définir les ressources qui vont être utilisées

Une fois que tous les serveurs ont été découverts, on peut alors démarrer la procédure de scan. Pour chacun des serveurs, la procédure de scan se déroule en trois étapes :

‘ Queued ’ : La ressource à scanner est mise dans la file d’attente.
‘Scanning x%’ : Le scan a commencé, et on peut suivre l’avancement du scan.
‘ Done ’ : Le scan est terminé.

Cependant il peut arriver que le scan échoue dans ce cas, il affichera ‘ Failed ’.

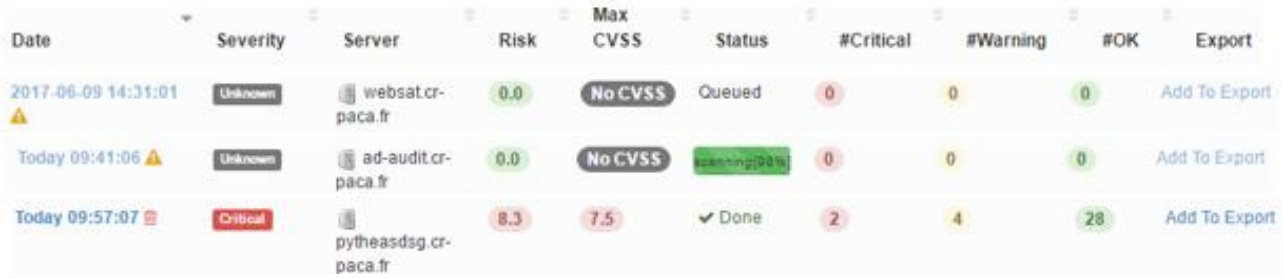


Figure 6 : Les différents états d'un scan

Si on ne rentre pas dans les détails, on peut voir plusieurs choses sur un scan réussi (voir figure 6) :

- L’état de la sécurité sur le serveur qui vient d’être scanné avec succès. Cet état diffère selon le nombre de failles et leur dangerosité. Il peut prendre trois valeurs ; Ok, Warning, ou Critical.

- Le taux de risque, noté sur 10.

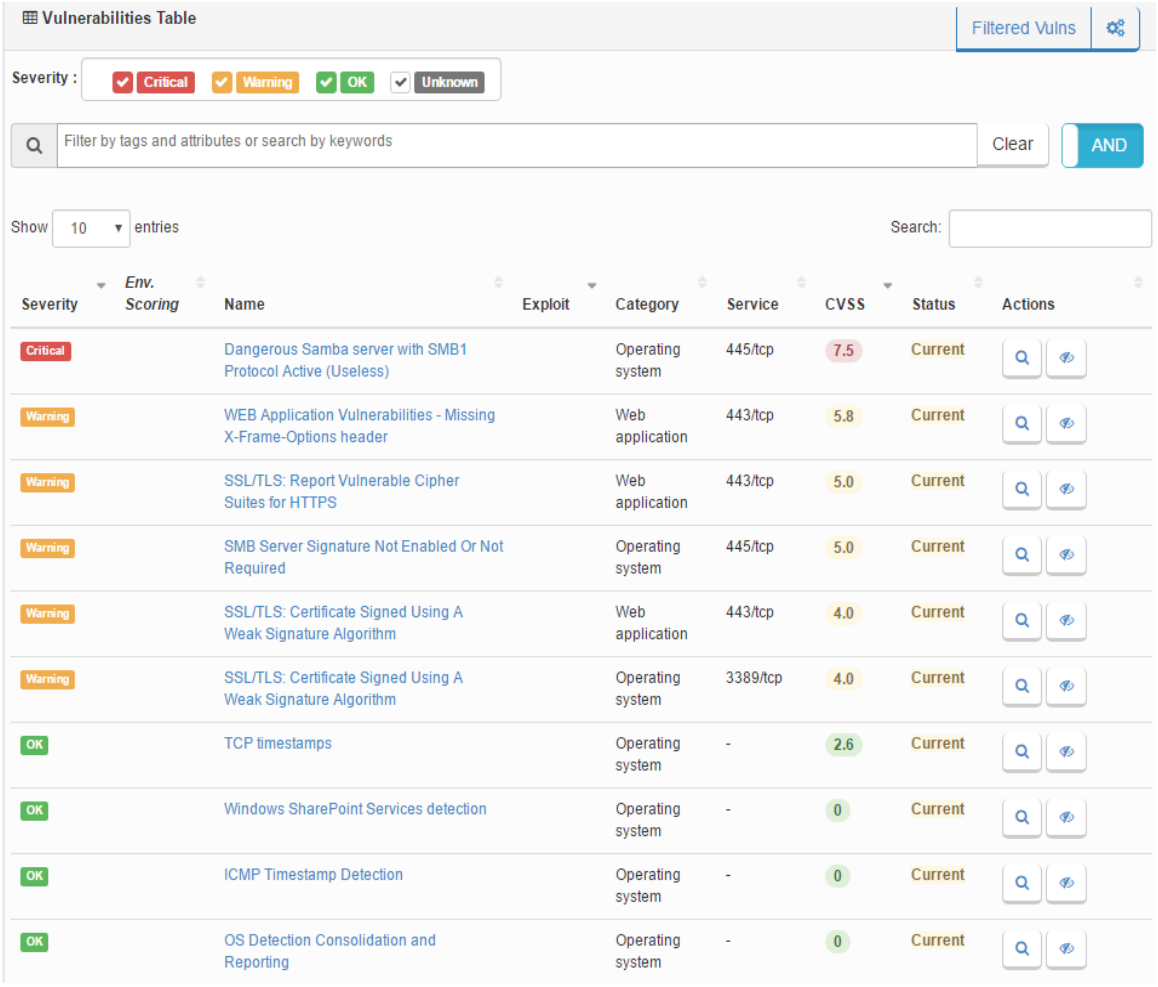
- Le taux maximum de **CVSS** qui est un système d'évaluation standardisé pour déterminer la gravité des vulnérabilités. Il est aussi noté sur 10.

- Le nombre de failles critiques.

- Le nombre de failles alarmantes.

- Le nombre de failles évités.

En cliquant sur la date du scan, nous avons accès à un rapport plus détaillé. Dans ce dernier, il y a le nom de chacune des vulnérabilités détectées, leur gravité, et si elles sont exploitables ou non. (voir figure 7)



Vulnerabilities Table

Filtered Vulns

Severity : Critical Warning OK Unknown

Filter by tags and attributes or search by keywords | Clear | AND

Show 10 entries | Search:

Severity	Env. Scoring	Name	Exploit	Category	Service	CVSS	Status	Actions
Critical		Dangerous Samba server with SMB1 Protocol Active (Useless)		Operating system	445/tcp	7.5	Current	
Warning		WEB Application Vulnerabilities - Missing X-Frame-Options header		Web application	443/tcp	5.8	Current	
Warning		SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		Web application	443/tcp	5.0	Current	
Warning		SMB Server Signature Not Enabled Or Not Required		Operating system	445/tcp	5.0	Current	
Warning		SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		Web application	443/tcp	4.0	Current	
Warning		SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		Operating system	3389/tcp	4.0	Current	
OK		TCP timestamps		Operating system	-	2.6	Current	
OK		Windows SharePoint Services detection		Operating system	-	0	Current	
OK		ICMP Timestamp Detection		Operating system	-	0	Current	
OK		OS Detection Consolidation and Reporting		Operating system	-	0	Current	

Figure 7 : Exemple de rapport plus détaillé

Nous pouvons avoir plus de précisions sur une erreur en cliquant dessus. Une explication de l'erreur, des sources, et une solution envisageable nous sont alors proposées

4.1.1.2 Le monitoring

Contrairement aux scans, le monitoring est basé sur le long terme. Il est synonyme de surveillance et de mesure d'une activité informatique.

En ce qui concerne Elastic Detector, il surveille 41 serveurs du Conseil Régional. Comme évoqué plus haut, la prévention est un point clé de cette solution. Il est défini par une surveillance en continu. Cette dernière se traduit, par la présence d'« auto check », des scans superficiels à intervalle régulier.

Le tableau de bord d'Elastic Detector, rend possible le suivi ininterrompu de l'état de sécurité des serveurs. De plus, plusieurs graphiques nous permettent de connaitre l'évolution du nombre de vulnérabilités et de leur sévérité. (Voir figure 8)

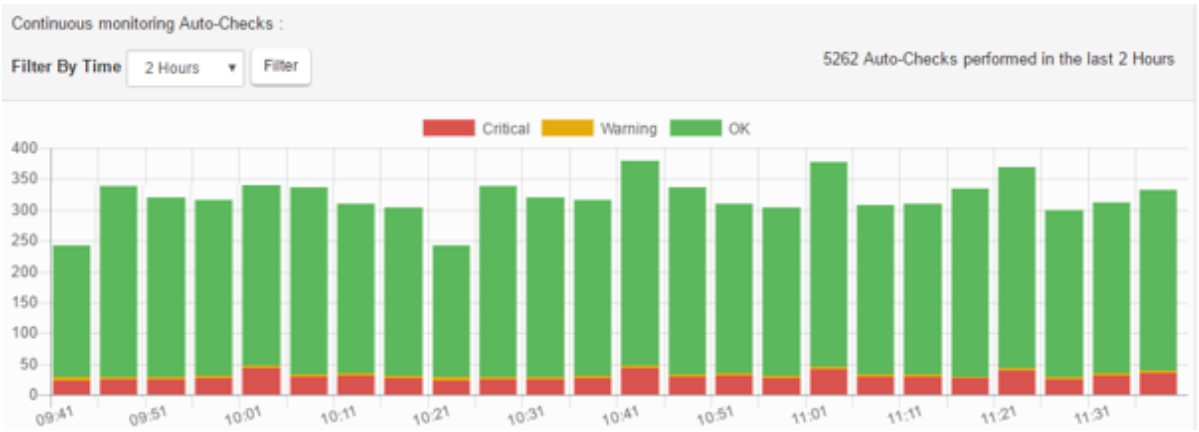


Figure **8** : Histogramme montrant l'évolution du nombre d'erreurs au cours du temps

4.2 Des exemples de vulnérabilités détectées

Elastic Detector détecte toutes sortes de failles de sécurités. Il les classe selon leur niveau de risque, et si elles sont exploitables facilement ou non. C'est à dire, si quelqu'un a déjà publié le code qui permet de les exploiter.

4.2.1 SMB1 Protocol Active

SMB est un protocole présent sur les systèmes Windows afin de gérer l'authentification réseau, que ce soit pour l'accès à des fichiers, le partage d'imprimantes ou encore l'administration à distance.
Il s'occupe des communications entre le client et le serveur, mais aussi des identifiants et mots de passe. Autrement dit, des données critiques qui tomberaient dans de mauvaises mains si le dit serveur est malveillant.

Il existe plusieurs versions de SMB1, SMB1 ou v1.0, SMB2 ou v2.0 et SMB3 ou V3.0 . C'est la première version qui présente un problème, elle présente plusieurs vulnérabilités à des **attaques DoS**, ou bien des attaques dites de «**l'homme du milieu»**. Elles permettent aussi des exécutions de code à distance.

Ces vulnérabilités permettraient de récupérer les identifiants de connexion d'un utilisateur, elle pourrait aussi provoquer le plantage des postes client. Mais ce qui la rend particulièrement dangereuse, c'est qu'elle est facile à exploiter, on peut trouver le code sur des forums de dépôt. Ce qui la rend accessible aux hackers en herbe.

De plus, de nouvelles failles ont été découvertes récemment, mais dans la version 2.0 cette fois. Ces failles ressembleraient beaucoup à celles de la première version. C'est d'ailleurs cette vulnérabilité qui a causé l'attaque informatique massive du week-end du 12 mai. Cette attaque cryptait tous les fichiers d'un ordinateur en demandant une rançon pour les déchiffrer.

Comment s'en protéger ? Il suffit juste de mettre à jour SMB en version 2 ou 3. Sans oublier de désactiver SMB1 qui ne sert qu'à ajouter des vulnérabilités après la mise à jour.

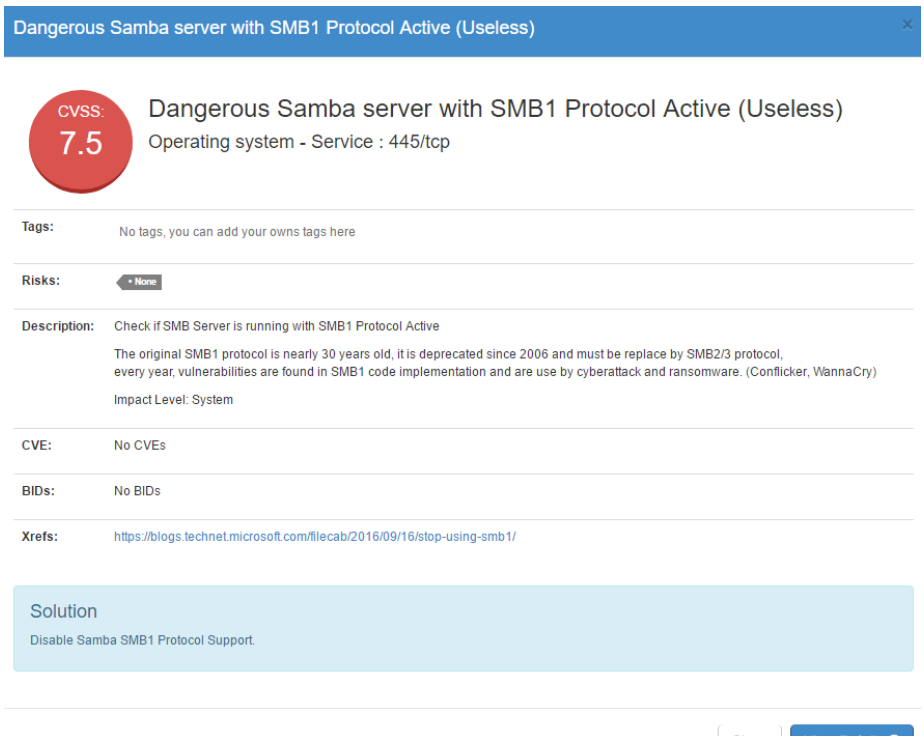


Figure 9 : Exemple de vulnérabilité de SMB1

4.2.2 SSL /TLS FREAK

SSL signifie « Secure Socket Layer », et TLS « Transport Layer Security ». Ces protocoles permettent l'échange de données sécurisées sur internet. Ce protocole est assez ancien puisque sa première version date de 1999 et a été développé par Netscape. A cette époque le **NSA** demandait des **clés publiques de chiffrement RSA** de 512 bits ou moins, afin de pouvoir facilement casser ce chiffrement.

Cependant depuis 2015, les augmentations de la puissance de calcul rendent l'opération de cassage possible par toute personne ayant accès à des ressources informatiques relativement modestes, par exemple via un service de cloud computing. Ce qui créa une faille de sécurité dans les connexions SSL/TLS qui proposent encore le chiffrement « export RSA ». Cette faille lui doit d'ailleurs son nom : «Factoring RSA EXPORT Attack Keys ».

Dans un exemple de connexion sécurisée avec un navigateur, où ce dernier demande un système de chiffrement fort, un pirate peut modifier la demande du navigateur. Le navigateur demanderait alors un système de chiffrement faible comme l'« export RSA ». Et le pirate n'aurait alors aucun mal à décrypter ce code grâce à la méthode de force brute. Cette méthode est d'essayer tous les mots de passe possibles jusqu'à trouver le bon. Suivant la complexité du mot de passe cela peut prendre plus ou moins de temps mais une fois ceci fait, il n'aura plus qu'à accéder aux données autrefois sécurisées.

Comment s'en protéger ? A part vérifier que notre navigateur est bien dans sa dernière version, il n'y a pas vraiment de solution. Cependant, cette faille requiert que de nombreuses conditions soient réunies et à ce titre, elle n'est pas très dangereuse.

4.2.3 OpenSLL HeartBleed

Figure 7 : Logo de la vulnérabilité HeartBleed

OpenSLL est une boite à outils de chiffrement open source en lien avec SSL et TLS. Le nom atypique de cette faille, qui a même un logo (voir figure 7) vient du mode de fonctionnement du logiciel. Il est supposé mettre en œuvre une fonction, appelée « heartbeat », qui maintient la connexion client –serveur même dans le cas où aucune donnée n'est à transmettre.

La faille est du côté du serveur. Il ne fait pas le lien entre le nombre de données indiqué par le client et le nombre actuel de données envoyées.

Ce qui signifie que le client peut indiquer avoir envoyé 42 000 octets de données alors qu'en réalité il n'en a envoyé que 2 000. Le serveur lui renverra les 2 000 octets reçus plus 42 000 octets récupérés de sa mémoire. Dans ces 42 000 octets, il peut y avoir des données sensibles comme des cookies, des mots de passe …

Cette faille est dangereuse car elle présente une manière de récupérer des identifiants qui pourront être ensuite utilisés pour accéder à d'autres fichiers.

Comment s'en protéger ? Il faut tester les différents sites internet grâce à des services en lignes (un exemple (3)) ou des scripts qui permettent de tester si les sites que l'on fréquente ou que l'on administre sont vulnérables. Enfin mettre à jour OpenSLL en attendant qu'un correctif sorte.

4.3 Mon expérience

4.3.1 Les missions

Durant toute la durée du stage, j'ai été appelée à mener à bien différentes missions pour aider à la mise en service de cette solution de supervision réseaux.

Avant la mise en place de la solution :

- Lire l'ensemble de la documentation et l'analyser en détails afin de bien identifier les prérequis nécessaires à l'installation de la solution.
- Préparation de la machine virtuelle (la Région utilise VMWare pour gérer les machines virtuelles) en :
    - Changeant l'adresse IP de la machine virtuelle pour qu'elle corresponde au plan du réseau ;
    - Changeant le nom d'hôte de la machine en « Elastic » ;
    - Configurant le clavier en français, azerty, à la place du qwerty anglais.

Pendant la venue du prestataire chargé de la mise en œuvre :

- Le technicien, M. Renard, est venu pendant une journée pour la mise en service du logiciel et j'ai été chargée de l'accompagner afin qu'il m'explique bien le paramétrage et le fonctionnement et que l'on échange sur les prérequis que j'avais définis.

Après la mise en œuvre :

- Saisir les noms de domaines des 22 sites applicatifs présents sur le **reverse proxy** suivant un document fourni par l'ingénieure réseaux (Mme Rome), joint en annexe 4.
  Il fallait également trouver un moyen de trier les sites par responsables applicatifs. Je suis donc allée dans la partie configuration, puis **credentials**, network du site pour y entrer les noms de domaine. M. Renard, le Technicien, m'avait dit que l'on pouvait insérer plusieurs noms de domaines dans une seule entrée. J'ai essayé, en nommant chaque entrée par le nom du responsable. Cependant, en vérifiant dans l'onglet Infrastructure, le résumé des sites que l'on pouvait scanner, on ne trouvait que le premier nom de domaine alors qu'il aurait dû y en avoir plusieurs.
  J'ai donc changé de stratégie et j'ai fait une entrée par nom de domaine. Par la suite, j'ai utilisé des étiquettes (tag) pour associer les responsables applicatifs aux différents sites qu'ils supervisaient. J'ai enfin créé des catégories pour les sites qui n'avaient pas de responsables applicatifs.
- Ajout de deux serveurs sur des machines virtuelles afin que ces dernières représentent un ensemble de serveurs Linux et un ensemble de serveur Windows. Ensuite j'ai dû trier les différents serveurs découverts selon leurs systèmes d'exploitation. Une fois encore j'ai utilisé des étiquettes pour les différencier.
- Rédaction d'un rapport qui résume les failles de sécurité les plus communes ainsi que les façons d'y remédier. En annexe 5, on trouvera un court résumé de ces failles et des propositions de corrections que j'ai faites.

- Planification des scans. Suivant la demande de M. Murtas, ingénieur réseau, une fréquence d'une semaine a été définie. Tous les dimanches soir, Elastic Detector procède à des scans sur la batterie de sites qu'il surveille.

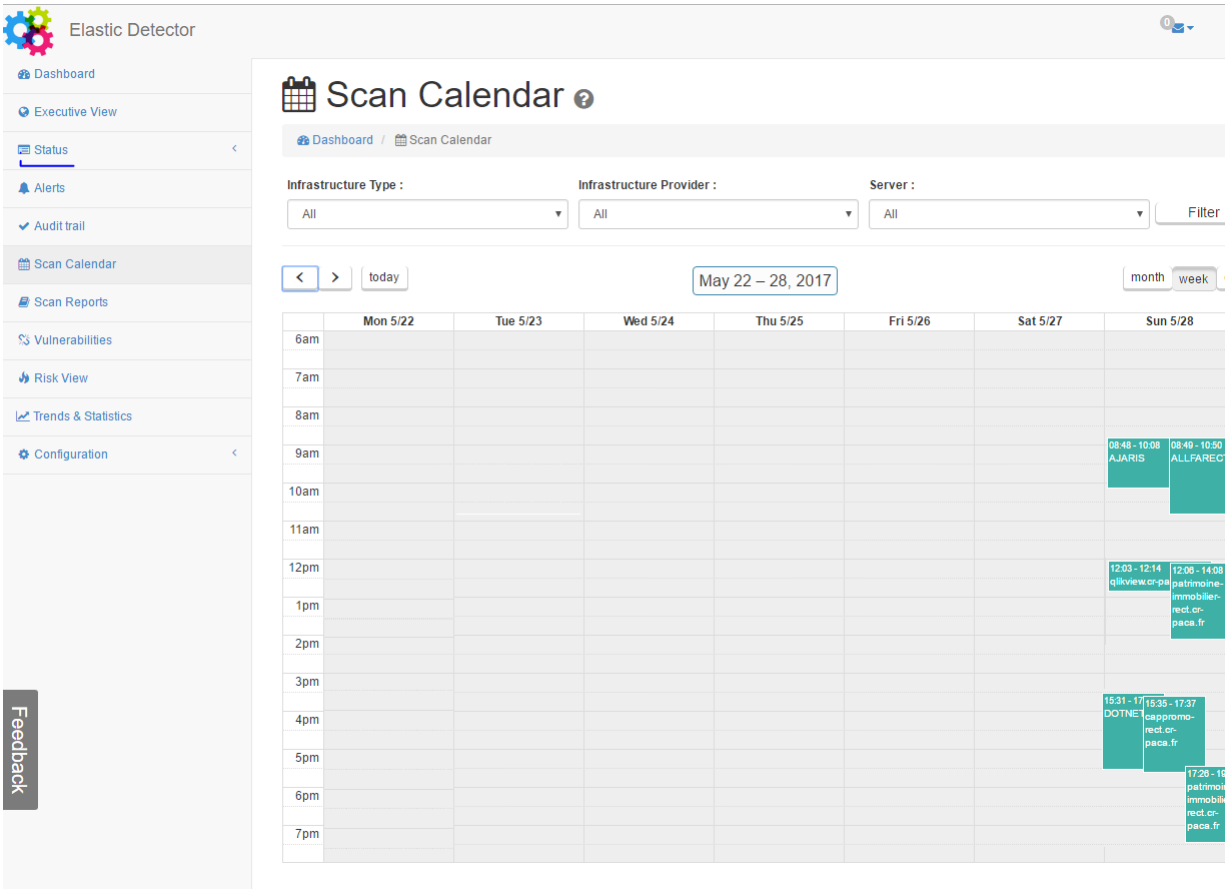


Figure 10 : Le calendrier des scans planifiés

- Test de la sécurité de nouveaux sites. Avant sa mise en production pour la cellule système, un nouveau site doit être recetté et validé. J'ai donc ajouté deux sites, « patrimoine-immobilier-rect.cr-paca.fr » et « cappromo-rect.cr-paca.fr » à la demande de M. Mori, ingénieur système. Je les ai scannés et lui ai renvoyé le rapport en PDF.
- Audits de 14 sites de téléservices, à la demande de M. Murtas. Ensuite, pour chacun d'eux, création d'un rapport sous format Excel (nommé par le nom du site surveillé, voir annexe 2), en omettant les failles jugées non dangereuses par la solution.

Enfin de façon générale, j'ai dû essayer, et la plupart du temps réussir, à résoudre les problèmes durant les scans, les ajouts de sites, la connexion au serveur, etc...

4.3.2 Les problèmes rencontrés et les résolution apportées

Lors de mes différentes missions, j'ai du faire face à plusieurs problèmes, certains était facile à résoudre, d'autres plus complexes et il y a certains d'entre eux dont je ne connais toujours pas la résolution.

Tout d'abord, durant l'installation par le prestataire, nous avions eu plusieurs ennuis. Une des fonctionnalité d'Elastic Detector était de pouvoir se connecter avec un compte de l'**Active Directory** de la DSI. Sauf que cette connexion ne fonctionnait pas, nous avons donc dû créer un compte sans lien avec l'Active Directory. L'incident a été reporté au service Recherche et Développement de SecludIt et nous n'avons pas eu de nouvelles depuis.

De même, il y a la possibilité de créer des utilisateurs à partir du compte administrateur pour leur donné le droit de consultation. M. Renard en créer un pour l'exemple, il le supprime mais impossible alors de recréer un compte utilisateur avec la même adresse. Il a dû effacer et recréer l'utilisateur en ligne de commande. Et nous a garantie que bientôt il y allait avoir un patch qui corrigerais ces erreurs.

Par la suite, nous eûmes un problème qui nous pris beaucoup de temps à résoudre. Elastic Detector permet de s'authentifier sur le site qu'il veut scanner, cependant cette authentification n'est pas obligatoire, elle permet juste de faire des analyses plus complètes.

Elle se fait sous forme ;

Login : NomDeDomaine/Identifiant

Password: MotDePasse

Cette authentification utilise le protocole SMB. D'un autre côté, plusieurs sites présenter une vulnérabilité concernant l'identification SMB. (Et mon tuteur pensait que c'était un faux positif. C'est-à-dire une erreur qui n'en n'est pas une.) Nous nous sommes dit que la faille devait être lier à authentification par SMB. Donc nous avons cherché comme régler ce problème.

Au début, nous avons pensé que la solution ne s'authentifier pas sur le serveur, car VmTools n'était pas installer. VmTools est un ensemble de mises à jour et de pilotes pour VMWare. Mais l'identification ne marchait toujours pas.

Par la suite, nous avons installé le patch fournit par M. Renard qui était censé être la solution. Ce ne fut pas concluant.

Puis, comme nous ne trouvons pas de solution. M. Murtas, et moi, nous avons assister à une vidéo conférence par Skype avec le prestataire, M. Renard.

Il nous a d'abord proposer d'inscrire le nom de domaine « cr-paca.fr » directement dans le code pour qu'il reste uniquement l'identifiant à rentrer.

Cela ne marcha pas mieux.

Enfin, il trouva la solution en cherchant dans la partie du code qui permettait de s'identifier. Le problème venait du mot de passe utilisé. Ce dernier était du type : « 1234$password »[1]. Cependant le signe ' $ ' est utilisé pour la lecture de variable en **Bash**. Donc « $password » signifiait lire la variable password, sauf que cette dernière n'hésitait pas et qu'il n'y avait aucun sens à avoir une lecture de variable dans un mot de passe.

M. Renard résolu ce problème en mettant le mot de passe attendu entre guillemet pour le ' $' ne soit plus détecté.

Quelque temps après, nous avons rencontrés un autre problème qui reste en partie non résolu. En regardant les résultats des scans fait sur des sites en recettes, je me suis rendu compte que la plupart avait échoué. J'ai donc refait un scan d'un des sites qui avait échoué, et il échoue de nouveau. En vérifiant les serveurs M. Murtas à remarquer que certain été éteint donc cela a permis de résoudre une partie du problème. Car une fois ces derniers rallumé, les scans des sites associés se sont remis fonctionné. Mais une partie des sites continua a échoué, sans que l'on trouve une explication.

Le dernier problème que j'ai résolu fut assez simple. Les sites que je voulais auditer ne se lancer pas et rester en 'Queue' c'est-à-dire en attente alors que c'était le seul qui exécuter. Je trouvais l'explication en me reconnectant sur le compte monitoring, ou là il y avait bien plusieurs sites en train d'être scanner. Je les ai donc arrêtées, pour pouvoir commencer les audits que j'avais à faire.

Conclusion

Mon stage au service Réseaux et Télécommunications du Conseil Régional Provence-Alpes-Côte d'Azur à Marseille, sous la responsabilité de l'administrateur et tuteur Mr Ruffin Jean-Michel a été une véritable expérience professionnelle et personnelle qui m'a beaucoup apporté. En cela ça a été pour moi une réussite.

J'ai eu l'opportunité de pouvoir suivre le déroulement entier d'un projet, du cahier des charges jusqu'à la finalisation et l'utilisation de cette solution de supervision réseau.

Malheureusement je ne serai pas là pour voir ce qu'apporteront les mises à jour, mais je sais d'ores et déjà ce qu'elles vont ajouter de plus. Comme, par exemple, la possibilité de trier automatiquement les rapports de scan pour les envoyer par la suite au bon responsable...

Ce project m'a permis de gérer des obstacles multiples, de prendre des initiatives, de reconnaître une hiérarchie, de la respecter, d'avoir une vision plus mûre d'un vrai travail responsable, et ainsi, de m'intégrer complètement au monde de l'entreprise.

Ce stage m'a aussi apporté des connaissances techniques sur le fonctionnement d'un réseau en entreprise, comme par exemple les différentes procédures de sauvegardes qu'il peut avoir, et comment elles permettent de protéger un réseau en cas de perte matérielle.

Enfin, ce projet m'a permis de découvrir un autre aspect de l'administration réseau.
En revanche, il m'a conforté dans mon idée que je préférerais envisager une carrière informatique axée sur le développement, plutôt qu'une carrière dans les réseaux. Cela dit, cela ne gâche en rien le très vif intérêt que j'ai porté à ce stage, et son apport à ma culture générale...

Glossaire

Définitions classées par ordre d'apparition.

SATA : (Serial Advanced Technology Attachement) Les disque durs SATA sont plus gros mais plus capacitif. C'est à dire qu'ils peuvent contenir plus de données.

SAS : (Serial Attached SC SI) Les disques durs SAS sont plus petits mais plus rapide, et donc sont utilisé pour les actions rapides.

VLAN : (Virtual Local Area Network) . Un réseau local virtuel, est un réseau informatique logique indépendant.

WAF : (Web Application Firewall) est un système de sécurité qui contrôle le trafic entrant et sortant des applications et sites Web.

Adresse IP (Internet Protocol) : Suite de numéros qui identifie un ordinateur, ou tout matériel informatique (routeur, imprimante) sur un réseau public ou privé.

Audits : Un audit est comme un scan mais en beaucoup plus approfondie et développé.

Asset : Terme anglais pour désigner une ressource numérique, qu'il est possible de réutiliser, dont on peut envisager une exploitation générique.

Malwares : Terme anglais signifiant nuisible / Malveillant. En somme un "malware" est donc un logiciel pouvant être un virus.

veille informatique : Activité qui consiste à se tenir au courant des avancées technologiques dans le domaine de l'informatique afin de tirer parti de ses avancées le plus rapidement possible.

infections zéro days : est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu.

ANSSI

OWASP

PCI Security

VMware Vsphere : Nom de marque de la famille de produits de virtualisation de VMware. Permet aux utilisateurs de se connecter à distance à vCenter Server, depuis n'importe quel PC Windows.

Vcenter : Point de contrôle central destiné aux services du datacenter, tels que le contrôle des accès, la surveillance des performances et la gestion des alarmes.

CVSS : Système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables. Cette évaluation est constituée de 3 mesures appelées métriques : la métrique de base, la métrique temporelle et la métrique environnementale.

SMB (Server Message Block) : Protocole permettant le partage de ressources (fichiers et imprimantes) sur des réseaux locaux avec des PC sous Windows.

attaques DoS (Denial of Service) : Le déni de service est une attaque qui vise à rendre une application informatique incapable de répondre aux requêtes de ses utilisateurs. Les serveurs de messagerie peuvent être victimes de ces attaques.

attaques dites de l'homme du milieu C'est un attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis.

Clé publique : Encodage rendu public dans le cadre d'un échange d'informations utilisant le principe de la cryptographie asymétrique. Un des rôles de la clé publique est de permettre le chiffrement ; c'est donc cette clé qu'utilisera Bob pour envoyer des messages chiffrés à Alice. La clé privée sert à déchiffrer.

Chiffrement RSA : Algorithme de cryptographie asymétrique, très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet.

reverse proxy : est un type de serveur, habituellement placé en frontal de serveurs web. Contrairement au serveur proxy qui permet à un utilisateur d'accéder au réseau Internet, le proxy inverse permet à un utilisateur d'Internet d'accéder à des serveurs internes.

Credentials : Un credential c'est un objet qui permet de s'authentifier. En général c'est un login/mot de passe/domaine.

Active Directory : C'est la mise en œuvre par Microsoft des services d'annuaire pour les systèmes d'exploitation Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

Bash (Bourne-Again Shell) : Langage de programmation sous forme de script.

Sources

Elastic Detector

https://elastic-detector.secludit.com/

DenyAll

https://www.denyall.com/fr/produits/web-application-firewall/

Qualys

https://www.qualys.com/

SMB

http://www.itespresso.fr/securite-it-protocole-smb-problematique-windows-93746.html#

https://www.it-connect.fr/arretez-dutiliser-smb-v1-0/

https://www.developpez.com/actu/83907/ReDirect-to-SMB-Windows-menace-par-une-faille-vieille-de-18-ans-Windows-10-serait-aussi-affecte-Microsoft-relativise/

http://www.itespresso.fr/securite-it-protocole-smb-problematique-windows-93746.html

https://www.tutos-informatique.com/virus-wanna-cry/

http://www.zdnet.fr/actualites/faille-windows-apres-wannacry-voici-adylkuzz-specialiste-du-cryptomining-39852564.htm

SSL /TLS Freaks

https://www.nextinpact.com/news/93310-faille-freak-quand-connexions-ssltls-se-contentent-dun-chiffrement-rsa-sur-512-bits.htm

http://thehackernews.com/2015/03/freak-openssl-vulnerability.html

https://www.us-cert.gov/ncas/current-activity/2015/03/06/FREAK-SSLTLS-Vulnerability

HeartBleed

http://www.lemonde.fr/technologies/article/2014/04/09/une-enorme-faille-de-securite-dans-de-nombreux-sites-internet_4397995_651865.html

http://www.orange-business.com/fr/blogs/securite/webtech/openssl-faille-heartbleed-comprendre-et-se-proteger

Table des illustrations

Annexes

Annexe 1 : Diagramme général du Conseil Régional au 1 er Février 2017

Annexe 2 : Exemple de rapport Excel

Elastic Detector®
Scan Report on Multiple Servers
Date: 2017-06-22 11:04:28

Name	Criticity	Risk	Exploit?	CVSS	Custom	Service	Server	Status	Description	Solution
Dangerous Samba server with SMB1 Protocol Active (Useless)	error	3		7.5		445/tcp	partimoine-immobilier-rect.cr-paca.fr	Current	Check if SMB Server is running with SMB1 Protocol Active The original SMB1 protocol is nearly 30 years old, it is deprecated since 2006 and must be replace by SMB2/3 protocol. every year, vulnerabilities are found in SMB1 code implementation and are use by cyber-attack and ransomware (ComRaker, WannaCry)	Disable Samba SMB1 Protocol Support.
SMB Server Signature Not Enabled Or Not Required	warning	2		5.0		445/tcp	partimoine-immobilier-rect.cr-paca.fr	Current	Check if SMB Server Use Signed message The SMB server does not support SMB message signing or it is not required. The server is vulnerable to man-in-the-middle attacks or SMB relay attacks. CVSS Severity: CVSS Base Score: 5.0 (AV:N/AC:L/Au:M/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 10.0 References: http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx http://support.microsoft.com/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html SMB1/V1 is available but the SMB message signing is not required SMB2/V2 is available but the SMB message signing is not required SMB3/V3 is available but the SMB message signing is not required	Force Server to use SMB message signing On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	warning	2	4.0			3389/tcp	partimoine-immobilier-rect.cr-paca.fr	Current	The remote service is using a SSL/TLS certificate chain that has been signed using a cryptographically weak hashing algorithm. The following certificates are part of the certificate chain but using insecure signature algorithms: Subject: CN=.ALLFAIRECT.cr-paca.fr Signature Algorithm: sha1WithRSAEncryption	Servers that use SSL/TLS certificates signed using an SHA-1 signature will need to obtain new SHA-2 signed SSL/TLS web browser SSL/TLS certificate warnings.