Gestion et remédiation des risques, alertes IDS et failles de sécurité

ACRONYME	GERRAS
MANDANT	Syselcom Mutuelle Informatique SA - Vincent Emery
ÉTUDIANT-E-S	Dylan Müller
PROFESSEUR-E-S	François Buntschu et Rudolf Scheurer
EXPERT-E	Pascal Graber et Sylvain Luiset
No	B19T10
TYPE	Projet de Bachelor
CONTACT	muller.dylan96@gmail.com

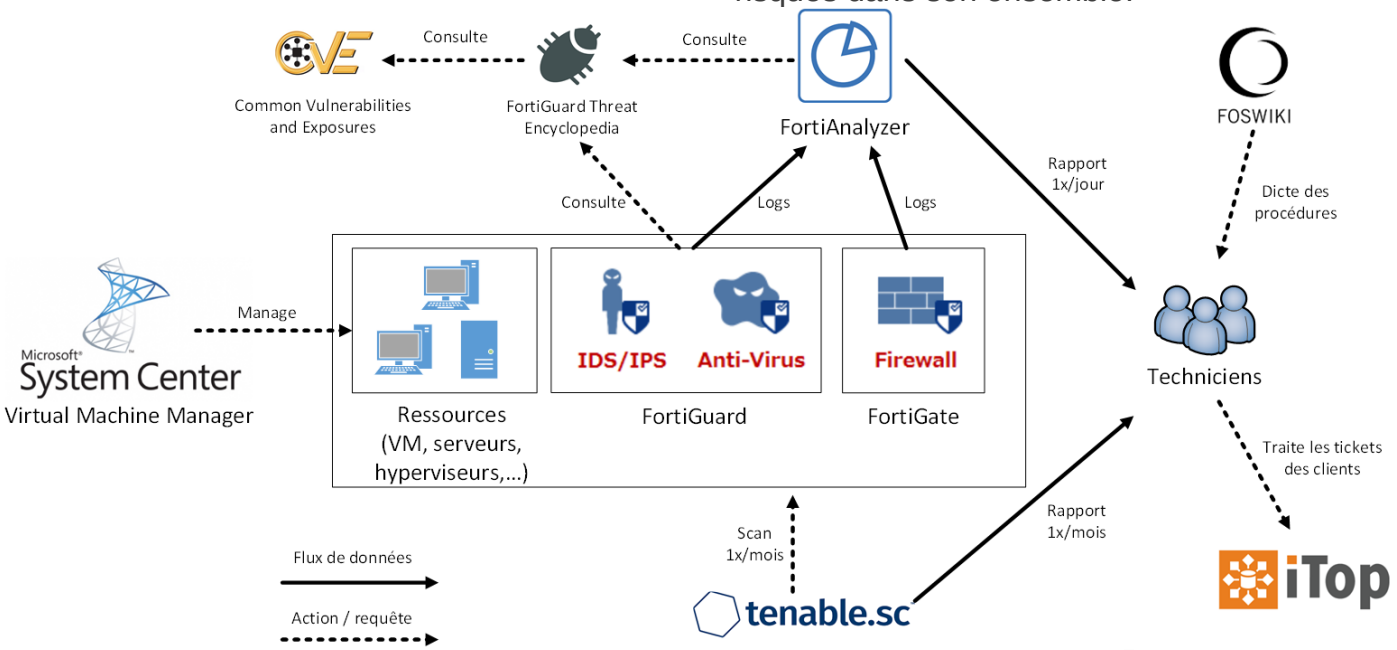
Contexte

Syselcom Mutuelle Informatique SA est un hébergeur de type Cloud. Petite entreprise de 20 employés, elle exploite néanmoins de grosses infrastructures réparties dans deux datacenters ou sont stocké les données de près de 200 clients.

Certifiée ISO 27001, la sécurité de l'information fait partie intégrante des activités quotidiennes de ses employés. Afin de se protéger contre les menaces et les cyber-attaques, des systèmes de détection et de prévention d'intrusions sont en placent et des scanners de vulnérabilités analysent en permanence les serveurs pour y trouver des failles de sécurité. Des alertes et des rapports sont envoyés quotidiennement par ces outils.

Le problème est que les techniciens passent beaucoup à analyser les rapports et les alertes afin de déterminer les mesures à prendre et que la méthodologie actuelle n'est pas idéale.

L'objectif global de ce projet est de réaliser un processus de gestion et de remédiation des risques dans son ensemble.



Classification des ressources, des risques et incidents

Le système de classification des ressources, des risques et incidents de l'entreprise a été analysé et retravaillé. Il est en effet important d'avoir une classification efficace afin de savoir quelles mesures de sécurité appliquer et prioriser le traitement des risques et incidents

La classification des ressources se fait selon la criticité et l'exposition aux risques de celle-ci. Le type de ressource est également pris en compte. Des mesures de sécurité préventives seront appliquées sur la ressource en fonction de cette classification.

La classification des risques et incidents se dait grâce au scoring CVSS, en prenant en compte l'impact sur la confidentialité, l'intégrité et la disponibilité des données. Le traitement du risque et de l'incident sera priorisé en fonction de sa sévérité.

Gestion des rapports

Les techniciens reçoivent régulièrement des rapports donnant des informations concernant l'état de la sécurité des équipements de l'entreprise.

Un des buts du projet étant d'automatiser la recherche d'informations et de générer un rapport complet avec toutes les informations dont les techniciens ont besoin.

Pour cela, des sources d'informations seront consultées grâce à un script qui requête les API de celles-ci et intègre les informations directement dans le rapport.

Rapport d'audit

Il est important que l'entreprise contrôle régulièrement si son infrastructure est bien sécurisée et si ce n'est pas totalement le cas d'appliquer des mesures de sécurité pour corriger les failles. Un nouveau rapport a donc été pensé afin d'avoir un aperçu de ce qu'Internet voit des adresses IP publiques de l'entreprises.

Pour cela, un script va générer un rapport en requêtant l'API de Shodan, un moteur de recherche d'adresses IP scannant régulièrement tout Internet afin de fournir des informations sur les adresses IP, comme sa localisation, ses ports ouverts ou les vulnérabilités détectées sur celles-ci. La consultation de ce moteur de recherche sur les adresses IP publique de l'entreprise nous fournit donc des informations importantes sur celles-ci concernant la sécurité.

#	Attack Source	Counts
1	185.48.149.115	1,322
2	66.240.205.34	42
3	219.234.5.48	42
4	78.106.165.138	37
5	178.87.69.105	28
6	94.28.122.134	28

#	IP Address	Name / Owner	Location	Reputation	Score	Counts
1	193.56.28.120	No data / sprint S.A.	United Kingdom	OK	1.76	349
2	111.230.252.45	No data / Shenzhen Tencent Computer Systems Company Limited	China	OK	1.65	329
3	120.52.152.16	No data / China Unicom IP network	China	Attacker	5.27	121
4	190.203.251.242	190-203-251-242.dyn.dsl.cantv.net / CANTV Servicios, Venezuela	Venezuela	OK	1.54	84