Professionele Bachelor Toegepaste Informatica

Systems & Networks

ONDERZOEK NAAR DE APPLICATIES EN HULPMIDDELEN VOOR HET OPSTARTEN VAN EEN SECURITY OPERATIONS CENTER

Stef Collart

Promotoren:

De heer Joris Meylaers — Data Unit nv
De heer Aubrey Beelen — Data Unit nv
De heer Peter Vaes — Hogeschool PXL Hasselt

Bachelorpaper Academiejaar 2017 - 2018

Professionele Bachelor Toegepaste Informatica

Systems & Networks

ONDERZOEK NAAR DE APPLICATIES EN HULPMIDDELEN VOOR HET OPSTARTEN VAN EEN SECURITY OPERATIONS CENTER

Stef Collart

Promotoren:

De heer Joris Meylaers — Data Unit nv
De heer Aubrey Beelen — Data Unit nv
De heer Peter Vaes — Hogeschool PXL Hasselt

Bachelorpaper Academiejaar 2017-2018

Dankwoord

Dit eindwerk is tot stand gekomen in het kader van de opleiding ‘Bachelor in de Toegepaste Informatica’ aan de PXL met afstudeerrichting ‘Systems & Networks’. Gedurende mijn opleiding heb ik kennis gemaakt met en inzicht gekregen in de verschillende aspecten van het vakgebied informatica. De stageopdracht ligt in lijn met mijn interesse voor het security aspect van informatica die ik tijdens mijn studiejaren aan de PXL heb ontwikkeld. De mogelijkheid om dit eindwerk tot een goed einde te brengen heb ik te danken aan vele personen. Enkele van hen wil ik via deze weg bedanken.

In de eerste plaats wil ik Data Unit bedanken voor de mogelijkheid om stage te lopen binnen het bedrijf. Binnen Data Unit wil ik voornamelijk mijn stagebegeleiders, de heer Joris Meylaers en de heer Aubrey Beelen bedanken voor de begeleiding.

Zeker wil ik ook nog mijn hogeschoolpromotor, de heer Peter Vaes, bedanken voor de begeleiding en het beantwoorden van mijn vragen met betrekking tot het eindwerk en mijn onderzoek.

Eveneens zou ik mijn vrienden en medestudenten willen danken voor alle steun en hulp. Ten slotte zou ik graag mijn ouders willen bedanken voor alle steun en de mogelijkheid om deze opleiding te volgen en af te ronden.

Abstract

Data Unit is een netwerk- en securitybedrijf met kantoren in Lummen, Brussel en Nederland. Om betere en extra diensten aan hun klanten te kunnen aanbieden wil men graag een Security Operations Center opzetten. In dit eindwerk worden er verschillende tools en applicaties onderzocht die nodig zijn om een Security Operations Center op te starten. Deze verschillende tools en applicaties moeten een aanvulling worden op de reeds gebruikte securityproducten.

In het onderzoeksrapport wordt er dieper ingegaan op de verschillende Security Information and Event Management (SIEM) producten die tijdens de stage gebruikt zijn. Een SIEM is namelijk een cruciaal onderdeel van een Security Operations Center om alle logs en informatie van toestellen binnen het netwerk te centraliseren en aan elkaar te koppelen.

Inhoudsopgave

Inhoud

Dankwoord 2

Abstract 3

Inhoudsopgave 4

Lijst van gebruikte figuren 6

Lijst van gebruikte tabellen 6

Lijst van gebruikte afkortingen 7

Verklarende woordenlijst 7

Inleiding 8

I. Stageverslag 9

1 Bedrijfsvoorstelling 9

2 Security Operations Center 10

2.1 Doel 10

2.2 Werking 10

2.3 Voordelen 11

2.3.1 Alle informatie centraal beschikbaar 11

2.3.2 Drastisch verlagen van de responstijd 11

2.3.3 Uitgebreidere en snellere analysemogelijkheden 11

2.3.4 Verhinderen gelijkaardige infecties in de toekomst 11

2.3.5 GDPR 12

2.4 Nadelen 12

2.4.1 Personeel 12

2.4.2 Extra systemen 13

3 Tools en applicaties 14

3.1 Huidige beveiligingstools 14

3.1.1 Barracuda Networks 14

3.1.2 Kaspersky Lab 15

3.2 Geteste beveiligingstools 16

3.2.1 Intrusion Detection System 16

3.2.2 Vulnerability Scanner 18

3.2.3 Log Management 19

3.2.4 Security Information and Event Management 20

4 Testfases 23

4.1 Fase 1 23

4.2 Fase 2 25
4.3 Fase 3 27
II. Onderzoekstopic: Vergelijking SIEM-oplossingen 30
1 Probleemstelling 30
2 Methode van onderzoek 30
2.1 Geteste SIEM-oplossingen 30
2.2 Aspecten van het onderzoek 30
3 Literatuurstudie 31
3.1 Solarwinds: Log & Event Manager 31
3.1.1 Belangrijkste functies en mogelijkheden 31
3.1.2 Correlatie van data 32
3.1.3 Vergelijking van kostprijs 33
3.1.4 Aanpassingsmogelijkheden van alerts 33
3.1.5 Gebruiksgemak en leercurve 33
3.1.6 Mogelijkheid om SIEM-as-a-service aan te bieden aan klanten 33
3.2 IBM QRadar SIEM 34
3.2.1 Belangrijkste functies en mogelijkheden 34
3.2.2 Correlatie van data 35
3.2.3 Vergelijking van kostprijs 35
3.2.4 Aanpassingsmogelijkheden van alerts 35
3.2.5 Gebruiksgemak en leercurve 36
3.2.6 Mogelijkheid om SIEM-as-a-service aan te bieden aan klanten 36
3.3 Alienvault Unified Security Management 37
3.3.1 Belangrijkste functies en mogelijkheden 37
3.3.2 Correlatie van data 38
3.3.3 Vergelijking van kostprijs 38
3.3.4 Aanpassingsmogelijkheden van alerts 38
3.3.5 Gebruiksgemak en leercurve 39
3.3.6 Mogelijkheid om SIEM-as-a-service aan te bieden aan klanten 39
3.4 Vergelijkingsmatrix van de functionaliteiten 39
4 Conclusie 40
5 Reflectie 42
6 Bibliografie 43

Lijst van gebruikte figuren

Figuur 1: Werking SIEM 10
Figuur 2: Onderverdeling SOC-personeel en hun taken 13
Figuur 3: Logo Barracuda [5] 14
Figuur 4: Logo Kaspersky Lab [8] 15
Figuur 5: Logo Snort [48] 16
Figuur 6: Logo Suricata [13] 17
Figuur 7: Logo OpenVAS [16] 18
Figuur 8: Logo Splunk Light [18] 19
Figuur 9: Logo Solarwinds [21] 20
Figuur 10: Realtime event correlatie Solarwinds 20
Figuur 11: Logo IBM [24] 21
Figuur 12: Logo Alienvault [26] 22
Figuur 13: Kill Calculator.exe rule 23
Figuur 14: Oinkmaster configuratie met oinkcode 23
Figuur 15: Snort ping detectie 24
Figuur 16: Suricata BlackSun detectie 24
Figuur 17: High severity vulnerabilities Solarwinds 25
Figuur 18: QRadar genormaliseerde firewall logs 26
Figuur 19: QRadar Bruteforce Offense 26
Figuur 20: Bruteforce top 5 events 26
Figuur 21: OTX informatie beschikbaar van IP-adressen 27
Figuur 22: Alienvault instellen vulnerability scan 28
Figuur 23: Alarm tijdens vulnerability scan 28
Figuur 24: Overzicht alarm 29
Figuur 25: Alarmen gerangschikt volgens Cyber Kill Chain 29

Lijst van gebruikte tabellen

Tabel 1: Vergelijking SIEM-oplossingen 39
Tabel 2: Vergelijking van kostprijs 40

Lijst van gebruikte afkortingen

SOC	Security Operations Center
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
SIEM	Security Information and Event Management
GDPR	General Data Protection Regulation
EPS	Events Per Second
MSP	Managed Service Provider
OISF	Open Information Security Foundation
NSM	Network Security Monitoring
OpenVAS	Open Vulnerability Assessment System
NVT	Network Vulnerability Test
OTX	Open Threat Exchange
CVE	Common Vulnerabilities and Exposures
DSM	Device Support Modules
HIDS	Host Intrusion Detection System

Verklarende woordenlijst

Command-and-control server	Een server waarmee aanvallers kunnen communiceren met door hun overgenomen systemen
Intrusion Detection System	Een systeem dat het netwerk monitort op kwaadaardig en verdacht netwerkverkeer
Intrusion Prevention System	Een systeem dat al het passerende netwerkverkeer controleert op kwaadaardig en verdacht netwerkverkeer
Deep packet inspection	Een netwerk pakket filter methode waarbij elk pakket uitgelezen wordt en gecontroleerd op inhoud
Agent	Een softwareprogramma dat hoort bij een SIEM-oplossing dat lokaal op een pc of server wordt geïnstalleerd

Inleiding

Tijdens mijn studies aan de Hogeschool PXL ben ik steeds meer geïnteresseerd geraakt in het security aspect van IT. Via de interesse in security ben ik uitgekomen bij het bedrijf Data Unit. Eind 2016 en midden 2017 heb ik reeds bij Data Unit gewerkt als jobstudent. Op deze manier was ik dus al goed bekend met het bedrijf en zijn werknemers. Mijn stage bij dit bedrijf lopen was dus een voor de hand liggende keuze.

Na een brainstorm sessie en een interne rondvraag over mogelijke stageopdrachten is dit onderwerp en bijhorend onderzoek uit de bus gekomen. Hierbij is er gekeken naar wat mijn interesses zijn en waar Data Unit op dit moment en in de toekomst nood aan heeft.

Wegens de steeds toenemende cyberdreiging waar de vraag verschuift van “Wordt mijn bedrijf aangevallen?” naar “Wanneer wordt mijn bedrijf aangevallen?” is er een steeds grotere noodzaak om over een Security Operations Center te beschikken. De aankomende nieuwe GDPR-wetgeving speelt hier ook een zekere rol in.

Bij een Security Operations Center heb je 3 grote factoren: personeel, *workflow* en technologie. Al deze factoren moeten op elkaar aansluiten om tot een goed werkend SOC te komen. In dit eindwerk wordt dieper ingegaan op het technologische aspect waarbij een aantal verschillende tools getest worden die nodig zijn om een SOC op te starten.

In het onderzoek gedeelte wordt er dieper ingegaan op de verschillende Security Information and Event Management *tools* die ik gebruikt heb tijdens deze stage.

I. Stageverslag

1 Bedrijfsvoorstelling

Data Unit is een bedrijf met een grote expertise in netwerk- en securityoplossingen.

Op vlak van netwerken biedt Data Unit hardware en services voor *switching* en *wireless*. Hiervoor werkt Data Unit samen met een aantal vaste leveranciers zoals HP Enterprise en Huawei. Data Unit kan voor zowel kleine bedrijven als voor grote *enterprise* omgevingen oplossingen aanbieden. Voor alle verschillende soorten omgevingen kunnen oplossingen aangeboden worden.

Deze oplossingen gaan van het ontwerpen van snelle, betrouwbare en veilige Netwerk/Security/Unified Communications oplossingen tot het installeren en onderhouden hiervan. Hierbij wordt er nog een nadruk gelegd op het bieden van toegevoegde waarde (*managed services*) aan de klanten.

Op vlak van netwerksecurity heeft Data Unit expertise bij de volgende fabrikanten: Barracuda Networks, Palo Alto, Kaspersky Lab en Pulse Secure.

Hier biedt Data Unit zowel *hosted services* als oplossingen *on-premise* aan. De belangrijkste producten hier zijn: firewalls, antivirus, antispam, VPN & WAN connectiviteit en data security.

De klanten van Data Unit bevinden zich zowel in de privésector als overheidsinstanties. In de privésector zijn het voornamelijk bedrijven met 20 tot 1000 werknemers. Bij de overheidsinstanties gaat dit van lokale gemeentebesturen tot OCMW en Vlaamse/federale overheidsinstellingen. Ook binnen Nederland is Data Unit actief in deze sectoren.

Het merendeel van de klanten van Data Unit bevindt zich dus in de mkb-markt met enkele uitschieters in beide sectoren. Een voorbeeld van enkele van deze klanten zijn: Air France, Carglass, De Lijn, Infrabel en VDAB.

2 Security Operations Center

2.1 Doel

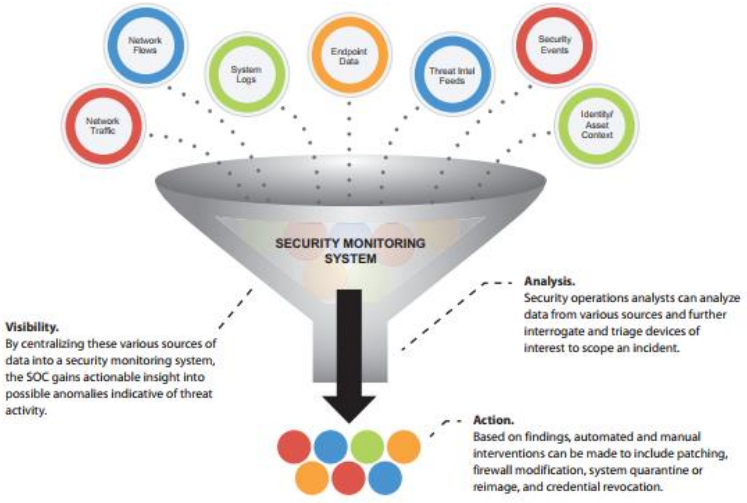
Met een Security Operations Center krijg je als organisatie vele extra mogelijkheden om dreigingen en incidenten binnen het bedrijfsnetwerk te detecteren. In een Security Operations Center kunnen ook inkomende dreigingen van buitenaf snel gedetecteerd en tegengehouden worden voor ze een echt gevaar betekenen voor de continuïteit van het bedrijf. Bij een Security Operations Center wordt alle informatie gecentraliseerd zodat de nodige informatie overzichtelijker en sneller beschikbaar is wanneer vereist.

2.2 Werking

Een bedrijf heeft meestal meerdere beveiligingslagen geïnstalleerd om dreigingen van buitenaf tegen te houden. De twee meest voorkomende zijn een *firewall* en een antivirusproduct die op de computers en laptops van de werknemers draaien. Deze verschillende beveiligingslagen complementeren elkaar maar werken allemaal afzonderlijk van elkaar op basis van beveiliging. Elk beveiligingsproduct genereert zijn eigen logs die bij een incident dienen nagekeken te worden. Dit vergt veel tijd en is behoorlijk omslachtig. Met de opkomst van steeds meer geavanceerde malware voldoet de oude manier van beveiligen niet meer. De malware weet namelijk elk apparaat afzonderlijk te omzeilen.

Bij een Security Operations Center wordt er gebruik gemaakt van een security information and event management systeem. Een SIEM-systeem is echter geen alleenstaand product. De goede werking hiervan is afhankelijk van de data die het systeem aangeleverd krijgt. Men gaat dus alle verschillende logs naar het SIEM systeem sturen. Dit kan zo uitgebreid als je zelf wenst en je SIEM toestaat. De meest voor de hand liggende zijn uiteraard de logs van je *firewall* en antivirus. SIEM systemen zijn er op voorzien om logs van enorm veel verschillende producten te ontcijferen en correct te interpreteren. Zo kan je de logs van je *active directory*, *intrusion detection system*, *switches*, routers en *vulnerability scanners* naar je SIEM sturen, om er maar enkele te noemen. Een SIEM-systeem staat dus centraal in een SOC.

Op basis van al de informatie die het SIEM-systeem binnenkrijgt, kan het beginnen met de data aan elkaar te koppelen. Het aan elkaar koppelen van deze data noemt men bij SIEM-producten correleren. Goede log correlatie is een basisvereiste voor een goed werkend SIEM-product. De mogelijkheid om de data van alle verschillende bronnen aan elkaar te koppelen en op deze manier bestaande of potentiële dreigingen waar te nemen is van cruciaal belang. De werking hiervan zie je visueel in figuur 1. [1]



Figuur 1: Werking SIEM

Het SIEM-systeem genereert events en alarmen op basis van al deze data. De gegenereerde events en alarmen worden in de gaten gehouden door het SOC-personeel.
Door het aan elkaar koppelen van logs uit meerdere bronnen kan de eerder genoemde geavanceerde malware gedetecteerd worden die niet door de individuele beveiligingsapparaten opgepikt wordt.

2.3 Voordelen

Door het centraliseren en correleren van alle inkomende data krijg je een aantal nieuwe mogelijkheden op vlak van beveiliging. Een aantal van deze voordelen worden hieronder verder toegelicht.

2.3.1 Alle informatie centraal beschikbaar

Alle informatie is vanaf één platform toegankelijk. Men moet niet op elk systeem apart inloggen om de logs te bekijken. Zo blijft het overzicht behouden tijdens het onderzoeken van een incident.

2.3.2 Drastisch verlagen van de responstijd

Bepaald verdacht verkeer en gebruik van systemen laat niet altijd een belletje rinkelen bij je *firewall* of antivirus. Op deze manier kunnen hackers zich maanden in je netwerk bevinden zonder dat je hiervan op de hoogte bent.
Door het combineren van informatie en logs van verschillende bronnen krijg je een completer beeld van wat er zich allemaal afspeelt in het bedrijfsnetwerk. Verkeer naar *command-and-control servers*, geavanceerde malware en hackers worden snel gedetecteerd voordat ze een kans hebben om schade aan te richten.

2.3.3 Uitgebreidere en snellere analysemogelijkheden

De centralisatie van de logs zorgt ervoor dat je sneller en uitgebreider je onderzoek naar incidenten binnen het bedrijfsnetwerk kan voeren. Door de correlatie van alle informatie krijg je snel een indicatie waar de infectie eerst heeft plaatsgevonden of welk systeem de hacker als eerste gecompromitteerd heeft en op welke manier. De impact op de bedrijfscontinuïteit kan snel worden bepaald door de grote hoeveelheid informatie.

Door de juiste filters toe te passen tijdens je onderzoek krijg je een goed overzicht over welke apparaten en systemen allemaal geïnfecteerd of gecompromitteerd zijn.

2.3.4 Verhinderen gelijkaardige infecties in de toekomst

De uitgebreide analyse- en onderzoeksmogelijkheden die je krijgt dankzij een SOC bieden de mogelijkheid om maatregelen te nemen. Zo kan je gelijkaardige infecties of aanvallen in de toekomst vermijden.

2.3.5 GDPR

De uitgebreidere en snellere analysemogelijkheden zijn een enorme troef, rekening houdend met de aankomende General Data Protection Regulation (GDPR) wet.
Deze Europese wet gaat van kracht op 25 mei 2018 en is van toepassing wanneer je als bedrijf persoonsgegevens verwerkt. [2]
Volgens deze nieuwe databeschermingswet moeten data-inbreuken zo snel mogelijk en niet later dan 72 uur na het ontdekken hiervan gerapporteerd worden aan de Privacycommissie. In het rapport dat wordt overgemaakt aan de Privacycommissie moet vermeld staan over welke soort data het gaat en de hoeveelheid data die mogelijk buit is gemaakt. Verder moeten ook de consequenties van de data-inbreuk gemeld worden en welke maatregelen er op voorhand waren genomen om dit te voorkomen en welke maatregelen je als bedrijf in de toekomst gaat nemen. [3]

Een Security Operations Center met een SIEM helpt het bedrijf niet enkel om dit te voorkomen maar ook om te voldoen aan de GDPR wetgeving in het geval van een data-inbreuk.

2.4 Nadelen

Uiteraard zijn er ook enkele nadelen bij het opzetten en draaiende houden van een Security Operations Center. Een aantal van deze voordelen worden hieronder verder toegelicht.

2.4.1 Personeel

Om een goed werkend 24/7 SOC te laten draaien heb je beduidend meer personeel nodig. Het SOC-personeel wordt in 3 niveaus opgedeeld.

Allereerst heb je analisten (*tier* 1) nodig die de events en alarmen controleren die het SIEM-systeem genereert en beslissen of er verdere aandacht moet worden geschonken aan een event of alarm.

Indien dit het geval is wordt dit nagekeken door een incident onderzoeker (*tier* 2). Een incident onderzoeker gaat dan een doorgedreven analyse uitvoeren aan de hand van alle beschikbare logs en bepaalt welke kritieke systemen bij het incident betrokken zijn. Na het incident helpt hij om de getroffen systemen te herstellen.

Als laatste heb je nog een expert (*tier* 3) nodig. Dit is iemand die in extreme gevallen mee helpt aan een uitvoerig onderzoek. Andere werkzaamheden zijn *reverse engineering* van aangetroffen malware en op zoek gaan naar informatie over de nieuwste malware en *exploits* om zo een aanval voor te kunnen zijn.

Al deze personen moeten getraind worden om met de systemen overweg te kunnen en up-to-date te blijven met de nieuwste technologieën. [1] Een grafische weergave van de verschillende *tiers* en hun bijhorende taken is te zien in figuur 2. [4]

Figuur 2: Onderverdeling SOC-personeel en hun taken

2.4.2 Extra systemen

Om dit allemaal op te zetten heb je natuurlijk heel wat server capaciteit nodig. Zo moet je ervoor zorgen dat de benodigde resources aanwezig zijn om alle virtuele machines op te zetten. Denk hierbij aan CPU-*cores*, RAM-geheugen en ruimte op de harde schijf. Verder kost het ook behoorlijk wat tijd om deze virtuele machines op te zetten en te testen in een lab omgeving.

Indien je de systemen na de testfase wilt integreren in de productieomgeving moet hier ook nog eens tijd voor vrijgemaakt worden.

Voor bepaalde producten heb je ook fysieke toestellen. Hier moet je dan eerst controleren of er voldoende plaats is in de *server rack*. Bij het aansluiten van fysieke apparaten dient er ook rekening gehouden te worden met vrije poorten op de switch om ervoor te zorgen dat de apparaten ook netwerkconnectiviteit hebben.

Bij een groot bedrijf met meerdere vestigingen wordt dit nog complexer om alle data van de verschillende kantoren naar je SOC te sturen zonder dat het netwerk verzadigd geraakt door al deze extra data. Bij enkele SIEM-systemen, waar ik in mijn onderzoeksrapport dieper op in ga, zijn daar oplossingen voor voorzien. Bij deze producten wordt er een apparaat in elke vestiging geplaatst dat het zware werk ter plaatse gaat doen en enkel gegenereerde events en alarmen gaat doorsturen naar het Security Operations Center. Dit kunnen zowel virtuele als fysieke apparaten zijn.

Het verzenden van deze data van de ene locatie naar de andere moet uiteraard ook op een secure manier gebeuren.

3 Tools en applicaties

Data Unit heeft als netwerk- en securitybedrijf uiteraard zelf ook al een aantal *tools* in productie om het netwerk, servers, pc's en laptops te beschermen. Van al deze *tools* ga ik Barracuda Networks en Kaspersky Lab verder uitlichten.

3.1 Huidige beveiligingstools

3.1.1 Barracuda Networks

Figuur 3: Logo Barracuda [5]

Barracuda Networks is een bekende speler wanneer het aankomt op netwerkbeveiligingsproducten. Barracuda maakt beveiligingsoplossingen die efficiënt werken en kosteffectief zijn. Zo hebben zij bij al hun producten een duidelijke prijs waar geen verborgen kosten aan vast zitten. De producten van Barracuda focussen zich hoofdzakelijk op drie verschillende markten:

- *Content security*
- *Networking and application delivery*
- *Data storage, protection and disaster recovery*

Dit geeft een bedrijf de mogelijkheid om een totaaloplossing af te nemen bij één producent.

Deze producten kunnen zowel via hardware als *virtual appliances* geïnstalleerd worden. In beperkte mate is een cloudoplossing ook mogelijk. [6]

Barracuda steunt en maakt ook gebruik van *open source* en community gebaseerde security projecten. Dit doen zij op verschillende manieren door hardware of geld te doneren. [7]

Data Unit is al lange tijd *reseller* van deze producten. Ondertussen verkopen en bieden zij support aan een groot deel van de Barracuda producten.

De producten die Data Unit verkoopt zijn:

- *Barracuda NextGen Firewall F-Series*
- *Barracuda Web Security Gateway*
- *Barracuda Web Application Firewall*
- *Barracuda Load Balancer ADC*
- *Barracuda Email Security Gateway*
- *Barracuda Sentinel*
- *Barracuda (Cloud-to-cloud) Backup*

De Barracuda NextGen Firewall doet binnen Data Unit ook dienst als Intrusion Prevention System (IPS).

Data Unit heeft ook zijn eigen NextGen Control Center vanwaar de firewalls die bij klanten staan beheerd kunnen worden. Op deze manier kan er een overzicht behouden worden over de *firewalls* die zich bij de klanten bevinden. Vanuit het Control Center kan er ingelogd worden op de gewenste *firewall* in plaats van steeds op iedere firewall apart in te loggen.

3.1.2 Kaspersky Lab

Figuur 4: Logo Kaspersky Lab [8]

Kaspersky Lab is een zeer bekend cybersecurity bedrijf dat opgericht is in 1997. Kaspersky Lab hun threat intelligence en expertise op vlak van security evolueert continue om bedrijven, kritieke infrastructuur, overheden en klanten over de hele wereld te beschermen. Het portfolio aan producten bevat onder andere *endpoint protection* en meerdere gespecialiseerde security oplossingen en diensten. Deze producten helpen om de steeds maar evoluerende bedreigingen het hoofd te bieden. [9]

Kaspersky Lab is één van de meest geteste beveiligingsproducten in de laatste jaren. Bij de testen haalt Kaspersky Lab consequent het hoogste percentage van top drie plaatsen vergeleken met alle andere beveiligingsproducten. Zo zijn de Kaspersky Lab producten in 2016 maar liefst 78 keer getest. In deze 78 testen behaalde Kaspersky Lab 55 keer de eerste plaats en maar liefst 70 keer een top drie notering. [10]

Vanwege deze uitstekende resultaten die Kaspersky Lab jaar in jaar uit weet te behalen werkt Data Unit samen met Kaspersky Lab sinds 2009. Als deel van het partner programma fungeert Data Unit als *reseller* en *Managed Service Provider* (MSP) voor Kaspersky Lab producten. Dit houdt in dat Kaspersky Lab producten verkocht worden met bijkomende service indien er problemen zijn en dat er ook installaties uitgevoerd worden indien een klant dit wenst.

3.2 Geteste beveiligingstools

3.2.1 Intrusion Detection System

3.2.1.1 Snort

Snort is het grootste en bekendste gratis *open source intrusion detection system* en *intrusion prevention system*. Het is gecreëerd door Martin Roesch in 1998. Snort wordt momenteel verder ontwikkeld door het bedrijf Sourcefire dat in 2013 door Cisco is opgekocht.

Figuur 5: Logo Snort [48]

Snort heeft de mogelijk om in realtime netwerkverkeer te analyseren. Snort kan onder andere *operating system fingerprinting*, semantic URL aanvallen, *buffer overflows* en (stealth) port scans detecteren. [11] De detectie van al deze verschillende soorten aanvallen gebeurt op basis van *rules*.

Dit heeft zo zijn voor- en nadelen. Zo moet er voor elke *exploit* of *vulnerability* een nieuwe *rule* gecreëerd worden. Echter is deze manier van werken beter dan *signatures*. Bij sig*nature-based detection* kunnen er meerdere *signatures* zijn voor één en dezelfde *exploit*. Een kleine wijziging zorgt voor een andere *signature* waarbij de *rule-based detection* methode van toepassing blijft op diezelfde *exploit*. [12]

Snort kan geconfigureerd worden in drie verschillende modi: sniffer, packet logger of intrusion detection. In sniffer modus gaat Snort alle netwerkpakketten uitlezen en tonen op de console. In packet logger modus worden alle pakketten bijgehouden op de harde schijf. Bij de intrusion detection modus gaat Snort al het netwerkverkeer monitoren en vergelijken met de gekende *rulesets*. Op basis hiervan gaat Snort dan actie ondernemen. [11]

Ondanks dat Snort puur *single-threaded* werkt, is het programma in staat om netwerkverkeer aan een hoge snelheid te verwerken. De maximale verwerkingssnelheid is gebaseerd op de grote van de *rulesets* waarmee Snort het verkeer moet analyseren.

Er is momenteel een Snort 3.0 versie in ontwikkeling waarbij volledig vanaf nul is begonnen. Hierdoor gaat er bij deze versie ook ondersteuning zijn voor *multi-threading*. Echter zit deze nieuwe versie nog in de alfafase van ontwikkeling en wordt niet aangeraden om het in productie te gebruiken.

3.2.1.2 Suricata

Figuur 6: Logo Suricata [13]

De eerste beta versie van Suricata is vrijgegeven in december 2009. De eerste volwaardige versie is in juli 2010 uitgebracht. De ontwikkeling van Suricata wordt gedaan door het Open Information Security Foundation (OISF). [14]

Suricata is net zoals Snort een gratis en *open source* intrusion detection system en intrusion prevention system. Hiernaast heeft Suricata nog enkele andere functies zoals Network Security Monitoring (NSM) en *offline* pcap verwerking. Met NSM kunnen niet enkel logs opgeslagen worden maar ook het opslaan van TLS certificaten en het opslaan van bestanden die gedownload worden door een gebruiker op het netwerk behoren tot de extra functionaliteiten.

Suricata kan overweg met dezelfde *rulesets* die ook op Snort werken. Dit vergemakkelijkt het ontwikkelen en delen van goede *rules* om nieuwe dreigingen te detecteren. Waar Snort compleet *single-threaded* werkt, is er bij Suricata wel ondersteuning ingebouwd om meerdere *threads* en *cores* te gebruiken. Hierdoor kan Suricata zonder problemen gigabit netwerkverkeer verwerken.

In Suricata is er ook de mogelijkheid om gebruik te maken van Lua scripting. Hierdoor heb je toegang tot extra functionaliteiten en kan er een uitgebreidere analyse op het netwerkverkeer gevoerd worden die niet mogelijk is met een normale *ruleset*.

Een andere handige functie is het automatisch detecteren van het gebruikte protocol. Onafhankelijk van de poort waar het verkeer doorkomt. Op basis hiervan wordt dan de juiste *rules* toegepast. Deze functie helpt met het detecteren van *malware* en communicatie met *command-and-control servers* die zelden de traditionele poorten gebruiken.

Omdat het verder ontwikkelen van Suricata gedaan wordt door de community is er een sterke focus op beveiliging, efficiëntie en bruikbaarheid van de tool. [15]

3.2.2 Vulnerability Scanner

3.2.2.1 OpenVAS

Figuur 7: Logo OpenVAS [16]

Open Vulnerability Assessment System (OpenVAS) is een *open source framework* van verschillende tools die je een uitgebreide mogelijkheid geven om *vulnerability scanning* en *vulnerability management* te gebruiken. Het OpenVAS *framework* is onderdeel van Greenbone Networks hun commerciële *vulnerability management* oplossing. Ontwikkelingen gedaan door Greenbone Networks stromen door naar de *open source* variant. Het open stellen hiervan gebeurd sinds 2009.

De *security scanner* beschikt over de Greenbone Community Feed waarin meer dan 50 000 Network Vulnerability Tests (NVT) verwerkt zitten. De NVT-lijst wordt bijgehouden en geüpdatet door Greenbone Networks. Greenbone Networks beschikt ook over een Greenbone Security Feed. Deze aparte *vulnerability* lijst is enkel beschikbaar wanneer je een commercieel product aankoopt bij Greenbone Networks. De gratis community feed komt met meer dan 95% overeen vergeleken met de commerciële security feed. Het is ook mogelijk om je eigen NVTs te schrijven. [17]

3.2.3 Log Management

3.2.3.1 Splunk Light

Figuur 8: Logo Splunk Light [18]

Splunk is een Amerikaans multinational bedrijf gebaseerd in San Francisco, California. Splunk ontwikkelt software om in eerste instantie logs te centraliseren om zo het zoeken in alle gegenereerde logs te vereenvoudigen. De gecentraliseerde logs kunnen dan geïndexeerd worden en hier wordt dan nog eens correlatie op toegepast. In de database die op die manier gecreëerd wordt kan je dan makkelijker gaan zoeken naar relevante logs zonder op elk verschillend toestel in te loggen en daarin de logs manueel te gaan doorzoeken. [19]

Splunk heeft sinds het ontstaan van het bedrijf zijn portfolio flink uitgebreid. Waar Splunk origineel werd gebouwd vanwege het gebrek aan een goede *log management tool* is het ondertussen veel meer dan dat geworden. In zijn kern is en blijft Splunk uiteraard nog altijd een zeer goede *log management tool*. Zo is er de mogelijkheid om apps en add-ons toe te voegen aan een Splunk Enterprise installatie.

Apps helpen je onder andere door makkelijkere (*point-and-click*) en uitgebreidere analyse mogelijk te maken, alsook het voorzien van voorgebouwde *dashboards* of rapporten. Met add-ons wordt de invoer van data vergemakkelijkt. Bijvoorbeeld, door het installeren van een Barracuda add-on worden de logs die Splunk binnen krijgt van Barracuda apparaten automatisch herkent. Alle velden worden correct geïdentificeerd zodat dit niet meer manueel moet worden gedaan aan de hand van reguliere expressies. [20]

Splunk Light zou tijdens mijn stage gebruikt worden om in eerste instantie alle logs te centraliseren. Van hieruit zouden dan alle logs doorgestuurd worden naar de SIEM-oplossing die ik op dat moment aan het testen was. Dit om te vermijden dat er gegevensverlies zou plaatsvinden en om elk SIEM-systeem te kunnen voorzien van historische data. Nadat alle systemen waren opgezet en hun logs doorstuurde richting Splunk werd het duidelijk dat het doorsturen van logs vanuit Splunk naar een derde partij enkel mogelijk was met de Enterprise versie van Splunk.

3.2.4 Security Information and Event Management

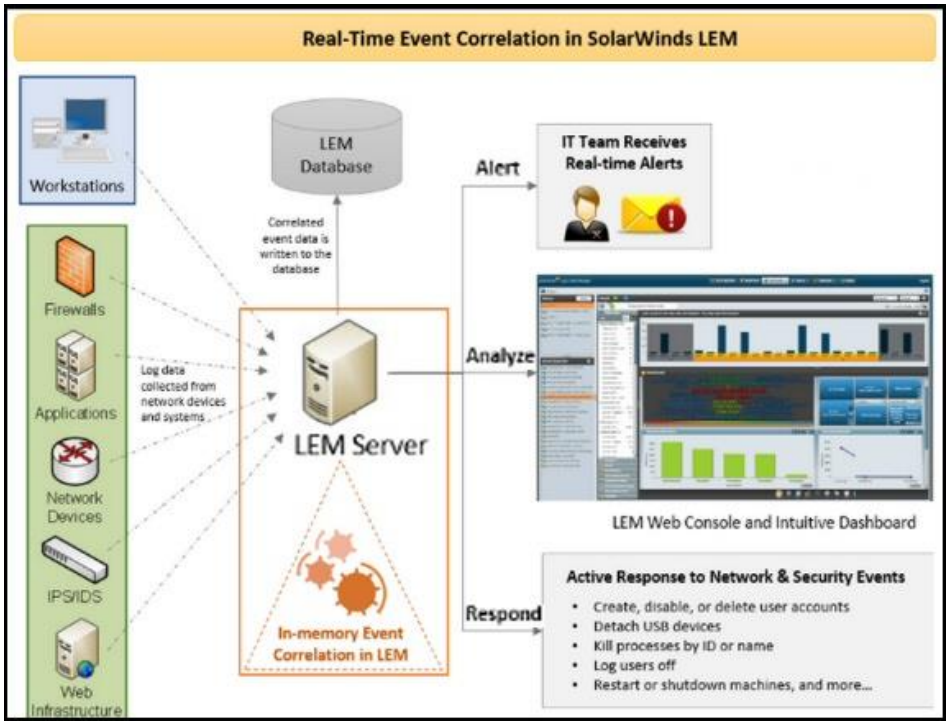
3.2.4.1 Solarwinds: Log & Event Manager

Figuur 9: Logo Solarwinds [21]

Solarwinds is een IT infrastructuur management software bedrijf dat is opgericht in 1999. Het Hoofdkantoor is gevestigd in Austin, Texas maar Solarwinds beschikt over kantoren over de hele wereld, van Europa tot Australië. Ondanks dat het bedrijf in 1999 werd opgericht, kwam hun eerste product pas beschikbaar in 2001. Dit was een *web-based netwerk performantie managment tool*. Door de jaren heen is het productportfolio van Solarwinds flink uitgebreid. Deze uitbreiding werd mede mogelijk gemaakt door het overnemen van vele verschillende bedrijven met allen een andere expertise. [22]

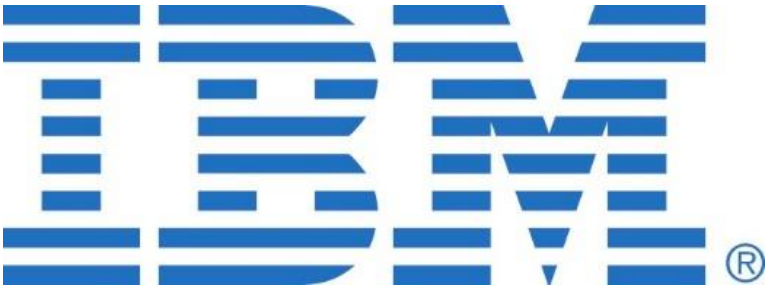
Tijdens mijn stage heb ik gebruik gemaakt van het security information and event management product van Solarwinds. Dit product is een combinatie van vele van hun reeds bestaande tools en enkele extra's die speciaal voor hun SIEM-product zijn ontwikkeld.

Enkele belangrijke features van dit product zijn realtime event correlatie. De werking hiervan is te zien in figuur 10. [23] Automatisch acties ondernemen wanneer bepaalde regels geactiveerd worden. USB-toestellen monitoren die worden aangesloten op een laptop of desktop. Uitgebreide zoekmogelijkheden en forensische analyse in de verzamelde logs. Meer en uitgebreidere informatie over deze en andere functies vindt u in het onderzoek gedeelte van dit eindwerk waar ik dieper in ga op dit product.



Figuur 10: Realtime event correlatie Solarwinds

3.2.4.2 IBM QRadar Community Edition SIEM



Figuur 11: Logo IBM [24]

Computing-Tabulating-Recording Company (CTR) werd in 1911 opgericht. In 1924 veranderde dit bedrijf hun naam naar International Business Machines (IBM). Een naam die ondertussen wereldwijd bekend is binnen de IT sector en ver daarbuiten.

Op het vlak van security heeft IBM vandaag de dag een hele resem aan producten en oplossingen in hun portfolio. Zo heeft IBM oplossingen beschikbaar voor *mobile device management*, fraude preventie, databescherming en toegangscontrole, *endpoint* beveiliging en in *identity management*. QRadar is het SIEM-platform van IBM. Dit platform werd in 2003 door IBM geïntroduceerd. Het behoorde tot een van de eerste SIEM-systemen op de markt. Vandaag de dag is het de leider in SIEM-systemen volgens Gartner's Magic Quadrant for SIEM. [25] Dit voor maar liefst het negende jaar op rij.

Gedurende de stage heb ik gebruik gemaakt van de recent beschikbaar gemaakte gratis *community edition* van IBM hun QRadar SIEM-oplossing. Deze versie is speciaal gemaakt om QRadar vrijuit te kunnen testen en gebruiken. Alhoewel deze versie beperkt is in mogelijkheden vergeleken met de commerciële QRadar is het toch een sterke basis om een eerste evaluatie te maken over het product. Alle basisvereisten zijn aanwezig zoals: aanpasbare *dashboards* en regels, rapporteringsfunctie, logcollectie, *network capture* en monitoring en een *ticketing* systeem om problemen op te lossen.

Diepgaandere informatie over QRadar Community Edition is beschikbaar in het onderzoeksgedeelte van dit eindwerk.

3.2.4.3 Alienvault USM

Figuur 12: Logo Alienvault [26]

In 2003 werd de ontwikkeling gestart van OSSIM. Dit project vormde de basis van wat later Alienvault zou worden. Het bedrijf Alienvault werd in 2007 opgericht en is van oorsprong een Spaans bedrijf. Ondertussen staat het hoofdkwartier in San Mateo, California. Alienvault heeft verder nog kantoren in de Verenigde Staten, Spanje en Ierland. [27]

Naast hun commerciële producten, Alienvault USM Appliance en Alienvault USM Anywhere, beheert en ontwikkelt Alienvault ook nog het OSSIM project waar het allemaal mee is begonnen. OSSIM is een gratis *open source* variant van het commerciële Alienvault product. Uiteraard ontbreken hier een aantal functies die wel beschikbaar en noodzakelijk zijn in een bedrijfsomgeving. Enkele van deze functies zijn: *log management*, integratie met *ticketing* systemen van derde partijen, telefoon en email *support*, om er maar enkele te noemen. [28]

Alienvault is naast de *community* de drijvende kracht achter het Open Threat Exchange (OTX) initiatief. Werelds eerste open *threat intelligence community*. Met ondertussen meer dan 65 000 deelnemers in 140 landen. Dagelijks komen er 14 miljoen *threat indicators* bij op het OTX platform. Deze informatie varieert van IP-adressen tot *file hashes* en Common Vulnerabilities and Exposures (CVE) nummers. [29] Sinds april 2017 is OTX een STIX/TAXII server. STIX is een gestandardiseerde manier om *threat intelligence* te beschrijven en TAXII is een methode om deze informatie te delen. Op deze manier kan er nog makkelijker gebruik gemaakt worden van OTX door derde partijen. Waar dit vroeger via een API moest gaan kan men nu dus ook gebruik maken van de STIX/TAXII server. Onder andere QRadar SIEM biedt ondersteuning om connectie te maken met zo een type server om gebruik te kunnen maken van extra *threat intelligence*. [30]

De commerciële versie van Alienvault die ik tijdens mijn stage heb gebruikt, wordt in de markt gezet als een soort SIEM 2.0. Het wordt door Alienvault zelf een Unified Security Management (USM) genoemd. Dit houdt in dat het zoals een SIEM-systeem niet enkel logs kan accepteren en correleren in combinatie met *netflow* gegevens om zo alarmen te genereren wanneer er iets niet pluis is. Bij Alienvault wordt er gebruik gemaakt van *open source* software om het platform uit te breiden. Zo wordt Suricata gebruikt als IDS, OpenVAS als vulnerability scanner, Nagios als *host monitor* en *service* beschikbaarheidssysteem alsook OSSEC dat dienst doet als host intrusion detection system wanneer er gebruik wordt gemaakt van de Alienvault *agent*. [31]

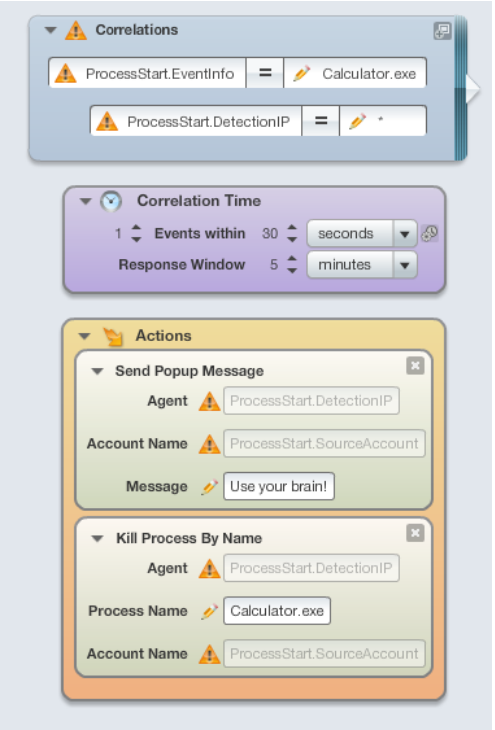
4 Testfases

Om al deze producten te onderzoeken heb ik het testen hiervan opgedeeld in drie delen. Het onderzoeken van de benodigdheden en eisen om een Security Operations Center op te zetten is een project van lange duur met meerdere werknemers. Tijdens het testen is er wegens tijdsgebrek niet de mogelijkheid geweest om diep in te gaan op de meeste producten die ik getest heb.

4.1 Fase 1

Als eerste SIEM heb ik Solarwinds: Log & Event Manager geïnstalleerd. Na de installatie is er eerst gefocust op het verkrijgen van een basis kennis van Solarwinds: Log & Event Manager. Doordat er niet onmiddellijk logs vanuit allerlei verschillende toestellen naar Solarwinds werden gestuurd vermeed ik een overvloed aan informatie terwijl ik een basiskennis opdeed van het programma.

Er kan gebruik worden gemaakt van een *agent* om zo extra informatie en functionaliteiten te gebruiken binnen Solarwinds: Log & Event Manager. Zo krijg je *File Integrity Monitoring* en USB-*monitoring* mogelijkheden op de *clients* waarop je een *agent* installeert. Ook heb je meer mogelijkheden wat betreft het automatisch actie ondernemen wanneer een *rule* geactiveerd wordt. Door gebruik van de *agent* krijg je de optie om programma's te verbieden. Zo heb ik een *rule* aangemaakt die het gebruik van 'calculator.exe' verbiedt. Zie figuur 13 voor een screenshot van deze *rule*.



Figuur 13: Kill Calculator.exe rule

In de eerste fase heb ik van zowel Snort als Suricata gebruik gemaakt als IDS. Beide werden op een aparte virtuele machine geïnstalleerd om ervoor te zorgen dat beide IDS tools elkaar niet zouden interfereren. Op zowel Snort als Suricata heb ik gebruik gemaakt van de *registered rulefeed* die gedownload kan worden op de website van Snort na registratie. [32] In de account instellingen vind je je persoonlijke 'oinkcode' terug. Deze oinkcode kan je dan gebruiken om de *registered rulefeed* te downloaden op je Snort virtuele machine. De *rulefeed* wordt bijgehouden door Talos, zij onderhouden de *rulefeed* zodat deze te allen tijde up-to-date is. [33] Voor zowel Snort als Suricata heb ik gebruik gemaakt van Oinkmaster om steeds de nieuwste versie van de *rulefeed* te downloaden. Een deel van het configuratiebestand is te zien in figuur 14.

```
# URL examples follows. Replace <oinkcode> with the code you get on the
# Snort site in your registered user profile.

# Example for Snort 2.9.11
url = http://www.snort.org/pub-bin/oinkmaster.cgi/e8c85335b                    94/snortrule
s-snapshot-29110.tar.gz
```

Figuur 14: Oinkmaster configuratie met oinkcode

In het local.rules bestand kunnen eigen regels toegevoegd worden die van toepassing zijn op de omgeving waarin Snort of Suricata draait.

Een regel bestaat uit meerdere variabelen waaraan een waarde toegekend moet worden. Een simpele voorbeeld regel ziet er als volgt uit:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:1000001; rev:001;)
```

De regel bestaat uit de volgende onderdelen:

alert: actie die wordt toegepast op trafiek dat voldoet aan de regel

icmp: het protocol

any any: *source address & port*

->: richting van het verkeer

$HOME_NET any: *destination address & port* ($HOME_NET = 10.143.150.0/24)

msg:"ICMP test": log bericht

sid:1000001: *unique rule identifier* (*local rules* moeten beginnen met 1000001 of hoger)

rev:001: regel versie nummer

Gedurende deze eerste fase was er nog geen beschikking over een span-poort om al het trafiek van andere toestellen te laten passeren langs beide IDS tools. Om te testen of zowel de *local rules* als de *registered rulefeed* correct geïmplementeerd zijn heb ik enkele pings uitgevoerd en een curl-commando uitgevoerd met "BlackSun" als HTTP *user-agent string*. Zie onderstaande screenshots ter verduidelijking van de detectie.

```
11/09-11:36:38.843523  [**] [1:1000001:1] ICMP test [**] [Priority: 0] {ICMP} 10.143.150.3 -> 10.143
.150.72
11/09-11:37:28.741056  [**] [1:1000001:1] ICMP test [**] [Priority: 0] {ICMP} 10.143.150.3 -> 10.143
.150.72
11/09-11:37:32.741202  [**] [1:1000001:1] ICMP test [**] [Priority: 0] {ICMP} 10.143.150.3 -> 10.143
.150.72
```

Figuur 15: Snort ping detectie

curl –A "BlackSun" www.google.com

```
 11/09/2017-11:17:54.569824  [**] [1:2008983:6] ET USER_AGENTS Suspicious User Agent (BlackSun) [**]
Classification: A Network Trojan was detected] [Priority: 1] {TCP} 10.143.150.4:46588 -> 172.217.17.100:80
```

Figuur 16: Suricata BlackSun detectie

Als *vulnerability scanner* werd er gebruik gemaakt van OpenVAS. Het is een *open source vulnerability scanner* die onder andere ook gebruikt wordt door Alienvault USM om *vulnerability scans* uit te voeren. Ik heb voor OpenVAS gekozen omdat dit *framework* zowel virtueel te installeren is als een fysieke *appliance* te verkrijgen via Greenbone Networks. Ook is er volgens de website van Greenbone Networks hebben zij slechts één partner in België. [34] Dit geeft enorm veel mogelijkheden om hiermee aan de slag te gaan.

De *vulnerability scanner* heb ik gebruikt om het test labo en mijn eigen laptop te scannen op kwetsbaarheden. Via OpenVAS heb ik ontdekt dat er meerdere ernstige bekende kwetsbaarheden zitten in Solarwinds: Log & Event Manager. Zo is, onder andere, het OS waarop Solarwinds draait, End Of Life (EOL). Voor de onderste twee kwetsbaarheden zijn er *hotpatches* beschikbaar. Echter waren deze niet toegankelijk voor de proefversie.

Vulnerability		Severity	QoD
OS End Of Life Detection		10.0 (High)	80%
SolarWinds Log and Event Manager SSH Jailbreak and Privilege Escalation Vulnerabilities		7.2 (High)	80%
SolarWinds Log and Event Manager Multiple Vulnerabilities		10.0 (High)	80%

Figuur 17: High severity vulnerabilities Solarwinds

4.2 Fase 2

In de tweede fase heb ik Solarwinds: Log & Event Manager vervangen met IBM QRadar Community Edition. De *Community Edition* was nog maar sinds enkele weken beschikbaar toen ik er mee aan de slag ging. Doordat het nog allemaal redelijk nieuw is werkte alles helaas niet naar behoren. Op deze problemen kom ik iets later in dit eindwerk nog terug.

Net zoals bij Solarwinds: Log & Event Manager heb ik na de installatie van QRadar Community Edition eerst wat rondgekeken en geëxperimenteerd met de mogelijkheden van het programma zonder externe log data. IBM heeft zelf een YouTube afspeellijst gemaakt om te helpen bij het installeren van QRadar en gebruikers wegwijs te maken binnen het programma. [35]

Omdat er enkel van SIEM gewisseld is, moest op de andere tools zoals Snort en Suricata enkel het IP-adres gewijzigd worden naar waar de logs gestuurd dienden te worden.

Eenmaal op alle *devices* de IP's waren gewijzigd was het tijd om te kijken of de logs correct aankomen op de QRadar Community Edition virtuele machine. Door naar het tabblad *Log Activity* te gaan krijg je een realtime stream van alle logs die binnenkomen. Standaard staat dit op genormaliseerd. Met enkele muisklikken kan ervoor gezorgd worden dat je de *raw logs* te zien krijgt in plaats van genormaliseerd.

In figuur 18 zie je de genormaliseerde *firewall* logs binnenkomen. Als een bepaalde log bekeken dient te worden moet de realtime *streaming* eerst op pauze gezet worden. Na het pauzeren, kan de log bekeken worden door te dubbelklikken op de log entry. Rechtermuisknop op de *log entry* geeft verschillende mogelijkheden afhankelijk van waar er geklikt wordt. Klik je binnen de kolom '*Source IP*' dan krijg je extra opties om snel te filteren om zo enkel logs te laten zien van dat *Source IP* of juist geen logs met dat *Source IP*.

Log Source	Event Coun	Time	Low Level Category	Source IP	Source Port	Destination IP
SIM Generic Log DSM-7 :: qradar	1	Jan 18, 2018, 4:47:29 ...	Unknown Generic Log Event	10.143.[redacted]	0	10.143.[redacted]
SIM Generic Log DSM-7 :: qradar	1	Jan 18, 2018, 4:47:29 ...	Unknown Generic Log Event	10.143.[redacted]	0	10.143.[redacted]
SIM Generic Log DSM-7 :: qradar	1	Jan 18, 2018, 4:47:29 ...	Unknown Generic Log Event	10.143.[redacted]	0	10.143.[redacted]
SIM Generic Log DSM-7 :: qradar	1	Jan 18, 2018, 4:47:27 ...	Unknown Generic Log Event	10.143.[redacted]	0	10.143.[redacted]

Figuur 18: QRadar genormaliseerde firewall logs

Door Device Support Modules (DSM) te installeren krijgt de QRadar instantie de nodige informatie om logs van bepaalde merken automatisch correct te interpreteren. Omdat de *Community Edition* pas zeer recent is uitgekomen en op de allernieuwste versie draait, waren er voor zowel Barracuda NG Firewalls als Kaspersky Security Center geen DSM's beschikbaar. Dit zorgt ervoor dat de logs niet correct verwerkt worden maar geïnterpreteerd als een standaard log zonder extra informatie. Vandaar de benaming *Generic Log* in figuur 18. QRadar heeft de mogelijkheid om manueel in logs te gaan verwerken. Door één enkele log erbij te nemen kan dan via reguliere expressie aangeduid worden welke waarde wat betekent zoals *Source IP* of *Destination IP*. Helaas werkte dit ook niet naar behoren en kreeg ik geen log te zien wanneer ik deze wou aanpassen in de *DSM Editor*. Het handmatig invoeren van een voorbeeldlog is mogelijk maar éénmaal er op *save* werd gedrukt en uit de *DSM Editor* werd gegaan was alles weer weg. Het werd niet correct verwerkt en opgeslagen.

Gelukkig kwamen de logs van de andere toestellen wel goed door. Hierdoor werden de aanvallen die de *vulnerability scanner* uitvoerde gedetecteerd en weergegeven in het '*Offenses'* tabblad.

Description	Offense Type	Offense Source	Magnitude
Multiple Login Failures for the Same User preceded by Multiple Login Failures to the Same Destinati...	Destination IP	10.143.150.3	
Multiple Login Failures for the Same User preceded by Multiple Login Failures to the Same Destinati...	Destination IP	10.143.150.4	

Figuur 19: QRadar Bruteforce Offense

Net zoals bij binnenkomende logs kan er door middel van een dubbelklik meer informatie verkregen worden. Zo krijg je een samenvatting van de belangrijkste info zoals: s*ource ip(s), destination ip(s)*, het aantal events dat betrekking hebben tot de aanval, begin tijdstip van de aanval, beschrijving en nog veel meer. Naast een samenvatting krijg je nog een hele reeks aan top 5 lijstjes van zaken waaronder gebruikers en categorieën van aanvallen, zoals te zien is in figuur 20.

Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows
User Login Failure		1	12
Remote Access Login Failed		1	1
SSH Login Failed		1	1,037
Admin Login Failure		1	58
Misc Login Failed		1	2

Figuur 20: Bruteforce top 5 events

4.3 Fase 3

In fase 3, de laatste fase, heb ik QRadar Community Edition ingeruild voor Alienvault USM. USM, wat staat voor Unified Security Management, is volgens Alienvault een combinatie tussen Unified Threat Management (UTM) en SIEM. Alienvault USM is dan ook meer dan een SIEM alleen. Het is een soort alles-in-eenoplossing. Naast SIEM functionaliteit maakt Alienvault ook gebruik van Suricata dat dienst doet als IDS. Om *vulnerability scanning* mogelijk te maken heeft Alienvault OpenVAS geïntegreerd. Daarnaast wordt ook nog eens van Nagios gebruik gemaakt om *hosts* en *services* te monitoren. Bijvoorbeeld de Apache *service* bij een webserver.

Omdat deze *open source* programma's al geïntegreerd zijn in Alienvault was het niet nodig om de configuratie van Snort, Suricata en OpenVAS aan te passen zodat ze hun logs richting Alienvault zouden sturen.

Tijdens de eerste opstart word je met behulp van een *getting started wizard* geholpen. Deze *wizard* helpt je om de initiële netwerkconfiguratie in te stellen. Zodra dit gedaan is kan het echte werk beginnen.

Aangezien Alienvault ook achter het Open Threat Exchange project zit is het koppelen van je OTX account met de Alienvault instantie het eerste wat best gedaan kan worden. Het enige wat je hiervoor nodig hebt is een OTX account. Hierop vind je je persoonlijke OTX *key* die je dan kan invoeren op de Alienvault *interface*.

Zodra dit gedaan was, heb ik weer even de tijd genomen om het systeem te begrijpen. De leercurve ligt niet zo hoog als bij QRadar. De meest gebruikte functionaliteiten zijn met enkele muisklikken te bereiken. Voor andere functionaliteiten moet je dan weer enkele niveaus diep gaan wat zeker in het begin wel wat tijd kost om het juiste te vinden.

Via enkele muisklikken krijg je toegang tot een realtime *stream* van de inkomende logs. Indien het logs zijn van een firewall waarbij een IP gekend is in de OTX-database dan krijg je een speciaal icoontje te zien waarop geklikt kan worden. Dit icoontje is te zien in figuur 21. Via dit icoontje word je naar het OTX-platform gebracht waar meer informatie te vinden is over de kwaadaardige activiteiten van dat IP-adres.

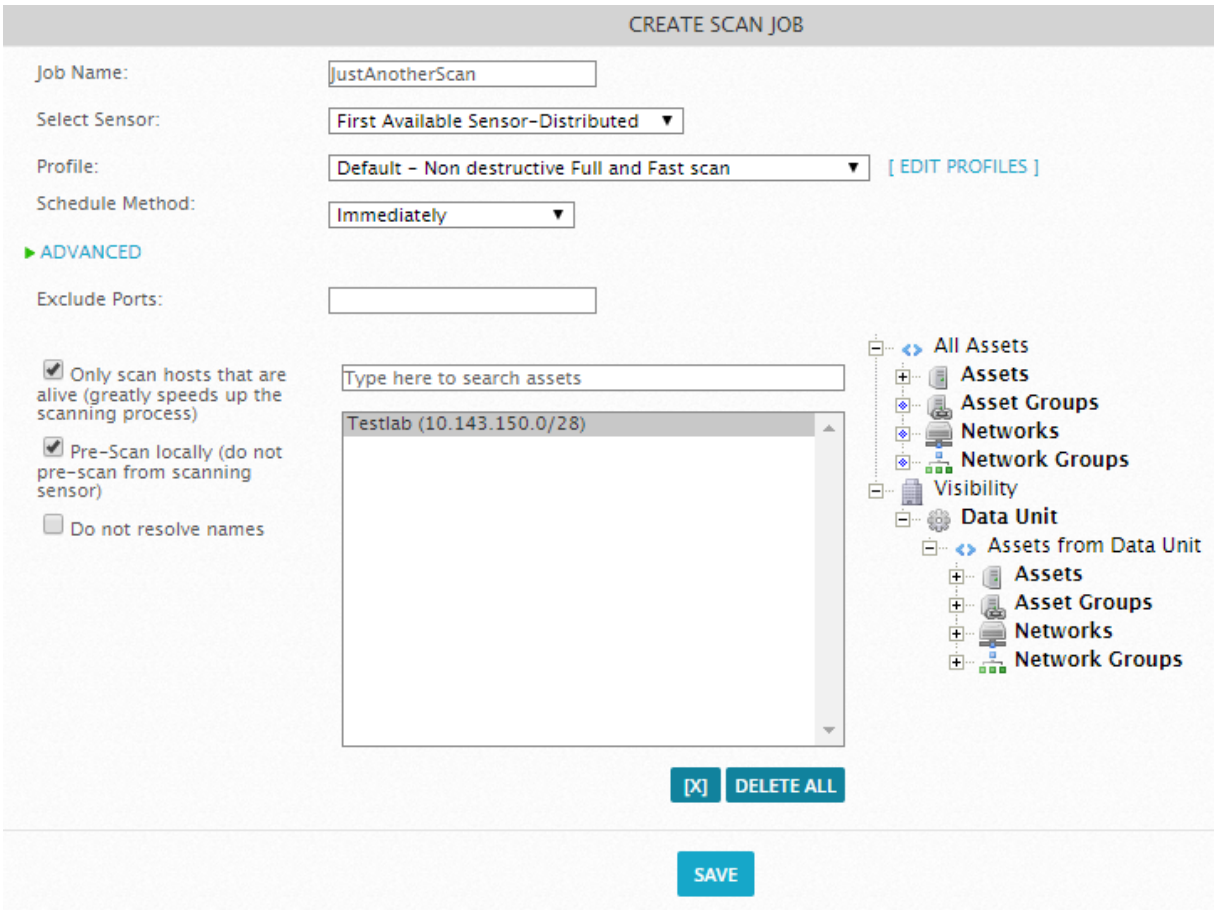
Figuur 21: OTX informatie beschikbaar van IP-adressen

De *network discovery* functionaliteit geeft je enkele verschillende mogelijkheden. Zo kan je manueel één voor één IP-adressen gaan toevoegen. Laten scannen op basis van *network ranges* of via een CSV-bestand alle informatie invoeren.

De Alienvault VMware *template* komt standaard met 5 *network interfaces*. Om een span-poort in te stellen moet er dus niets via *commandline* aangepast worden in de netwerk configuratie bestanden. Dit kan simpelweg via de *web interface*.

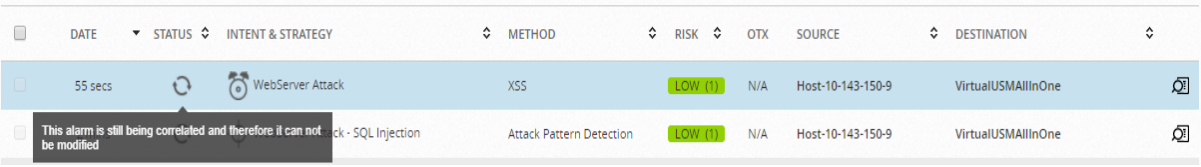
Het uitvoeren van *vulnerability scans* kan gemakkelijk geconfigureerd worden via de *web interface*. Hierin krijg je standaard 3 verschillende scanmodi. Een trage volledige en niet destructieve scan, een snelle volledige en niet destructieve scan of een volledige snelle scan met destructieve tests. Ook is er de mogelijkheid om zelf een scanprofiel aan te maken waarbij zelf de verschillende categorieën gekozen kunnen worden waarop getest dient te worden.

Naast de mogelijkheid om te kiezen wanneer de scan wordt uitgevoerd is er ook een uitgebreide mogelijkheid om te selecteren welke toestellen allemaal gescand dienen te worden. Op deze manier kan er perfect ingesteld worden welke scans wanneer moeten worden uitgevoerd en op welke toestellen.



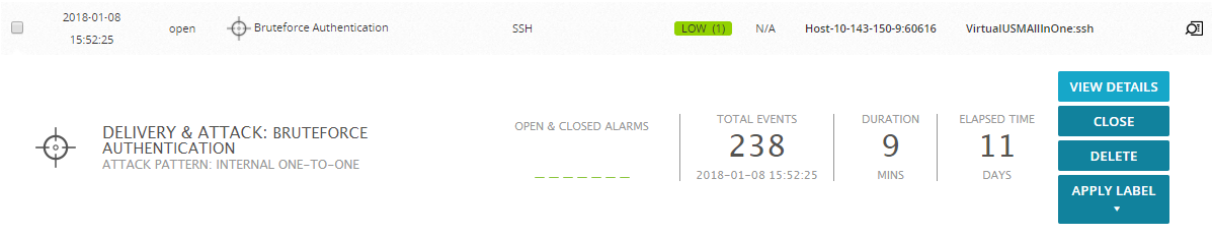
Figuur 22: Alienvault instellen vulnerability scan

Tijdens de *vulnerability scan* worden er alarmen gegenereerd. Dit is normaal en zo krijg je ook extra inzicht in wat voor soort scans er allemaal worden uitgevoerd. Tijdens een aanval kan er al naar de details van het alarm genavigeerd worden om een beter overzicht te krijgen wat er aan het gebeuren is.



Figuur 23: Alarm tijdens vulnerability scan

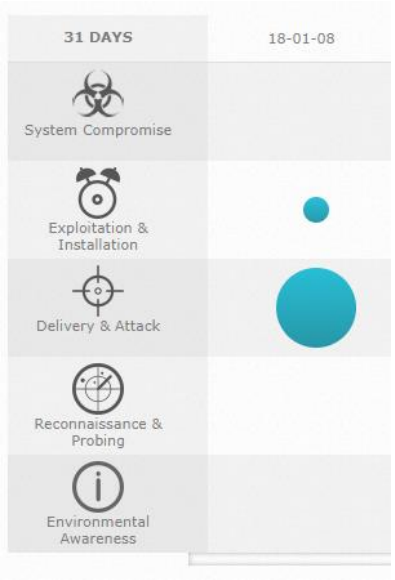
Zodra de aanval afgelopen is en correlatie van alle relevante logs heeft plaatsgevonden kunnen de details van het alarm opgevraagd worden. Hier krijg je te zien hoe lang de aanval geduurd heeft, het aantal logs/events dat tijdens de aanval zijn gegenereerd. De bron van de aanval en welk IP-adres of adressen zijn aangevallen. Als er al eens eerder een *vulnerability scan* is uitgevoerd op het doelwit van de aanval dan is er in een oogopslag ook zichtbaar over welke kwetsbaarheden er zijn op het doelwit. Indien Alienvault met OTX gekoppeld is en het IP van de aanvaller bij OTX bekend staat wordt deze informatie ook aangeboden.



Figuur 24: Overzicht alarm

Elk alarm wordt ook gerangschikt volgens de Lockheed Martin Cyber Kill Chain. Deze Cyber Kill Chain bestaat uit zeven categorieën gebaseerd op wat soort aanval er wordt uitgevoerd. Alienvault heeft de Cyber Kill Chain samengevat tot vijf categorieën. De Cyber Kill Chain gaat van *reconaissance*, het verzamelen van informatie over het slachtoffer, tot *system compromise* waarbij de aanvaller volledige controle heeft over het toestel.

Op deze manier krijg je als analist snel een overzicht van het type aanvallen die in het bedrijfsnetwerk plaatsvinden. Hoe groter de cirkel in een bepaalde categorie, hoe groter het aantal aanvallen dat hebben plaatsgevonden.



Figuur 25: Alarmen gerangschikt volgens Cyber Kill Chain

Alienvault beschikt ook over een Host Intrusion Detection System (HIDS). Hiervoor dient echter wel een *agent* geïnstalleerd te worden op de *host* zelf. Deze *agents* kunnen automatisch geïnstalleerd worden vanuit de Alienvault *web interface*. In mijn geval was dit echter niet mogelijk omdat Kaspersky Endpoint Protection dit steeds blokkeerde. Wanneer dit het geval is, is er nog steeds te mogelijkheid om de *agent installer* te downloaden en manueel te installeren op een *host*. Dit is echter heel omslachtig omdat elke *agent* geconfigureerd wordt op basis van het *host* besturingssysteem.

Na het installeren van de *agent* krijg je een heel aantal extra functionaliteiten. Op Windows besturingssystemen heb je nu, onder andere, de mogelijkheid tot *file integrity monitoring*. Automatisch wordt ook de system32 *folder* en bepaalde delen van het register in de gaten gehouden op wijzigingen.

II. Onderzoekstopic: Vergelijking SIEM-oplossingen

1 Probleemstelling

Bij een Security Operations Center (SOC) staat meestal een Security Information and Event Management (SIEM) oplossing centraal. De functie van een SIEM is het verzamelen van alle logs en daarop correlatie en realtime analyse uitvoeren. Op basis hiervan worden dan *security alerts* gegenereerd. Aangezien dit een cruciaal element is van een SOC gaan er verschillende SIEM-oplossingen met elkaar vergeleken worden.

2 Methode van onderzoek

Het onderzoek bestaat uit zowel theoretische kennis als ervaring opgedaan met het desbetreffende product. Theoretische kennis komt neer op het vergelijken van reviews van verschillende onafhankelijke partijen en die beschikbaar is op de website van de ontwikkelaar van iedere SIEM-oplossing.

De verschillende SIEM-systemen zijn één voor één getest geweest wegens de tijdsbeperkingen die op de proefevaluaties staan. Initieel was het de bedoeling om met een aparte *log manager* (Splunk Light) te werken. Zo zou er dan de mogelijkheid zijn om over historische data te beschikken en deze data naar ieder SIEM-systeem te sturen. Helaas is dit enkel mogelijk met de Splunk Enterprise versie.

2.1 Geteste SIEM-oplossingen

De SIEM-oplossingen die getest gaan worden zijn:

- *Solarwinds SIEM: Log & Event Manager*
- *IBM QRadar SIEM**
- *Alienvault***

* Bij QRadar wordt er gebruik gemaakt van de gratis Community Edition.

**Bij Alienvault wordt er gebruik gemaakt van Alienvault Unified Security Management (USM) Platform. Voor het onderzoeksrapport wordt er in deze alles-in-eenoplossing dieper ingegaan op het SIEM gedeelte.

2.2 Aspecten van het onderzoek

- *Vergelijking van de belangrijkste functies en mogelijkheden*
- *Correlatie van data*
- *Vergelijking van kostprijs*
- *Aanpassingsmogelijkheden van alerts*
- *Gebruiksgemak/leercurve*
- *Mogelijkheid om SIEM-as-a-service aan te bieden aan klanten*

3 Literatuurstudie

SIEM-oplossingen zijn een niche-product, hierdoor is het niet mogelijk om reviews over alle producten uit één bron te halen en deze te vergelijken. Omwille van deze reden zullen er meerdere bronnen geraadpleegd worden. Per bron is er steeds voor slechts één of twee producten een review beschikbaar.

3.1 Solarwinds: Log & Event Manager

Solarwinds: Log & Event Manager (LEM) is het SIEM-platform van het bedrijf Solarwinds. Solarwinds heeft vele verschillende producten die betrekking hebben tot netwerk, systeem- en databasemanagement, security, *helpdesk* en *cloudtools*. Solarwinds: Log & Event Manager is een combinatie van verschillende producten van Solarwinds die gecombineerd zijn in één nieuw pakket.

3.1.1 Belangrijkste functies en mogelijkheden

- *Realtime event correlatie*
- *Threat intelligence*
- *Actieve respons*
- *Uitgebreide zoekfunctie en forensische analyse*
- *USB-monitoring*
- *Rapportering (compliance)*

Realtime event correlatie

Door alle binnenkomende logs in realtime te verwerken kan er onmiddellijk actie ondernomen worden. Dit kan zowel manueel aan de hand van de gegenereerde alerts of volledig automatisch op basis van op voorhand gedefinieerde regels. Deze regels kunnen zeer eenvoudig gemaakt worden door middel van *drag-and-drop*.

Threat intelligence

De ingebouwde *threat intelligence* zorgt ervoor dat het systeem steeds up-to-date is met bekende hosts en IP-adressen die gebruikt worden door cybercriminelen. Op deze manier wordt, bijvoorbeeld, verkeer met een *command and control server* snel waargenomen en kan er actie ondernomen worden.

Actieve respons

Op basis van ingestelde regels kan er automatisch actie ondernomen worden om onmiddellijk dreigingen te stoppen. Indien gewenst kunnen een beperkt aantal acties ook handmatig worden uitgevoerd in slechts enkele muisklikken. Zo kan een *USB-stick* softwarematig ontkoppeld worden wanneer er een virus op gedetecteerd wordt. Gebruikers kunnen in quarantaine geplaatst worden wanneer er contact gemaakt wordt met een IP-adres dat bekend staat om kwaadaardige activiteit. Er zijn enorm veel gelijkaardige mogelijkheden binnen Solarwinds. [36]

Uitgebreide zoekfunctie en forensische analyse

Via nDepth wordt er toegang verkregen tot overzichtelijke grafieken die het aantal events die onderzocht moeten worden snel worden weergegeven. Aan de hand van additionele filters zoals IP-adres, gebruikersnaam of de zwaarte van het event kan er snel een overzicht gecreëerd worden van het eerste event dat aan de voorwaarde voldoet en alle daaropvolgende events. Op deze manier wordt er geen tijd verloren bij het onderzoeken van alarmen en incidenten. [37]

USB-monitoring

Met de USB-monitoring kan er een overzicht gecreëerd worden van alle aangesloten USB-apparaten. Zo kan er gezien worden welke data van de USB afkomt, wordt aangepast of naartoe gekopieerd.

Rapportering

Met de ingebouwde rapporteringsfunctie kunnen er zeer snel rapporten gegenereerd worden om aan te tonen dat de regelgeving correct gevolgd wordt. Alhoewel dit voornamelijk voor de Amerikaanse klanten zeer belangrijk is, wordt dit binnenkort ook van cruciaal belang bij het in werking treden van de GDPR in Europa.

3.1.2 Correlatie van data

Wanneer een event geselecteerd wordt in de *alert stream* kan via nDepth de datacorrelatie bekeken worden. Hier wordt overzichtelijk getoond hoe vaak het evenement zich heeft voorgedaan en op welke tijdstippen. Er kan extra gefilterd worden op basis van alle waarden die in het event beschikbaar zijn zoals onder andere een IP-adres of het apparaat waarop het event is gedetecteerd (bijvoorbeeld *firewall*). Ook kan er manueel een extra filter aan toegevoegd worden. In nDepth is er naast vele andere aanpasbare grafieken ook een *word cloud* beschikbaar. Op deze manier wordt er snel een overzicht gecreëerd van de meest voorkomende termen die dan kunnen helpen met het onderzoek. [37]

3.1.3 Vergelijking van kostprijs

De prijs bij Solarwinds: Log & Event Manager is gebaseerd op basis van *nodes*. Solarwinds: Log & Event Manager begint vanaf 3.665 euro per jaar voor 30 *nodes*.

3.1.4 Aanpassingsmogelijkheden van alerts

Er kan geselecteerd worden wanneer een *rule* geactiveerd wordt op basis van het aantal events binnen een bepaald tijdsframe. Zo kan je een alert laten genereren wanneer er slechts 1 event is in een tijdsframe van 1 seconde. Hierdoor wordt er onmiddellijk actie ondernomen. Het aantal events dat er moeten gebeuren kan aangepast worden alsook de tijd waarin deze events voorkomen. Zo kan de tijd waarin het aantal events voorkomen vooraleer de *rule* wordt geactiveerd aangepast worden van seconden tot uren.

3.1.5 Gebruiksgemak en leercurve

Solarwinds: Log & Event Manager wordt aangeleverd als virtuele *appliance* of als fysieke *appliance*. Op deze manier heb je weinig kennis nodig om het systeem draaiende te krijgen zodat je snel kan beginnen met je bestaande systemen te koppelen aan Solarwinds: Log & Event Manager. De initiële webinterface die je te zien krijgt na installatie is redelijk overweldigend in het begin. Gelukkig is er een '*Getting Started*'-sectie die je verder helpt om aan de slag te gaan met Solarwinds: Log & Event Manager.

Dankzij de *drag-and-drop*manier die gebruikt wordt om *rules* te creëren is ook hier niet veel voorkennis voor nodig. Er zijn veel verschillende mogelijkheden waarop je *rules* kan baseren wat zeer verwarrend is in het begin wegens de overvloed aan informatie en mogelijkheden.

3.1.6 Mogelijkheid om SIEM-as-a-service aan te bieden aan klanten

Er is slechts een beperkte mogelijkheid om SIEM-as-a-service aan te bieden. Er is geen *multi-tenancy* mogelijkheid beschikbaar waardoor je logs rechtstreeks van de klant naar je eigen SIEM-opstelling gestuurd moeten worden. Dit veroorzaakt een grote netwerk belasting wanneer dit bij meerdere grote klanten wordt gedaan.

Een andere oplossing is om bij elke klant lokaal een systeem op te zetten om dan van op afstand in te loggen op hun systeem.

3.2 IBM QRadar SIEM

QRadar is het security platform van technologie reus IBM. In 2003 heeft IBM QRadar SIEM geïntroduceerd. Het behoorde tot een van de eerste SIEM-systemen op de markt. Vandaag de dag is het de leider in SIEM-systemen volgens Gartner's Magic Quadrant for SIEM. [25] QRadar SIEM is, net zoals bij Solarwinds, een combinatie van meerdere producten. Hierbij heb je nog eens de mogelijkheid om extra *add-ons* te installeren om zo je SIEM uit te breiden naar gelang de behoefte van je organisatie of klanten. [38]

3.2.1 Belangrijkste functies en mogelijkheden

- Detectie van geavanceerde aanvallen
- Realtime event correlatie
- Koppelen van incidenten en gevaren
- Uitgebreide rapportering om het bedrijfsbeleid na te streven
- Mogelijkheid om *add-ons* te installeren

Detectie van geavanceerde aanvallen

Vanwege de mogelijkheid om vele verschillende soorten logs en events van verschillende bronnen te implementeren is het systeem in staat om geavanceerde aanvallen te detecteren. Deze aanvallen zouden door de individuele beveiligingsproducten zoals een firewall nooit gedetecteerd kunnen worden.

Realtime event correlatie

Door de grote hoeveelheid logs en events die binnenkomen eerst te normaliseren alvorens correlatie op toe te passen krijg je een bijna realtime correlatie systeem. Door eerst een basislijn te creëren kan er achteraf sneller kwaadaardig verkeer gedetecteerd worden. Indien je dit combineert met de IBM X-Force Threat Intelligence *add-on* is het systeem ook bekend met IP adressen die door cyber criminelen worden gebruikt.

Koppelen van incidenten en gevaren

QRadar SIEM kan niet enkel analyse uitvoeren op data die het op dat moment binnenkrijgt maar ook op historische data die je in het systeem inbrengt. Als extra bescherming zijn hier ook weer add-ons beschikbaar die een dieper inzicht kunnen brengen in het netwerkverkeer door *deep packet inspection* toe te passen op *layer* 7 netwerk verkeer.

Uitgebreide rapportering om het bedrijfsbeleid na te streven

De ingebouwde rapportage functie zorgt ervoor dat iedereen gemakkelijk rapporten kan maken die snel een overzicht geven over wat er allemaal gaande is binnen de organisatie op vlak van computergebruik en netwerkverkeer. Hierdoor heb je geen kennis nodig van database functies om aan de manager een rapport te kunnen geven wanneer hiernaar gevraagd wordt.

Mogelijkheid om *add-ons* te installeren

Zoals al eerder aangehaald heb je bij QRadar SIEM de mogelijkheid om *add-ons* te installeren naargelang de behoefte hiernaar. Op deze manier krijg je een goed werkend basis product met de mogelijkheid om extra functionaliteit toe te voegen. De keerzijde van de medaille is dan weer dat sommige functionaliteiten eerst als *add-on* geïnstalleerd moeten worden waar dit bij andere SIEM-systemen standaard zit ingebouwd. [39]

3.2.2 Correlatie van data

QRadar SIEM past eerst normalisatie toe op de binnenkomende data zodat de vele inkomende logs en *alerts* gereduceerd worden tot een gemakkelijk verwerkbaar aantal. Er zijn vele regels reeds geactiveerd bij installatie die eenvoudig aangepast kunnen worden naar eigen wens. Met slechts enkele muisklikken kan er gekozen worden welke events zichtbaar zijn, de genormaliseerde events of de rauwe logs zoals ze binnenkomen in QRadar. [40]

3.2.3 Vergelijking van kostprijs

De kostprijs voor QRadar SIEM is gebaseerd op Events Per Second (EPS). Voor QRadar *on premise* is het startbedrag 10 400 dollar met een maximum van 1000 EPS. Indien een *cloud-based* oplossing de voorkeur heeft is de laagste prijs 800 dollar per maand voor een minimumtermijn van 1 jaar.

3.2.4 Aanpassingsmogelijkheden van alerts

Alle regels, zowel op voorhand gedefinieerde als zelfgemaakte, kunnen volledig naar eigen wens worden aangepast. De mogelijkheden zijn vergelijkbaar met die van Solarwinds: Log & Event Manager.

3.2.5 Gebruiksgemak en leercurve

Ook bij QRadar SIEM is de initiële installatie en configuratie zeer gemakkelijk. IBM heeft voor de QRadar Community Edition een YouTube afspeellijst gemaakt waarin de initiële installatie en configuratie te volgen is. Van het aanmaken van een CentOS virtuele machine tot het toevoegen van logs en aanpassen van detectieregels.

QRadar zelf daarentegen heeft een redelijk steile leercurve. Dit is gedeeltelijk omdat QRadar zo uitgebreid is dat er enorm veel verschillende menu's zijn. De *user interface* zelf is ook niet altijd vanzelfsprekend waardoor het niet altijd even gemakkelijk is om efficiënt te navigeren naar wat je opzoek bent.

3.2.6 Mogelijkheid om SIEM-as-a-service aan te bieden aan klanten

QRadar SIEM is beschikbaar in verschillende producten. Zo heb je *all-in-one appliances* die ideaal zijn voor kmo's. Heb je echter te maken met grotere klanten dan kan je verschillende *appliances* installeren die allemaal een eigen rol hebben. [41]

Een Event Collector verzamelt dan alle events en stuurt deze door naar een Event Processor die al het zware werk doet. De Event Processor stuurt dan zijn bevindingen door naar de Magistrate die vervolgens de ingestelde regels gaat toepassen op deze data en alerts gaat genereren. Via de Console dat de user interface voor zijn rekening neemt, kunnen alle realtime *events* en *alerts* bekeken worden die de Magistrate heeft gegenereerd. Op de Console kunnen ook rapporten gegenereerd worden, informatie over netwerktoestellen opgevraagd en administratieve functies uitgevoerd worden.

Er zitten uitgebreide mogelijkheden in QRadar om een *multi-tenant* setup op te zetten. Voor elke klant kan een domein aangemaakt worden zodat alles steeds netjes gescheiden blijft.

3.3 Alienvault Unified Security Management

Alienvault is een redelijk nieuwe speler op de SIEM markt. Echter hebben zij zichzelf geëvolueerd naar een product met een groot klantenbestand waaronder vele bekende bedrijven. Al een heel aantal jaren (sinds 2013) is Alienvault het enige product dat in categorie '*Visionary*' staat in de Gartner's Magic Quadrant for SIEM. Alienvault is een product dat gemaakt is om ook gebruikt te worden door kleinere security teams van slechts 5 personen, vergeleken met de meeste SIEM-oplossingen waar dit niet het geval is en een team van minstens 10 man alles in de gaten houdt. [42] [43] [44] [45]

3.3.1 Belangrijkste functies en mogelijkheden

- *Asset discovery & inventarisatie*
- *Vulnerability assessment*
- *Intrusion detection*
- *Gedragsmonitoring*
- *Event correlatie*

Asset discovery & inventarisatie

Alienvault heeft een *asset discovery* functie die alle toestellen en apparaten in het netwerk opspoort en maakt hier een inventaris van. Niet enkel het apparaat zelf wordt bijgehouden maar ook welke *services* hier op draaien. Zo kan er bij een webserver gedetecteerd worden wanneer de Apache *service* niet meer beschikbaar is en hier een alarm voor genereren.

Er zijn drie verschillende manieren om aan *asset discovery* te doen. Manueel één per één toevoegen, op basis van *network ranges* of via een CSV-bestand.

Vulnerability assessment

Alienvault maakt gebruik van Open Vulnerability Assessment System (OpenVAS). Dit is een *open source vulnerability scanner*. Met deze functie kun je de bekende *vulnerabilities* combineren met alle andere informatie om zo sneller en beter gevaren binnen je netwerken op te sporen en te elimineren. Deze functie zit bij Alienvault in het pakket ingebouwd. Iets waar je bij andere SIEM-oplossingen extra voor moet betalen of een apart *vulnerability* systeem voor moet worden geïmplementeerd in het netwerk.

Intrusion detection

Alienvault beschikt over een Network Intrusion Detection System (NIDS), Host Intrusion Detection System (HIDS) en File Integrity Monitoring (FIM). Net zoals bij *vulnerability management* zorgt dit er voor dat er geen extra systemen moeten worden opgezet om deze taken te vervullen. Indien je opteert voor de *Cloud*-oplossing van Alienvault beschik je ook over *Cloud* IDS om je Amazon Web Services (AWS) en Microsoft Azure-omgevingen in de gaten te houden. [46]

Gedragsmonitoring

Net als andere hedendaagse SIEM-producten beschikt ook Alienvault over de mogelijkheid om gedragsmonitoring toe te passen. Door het verkeer en de inkomende logs te vergelijken met het normale gedrag binnen het netwerk kunnen er onaardigheden gedetecteerd worden.

Event correlatie

De realtime event correlatie zorgt ervoor dat je steeds op de hoogte bent van alle incidenten die zich voordoen binnen het netwerk. Wanneer een *rule* geactiveerd wordt, dan wordt deze ook altijd gerangschikt volgens de *Cyber Kill Chain* ontwikkeld door Lockheed Martin. Zo kan je snel en overzichtelijk zien hoe gevaarlijk de dreiging is. [47]

3.3.2 Correlatie van data

Gelijkaardig aan IBM QRadar SIEM past ook Alienvault eerst normalisatie toe alvorens de data te correleren. Wanneer er ergens dieper op in wordt gegaan, kan er gefilterd worden op onder andere *event* naam en IP-adres. Bij elk *event* is er een beschrijving van het *event* zelf en een indicatie van de ernst van de dreiging. Ook is het IP-adres te zien vanwaar de dreiging afkomstig is en het interne IP-adres dat wordt aangevallen. Indien het IP-adres van waaruit de aanval afkomstig is bekend is bij Alienvault's Open Threat Exchange (OTX) kan er meer informatie over deze *host* bekomen worden via het OTX platform. De rauwe log en event data kan ook steeds bekeken worden, mocht dit gewenst zijn.

3.3.3 Vergelijking van kostprijs

De kostprijs voor de goedkoopste fysieke *all-in-one* bedraagt 5 595 dollar per jaar. Hier kunnen 25 *assets* mee gemonitord worden. De goedkoopste *cloud*-oplossing (Essentials) bedraagt 650 dollar per maand met een maximum van 250GB aan data en 1 sensor. De kostprijs gaat omhoog naargelang er meer data verbruikt wordt. Ook heb je nog 2 hogere pakketten genaamd Standard en Enterprise met respectievelijk 2 en 10 sensors ter beschikking. Standard begint op 1575 dollar per maand op basis van 250GB aan data. Voor Enterprise is een prijs niet vrij beschikbaar maar dient de sales afdeling van Alienvault gecontacteerd te worden.

3.3.4 Aanpassingsmogelijkheden van alerts

Net zoals bij Solarwinds: Log & Event Manager en IBM QRadar SIEM kunnen alle regels, zowel op voorhand gedefinieerde als zelfgemaakte regels, naar eigen wens worden aangepast.

3.3.5 Gebruiksgemak en leercurve

Alienvault is net zoals de andere SIEM-systemen gemakkelijk te installeren en om het systeem draaiende te krijgen. Doordat Alienvault vele functies reeds heeft ingebouwd zoals IDS en *vulnerability scanning* bespaart het tijd en moeite om deze systemen zelf op te zetten en te implementeren in Alienvault. Van al de geteste SIEM-producten is Alienvault het makkelijkste om mee aan de slag te gaan zonder enige voorkennis.

3.3.6 Mogelijkheid om SIEM-as-a-service aan te bieden aan klanten

Alienvault beschikt over een, zoals ze het zelf noemen, *Federated Architecture*. Dit zorgt ervoor dat je als groot bedrijf alle data van meerdere locaties kunt doorsturen naar de plaats waar het security team zich bevindt. Deze lijn kan doorgetrokken worden naar *SIEM-as-a-service*. Het zware werk wordt gedaan door een *appliance* die bij de klant wordt geplaatst. Deze *appliance* stuurt zijn informatie gecomprimeerd door naar de hoofdserver in het Security Operations Center zodat van daaruit alles in de gaten gehouden kan worden. Om alles netjes gescheiden en overzichtelijk te maken kunnen er groepen gecreëerd worden per klant.

3.4 Vergelijkingsmatrix van de functionaliteiten

Tabel 1: Vergelijking SIEM-oplossingen

	SOLARWINDS	QRADAR	ALIENVAULT
LOG CORRELATIE	X	X	X
AGENTLESS LOG COLLECTIE	X	X	X
CLOUD SERVICE MOGELIJKHEID		X	X
INTRUSION PREVENTION		Betaalde add-on	X
DATA LOSS PREVENTION	USB only		X
RAPPORTERING TEMPLATES	X	X	X
GEAUTOMATISEERD ACTIES ONDERNEMEN	X	X	
MULTI-TENANT		X	X

4 Conclusie

Uit zowel de stageopdracht als de onderzoeksopdracht blijkt, voor Data Unit, Alienvault USM het meest geschikt te zijn om een Security Operations Center op te starten. Hieronder ga ik nog een aantal belangrijke punten aanhalen om mijn conclusie te motiveren.

Personeel

Om een Security Operations Center op te zetten heb je personeel nodig die alles in de gaten kan houden en ingrijpen wanneer het fout gaat. Ook wanneer er eerst klein wordt opgestart met enkel tier 1 functionaliteit is extra personeel vereist.

Alienvault is ontworpen om ook gebruikt te worden door een kleiner SOC team.

Kennis personeel en leercurve

Met het opzetten van een Security Operations Center moet ook de kennis van het personeel uitgebreid worden. Er komen namelijk nieuwe producten bij waarmee het personeel moet werken. Aangezien Alienvault een alles-in-eenoplossing is moet er slechts van één nieuw product kennis opgedaan worden.

Bij het ontwikkelen van Alienvault is naast een kleiner SOC team ook rekening gehouden met de leercurve die gepaard gaat met gebruiken van Alienvault. De menu's en *dashboards* zijn overzichtelijk zonder dat je overdonderd wordt door de hoeveelheid informatie. De meest gebruikte functionaliteiten zijn snel en gemakkelijk bereikbaar zonder compromis op de complexere functionaliteiten.

Kostprijs

Ondanks dat Alienvault op papier niet als goedkoopste uit onderstaande tabel komt, is het toch zeer competitief geprijsd. Waar Solarwinds puur een SIEM is, krijg je bij Alienvault niet enkel SIEM mogelijkheden maar ook nog *asset discovery & monitoring*, IDS, *vulnerability scanning* en nog veel meer.

Tabel 2: Vergelijking van kostprijs

	SOLARWINDS	QRADAR	ALIENVAULT
AANTAL DEVICES/EPS	**30 devices**	**1000 EPS**	**25 devices**
KOSTPRIJS	**€ 3 665**	**$ 10 400**	**€ 5 595**

SIEM-as-a-service

Een belangrijke *requirement* voor de gekozen SIEM-oplossing is het kunnen aanbieden van SIEM-as-a-service. Op deze manier kan Data Unit een extra service aanbieden aan nieuwe en huidige klanten. Waaronder velen reeds over Barracuda en/of Kaspersky producten via Data Unit.

Met Alienvault is er de mogelijkheid om dit aan te kunnen bieden als extra dienst vanwege *Federated Deployment*. Zo wordt er bij de klant een Alienvault sensor in het interne netwerk geplaatst die alle logs gaat verzamelen en alarmen genereren. Deze alarmen worden dan doorgestuurd naar de Alienvault server in het SOC van Data Unit.

5 Reflectie

Voor de start van mijn stage was ik zowel nieuwsgierig als nerveus. Langs de ene kant heb ik een sterke interesse in security en was ik zeer enthousiast om aan de stage te beginnen. De security tak binnen informatica is een richting die ik na mijn studies ook verder wil uitgaan. Langs de andere kant was het een hele grote opdracht boordevol elementen die mij onbekend waren. Het was dus een ware sprong in het duister. Security is namelijk iets wat, tijdens mijn studie, slechts in beperkte maten aan bod is gekomen. Het zorgde echter wel voor een goede basis waar ik mee aan de slag kon.

In de eerste weken van mijn stage heb ik veel bijgeleerd over wat er allemaal komt kijken bij het opzetten van een Security Operations Center en wat het allemaal inhoudt. Tijdens deze theoretische onderzoeksfase heb ik uiteraard ook veel bijgeleerd over security in het algemeen. Gedurende de stage heb ik zo goed als enkel met software gewerkt waar ik nog nooit eerder mee in aanraking was gekomen. Dit was in het begin een grote uitdaging en zorgde van tijd tot tijd tot problemen. Deze problemen waren er voornamelijk met het opzetten van een aantal systemen. Hier is er redelijk wat tijd gespendeerd en verloren om alles werkend te krijgen. Op dit vlak heeft het deftig leren documenteren tijdens het opzetten van systemen enorm geholpen. Het initiële opzetten en installeren duurt aanzienlijk langer. Wanneer er fouten tijdens de installatie zijn ingeslopen of een volledige herinstallatie vanaf nul nodig is. Op zo een momenten heb je dan een goed document dat als leidraad gebruikt kan worden.

Ik kan met tevredenheid terugkijken op mijn stage periode. Ik heb met vele nieuwe technologieën mogen werken en behulpzame collega's die mij steeds trachtte verder te helpen wanneer ik vragen had.

6 Bibliografie

[1] A. Torres, „Building a World-Class Security Operations Center: A Roadmap," 10 2017. [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907.

[2] „Wikipedia GDPR," 23 11 2017. [Online]. Available: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.

[3] I. c. services, „GDPR Info," 23 11 2017. [Online]. Available: https://gdpr-info.eu/art-33-gdpr/.

[4] Splunk, „Building a SOC with Splunk," 11 2017. [Online]. Available: https://www.splunk.com/pdfs/technical-briefs/building-a-soc-with-splunk-tech-brief.pdf.

[5] B. Networks, Artist, *Logo Barracuda.* [Art]. Barracuda Networks, 2017.

[6] „Barracuda Company Overview," Barracuda, 12 2017. [Online]. Available: https://www.barracuda.com/company/index.

[7] „Barracuda Open Source," 12 2017. [Online]. Available: https://www.barracuda.com/company/opensource.

[8] K. Lab, Artist, *Logo Kaspersky Lab.* [Art]. Kaspersky Lab, 2017.

[9] „Kaspersky: About," 12 2017. [Online]. Available: https://www.kaspersky.com/about.

[10] „Kaspersky Top 3," 12 2017. [Online]. Available: https://www.kaspersky.com/top3.

[11] „Snort Wikipedia," 12 12 2017. [Online]. Available: https://en.wikipedia.org/wiki/Snort_(software).

[12] „Snort FAQ," 12 12 2017. [Online]. Available: https://www.snort.org/faq.

[13] Suricata, Artist, *Logo Suricata.* [Art]. Suricata, 2017.

[14] „Suricata Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Suricata_(software). [Geopend 12 12 2017].

[15] „Suricata," Suricata, 12 12 2017. [Online]. Available: https://suricata-ids.org/.

[16] OpenVAS, Artist, *Logo OpenVAS.* [Art]. OpenVAS, 2017.

[17] „OpenVAS Homepage," [Online]. Available: http://openvas.org/. [Geopend 01 2018].

[18] Splunk, Artist, *Logo Splunk Light.* [Art]. Splunk, 2017.

[19] „Wikipedia Splunk," [Online]. Available: https://en.wikipedia.org/wiki/Splunk. [Geopend 01 2018].

[20] Splunk, „Splunk apps en adds-on," Splunk, 01 2018. [Online]. Available: https://www.splunk.com/en_us/products/apps-and-add-ons.html.

[21] Solarwinds, Artist, *Logo Solarwinds.* [Art]. 2018.

[22] „Wikipedia Solarwinds," 01 2018. [Online]. Available: https://en.wikipedia.org/wiki/SolarWinds.

[23] Solarwinds, Artist, *Real-time event correlatie.* [Art]. Solarwinds, 2018.

[24] IBM, Artist, *Logo IBM.* [Art]. IBM, 2018.

[25] „SI Gartner 2017 Magic Quadrant for SIEM," Secuirty Intelligence, 1 2018. [Online]. Available: https://securityintelligence.com/ibm-security-maintains-a-leadership-position-in-the-gartner-2017-siem-magic-quadrant/.

[26] Alienvault, Artist, *Logo Alienvault.* [Art]. Alienvault, 2018.

[27] Alienvault, „AV Fact Sheet," Alienvault, 01 2018. [Online]. Available: https://www.alienvault.com/docs/AlienVault_Fact_Sheet.pdf.

[28] Alienvault, „OSSIM/USM vergelijking," Alienvault, 01 2018. [Online]. Available: https://www.alienvault.com/products/ossim/compare.

[29] Alienvault, „Alienvault OTX," Alienvault, 01 2018. [Online]. Available: https://www.alienvault.com/open-threat-exchange.

[30] Alienvault, „OTX STIX/TAXII," Alienvault, 01 2018. [Online]. Available: https://www.alienvault.com/blogs/security-essentials/otx-is-now-a-free-stix-taxii-server.

[31] Wikipedia, „Wikipedia OSSIM Components," 11 01 2018. [Online]. Available: https://en.wikipedia.org/wiki/OSSIM.

[32] Snort, „Snort homepage," Snort, 01 2018. [Online]. Available: https://www.snort.org/.

[33] Snort, „Snort Uitleg Talos," Snort, 01 2018. [Online]. Available: https://www.snort.org/faq/what-is-the-role-of-talos.

[34] Greenbone, „Greenbone Partners," Greenbone, 01 2018. [Online]. Available: https://www.greenbone.net/en/find-a-partner/.

[35] J. Bravo, „Youtube QRadar Community Edition Playlist," IBM, 01 2018. [Online]. Available: https://www.youtube.com/watch?v=Ii62Qy3ggnQ&list=PLHh9jhztlMyom5iT0a1JCpQgeK8j3blZf.

[36] Solarwinds, „Solarwinds info pagina," Solarwinds, 01 2018. [Online]. Available: https://www.solarwinds.com/siem-security-information-event-management-software.

[37] A. Leskim, „NMS LEM review," Network Management Software, 01 2018. [Online]. Available: http://www.networkmanagementsoftware.com/log-and-event-manager-review/.

[38] „QRadar," QRadar, 14 12 2017. [Online]. Available: https://www.ibm.com/us-en/marketplace/ibm-qradar-siem.

[39] „QRadar App Exchange," QRadar, 14 12 2017. [Online]. Available: https://www.ibm.com/security/community/app-exchange.

[40] D. Robb, „eSecurity Planet IBM QRadar SIEM review," eSecurity planet, 11 2017. [Online]. Available: https://www.esecurityplanet.com/products/ibm-security-qradar-siem.html.

[41] QRadar, „QRadar Datasheet," QRadar, 11 2017. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGD03021USEN.

[42] Gartner, Artist, *Gartner Magic Quadrant for SIEM.* [Art]. Gartner, 2013.

[43] Gartner, Artist, *Gartner Magic Quadrant for SIEM.* [Art]. Gartner, 2014.

[44] Gartner, Artist, *Gartner Magic Quadrant for SIEM.* [Art]. Gartner, 2015.

[45] Gartner, Artist, *Gartner Magic Quadrant for SIEM.* [Art]. Gartner, 2016.

[46] Alienvault, „Alienvault IDS," Alienvault, 11 2017. [Online]. Available: https://www.alienvault.com/solutions/intrusion-detection-system.

[47] „Lockheed Martin Cyber Kill Chain," Lockheed Martin, 11 2017. [Online]. Available: https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html.

[48] Snort, Artist, *Logo Snort.* [Art]. Snort, 2017.