Professionele Bachelor Toegepaste Informatica

Endpoint Detection and Response: een vergelijkende studie

Glen Kenens

Promotoren:

Raphael Cox — SecWise
Gert Van Waeyenberg — Hogeschool PXL Hasselt

Bachelorpaper Academiejaar 2018-2019

Professionele Bachelor Toegepaste Informatica

SecWise

Endpoint Detection and Response: een vergelijkende studie

Glen Kenens

Promotoren:

Raphael Cox
SecWise
Gert Van Waeyenberg
Hogeschool PXL Hasselt

Bachelorpaper Academiejaar 2018-2019

Dankwoord

Voor aanvang van dit eindwerk zou ik graag even de tijd nemen om iedereen te bedanken die mee heeft geholpen om dit eindwerk tot een goed einde te brengen.

De eerste personen die ik graag zou willen bedanken zijn mijn begeleiders binnen SecWise. Keith Custers, Koen Jacobs en Raphael Cox. Zij stonden altijd voor mij klaar als ik vragen had, maar gaven me ook voldoende ruimte om zelfstandig mijn eindwerk tot een goed einde te brengen. Ik heb ongelofelijk veel dingen bijgeleerd tijdens mijn stage bij SecWise en zou hen graag bedanken voor deze geweldige kans.

Verder wil ik ook alle PXL-lectoren bedanken die hebben bijgedragen aan het voltooien van dit eindwerk. In het bijzonder wil ik mijn hogeschoolpromotor Gert Van Waeyenberg bedanken voor het goede advies en de constructieve kritiek.

Abstract

Security in de informaticasector heeft de laatste jaren een grote evolutie meegemaakt. Aanvallers gebruiken steeds vaker technieken waarmee traditionele antivirustoepassingen geen raad weten. Hier komt nog eens bovenop dat de hoeveelheid aanvallen zo groot wordt dat het voor securityexperts onmogelijk wordt om nog een duidelijk overzicht te krijgen van wat er precies in hun netwerk gebeurt. Combineer dit met de overstap naar cloudomgevingen die veel bedrijven de dag van vandaag overwegen en het wordt duidelijk dat een investering in security bijna onvermijdelijk is.

Een oplossing voor dit probleem is een Endpoint Detection and Response (EDR)-systeem. Dit verzamelt data van *endpoints* en kan op die manier niet alleen tijdig ingrijpen wanneer er verdachte handelingen gebeuren, maar ook bepalen wat er is misgegaan als er toch aanvallers binnen geraken. Op die manier kunnen securityexperts snel zien wat er aangetast is en hoe ze dit in de toekomst kunnen vermijden. Omdat deze systemen werken op basis van het patroon dat een aanval volgt, zijn ze ook beter bestand tegen onbekende aanvallen. Dit veroorzaakt wel een nieuw probleem, namelijk: hoe bepaalt een bedrijf welke EDR-tool het best bij hen past?

In dit eindwerk wordt er een uitgebreide analyse gemaakt van de verschillende EDR-toepassingen die er momenteel op de markt zijn. Er wordt een vergelijking gemaakt van de besturingssystemen die ondersteund worden. Daarnaast wordt er een overzicht gegeven van wat de toepassing biedt, van de manieren waarop de tool gebruikt kan worden om in te grijpen in het geval van een inbraak en van de verschillende manieren waarop een tool bedreigingen detecteert. Ook de investering die nodig is wat betreft systeemresources wordt in kaart gebracht.

Verder wordt er in dit eindwerk ook onderzoek gedaan naar extra oplossingen die de onderzochte bedrijven aanbieden.

Het resultaat is een eindwerk waarin wordt toegelicht in welke netwerken een EDR-toepassing een meerwaarde kan bieden en welke producent het best geschikt is in welke situaties.

Inhoudsopgave

Lijst van gebruikte figuren

Lijst van gebruikte tabellen

Lijst van gebruikte afkortingen en begrippen

Begrip	Verklaring
Agent	Software die geïnstalleerd wordt op een *endpoint* en die ervoor zorgt dat deze kan communiceren met een centrale EDR toepassing.
CLI	Command Line Interface
EDR	Endpoint Detection and Response
Endpoint	Een fysiek toestel dat kan connecteren met het internet en zich op het netwerk bevindt.
IRM	Information Rights Management
OME	Office 365 Message Encryption
RBAC	Role Based Access Control: Een systeem waarmee de toegang die gebruikers tot een systeem hebben beperkt wordt door de rollen die ze toegewezen krijgen.
SaaS	Software as a Service: Een toepassing die online in de cloud aangeboden wordt. Hierdoor moeten klanten zelf geen infrastructuur voorzien.
VM	Virtuele Machine
RCA	Root Cause Analysis

Inleiding

Elk bedrijf krijgt dezer dagen te maken met cybercriminelen. Het is niet langer de vraag of een bedrijf wordt aangevallen maar wanneer. Hierdoor implementeren steeds meer bedrijven geavanceerde security tools. Een van zulke tools is een EDR-oplossing. Deze stelt bedrijven in staat om een vollediger beeld van een cyberaanval te vormen. Zo wordt er niet enkel gekeken naar de gedetecteerde bedreiging, maar ook aan alle acties die eraan vooraf gingen.

In opdracht van SecWise NV is er onderzoek verricht naar de verschillende EDR-tools die enkele bedrijven aanbieden. Op deze manier zal duidelijk worden wat de sterke en zwakke aspecten van elke tool zijn. Ook is er onderzoek verricht naar de volledigheid van het aanbod van deze onderzochte bedrijven.

In dit eindwerk zullen eerst de analyses van de verschillende EDR-tools besproken worden. Aan de hand van een vergelijkingsmatrix worden deze tools vervolgens objectief met elkaar vergeleken. Op basis van deze vergelijkingsmatrix kan er dan een beeld gevormd worden van de optimale omstandigheden voor elke tool.

Verder is de performantie van de tools getest in een virtuele testomgeving. Op basis van deze resultaten zijn de onderzochte tools onderverdeeld in lichte, gemiddelde en zware tools.

Tot slot wordt van de belangrijkste security oplossingen besproken welke bedrijven een soortgelijke tool in hun gamma hebben, en wat deze onderscheidt van de concurrentie. Deze informatie wordt weergeven in een vergelijkingsmatrix zodat het volledige aanbod van de verschillende bedrijven met elkaar vergeleken kan worden.

I. Stageverslag

1 Bedrijfsvoorstelling

SecWise is een bedrijf gevestigd te Leuven dat zich specialiseert in het uitwerken en implementeren van securityoplossingen voor cloudomgevingen met behulp van de Microsoft-*suite*. Het logo van SecWise is terug te vinden op deze pagina als figuur 1.

Figuur 1: Logo SecWise

De diensten die aangeboden worden, zijn onder te verdelen in drie categorieën. De eerste categorie is identiteits- en toegangscontrole. Dit houdt in dat SecWise ervoor zorgt dat alle beveiliging in het bedrijf met betrekking tot accounts en rechten correct is ingesteld.

De volgende categorie is "*cyber attack*" preventie en bescherming. Dit houd in dat SecWise, bedrijven begeleidt bij het implementeren van Microsoft gerelateerde beveiligingssystemen. Ook biedt SecWise "*threat hunting*" diensten aan waarbij er proactief naar bedreigingen wordt gezocht.

De laatste categorie is databescherming. Dit houdt in dat gevoelige data van klanten beschermt wordt zodat deze niet in de verkeerde handen terecht komt. Verder is het ook mogelijk voor klanten om hulp of advies te vragen wat betreft het volgen van industriestandaarden op het gebied van gegevensbescherming.

2 Inleiding

Vanuit SecWise was er vraag naar een vergelijkende studie van enkele marktleiders op het gebied van EDR-toepassingen. Uit deze studie zou moeten blijken welke tools het beste presteren in welke omstandigheden. Dit is belangrijke informatie bij de keuze voor een specifieke oplossing.

In de volgende hoofdstukken wordt van elke onderzochte oplossing een evaluatie gemaakt van de functies van de tool, de gebruiksvriendelijkheid en de sterktes en de zwaktes. Aan het einde van dit deel van het eindwerk volgt een vergelijkingsmatrix die alle mogelijke functies per tool naast elkaar zet om zo een duidelijk beeld te vormen van de situatie waarin elke toepassing uitblinkt.

3 Analyses

3.1 Carbon Black

Figuur 2: Logo Carbon Black

Door een gebrek aan een trial is deze analyse tot stand gekomen op basis van de bronnen beschikbaar op de website van Carbon Black [4] en de *on demand product* demo die eveneens beschikbaar is op hun website.

Carbon Black biedt een *endpoint protection suite* aan die volledig cloudbased is. Alle toepassingen zijn beschikbaar via één console waarmee beheerders al hun producten kunnen beheren. Mocht er nood zijn aan een *on-premise* alternatief, is er ook een tool die dezelfde functionaliteiten aanbiedt. De Carbon Black *agent* maakt gebruik van een technologie die hen in staat stelt om alle data van het *endpoint* te versturen naar de cloud. Deze data wordt hier 30 dagen bijgehouden. Mocht data gemarkeerd zijn als verdacht of gevaarlijk, wordt ze bijgehouden voor respectievelijk 60 en 90 dagen.

3.1.1 Agent

De Carbon Black-*suite* maakt gebruik van één *agent* om al hun toepassingen van data te voorzien. Deze *agent* is beschikbaar voor alle besturingssystemen [11], maar niet voor mobiele *endpoints*. Hierdoor is de *suite* bruikbaar in netwerken die opgebouwd zijn uit *endpoints* met diverse besturingssystemen. De *suite* heeft wel geen *agent* voor mobiele *endpoints*.

3.1.2 Eindgebruiker

Wanneer er een bestand geblokkeerd wordt op het *endpoint* van de eindgebruiker krijgt deze een melding die de gebruiker de keuze geeft om meer informatie te vragen of om de melding te negeren.

3.1.3 Dashboard

De *suite* biedt een eenvoudig dashboard met beperkte mogelijkheden om het aan de persoonlijke voorkeur van de beheerder aan te passen.

3.1.4 Overzicht

De Carbon Black-oplossing biedt beheerders een uitgebreid *event chain view* waarin wordt weergegeven hoe een aanval tot stand kwam en welke programma's er gebruikt werden. Verder is het ook mogelijk om query's uit te voeren op alle *endpoints* om zo naar verdachte files te zoeken. Dit heeft als voordeel dat de tool ook gebruikt kan worden om naar inbraken te zoeken die plaatsvonden voor de initiële installatie van de *agent*.

3.1.5 Detectie

De Carbon Black-*suite* maakt gebruik van een speciale *streaming prevention*-techniek die hen in staat stelt zowel bekende als onbekende malware en aanvallen te herkennen en isoleren voor ze schade kunnen aanrichten. Ook hebben beheerders de mogelijkheid om hashes toe te voegen aan zowel een white- als een blacklist.

3.1.6 Interventies

Beheerders kunnen met behulp van de quarantaine-functionaliteit *endpoints* afzonderen van het netwerk waardoor ze enkel nog met de Carbon Black-cloud kunnen communiceren. Hierdoor blijven aanvallers beperkt tot één *endpoint*. Ook is er de mogelijkheid om met de *command line* bestanden te kopiëren en te verwijderen, de processen op het systeem op te lijsten en te stoppen, en kunnen er commando's doorgestuurd worden naar de Command Line Interface (CLI) van het besturingssysteem dat draait op het *endpoint*.

Een minpunt is dat bestanden niet hersteld kunnen worden, na bijvoorbeeld een aanval door ransomware die niet gedetecteerd werd, zonder integraties van derden.

3.1.7 Samenvatting

De Carbon Black tool vervult de rol van *endpoint protection* oplossing uitstekend, maar doet weinig extra's dat hen van de competitie zou kunnen onderscheiden. Ook wordt voor veel dingen vertrouwd op integraties van derden, zoals bijvoorbeeld een uitgebreid dashboard, automatische deceptie en het herstellen van bestanden.

3.2 Crowdstrike

Figuur 3: Logo Crowdstrike

Door een gebrek aan een trial is deze analyse tot stand gekomen op basis van de bronnen beschikbaar op de website van Crowdstrike [10] en de on-demand product demo die eveneens beschikbaar is op hun website.

Crowdstrike biedt een *endpoint protection suite* aan via het Falcon-platform. Dit platform wordt gebruikt om alle toepassingen van Crowdstrike te beheren via een webinterface. Omdat de hele *suite* via de cloud beschikbaar is, kunnen alle toepassingen op één plek ingesteld en beheerd worden. De Falcon-*agent* stuurt continu data naar de cloudomgevingen van Crowdstrike en dus niet alleen wanneer er verdachte activiteiten plaatsvinden. Deze data wordt gedurende een periode van 90 dagen bewaard.

3.2.1 Agent

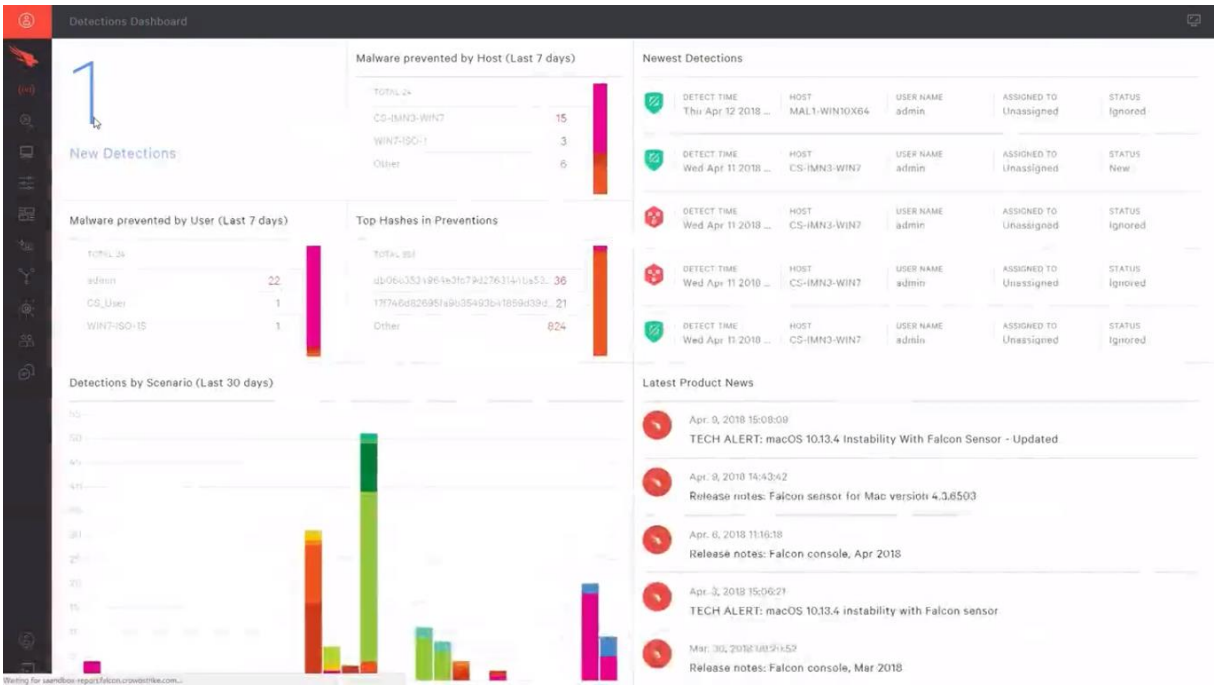
De Falcon-cloudsuite gebruikt één *agent* voor alle toepassingen die ondersteund wordt door de meeste gangbare besturingssystemen met uitzondering van Windows 8(.1). Hierdoor kan de *suite* gebruikt worden in netwerken die opgebouwd zijn uit *endpoints* met verschillende besturingssystemen. Ook is het belangrijk te vermelden dat Crowdstrike de enige EDR-toepassing aanbiedt die ook overweg kan met mobiele *endpoints*.

3.2.2 Eindgebruiker

Wanneer er een interventie plaatsvindt op het *endpoint* van een eindgebruiker, krijgt deze een eenvoudige melding die de gebruiker informeert dat er kwaadaardige activiteiten hebben plaatsgevonden op zijn *endpoint* en dat deze zijn geblokkeerd. Extra informatie is enkel beschikbaar via de cloud-interface.

3.2.3 Dashboard

Op het dashboard is een overzicht beschikbaar van recente detecties, vaak voorkomende malware en nieuws over het product. Dit geeft een goed overzicht van de actuele toestand van het netwerk wat betreft aanvallen. Dit dashboard is te zien in figuur 4.



Figuur 4: Crowdstrike dashboard

3.2.4 Overzicht

Beheerders kunnen via de webinterface een *event chain* bekijken van gedetecteerde aanvallen en verdachte events. In dit overzicht kan er nagegaan worden welke programma's zijn uitgevoerd, welke commando's er gebruikt zijn en welke bekende hackerscollectieven dit soort aanvallen gebruikt. Hierdoor kan een beheerder snel de gevolgen van een aanval overzien, maar zich ook voorbereiden op andere aanvallen van hetzelfde hackerscollectief.

Ook is het mogelijk voor beheerders om het hele netwerk te doorzoeken naar hashcodes van bestanden en connecties. Op deze manier kan er snel gedetecteerd worden of er andere *endpoints* geïnfecteerd zijn.

Als extra kan alle data naar een SIEM-installatie binnen het netwerk verstuurd worden voor extra analyse en eventueel een extra grafische voorstelling van de data.

3.2.5 Detectie

Detectie gebeurt volledig in de cloud met een beperkte versie die offline beschikbaar is. De bescherming van Crowdstrike detecteert zowel traditionele malware als malware die werkt zonder bestanden te gebruiken op de *endpoint*. Hiervoor wordt gebruikgemaakt van enerzijds de *signatures* van bekende malware om deze snel te detecteren en anderzijds wordt gebruikgemaakt van gedragsanalyse en *machine learning* om onbekende en *fileless* malware te detecteren. Ook kunnen beheerders hashes blacklisten om te vermijden dat deze nog in het netwerk terechtkomen.

3.2.6 Interventies

Beheerders kunnen handmatig ingrijpen door *endpoints* in quarantaine te plaatsen. Op deze manier wordt vermeden dat indringers zich door het netwerk zouden kunnen verplaatsen. Het is ook mogelijk om via een *command line* in de webinterface bestanden te kopiëren en te verwijderen, aanpassingen in het register die gedetecteerd zijn ongedaan te maken en processen te beëindigen. Dit heeft wel ingrijpende gevolgen voor de ervaring van de eindgebruiker aangezien deze zijn bestanden ziet sluiten of verdwijnen.

3.2.7 Samenvatting

De Crowdstrike-*suite* stelt securityteams in staat om snel te bepalen of aanvallen in hun netwerk eventueel van een bekend hackerscollectief kunnen komen. Op basis van deze informatie kunnen er dan maatregelen genomen worden tegen de andere technieken die deze groep gebruikt. Het enige nadeel van deze functie is dat het handmatig maatregelen nemen een hoop extra werk met zich meebrengt. Een manier om dit op te vangen is door de Falcon Overwatch-*suite* te gebruiken. Deze *suite* biedt extra hulp van Crowdstrike-securitypersoneel aan bovenop het basispakket.

Er kan dus geconcludeerd worden dat de Crowdstrike-*suite* de nadruk legt op het menselijke aspect van security. Dit word verder bevestigd door het businessmodel van de Crowdstrike Overwatch-*suite*.

3.3 Sophos

Figuur 5: Logo Sophos

Sophos biedt een cloudbased platform aan voor alle securityoplossingen die ze aanbieden. Dit gaat dan over *endpoint protection*, firewalls, phishing training en dergelijke. Een *endpoint* toevoegen aan dit platform gebeurt via een *agent* die handmatig geïnstalleerd kan worden via het installatiebestand of in bulk. Alle data wordt door Sophos 90 dagen bijgehouden.

3.3.1 Agent

Sophos gebruikt een *agent* die beschikbaar is voor Windows servers, Windows desktops, Linux servers en macOS *endpoints*. Hierdoor kan de *suite* gebruikt worden in netwerken die gebruik maken van een combinatie van besturingssystemen.

Er is ook een *agent* beschikbaar voor mobiele systemen, maar deze is niet gekoppeld aan de EDR-toepassing. Deze tool zorgt dus enkel voor *endpoint protection*.

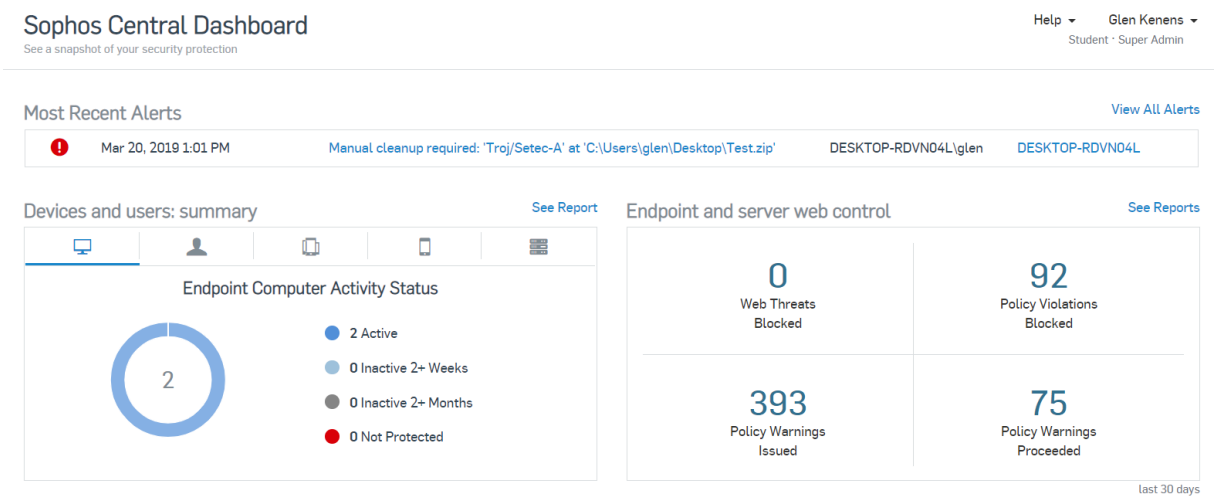
3.3.2 Eindgebruiker

Wanneer er een bestand geblokkeerd wordt op het *endpoint* van de eindgebruiker krijgt deze een melding die eventueel gedeeltelijk gepersonaliseerd kan worden door de beheerder. Op deze manier is het mogelijk om eindgebruikers informatie door te geven die enkel binnen het bedrijf gebruikt wordt, zoals bijvoorbeeld het telefoonnummer van de helpdesk. Dit biedt de tool een groot voordeel wat betreft gebruiksvriendelijkheid ten opzichte van de eindgebruiker.

3.3.3 Dashboard

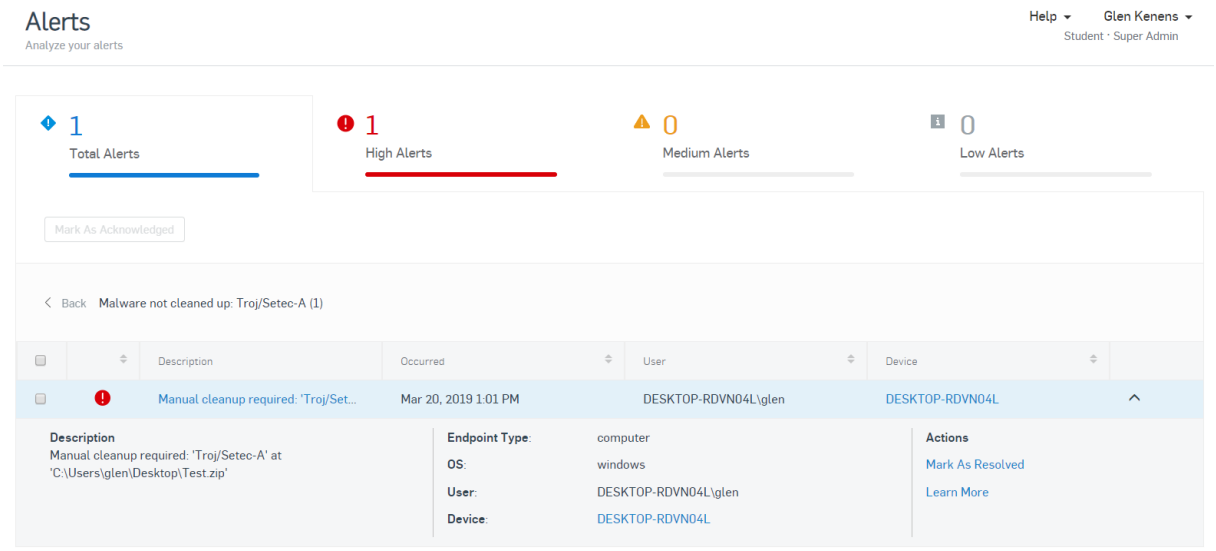
De grafische interface is niet aanpasbaar door de beheerders. Ook zijn er geen links tussen verschillende pagina's waar deze wel handig zouden kunnen zijn zoals bijvoorbeeld tussen een melding van een gedetecteerde aanval en het rapport van deze aanval. Verder kan er niet tussen de functionaliteiten van de *suites* gewisseld worden zonder eerst helemaal terug te gaan naar het beginscherm. Dit heeft als resultaat dat het moeilijk is om te navigeren tussen de verschillende delen van de *suite*.

Het centrale dashboard geeft de belangrijkste alerts, de status van de *endpoints* en het aantal gedetecteerde bedreigingen weer. Dit dashboard is te zien in figuur 6.



Figuur 6: Sophos centrale dashboard

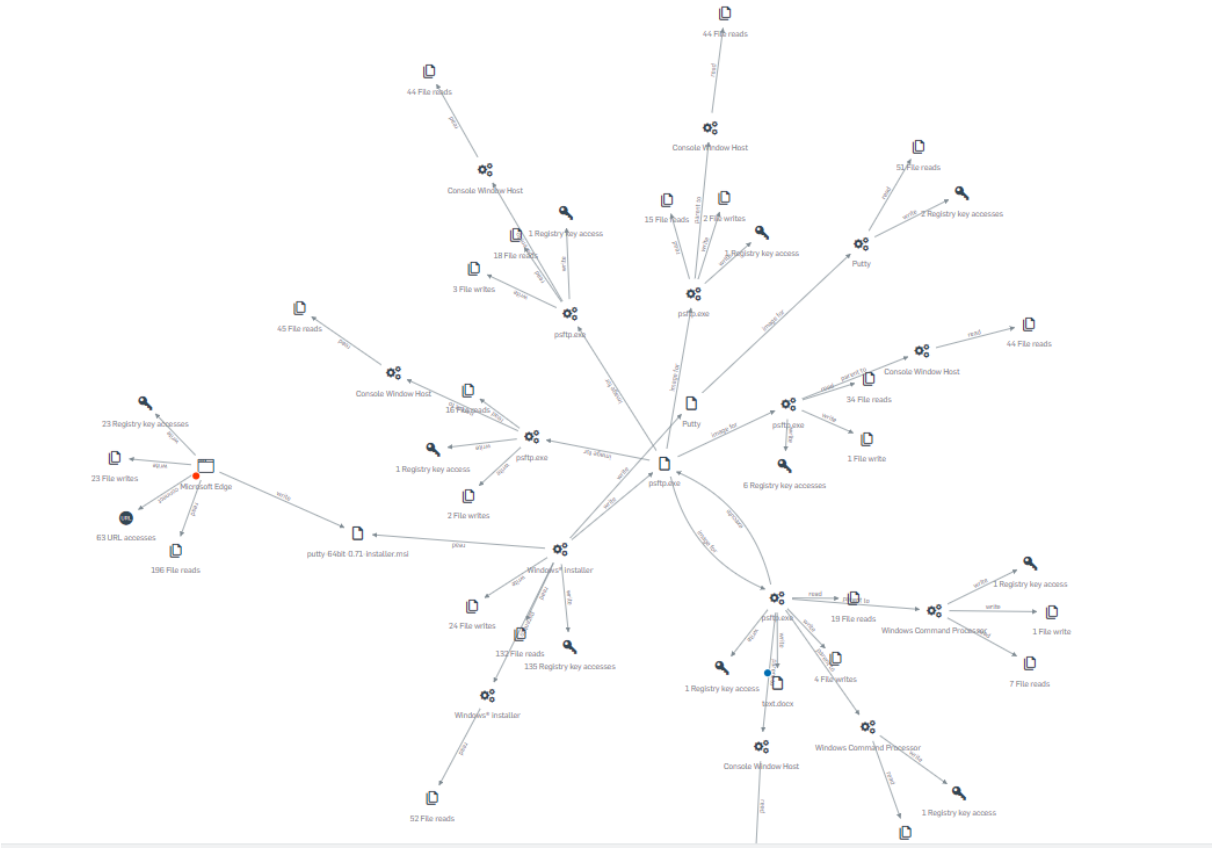
Het alert dashboard geeft een overzicht van alle alerts op het netwerk. Hier kunnen beheerders zien welke alerts op dat moment hun aandacht nodig hebben. Een voorbeeld van dit dashboard is te zien in figuur 7.



Figuur 7: Sophos Alert dashboard

3.3.4 Overzicht

De *suite* biedt beheerders een *event chain view* aan waar extra informatie te vinden is over een geblokkeerde aanval. Dit rapport geeft wel veel meer informatie als nodig is om de situatie te begrijpen wat ervoor zorgt dat het overzicht verloren gaat. Hierdoor wordt het moeilijker om snel en efficiënt een aanval te analyseren en extra maatregelen te treffen mocht dit nodig zijn. Dit wordt geïllustreerd in figuur 8.



Figuur 8: Sophos uitgebreide event chain

Er is ook een versimpelde versie beschikbaar van het evenchain overzicht dat vaak duidelijker is als de uitgebreide versie. Deze biedt geen overbodige informatie, maar heeft als nadeel dat sommige belangrijke informatie niet langer zichtbaar is. Dit is te zien op figuur 9.

Figuur 9: Sophos versimpelde event chain

Een ander nadeel is dat soms essentiële informatie niet terug te vinden is tenzij de detectie handmatig is uitgevoerd. Hierdoor hebben beheerders geen totaalbeeld van de aanval.

3.3.5 Detectie

Sophos maakt gebruikt van verschillende detectie technieken. Zo word *deep learning* gebruikt om verdachte bestanden te vergelijken met datasets waarvan zeker is dat ze goed- of kwaadaardig zijn. Ook wordt er gedetecteerd op basis van *signatures*.

De *suite* heeft het wel moeilijk met het detecteren van malware die samen verpakt is met niet-schadelijke bestanden.

Ook detecteert de *suite* niet altijd alle toepassingen die vooraf gingen aan een detectie. Dit heeft als gevolg dat malware wel verwijderd word, maar de scripts die de malware installeerden niet.

3.3.6 Interventies

De Sophos-*suite* biedt beheerders de mogelijkheid om *endpoints* in quarantaine te plaatsen. Dit neemt wel een aanzienlijke tijd in beslag. Ook kan dit voor problemen zorgen wanneer een toestel net wordt uitgeschakeld als het in quarantaine wordt geplaatst. Verder is er nog de optie om vanop afstand een virusscan uit te voeren.

3.3.7 Samenvatting

De *suite* van Sophos is zeker geen slechte EDR-toepassing maar heeft enkele ongemakken die het beheerders moeilijker kunnen maken om efficiënt te werken. De interface heeft een aantal hyperlinks die naar online rapporten van bedreigingen gaan wanneer eigenlijk verwacht wordt dat deze verwijzen naar de interne rapporten van de bedreiging waar ze bij stonden.

Een ander klein minpunt is het gebrek aan personalisatie opties wat betreft de dashboards. Hieraan kan een beheerder zelf niks aanpassen. Dit is geen groot nadeel maar extra opties wat betreft het dashboard zouden het navigeren van de tool een stuk gemakkelijker maken.

Verder is de tool perfect in staat om bedreigingen en hun oorsprong te detecteren, maar stelt deze niet altijd even duidelijk voor. Zelfs de simpelste malware heeft een uitgebreide *event chain* eraan gekoppeld die eigenlijk een hele hoop informatie bevat die niet relevant is. Een pluspunt is wel dat van elke detectie standaard een *event chain* beschikbaar is. Ook kan in dit rapport een Virustotal search van sommige verdachte bestanden gedaan worden. Bestanden die gedetecteerd worden door het deep-learning systeem krijgen ook een uitgebreid rapport met de redenen waarom deze gedetecteerd zijn.

Ook de beperkte response opties in het geval van een detectie zijn een minpunt. Wanneer een antivirusscan het gedetecteerde bestand niet verwijderd krijgt moet dit manueel verwijderd worden. Bij een groter aantal gefaalde opruimingsacties kan dit tot een aanzienlijke hoeveelheid manueel werk leiden.

Er kan geconcludeerd worden dat de Sophos tool voldoende bescherming biedt, maar de hoeveelheid nuttige informatie die wordt aangeboden schiet tekort. Dit in combinatie met de verwarrende lay-out van de tool zorgt ervoor dat het resultaat maar matig overtuigend is.

3.4 Trend Micro

Figuur 10: Logo Trend Micro

Trend Micro biedt zowel een cloudbased als een *on-premise* oplossing aan. Alle producten gebruiken dezelfde *agent* en dezelfde console. Dit heeft als gevolg dat de Trend Micro-*suite* gemakkelijk te installeren en beheren is. Beheerders kunnen zelf kiezen hoe lang data wordt bijgehouden, de standaardinstellingen houden alles gedurende 90 dagen bij, maar dit kan verhoogd worden tot 370 dagen. Verder biedt de *suite* ook de mogelijkheid om rechten toe te kennen op basis van een Role Based Access Control (RBAC) systeem. Dit geeft beheerders de mogelijkheid om gebruikers aan te maken en op basis van deze accounts rechten toe te kennen.

3.4.1 Agent

Trend Micro gebruikt een *agent* die compatibel is met Windows computers en servers en met macOS besturingssystemen. Dit heeft als gevolg dat de *suite* niet veel kan bieden in netwerken die voornamelijk op Linux gebaseerde besturingssystemen gebruiken.

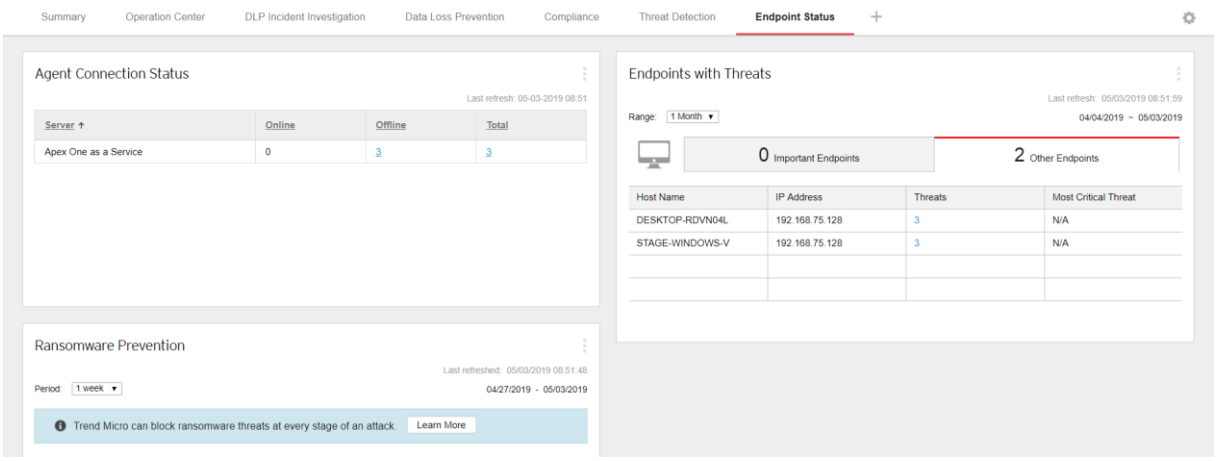
3.4.2 Eindgebruiker

De eindgebruiker krijgt een pop-up met een melding dat er een bedreiging gedetecteerd is wanneer er een verdachte file op de computer wordt aangetroffen. Wanneer de eindgebruiker probeert malware te downloaden krijgt deze echter geen melding. Hierdoor kan het zijn dat eindgebruikers niet doorhebben dat ze iets mis hebben gedaan en gewoon de malware opnieuw proberen te downloaden. Dit kan leiden tot een grotere hoeveelheid alerts.

De pop-up die tevoorschijn komt bij een detectie moet ook met de hand weg geklikt worden. Dit is een onhandigheid voor de eindgebruiker maar op deze manier is het wel zeker dat de eindgebruiker de melding ook effectief gezien heeft.

3.4.3 Dashboard

De Trend Micro-*suite* heeft een uitgebreid dashboard dat aan de persoonlijke voorkeur van de beheerder kan aangepast worden met behulp van een aantal widgets. Hierdoor is het dashboard geschikt voor elke omgeving. Ook is er de mogelijkheid om meerdere dashboard tabs in te stellen. Hierdoor kan er ingespeeld worden op de vereisten die verschillende mensen in het securityteam kunnen hebben. Dit dashboard is te zien op figuur 11.



Figuur 11: Trend Micro custom dashboard

3.4.1 Overzicht

Beheerders kunnen een Root Cause Analysis (RCA) aanvragen van files en bedreigingen. Het resultaat is dan een *event chain* die geleid heeft tot het bestand waarop de RCA is uitgevoerd. Hierdoor kan er snel nagegaan worden hoe een bedreiging het netwerk is binnengeraakt. Ook biedt dit overzicht de mogelijkheid om gedetecteerde processen te stoppen vanop afstand en verdachte files te blacklisten.

3.4.2 Detectie

De Trend Micro-*suite* maakt gebruik van onder andere *machine learning* en gedragsanalyse om bedreigingen te detecteren. Zo kunnen bedreigingen gedetecteerd worden voor ze uitgevoerd worden en tijdens het uitvoeren. Dit heeft als voordeel dat ook onbekende aanvallen herkend kunnen worden aan de hand van het patroon dat ze volgen.

Verder is de *suite* in staat om kwaadaardige bestanden uit gecomprimeerde folders te halen wanneer deze gedownload worden. Het moet wel vermeld worden dat een Word-file met een exploit niet gedetecteerd werd tijdens de tests.

De *suite* is ook in staat om ransomware te herkennen en versleutelde bestanden terug te herstellen.

3.4.3 Interventies

Beheerders kunnen *endpoints* die besmet zijn met malware isoleren van de rest van het netwerk om zo te vermijden dat indringers zich doorheen het netwerk verspreiden. Ook is er de mogelijkheid om services te stoppen vanuit het *event chain* venster.

3.4.4 Samenvatting

De Trend Micro-*suite* biedt een uitstekende bescherming tegen aanvallen. De *suite* kan tijdens het downloaden de inhoud van een gecomprimeerd bestand verwijderen als dit schadelijke bestanden bevat. De *suite* heeft wel moeite met het efficiënt detecteren van bedreigingen wanneer het *endpoint* offline is. Er is wel een instelling beschikbaar die ervoor zorgt dat het *endpoint* ook offline volledig beschermd is.

De online console biedt meerdere dashboards aan met de optie om zelf dashboards toe te voegen en aan de persoonlijke voorkeur aan te passen. Hierdoor kan er met een beetje werk snel genavigeerd worden doorheen de tool wat het gemakkelijker maakt om snel te reageren op bedreigingen.

Een minpunt is dat er niet van elke gedetecteerde bedreiging een *event chain* beschikbaar is. Deze moet met de hand aangevraagd worden. Hierdoor is niet meteen duidelijk waar de aanval precies vanaf kwam en wat het doel was.

Er kan dus besloten worden dat de Trend Micro uitstekend geschikt is voor teams omwille van het RBAC model dat gebruikt wordt en het feit dat voor elke gebruiker een apart dashboard gemaakt kan worden.

Ook is het belangrijk te vermelden dat er geen default policy's voorzien zijn. Hierdoor is het onmogelijk om instellingen te configureren zonder hierover na te denken. Dit heeft als gevolg dat de initiële configuratie meer tijd in beslag neemt, maar er is wel minder kans op configuratiefouten.

3.5 Symantec

Figuur 12: Logo Symantec

Symantec biedt momenteel hybride oplossingen aan waarbij een deel van de tool zich in de cloud bevindt maar waar er toch nog enkele *on-premise* installaties nodig zijn. Ook bieden ze volledige *on-premise* oplossingen aan voor klanten die hun data liever lokaal houden. Dit heeft als gevolg dat er altijd nog extra hardware moet voorzien worden voor de Symantec-*suite*. Data die de *suite* verzameld wordt standaard 90 dagen bijgehouden, maar dit kan handmatig aangepast worden.

3.5.1 Agent

De Symantec-*suite* gebruikt enkel een *agent* voor het *endpoint protection* gedeelte van de *suite*. Het EDR gedeelte wordt zonder *agent* uitgevoerd met behulp van een *on-premise* server die de data verzameld en doorstuurt. De *suite* ondersteund Windows en macOS besturingssystemen. Dit heeft als gevolg dat de *suite* niet veel kan bieden in netwerken met veel Linux toestellen.

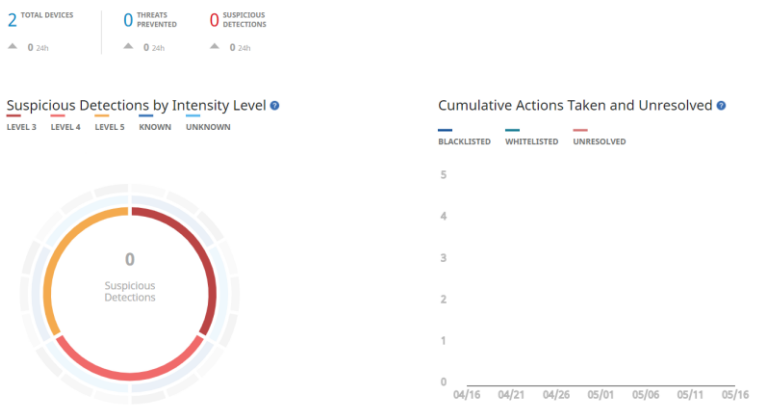
3.5.2 Eindgebruiker

De eindgebruiker ondervindt niet veel hinder van de *agent*. Alerts gebruiken een klein tekstvak dat de eindgebruiker niet stoort. Er is ook geen nood aan handmatige input wat betreft scans en malware opruiming.

3.5.3 Dashboard

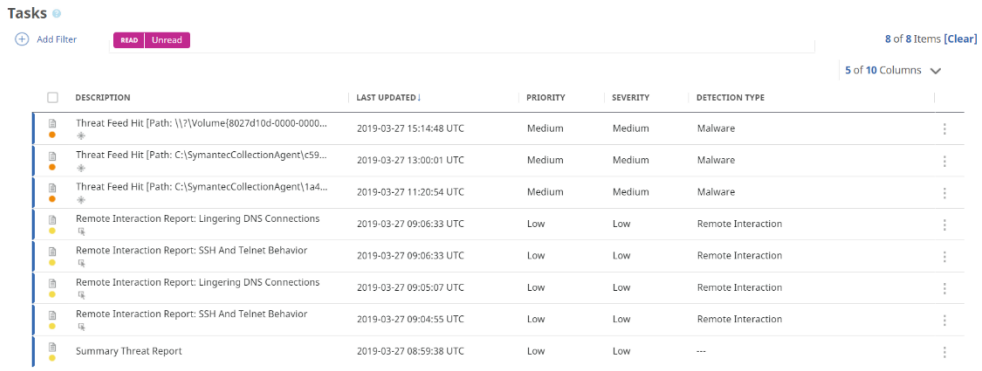
De Symantec-*suite* gebruikt een standaard dashboard voor hun *endpoint protection* dat niet aangepast kan worden en een ander dashboard voor de EDR-*suite*. Dit heeft als gevolg dat beheerders meerdere dashboards moeten gebruiken die niet aangepast kunnen worden.

Het dashboard van de SEP-Manager geeft een overzicht van de gedetecteerde bedreigingen. Ook is hier een overzicht beschikbaar van de genomen interventiemaatregels. Dit dashboard is te zien op figuur 13.



Figuur 13: Symantec SEPM dashboard

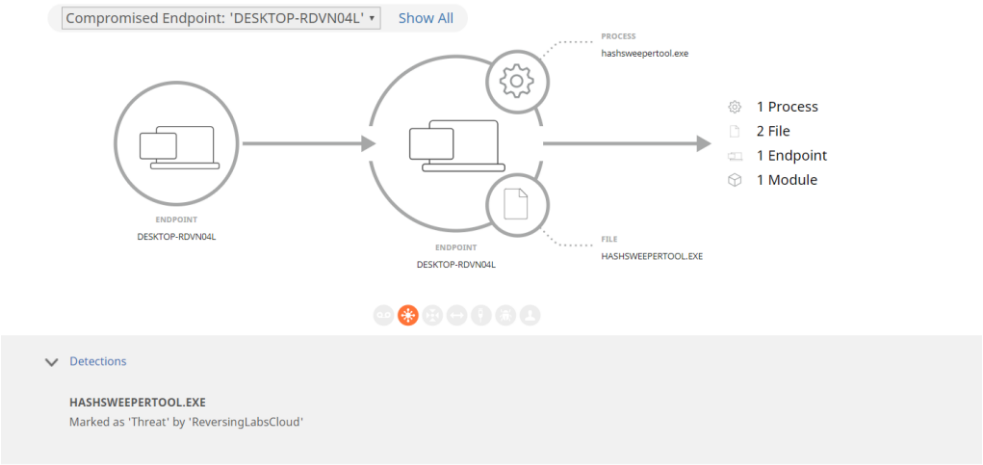
Verder is er ook een dashboard voor de EDR-toepassing. Deze geeft een overzicht van alle bedreigingen die gedetecteerd zijn door de EDR-tool. Beheerders kunnen via deze meldingen toegang krijgen tot het gedetailleerde rapport van de bedreiging. Dit is te zien op figuur 14.



Figuur 14: Symantec EDR dashboard

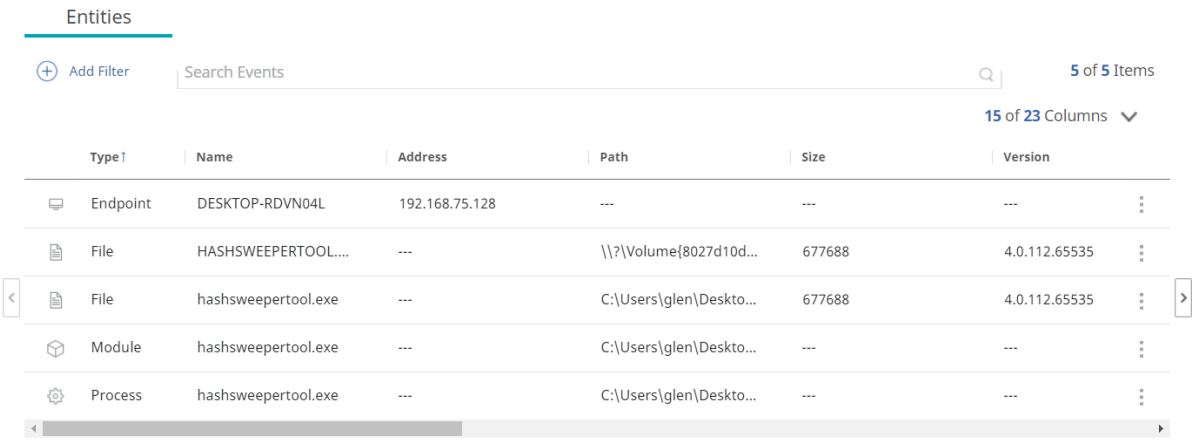
3.5.4 Overzicht

Van bereidingen die gedetecteerd worden door de EDR-toepassing is er een grafische voorstelling van de bedreiging beschikbaar. Beheerders kunnen deze gebruiken om extra informatie te krijgen over de gedetecteerde bedreiging. Deze grafische voorstelling is te zien op figuur 15.



Figuur 15: Symantec threat graph

In ditzelfde overzicht is ook een lijst van de verschillende entiteiten van de aanval beschikbaar. Dit is te zien in figuur 16.



Figuur 16: Symantec entity lijst

3.5.5 Detectie

De Symantec-*suite* detecteert op basis van gedragsanalyse, geheugenanalyse, *machine learning*, reputatieanalyses en *signatures*. Dit heeft als gevolg dat de *suite* bedreigingen op meerdere verschillende manieren kan detecteren. Er moet wel vermeld worden dat de *suite* vaak pas bedreigingen detecteert wanneer ze uitgevoerd worden en dus niet wanneer ze op het systeem terecht komen. Dit heeft als gevolg dat wanneer een bedreiging langer als de maximale log leeftijd op een systeem blijft het moeilijk kan worden om de oorsprong te achterhalen.

3.5.6 Interventies

Beheerders kunnen *endpoints* isoleren door een hiervoor voorziene policy op deze *endpoints* toe te passen.

3.5.7 Samenvatting

Het *endpoint protection* gedeelte van de Symantec-*suite* doet uitstekend zijn werk. Alle aanvallen worden gedetecteerd zodra een gebruiker ermee in contact komt. Zodra er een detectie plaatsvindt, wordt er een alert gegenereerd op zowel de lokale management server als de cloud variant wanneer deze aanwezig is.

Een nadeel is dat er nog steeds *on-premise* componenten nodig zijn voor het correct functioneren van de *suite*. Dit zorgt ervoor dat de *suite* niet geschikt is voor bedrijven die zoeken naar een oplossing waar ze zelf geen onderhoudskosten aan hebben. Voor bedrijven die een volledige *on-premise* setup willen is er wel een optie voorzien.

Het EDR-gedeelte van de *suite* staat volledig los van de *endpoint protection suite*. Dit brengt enkele nadelen met zich mee zoals het feit dat er meerdere consoles nodig zijn om de *suite* te beheren. Een ander nadeel van de EDR-*suite* is dat er enkel op vaste intervallen informatie verzameld wordt. Standaard is deze periode ingesteld op één dag. Op deze tijd kan een indringer zich ver binnen het netwerk verspreiden wat uiteindelijk leidt tot meer werk voor het aanwezige securitypersoneel.

3.6 Windows Defender ATP

Figuur 17: Logo Windows Defender ATP

De Windows Defender ATP-*suite* is de cloudbased EDR-oplossing van Microsoft. Deze *suite* werkt *agentless* op *endpoints* met een Windows besturingssysteem. *Endpoints* kunnen toegevoegd worden door middel van een script dat terug te vinden is in de cloudconsole. Een andere optie waarmee *endpoints* kunnen toegevoegd worden is de Microsoft SCCM-*suite*. Verder kunnen *endpoints* ook via Group Policy of Intune worden toegevoegd. *Endpoints* met een Linux besturingssysteem kunnen enkel toegevoegd worden met behulp van een externe partner. Er kan dus besloten worden dat de Microsoft EDR-*suite* het best gebruikt wordt in omgevingen waar al een Microsoft omgeving opgezet is.

3.6.1 Agent

Omdat Microsoft eigenaar is van zowel het Windows besturingssysteem als de Windows Defender ATP-*suite* is het mogelijk om *endpoints* met een Windows besturingssysteem zonder *agent* toe te voegen. Voor *endpoints* met een ander besturingssysteem moet wel gebruikgemaakt worden van een externe partner.

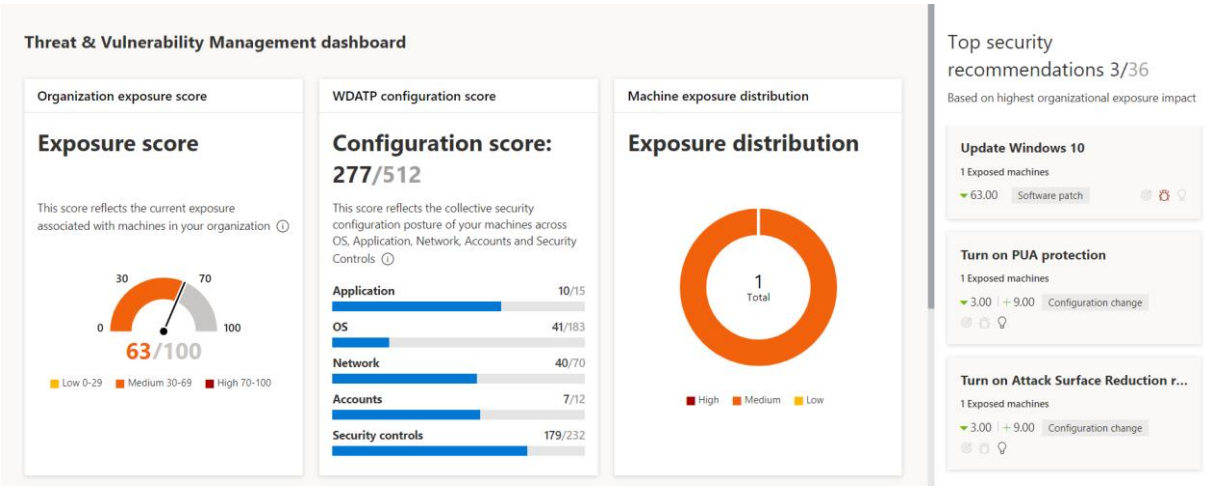
3.6.2 Eindgebruiker

Voor de eindgebruiker verandert er niets vergeleken met de standaard Windows Defender toepassing. Wanneer er bedreigingen worden aangetroffen krijgt de eindgebruiker een melding die na enkele seconden weer verdwijnt. Door op de melding of de bijbehorende notificatie te klikken kan de eindgebruiker extra informatie opvragen.

3.6.3 Dashboard

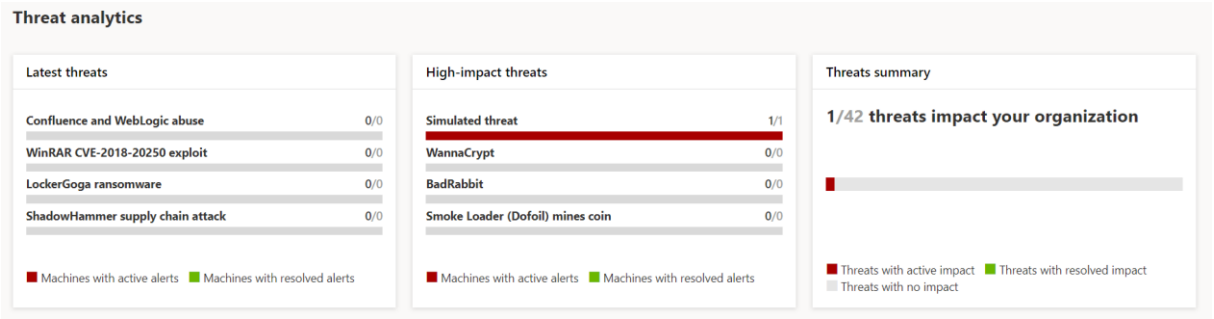
De Windows Defender ATP-*suite* heeft enkele *built-in* dashboards waarop beheerders de toestand van de *endpoints* kunnen bekijken. Als beheerders deze aan hun voorkeur willen aanpassen moet er wel gebruikgemaakt worden van een andere Microsoft tool.

Uniek aan de Windows toepassing is het dashboard voor “Threat & Vulnerability Management”. Hier kunnen beheerders zien welke configuraties er nog nodig zijn voordat het netwerk optimaal beschermt is. Dit wordt weergegeven aan de hand van een puntensysteem waarbij belangrijke configuraties meer punten waard zijn. Dit dashboard is te zien op figuur 18.



Figuur 18: Windows ATP vulnerability management

Verder is er ook nog het threat analytics overzicht waar beheerders kunnen zien welke bedreigingen er momenteel veel voorkomen en hoe vaak ze gedetecteerd zijn binnen het netwerk. Dit heeft als grote voordeel dat het snel duidelijk is of het bedrijf slachtoffer is geworden van een recente uitbraak. Een voorbeeld hiervan is te zien op figuur 19.

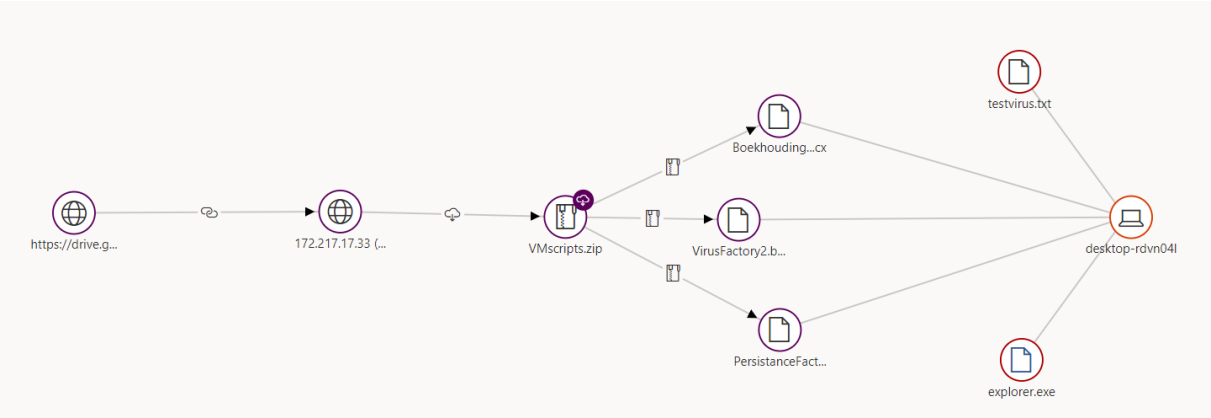


Figuur 19: Windows ATP Threat analytics

3.6.4 Overzicht

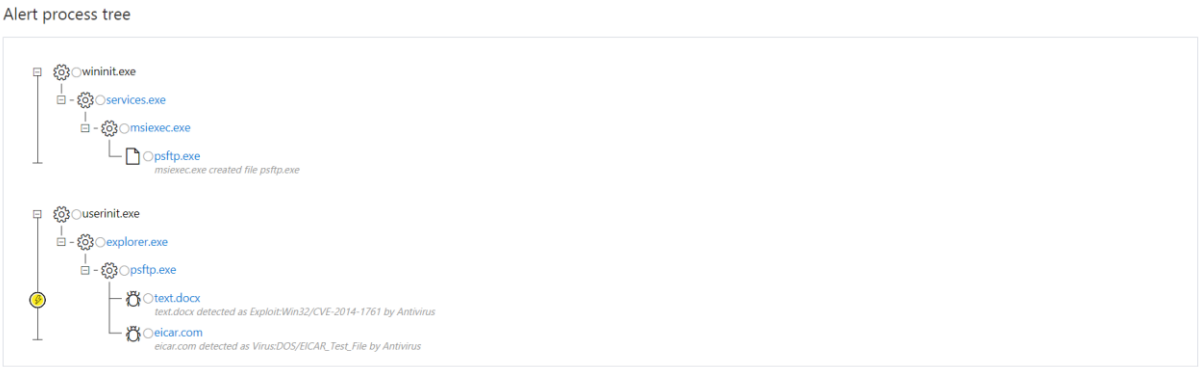
De Microsoft-*suite* verdeeld bedreigingen onder in incidenten en alerts. Hierdoor kunnen meerdere alerts die samen horen gegroepeerd worden onder een incident. Dit heeft als voordeel dat beheerders direct kunnen zien welke alerts samen horen. Hierdoor kan er ook per incident gewerkt worden en moeten beheerders dus niet zelf uitzoeken welke alerts bij elkaar horen terwijl het onderzoek gaande is.

Voor incidenten is er ook een *event chain* grafiek beschikbaar waarin beheerders een overzicht krijgen van de verschillende stappen die een aanval overlopen heeft. Hierdoor kan er snel een analyse gemaakt worden van de gevolgen van een aanval maar ook van de stappen die vooraf gingen aan deze aanval. Een voorbeeld hiervan is te zien op figuur 20.



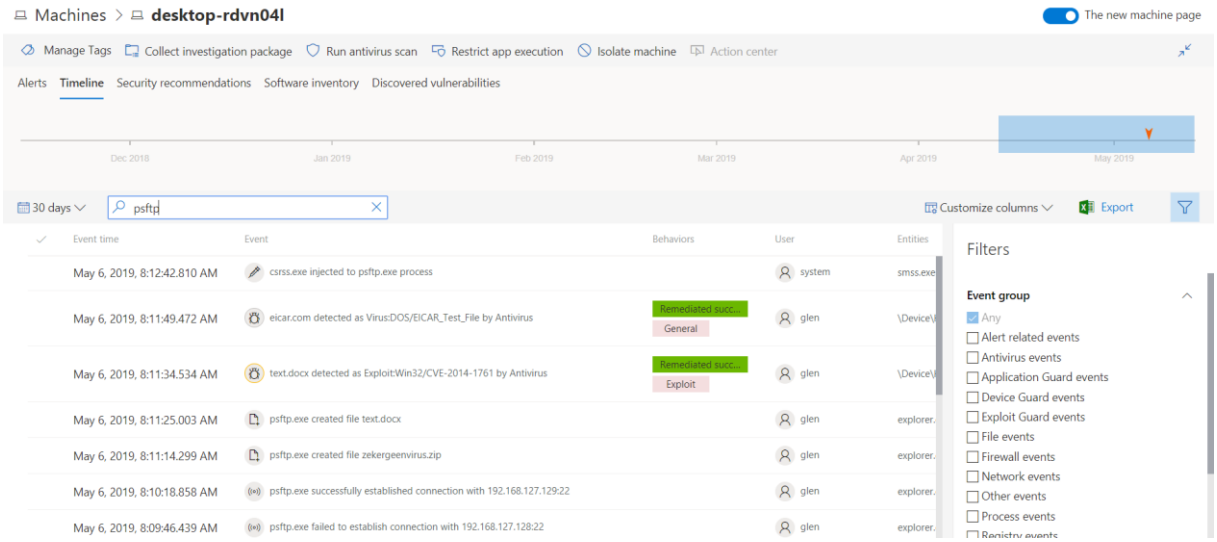
Figuur 20: Windows ATP event chain

Voor alerts is er een *process tree* en een grafiek beschikbaar waarmee beheerders een overzicht krijgen van alle factoren die meegespeeld hebben in de aanval. Aan de hand van deze gedetailleerde gegevens kan de oorsprong van de aanval achterhaald worden mocht deze nog niet bekend zijn. Dit is te zien op figuur 21.



Figuur 21: Windows ATP process tree

Tot slot is er nog de *timeline* van een *endpoint* waarin gezocht kan worden naar specifieke connecties, bestanden en events die mogelijk verdacht zouden kunnen zijn. Hiervan is een voorbeeld te zien op figuur 22.



Figuur 22: Windows ATP timeline

3.6.5 Detecties

De Windows Defender ATP-*suite* kan bedreigingen detecteren aan de hand van patronen, *signatures*, geheugenanalyse en verdachte commando's. Hierdoor is de *suite* in staat om te beschermen tegen zowel bekende als onbekende bedreigingen.

De *suite* biedt ook een overzicht van alle bedreigingen die momenteel relevant zijn en hoe vaak deze gesignaleerd zijn binnen het netwerk. Ook is er van deze bedreigingen een rapport beschikbaar waarin een korte beschrijving van de bedreiging is terug te vinden evenals enkele tips om deze bedreiging tegen te gaan.

3.6.6 Interventies

De *suite* geeft beheerders de mogelijkheid om *endpoints* die mogelijk geïnfecteerd zijn te isoleren. Hierdoor kunnen aanvallers zich niet langer verspreiden over het netwerk. Ook is er de mogelijkheid om bestanden te stoppen en in quarantaine te plaatsen. Dit heeft als grote voordeel dat er geen connectie gemaakt moet worden met een *endpoint* om verdachte bestanden te isoleren. Tot slot is er ook nog de optie om vanop afstand een scan te starten op het geïnfecteerde *endpoint*.

3.6.7 Samenvatting

De Windows Defender ATP-*suite* is gemakkelijk te beheren en te installeren. Er zijn meerdere dashboards beschikbaar wat het gemakkelijk maakt om het overzicht te behouden. Een minpunt is wel dat de dashboards niet aan de persoonlijke voorkeur van de beheerder kunnen aangepast worden zonder extra toepassingen te installeren.

Een groot pluspunt is dat er van elke gedetecteerde bedreiging een *event chain* beschikbaar is. Ook wordt deze automatisch in een incident gestoken met andere bedreigingen die mogelijk verband houden. Hierdoor kan elke detectie verder onderzocht worden.

Verder is er een overzicht beschikbaar met de onderdelen van de *suite* die nog niet optimaal geconfigureerd zijn. Hierdoor is de kans dat er iets vergeten wordt tijdens de initiële configuratie kleiner.

Er kan besloten worden dat de Windows Defender ATP-*suite* een van de betere *suites* is over de grote lijn. Zeker in Windows 10 omgevingen zijn er weinig tools die dezelfde functionaliteiten aanbieden als de Windows-*suite*. De hoeveelheid data die aangeboden wordt zorgt ervoor dat er altijd handmatig gezocht kan worden naar extra informatie. Dit heeft al grote voordeel dat er niet volledig op de detectiecapaciteiten van de *agent* vertrouwd wordt.

Een nadeel is dat de *suite* minder functionaliteiten heeft bij Windowsversies ouder dan Windows 10. Ook het feit dat er voor Linux, macOS en mobiele systemen gerekend moet worden op een externe partner is een minpunt.

4 Conclusie

Uit onderstaande vergelijkingsmatrix valt af te leiden dat alle onderzochte bedrijven hun toepassing aanbieden op Windows *endpoints*. Er kan pas echt een onderscheid gemaakt worden wanneer het aanbod voor Linux toestellen vergeleken word. Hierbij valt op dat de helft van de onderzochte bedrijven ook een oplossing aanbiedt voor Linux *endpoints*. Hieruit kan afgeleid worden dat ondanks de relatief kleine markt voor Linux security toepassingen er toch in geïnvesteerd wordt.

Wat ook opvalt is dat er maar één bedrijf een volwaardige EDR-toepassing aanbiedt voor mobiele toestellen, namelijk Crowdstrike. Andere bedrijven bieden wel antivirus toepassingen aan voor Android en iOS maar geen EDR-functionaliteiten.

Er kan dus geconcludeerd worden dat voor Linux omgevingen er beter gekozen wordt voor Carbon Black, Crowdstrike of Windows Defender ATP. Deze laatste tool is wel enkel beschikbaar voor Linux toestellen met behulp van een externe partner.

Mocht er een grote behoefte zijn aan een EDR-toepassing voor mobiele toestellen is enkel Crowdstrike een optie.

Tabel 1: Vergelijkingsmatrix besturingssystemen

Ondersteunde besturingssystemen	Carbon Black	Crowd strike	Sophos	Trend Micro	Symantec	Windows
Windows clients	✓	✓	✓	✓	✓	✓
Windows servers	✓	✓	✓	✓	✓	✓
Linux clients	✓	✓	✗	✗	✗	✓
Linux servers	✓	✓	✓	✗	✗	✓
macOS	✓	✓	✓	✓	✓	✓
Mobile	✗	✓	✓	✓	✓	✓

Uit de manageability vergelijkingsmatrix valt af te leiden dat er weinig bedrijven geïnvesteerd hebben in een uitgebreid personaliseerbaar dashboard. Deze functionaliteit is vooral handig wanneer er ook een RBAC model ondersteund wordt omdat op deze manier iedere gebruiker zijn eigen dashboard heeft. Het valt echter op dat er maar één bedrijf beide functionaliteiten heeft, namelijk Trend Micro™. Carbon Black biedt wel een beperkt personaliseerbaar dashboard aan en Windows biedt customiseerbare dashboards aan via een andere Windows tool.

Waar alle bedrijven het over eens zijn is dat hun toepassing bruikbaar moet zijn met maar één *agent*. Dit zorgt ervoor dat de initiële installatie van de toepassing een stuk vlotter verloopt als wanneer er meerdere *agents* nodig zijn. Ook hebben alle bedrijven, op Symantec na, een console waarin zowel de *endpoint protection* als de EDR-toepassing beheerd kunnen worden.

Wanneer de cloud en on-premise mogelijkheden met elkaar vergeleken worden wordt duidelijk dat slechts drie bedrijven een on-premise toepassing aanbieden. Dit betekend dat wanneer er nood is aan een on-premise tool enkel Carbon Black, Trend Micro en Symantec een oplossing aanbieden. Aan de andere kant is Symantec het enige bedrijf dat geen volledige oplossing in de cloud aanbiedt.

Tabel 2: Vergelijkingsmatrix manageability

Manageability	Carbon Black	Crowd strike	Sophos	Trend Micro	Symantec	Windows
Personaliseerbaar dashboard	✓	Geen data	✗	✓	✗	✓
RBAC	✓	Geen data	✓	✓	✓	✓
Single *agent*	✓	✓	✓	✓	✓	✓
Single console	✓	✓	✓	✓	✗	✓
Cloud based	✓	✓	✓	✓	✓	✓
On-premise	✓	✗	✗	✓	✓	✗
AD integration	Geen data	Geen data	✓	✓	✓	✓
Event chain zonder aanvraag	Geen data	Geen data	✓	✗	✗	✓
Report generator	Geen data	Geen data	✓	✓	✓	✓

Uit de detectie vergelijkingsmatrix blijk dat zo goed als alle bedrijven de meest gangbare manier van detecties ondersteunen.

Tabel 3: Vergelijkingsmatrix detections

Detections	Carbon Black	Crowd strike	Sophos	Trend Micro	Symantec	Windows
Signature based	✓	✓	✓	✓	✓	✓
Machine learning	✓	✓	✓	✓	✓	✓
Behaviour based	✓	✓	✓	✓	✓	✓
Fileless	✓	✓	Geen data	✓	Geen data	✓

Wat betreft de *remediation* capaciteiten van de onderzochte tools valt op dat enkel Carbon Black en Crowdstrike een *command line* kunnen openen op *endpoints* om te reageren op aanvallen. Wat ook opvalt is dat enkel Trend Micro en Windows Defender ATP in staat zijn om bestanden die tijdens een ransomware aanval geëncrypteerd werden te herstellen.

Tabel 4: Vergelijkingsmatrix remediation

Remediation	Carbon Black	Crowd strike	Sophos	Trend Micro	Symantec	Windows
Quarantine	✓	✓	✓	✓	✓	✓
Live commandline*	✓	✓	✗	✗	✗	✗
Restore ransomware	✗	✗	✗	✓	✗	✓
Remote scan	✗	✗	✓	✓	✓	✓
Whitelisting	✓	✓	✓	✓	✓	✓
Blacklisting	✓	✓	✓	✓	✓	✓

*De Windows Defender ATP live *command line* functionaliteit die beschikbaar werd na deze conclusie wordt besproken in bijlage 2: Extra Windows Defender ATP feature.

5 Performance onderzoek

5.1 Inleiding

Niet alleen de gebruiksvriendelijkheid en de detecties van een EDR-toepassing zijn belangrijk ook de performance van de *agent* kan een grote rol spelen bij het kiezen van een EDR-toepassing. In het volgende hoofdstuk worden de prestaties van de geëvalueerde bedrijven onderzocht. Het resultaat is een tabel waarin te zien is hoeveel elke *agent* vraagt van het systeem waarop de *agent* draait.

Om ervoor te zorgen dat er geen externe factoren een invloed kunnen hebben op de tests worden deze uitgevoerd op een nieuwe virtuele machine. De instellingen van deze machine worden hieronder uitgebreid besproken.

5.2 Belasting van de *endpoints*

5.2.1 Opstelling

Er wordt gestart vanuit een nieuwe installatie van Windows 10. Alle tests worden uitgevoerd op een nieuwe installatie er worden dus geen snapshots of back-ups gebruikt om naar terug te gaan. Dit om te vermijden dat een *agent* de performance van zijn opvolgers kan beïnvloeden. Verder worden alle tests uitgevoerd op een host met het maximale prestaties energieschema, hiermee wordt vermeden dat de resultaten worden beïnvloed door een verschillend energieschema op de host. Automatische updates van de host worden uitgeschakeld om te vermijden dat deze eventuele resultaten beïnvloed. Ook worden alle *agents* vergeleken met een gratis antivirus zonder EDR-capaciteiten.

De opstelling van de virtuele machine is als volgt:

Tabel 5: Instellingen Test VM

Naam	Stage-Test-VM
Besturingssysteem	Windows 10 Pro N
RAM	4 GB / 4096 MB
CPU	1
Cores	2
Automatische updates	Nee
Netwerk	Custom: Geen internetconnectie en geen verbinding met de host
Geopende programma's	Performance Monitor

Een installatiegids met een gedetailleerde opsomming van de gekozen instellingen is beschikbaar als bijlage onder de naam "Bijlage A: installatiegids Windows testmachine".

We vergelijken alle machines in een inactieve toestand elke 5 minuten gedurende een periode van 3 uur. Hierdoor worden de resultaten minder beïnvloed door pieken in het verbruik. Om zeker te zijn dat iedere tool evenveel datapunten heeft worden alleen de eerste dertig resultaten gebruikt. Na de installatie van iedere *agent* wordt de cliënt heropgestart om zeker te zijn van een correcte werking van zowel het besturingssysteem als de *agent*. Voor het begin van elke test run wordt de virtuele machine nogmaals heropgestart zonder internettoegang om te vermijden dat de testresultaten worden beïnvloed door automatische updates. Elke toepassing krijgt 2 minuten de tijd vanaf het moment dat het bureaublad zichtbaar is om op te starten daarna start de timer.

Het monitoren van de performance statistieken wordt gedaan met behulp van de ingebouwde tool Performance Monitor. Met deze tool worden de resources automatisch gelogd op vooraf bepaalde tijdstippen. De resources die gemonitord gaan worden zijn "% Processor time" en "Working Set – Private".

5.2.2 Tests antivirus

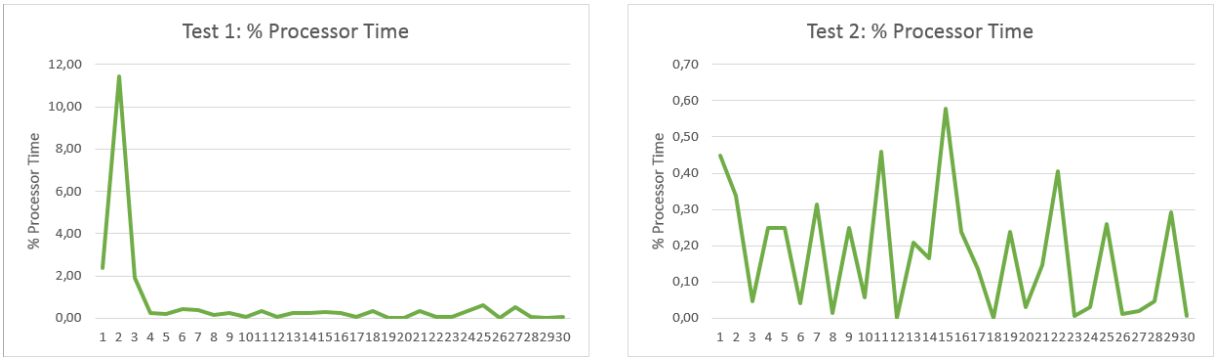
Om de geteste tools te kunnen vergelijken met een normale antivirus tool wordt er ook een free antivirus-tool getest. Uit deze tests zijn de volgende resultaten gekomen.

Tabel 6: Testresultaten Antivirus

	Gemiddelde % Processor Time	Gemiddelde Working Set – Private
Test 1	0,71 %	75,60 MB
Test 2	0,18 %	52,79 MB
Gemiddelde	0,45 %	64,20 MB

Deze resultaten liggen redelijk ver uit elkaar maar in beide tests zit de tool in dezelfde categorie. Wat betreft CPU gebruik doet de tool het goed met een verbruik van minder als 1%. Het RAM gebruik is wel aan de hoge kant in beide runs maar niet problematisch hoog.

Uit onderstaande grafieken valt af te leiden dat het CPU-verbruik van de antivirus-tool redelijk stabiel is. Er is slechts één piek in het verbruik in beide tests. De tweede grafiek doet vermoeden dat er veel pieken in het verbruik zijn, maar dit is te wijten aan de schaalverdeling.



Figuur 23: Grafiek CPU Antivirus

Op basis van onderstaande grafiek valt ook te besluiten dat het RAM verbruik consistent is. Gedurende de twee tests zijn er nergens noemenswaardige pieken in het verbruik.

Figuur 24: Grafiek RAM Antivirus

5.2.3 Tests Symantec

Uit de tests die uitgevoerd zijn op de Endpoint Protection *suite* van Symantec zijn volgende resultaten gekomen.

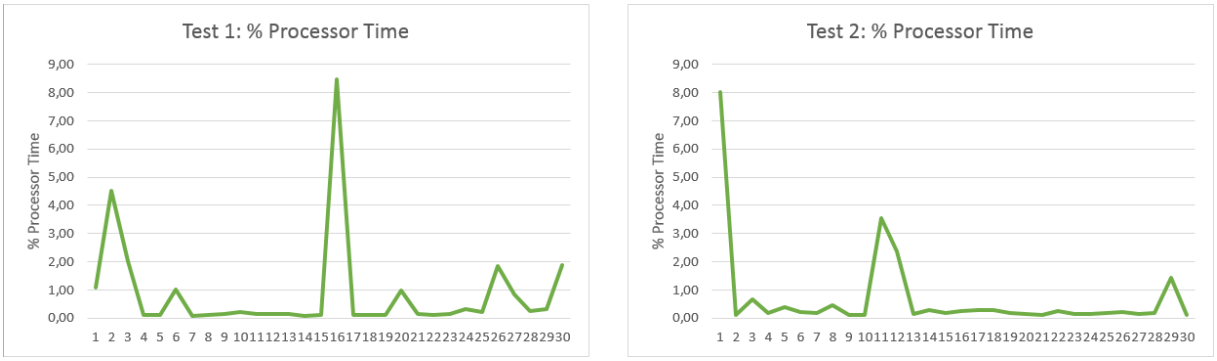
Tabel 7: Testresultaten Symantec

	Gemiddelde % Processor time	Gemiddelde Working Set – Private
Test 1	0,87 %	28,43 MB
Test 2	0,71 %	24,13 MB
Gemiddelde	0,79 %	26,28 MB

Aangezien deze resultaten redelijk dicht bij elkaar liggen kan er vanuit gegaan worden dat deze een redelijk nauwkeurige weerspiegeling van de realiteit zijn. Als deze vergeleken worden met het streefdoel van minder dan 1 % CPU gebruik en minder als 30 MB RAM gebruik dan kan besloten worden dat de Symantec *agent* hieraan voldoet. Omdat de Symantec-*suite* EDR gebruikt zonder *agent* had het EDR-aspect van de *suite* geen invloed op deze resultaten. Deze test geeft dus enkel het verbruik weer van de Symantec Endpoint Protection tool.

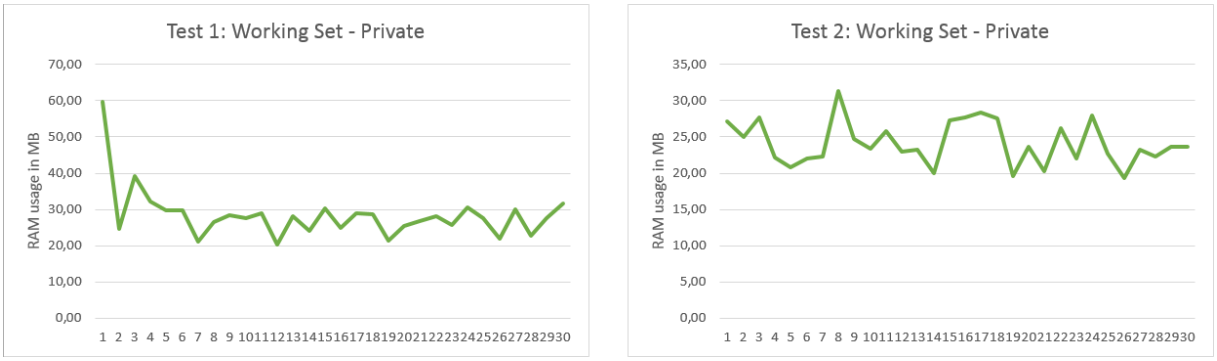
Dit heeft als gevolg dat de Symantec *agent* geen doorslaggevende invloed zal hebben op de systeemvereisten voor *endpoints*. Hierdoor is de tool geschikt voor bedrijven die lichte *endpoints* gebruiken op basis van een cloud abonnement. Ook kan de tool hierdoor gebruikt worden op *endpoints* die zelf erg veel resources gebruiken zonder dat er gevaar is dat deze minder goed zullen werken door de *Endpoint Protection* tool.

Zoals in onderstaande grafieken te zien is blijft het CPU verbruik van de Symantec *agent* consistent doorheen de hele test met uitzondering van enkele pieken.



Figuur 25: Grafiek CPU Symantec

Ook het RAM-verbruik blijft consistent gedurende de test.



Figuur 26: Grafiek RAM Symantec

5.2.4 Tests Sophos

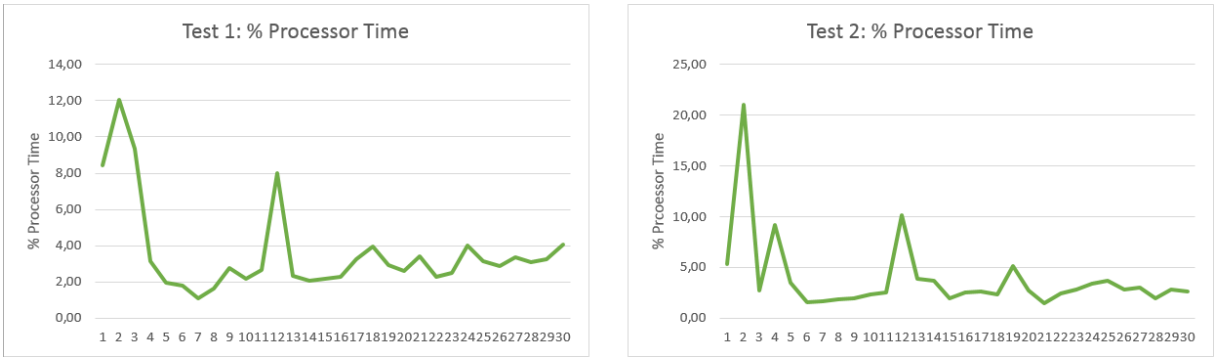
De tests van de Sophos-*suite* zijn uitgevoerd op de *agent* die zowel instond voor de *endpoint protection* als voor de EDR-capaciteiten van de *suite*.

Tabel 8: Testresultaten Sophos

	% Processor Time	Working Set – Private
Test 1	3,62 %	477,37 MB
Test 2	3,85 %	476,82 MB
Gemiddelde	3,74 %	477,01 MB

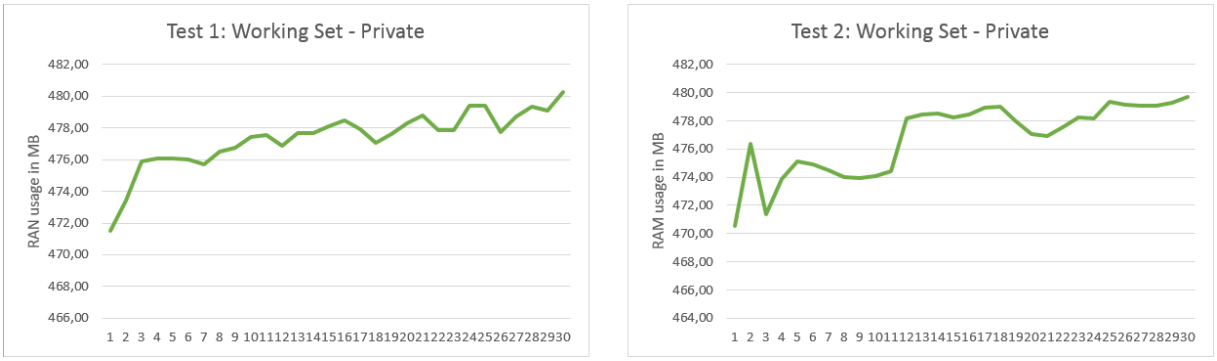
Het eerste wat opvalt is dat deze resultaten ver boven het gemiddelde van de andere geteste tools uitsteken. Met een gemiddeld RAM verbruik van 477,37 MB tijdens de eerste tests en 476,82 MB tijdens de tweede tests kan de *agent* klanten dwingen om over te stappen op een cloud abonnement met meer resources. Dit kan op lange termijn een grote investering zijn. Ook is het verbruik van de processor meer dan drie keer zoveel als dat van sommige andere tools. Op basis van deze resultaten kan besloten worden dat de tool enkel bruikbaar is in omgevingen die een grote hoeveelheid aan extra resources hebben, of in bedrijven die bereid zijn om een aanzienlijke extra investering te maken.

Uit onderstaande grafieken valt af te leiden dat het CPU-verbruik van de Sophos-*suite* piekt aan het begin van de test en vervolgens nog enkele malen gedurende de rest van de test. Hierdoor zullen de gemiddelde resultaten iets hoger liggen dan verwacht.



Figuur 27: Grafiek CPU Sophos

Uit onderstaande grafieken kan afgeleid worden dat het RAM-verbruik, in tegenstelling tot het CPU-verbruik, laag start en geleidelijk aan hoger klimt tot het consistent blijft rond 480 MB. Dit heeft als gevolg dat de gemiddelde waardes uit de tests lager gaan liggen als het RAM-verbruik in de realiteit nadat er een paar uur verstreken zijn.



Figuur 28: Grafiek RAM Sophos

5.2.5 Tests Trend Micro

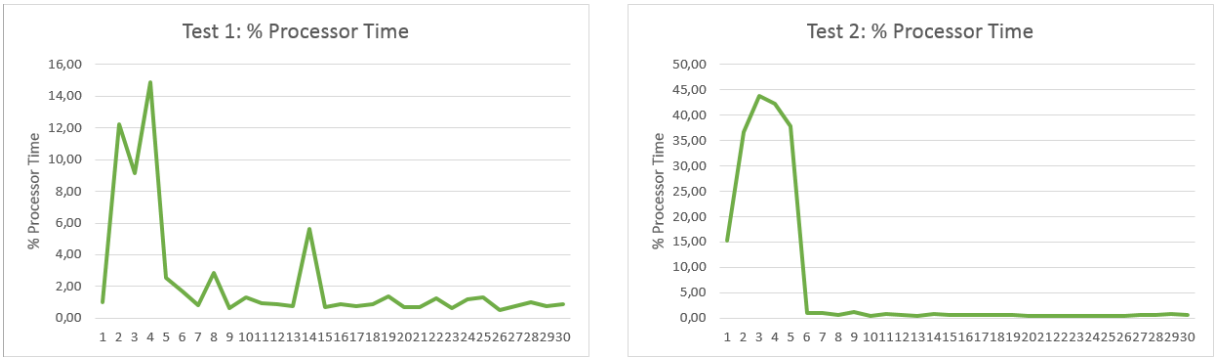
De tests van de Trend Micro-*suite* zijn uitgevoerd op de *agent* die zowel instond voor de *endpoint protection* als voor de EDR-capaciteiten van de *suite*.

Tabel 9: Testresultaten Trend Micro

	% Processor Time	Working Set -Private
Test 1	2,32 %	65,98 MB
Test 2	6,41 %	70,92 MB
Gemiddelde	4,37 %	68,45 MB

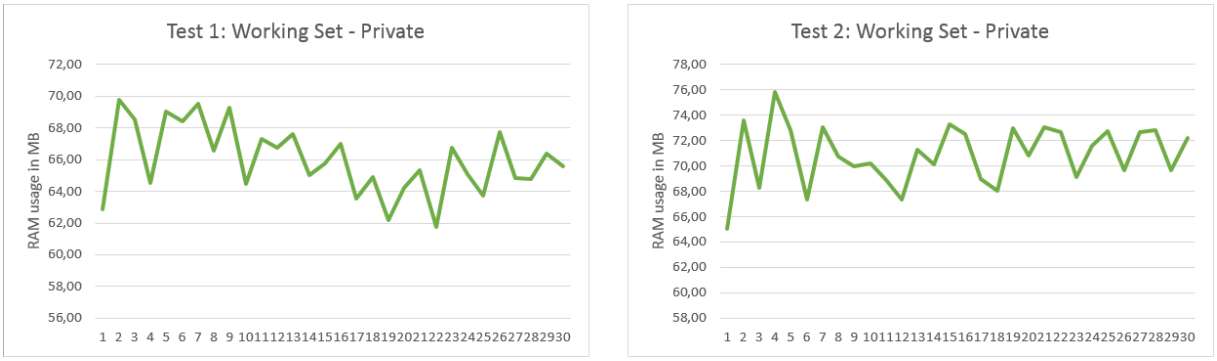
Wat opvalt aan deze data is dat de resultaten voor het CPU gebruikt tijdens de tweede test uitzonderlijk hoog zijn. Uit de grafieken is af te leiden dat dit veroorzaakt werd door enkele pieken aan het begin van de test.

Uit de grafiek van de tweede test kan er afgeleid worden dat het gemiddelde resultaat hoger ligt dan verwacht door een piek in het CPU-verbruik van ongeveer 30 minuten. Een kleinere piek aan het begin van de test is ook terug te vinden in de resultaten van de eerste test.



Figuur 29: Grafiek CPU Trend Micro

Het RAM-verbruik van de Trend Micro *agent* blijft consistent doorheen beide tests zoals te zien is in bovenstaande grafieken.



Figuur 30: Grafiek RAM Trend Micro

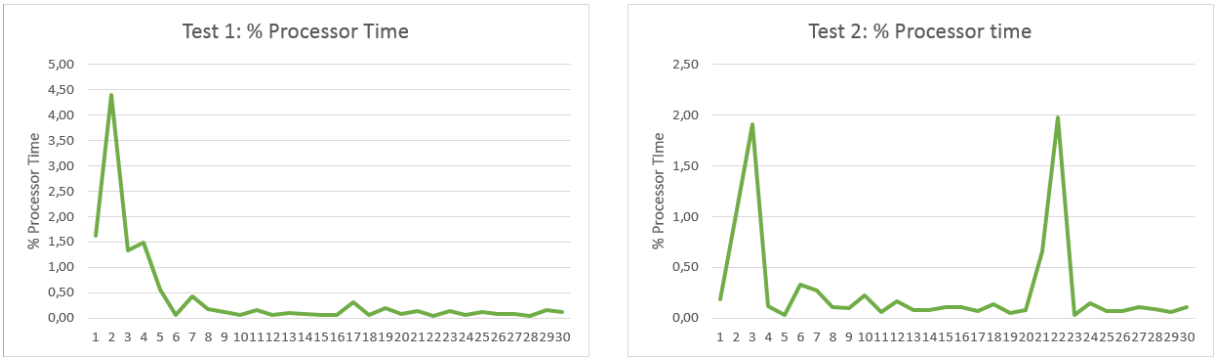
5.2.6 Tests Windows Defender ATP

De tests van de Microsoft-*suite* zijn uitgevoerd op een *endpoint* nadat dit was toegevoegd aan de ATP-*suite*.

Tabel 10: Testresultaten Windows Defender ATP

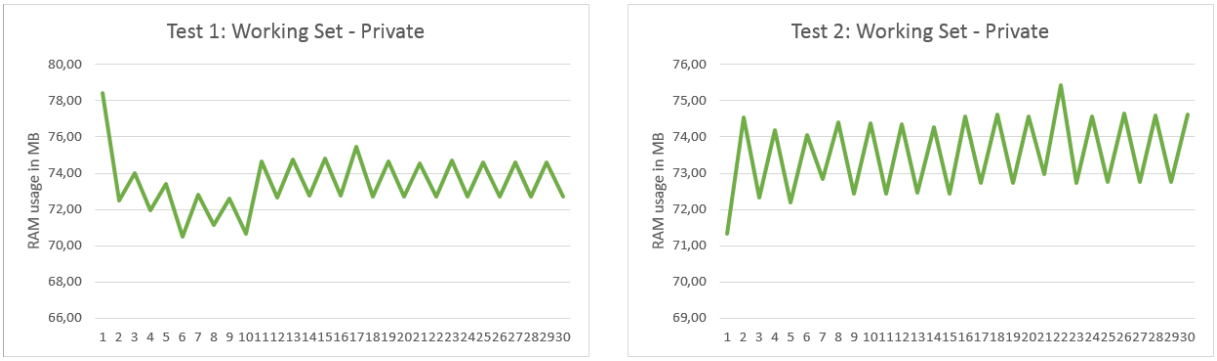
	% Processor Time	Working Set - Private
Test 1	0,42 %	73,41 MB
Test 2	0,29 %	73,52 MB
Gemiddelde	0,36 %	73,47 MB

In beide grafieken is een piek terug te vinden rond het begin van de test. Hierdoor zullen de resultaten iets hoger liggen dan verwacht. De omvang van de piek is echter niet zo groot dus het effect op het gemiddelde resultaat is verwaarloosbaar.



Figuur 31: Grafiek CPU Windows Defender ATP

Het RAM-verbruik van de Windows Defender ATP *agent* is opmerkelijk consistent. Uit onderstaande grafieken valt af te leiden dat het RAM-verbruik schommelt, maar het gemiddelde blijft wel doorheen de hele test ongeveer hetzelfde.



Figuur 32: Grafiek RAM Windows Defender ATP

5.3 Rangschikking

Op basis van de gegevens uit voorgaande test kan er nu een rangschikking worden opgesteld van de onderzochte tools. Deze is hieronder terug te vinden.

Tabel 11: Resource tests rangschikking

Positie	CPU verbruik	RAM verbruik
1ste	Windows Defender ATP (0,36 %)	Symantec (26,28 MB)
2de	Antivirus (0,45 %)	Antivirus (64,20 MB)
3de	Symantec (0,79 %)	Trend Micro (68,45 MB)
4de	Sophos (3,74 %)	Windows Defender ATP (73,47 MB)
5de	Trend Micro (4,37 %)	Sophos (477,01 MB)

Wat opvalt is dat ondanks het feit dat de antivirus tool geen EDR-functionaliteiten had, deze toch in geen van beide tests als eerste eindigde.

Hieruit kan ook afgeleid worden dat zowel de Symantec tool als de Windows tool weinig vragen van de systemen waarop ze draaien. Dit biedt een voordeel aan deze tools in omgevingen waar er zuinig moet worden omgesprongen met resources. Een voorbeeld hiervan zijn endpoints die gebruik maken van gehuurde cloud-infrastructuur.

Wat ook opvalt is dat zowel bij beide tests de tool die eerste eindigde meer dan 10 keer minder vroeg van het systeem vergeleken met de laatste tool. Bij de eerste test was het verbruik ongeveer 12 keer minder en bij de tweede ongeveer 18 keer minder. Hieruit kan afgeleid worden dat de keuze van tool niet alleen wat betreft gebruiksgemak en detecties een voor- of nadeel kan bieden maar ook wat betreft performance. Het is dus belangrijk dat bedrijven niet alleen rekening houden met de kwaliteiten van een tool, maar ook met de investering wat betreft resources.

Dit wordt verder geïllustreerd in figuur 33 waarin de resultaten van alle tests langs elkaar worden weergegeven.

Figuur 33: Grafieken performance conclusie

II. Onderzoekstopic

1 Inleiding onderzoekstopic

1.1 Probleemstelling

Een EDR-toepassing is een grote aanwinst voor een bedrijf op het vlak van security. Toch kan een EDR-toepassing geen volledige bescherming bieden zonder ondersteunende programma's. Om een totaalbeeld te schetsen van het aanbod van de geëvalueerde bedrijven wordt er ook een onderzoek gedaan naar de andere securityoplossingen die de bedrijven aanbieden. De vraag die hiermee beantwoord wordt is "Welk bedrijf biedt de meest volledige *suite* aan?".

In dit onderzoek wordt vermeld welke oplossingen een bedrijf aanbiedt, waar deze voor dienen en wat de meerwaarde van deze oplossing is. Het resultaat is een vergelijkingsmatrix waaruit afgeleid kan worden welke oplossingen zich in het gamma van de onderzochte bedrijven bevinden.

1.2 Onderzoeksmethode

Om tot deze matrix te komen wordt gebruikgemaakt van een literatuurstudie van de bronnen die door de bedrijven zelf worden aangeboden. Waar mogelijk wordt ook verder gebouwd op het onderzoek dat verricht is in het eerste gedeelte van dit eindwerk.

Eerst wordt voor elke tool die onderzocht zal worden een korte beschrijving gegeven over het nut van de tool en de situatie waarin deze gebruikt kan worden. Vervolgens wordt voor elk bedrijf dat deze oplossing aanbiedt besproken wat hun oplossing speciaal maakt. Tot slot wordt al deze informatie verwerkt tot een vergelijkingsmatrix waaruit afgeleid kan worden welke bedrijven het meest volledige aanbod hebben.

Tools die worden aangeboden door partners van het onderzochte bedrijf worden niet opgenomen in deze vergelijking.

2 Uitwerking onderzoekstopic

2.1 Threat Hunting

Om ervoor te zorgen dat het bedrijfsnetwerk te allen tijde zo veilig mogelijk is, volstaat het niet om enkel te vertrouwen op de aanwezige preventie-*tools*. Het is ook nodig dat het securityteam proactief gaat zoeken naar bedreigingen die mogelijk onder de radar zijn gebleven. Om dit te doen helpt een *threat hunting* tool door bijvoorbeeld query's uit te voeren op de *endpoints*. Op deze manier kan het securityteam zoeken naar verdachte symptomen op *endpoints*, verdachte hashes die tijdens eerdere detecties aan het licht zijn gekomen en verdachte handelingen die niet automatisch gedetecteerd werden.

Door proactief naar bedreigingen te zoeken kunnen bedreigingen aan het licht komen voor ze grote schade kunnen aanrichten. Ook kan op deze manier onbekende malware gedetecteerd worden omdat er niet op automatische detectie vertrouwd wordt.

Het spreekt voor zich dat proactief op bedreigingen jagen niet voor elk securityteam is weggelegd. Er is niet alleen een extra tool voor nodig in sommige gevallen, maar ook een securityteam met de kennis en tijd om op bedreigingen te jagen.

Ondanks het feit dat *threat hunting* niet geschikt is voor elk securityteam biedt wel elk bedrijf een manier aan om aan *threat hunting* te doen. Het feit dat alle geëvalueerde bedrijven een vorm van *threat hunting* aanbieden illustreert hoe belangrijk dit is binnen een netwerk.

2.2 Phishing Training

Phishing is een nog altijd vaak voorkomende manier waarop aanvallers een netwerk binnen geraken. Dit komt grotendeels omdat bestaande security-infrastructuur niet altijd kan voorkomen dat een eindgebruiker op een kwaadaardige link of bijlage klikt. Daarom is het belangrijk dat eindgebruikers vaak getest worden op hun kennis wat betreft phishing en indien nodig gesensibiliseerd worden. Omdat dit een hele hoop werk met zich meebrengt als dit manueel gedaan wordt, zijn phishing-trainingstools een uitstekende aanwinst voor een securityteam. Deze tools geven beheerders de mogelijkheid om te kiezen uit een aantal phishingmailtemplates en deze vervolgens te versturen naar de gekozen eindgebruikers.

Uit de resultaten van deze campagne krijgt het securityteam dan een duidelijk beeld wat betreft de hoeveelheid eindgebruikers die op links of bijlagen klikt. Indien nodig kan er dan bijgestuurd worden met behulp van sensibiliseringsacties.

Indien dit ondersteund wordt door de tool, kan het sensibiliseren automatisch gebeuren met behulp van een verplichte training die de eindgebruiker moet volgen als er wordt ingegaan op het verzoek in de phishing-mail.

Deze tools zijn effectiever in bedrijven waar er een groot percentage van de eindgebruikers klikt op verdachte links.

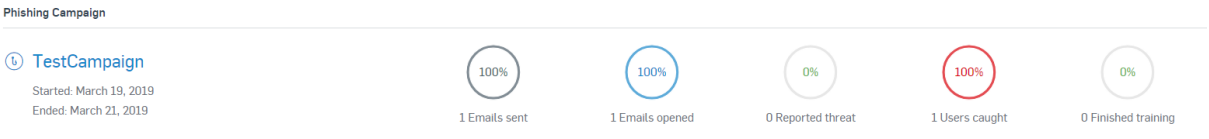
2.2.1 Sophos

De Sophos tool onderscheid zich van de competitie door de tool te integreren met de rest van het Sophos gamma. Hierdoor kunnen beheerders die al Sophos producten gebruiken de phishing training tool beheren vanuit dezelfde cloudconsole.

Een ander voordeel dat de tool biedt is dat er mails verstuurd kunnen worden naar adressen van gebruikers buiten het domein. Op deze manier kunnen ook de persoonlijke e-mailadressen van gebruikers getest worden.

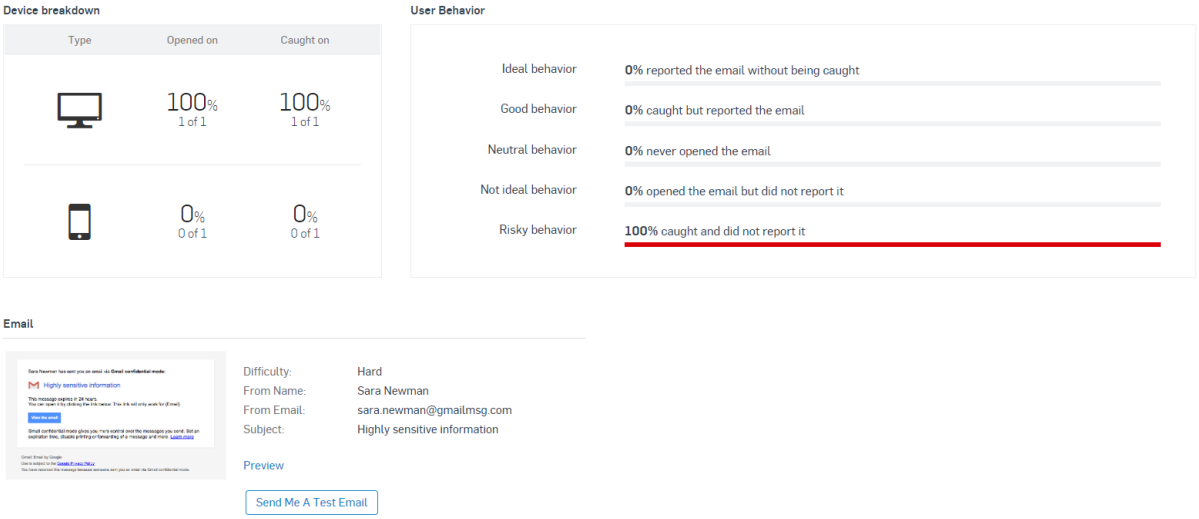
Verder is er ook een outlook plugin beschikbaar waarmee gebruikers verdachte mails kunnen rapporteren. De hoeveelheid gebruikers die een phishingmail rapporteert is te zien in het overzicht van de campagne.

Een voorbeeld van het overzicht van een phishing campagne is te zien in figuur 34.



Figuur 34: Sophos Phishing campagne overview

Er is ook een gedetailleerdere versie van dit overzicht beschikbaar wat eruitziet als figuur 35.



Figuur 35: Sophos Phishing campagne detail view

2.2.2 Trend Micro

Het grote voordeel van de Trend Micro phishing tool is dat deze gratis te downloaden is. Deze tool hangt ook niet vast aan een ander Trend Micro product en kan dus door iedereen gratis gebruikt worden.

Een nadeel van de tool is dat er maximaal 200 phishingmails per campagne verstuurd kunnen worden. Ook kunnen er enkel mails verstuurd worden naar adressen uit hetzelfde domein als het adres waarmee de tool geregistreerd is.

Ondanks deze beperkingen is dit een uitstekende tool voor bedrijven die op kleine schaal werknemers willen sensibiliseren over de gevaren van phishingmails. [15]

2.2.3 Symantec

Het voordeel dat de Symantec tool heeft over de Trend Micro tool is dat er een ongelimiteerd aantal mails verstuurd kunnen worden. Hierdoor is de tool ook geschikt voor grotere bedrijven. De andere functionaliteiten van de tool zijn grotendeels hetzelfde als die van de concurrentie. [16]

2.2.4 Microsoft

Microsoft biedt klanten die een “Office 365 threat investigation and response” subscriptie hebben, hebben de mogelijkheid om een aantal aanvalsscenario’s te simuleren. Eén van deze scenario’s is een gerichte phishing aanval. Hier kunnen beheerders een via HTML een mail opstellen en deze hierna versturen vanuit een vals e-mailadres.

Een voordeel dat deze tool biedt is dat de mail opgesteld kan worden met HTML. Hierdoor kan de mail zo realistisch gemaakt worden als nodig is.

Deze tool heeft wel enkele beperkingen. Zo kunnen er maar vijhonderd mails tegelijkertijd verstuurd worden. Ook is de simulatie enkel beschikbaar wanneer de mailserver van het bedrijf in de cloud gehost wordt. Verder moeten de doelwitten een mailbox op deze server hebben, de tool kan dus niet gebruikt worden om phishingmails naar gebruikers buiten het bedrijf te sturen. [17]

2.3 E-mailfilters

E-mailfilters zorgen ervoor dat spam en phishing-e-mails gestopt worden voor deze de eindgebruiker bereiken. Dit heeft als grote voordeel dat de eindgebruiker nooit de kans krijgt om op de phishingmail te klikken. Wanneer phishingtraining geen optie is, kan dit soort tools er toch voor zorgen dat eindgebruikers veiliger zijn voor phishingmails. Het grote voordeel dat deze tool biedt, is dat mails nooit tot bij de eindgebruikers geraken. Op deze manier is er dus geen enkele kans dat de kwaadaardige e-mails geopend worden.

Toch moet er rekening gehouden worden met het feit dat er altijd een kans bestaat dat een e-mail voorbij de filter geraakt. Wanneer dit gebeurt, kan de filter niet langer garanderen dat de e-mail ongeopend blijft.

2.3.1 Sophos

De e-mailfilter uit de Sophos-*suite* noemt Sophos Email Security. Het grote voordeel dat deze tool biedt ten opzicht van de concurrentie is dat de tool werkt op basis van artificiële intelligentie. Een ander groot voordeel is dat de tool al geïntegreerd is in de cloudconsole van Sophos. Als een bedrijf ervoor kiest om zowel de *endpoint* protectie toepassingen als de e-mail filter van Sophos te gebruiken kunnen deze beide vanuit dezelfde console beheerd worden. [18]

2.3.2 Trend Micro

Een van de grote voordelen van de Trend Micro e-mailprotectie-*suite* is dat deze de mogelijkheid heeft om de schrijfstijl van binnenkomende mails te analyseren en te vergelijken met de effectieve schrijfstijl van de afzender. Op deze manier wordt het voor aanvallers moeilijker om zich voor te doen als iemand anders.

De *suite* maakt ook gebruik van *machine learning* om verdachte patronen te herkennen en op deze manier kwaadaardige mails de onderscheppen voor ze de eindgebruiker bereiken. Verder worden ook hyperlinks geanalyseerd en wordt gebruikgemaakt van *sandboxing*. [19]

2.3.3 Symantec

De Symantec-*suite* onderscheid zich van de concurrentie door isolatie technieken aan te bieden waarmee de gevaarlijke stukken van mails en websites geïsoleerd kunnen worden. Op deze manier kunnen gebruikers veilig hun mails openen zonder dat ze zich zorgen moeten maken over eventuele kwaadaardige links. [20]

2.3.4 Microsoft

De Microsoft-*suite* biedt geen extra's aan ten opzichte van hun concurrenten. Ook is hun *suite* enkel beschikbaar voor Exchange mail. [21]

2.4 Encryptie

Om te vermijden dat gevoelige informatie verloren gaat wanneer er een mobiel *endpoint,* zoals bijvoorbeeld een laptop, gestolen wordt, kan er aan encryptie gedaan worden. Dit kan manueel ingesteld worden voor elk *endpoint*. Dit brengt echter een hele hoop extra werk met zich mee. Een tool die automatisch aan alle *endpoints* encryptie oplegt kan dus een hele hoop tijd besparen. Er zijn verschillende vormen van encryptie die gebruikt kunnen worden en deze hebben elk hun voor- en nadelen.

Een eerste encryptiestrategie die gebruikt kan worden is harde schijf-encryptie. Hiermee wordt de volledige harde schijf geëncrypteerd. Dit heeft als voordeel dat er geen gegevens van de harde schijf gestolen kunnen worden. Wanneer voor deze manier gekozen wordt encrypteert een *endpoint* zichzelf bij het afsluiten en decrypteert dit *endpoint* zichzelf weer bij het opstarten. Dit heeft als nadeel dat deze manier van encrypteren geen extra beveiliging biedt wanneer de *endpoints* actief zijn.

Om dit nadeel tegen te gaan kan er aan file encryptie gedaan worden. Door deze manier van encrypteren te gebruiken worden bestanden apart versleuteld. Hierdoor zijn deze bestanden ook veilig wanneer het *endpoint* actief is. Deze bestanden moeten wel voor gebruik gedecrypteerd worden wat het openen mogelijk trager maakt.

Tot slot is er ook nog de mogelijkheid om externe media zoals usb-sticks te encrypteren. Hiermee wordt hetzelfde bereikt als met een harde schijf encryptie, de data is beschermd wanneer de media gestolen worden, maar niet wanneer ze gebruikt worden.

Met behulp van deze tools heeft een securityteam een duidelijk overzicht van de *endpoints* die geëncrypteerd zijn en kunnen nieuwe *endpoints* ook eenvoudig geëncrypteerd worden. Dit is vooral nuttig in bedrijven met een groot aantal mobiele *endpoints*.

2.4.1 Sophos

Sophos biedt alle drie manieren van encryptie aan in hun Sophos Safeguard-tool. Door gebruik te maken van deze tool kunnen beheerders gecentraliseerd de encryptie van *endpoints* beheren. Een voordeel van deze tool is dat deze geïntegreerd is in het cloudplatform van de Sophos-*suite*. Ook kan er met één klik een wachtwoord worden aangemaakt voor bestanden die extern gedeeld moeten worden.

De toepassing biedt harde schijf encryptie aan door gebruik te maken van Bitlocker voor Windows systemen en FileVault voor macOS systemen. [22]

2.4.2 Trend Micro

De Apex One Endpoint Encryption-tool van Trend Micro kan gebruikt worden door beheerders voor alle onderzochte vormen van encryptie. Deze tool heeft als grote voordeel dat alle tools vanaf hetzelfde platform beheerd kunnen worden. Een ander voordeel dat deze tool biedt is de mogelijkheid om te integreren met Active Directory. Ook is er de mogelijkheid om multi-factor authenticatie te gebruiken. Tot slot biedt de *endpoint protection suite* van Trend Micro ook de mogelijkheid om Bitlocker en Filevault te beheren.[23]

2.4.3 Symantec

De Symantec-*suite* biedt encryptie aan met behulp van de Symantec Endpoint Encryption-tool. Deze tool kan gebruik maken van alle onderzochte manieren van encryptie. Het grootste voordeel dat

deze tool biedt is de integratie met de DLP-*suite* van Symantec. Hierdoor kunnen deze twee vormen van databescherming samen beheerd worden. [24]

2.4.4 Microsoft

Het aanbod van Microsoft wat betreft encryptie is beperkt tot harde schijf encryptie met behulp van Intune. Er kunnen wel files geëncrypteerd worden door gebruik te maken van het besturingssysteem zelf, maar omdat dit niet gecentraliseerd gebeurt wordt hier geen rekening mee gehouden tijdens dit onderzoek.

Omdat dit slechts één van de drie verschillende manieren van encryptie is wordt dit opgenomen in de vergelijkingsmatrix als niet aanwezig.

2.5 Mail Encryptie

Mail encryptie tools encrypteren en decrypteren mails die verstuurd worden vanuit het netwerk. Op deze manier kunnen onderschepte mails niet gelezen worden door aanvallers.

2.5.1 Sophos

E-mail encryptie zit standaard inbegrepen in de Email Advanced-subscriptie die Sophos aanbiedt. Deze tool geeft gebruikers de mogelijkheid om zowel volledige e-mails als bijlagen te encrypteren voor deze verzonden worden.

Ontvangers van de geëncrypteerde mails hebben enkel het juiste wachtwoord nodig om de mail te lezen. [25]

2.5.2 Trend Micro

De Trend Micro Email Encryption Solutions-*suite* geeft gebruikers de kans om mails te encrypteren met een sleutel die aangemaakt wordt op basis van het e-mailadres van de bestemming. Hierdoor moeten er geen sleutels beheerd worden voordat er efficiënt mails geëncrypteerd kunnen worden.

Trend Micro biedt ook de mogelijkheid om de aangemaakte sleutels door Trend Micro te laten beheren. Dit heeft als voordeel dat er de klok rond een back-up van de sleutels beschikbaar is. [26]

2.5.3 Symantec

Symantec biedt een client-versie en een gateway-versie van hun e-mail encryptie service. Hierdoor kunnen bedrijven die werken met hun eigen e-mail gateways gemakkelijk encryptie implementeren. De tool encrypteert, decrypteert, tekent en verifieert mails automatisch. Hierdoor moeten gebruikers zelf nergens rekening mee houden. [27] [28]

2.5.4 Microsoft

Microsoft biedt bedrijven die gebruik maken van Office 365 de mogelijkheid om te kiezen uit enkele verschillende manieren om mails te encrypteren. De mogelijke opties zijn Office 365 Message Encryption (OME), Information Rights Management (IRM) en S/MIME.

OME heeft als voordeel dat het werkt met andere e-mail services. Ook kan de mail geopend worden zonder dat hier extra software voor nodig is. Dit heeft als voordeel dat eindgebruikers weinig tot geen hinder ondervinden van deze manier van encrypteren. Een nadeel aan deze technologie is dat er geen controle is nadat de mail is aangekomen. De ontvanger kan er dus voor kiezen om de gedecrypteerde mail door te sturen naar andere eindgebruikers.

IRM heeft wel de optie om regels in te stellen wat betreft het doorsturen van de mail.

S/MIME gebruikt sleutels om mails te encrypteren. Om mails te kunnen versturen moet de afzender toegang hebben tot de publieke sleutel van de ontvanger. Hierdoor moet er aan sleutelmanagement gedaan worden voordat deze manier efficiënt gebruikt kan worden. Deze manier van encrypteren wordt dus ook alleen maar gebruikt wanneer dit echt nodig is. [29]

2.6 Data Loss Prevention

Om te vermijden dat eindgebruikers of indringers gevoelige informatie verplaatsen naar externe locaties kan er een Data Loss Prevention (DLP)-tool gebruikt worden. Deze tool zorgt ervoor dat beheerders kunnen aangeven welke data belangrijk is. Dit gebeurt bijvoorbeeld door een blauwdruk van gevoelige informatie op te stellen of door handmatig in te stellen welke informatie belangrijk is. Deze informatie kan dan afhankelijk van de instellingen niet langer verplaatst, gekopieerd of verwijderd worden. Deze tools bieden een uitstekende extra beveiligingslaag aan informatie zoals bijvoorbeeld creditcard gegevens.

Dit soort tools werkt het best in combinatie met encryptie tools. Op deze manier wordt voorkomen dat data het netwerk verlaat wanneer dit niet de bedoeling is, maar wanneer dit toch gebeurt is de data niet bruikbaar zonder de correcte sleutel.

2.6.1 Sophos

De Sophos DLP-oplossing bestaat uit een extra set regels die geactiveerd kunnen worden in de cloud console. Door de DLP-regels te integreren met de *endpoint protection* regels is het mogelijk om snel en eenvoudig alle regels in één keer te configureren. De oplossing maakt gebruik van templates van gevoelige data die door Sophos zijn samengesteld. Hierdoor moeten beheerders enkel aangeven welke data ze willen beschermen. Een nadeel dat deze manier van werken met zich meebrengt is dat de *suite* moeilijk overweg kan met gevoelige data die niet aan een template voldoet. [30]

2.6.2 Trend Micro

De Trend Micro-*suite* biedt een DLP-oplossing aan in dezelfde cloudconsole als de *endpoint protection* oplossing. Deze tool geeft beheerders de mogelijkheid om een template te kiezen of om er zelf één samen te stellen waaraan de gevoelige data moet voldoen. De tool geeft beheerders ook de mogelijkheid om het gebruik van externe media in te perken.

Ook geeft de tool uitgebreide rapporten over eindgebruikers die vaak deze regels schenden. Hierdoor is het gemakkelijk om het overzicht te bewaren. Dit heeft ook als gevolg dat probleemgebruikers snel geïdentificeerd kunnen worden en vervolgens gesensibiliseerd. Om de privacy van eindgebruikers beter te beschermen zijn er wel speciale rechten nodig om deze rapporten in te kijken. [31]

2.6.3 Symantec

De Symantec-*suite* gebruikt een aantal verschillende manieren om aan DLP te doen. Eén van de manieren waarop ze gevoelige data detecteren is met *machine learning*. Deze techniek leert welke data IP van het bedrijf is en beschermt deze.

Ook doet de DLP-tool aan afbeeldingsherkenning, dit helpt de tool met het herkennen van gevoelige data nadat deze gescand of gefotografeerd is.

Ook kan de tool een verband leggen tussen data en deze beschermen wanneer deze samen voorkomen.

Verder kan de tool ook gedeeltelijke stukken van gevoelige data herkennen. Hierdoor kunnen aanvallers de DLP-tool niet omzeilen door de data in stukken te verdelen en deze zo te naar buiten te versturen. [32]

2.6.4 Microsoft

De DLP-regels van Microsoft beschermen gevoelige data op locaties die aangeboden worden door Microsoft zoals bijvoorbeeld Exhange. De regels zijn opgebouwd uit 3 delen namelijk de locatie waar de regel geldt, de omschrijving waaraan de data moet voldoen en de acties die ondernomen worden als aan deze omschrijving voldaan is. [33]

2.7 Device Control

Om het netwerk te beschermen tegen geïnfecteerde *devices* die van buitenaf worden binnengebracht kunnen beheerders met een *device control* tool bepalen welke externe media er gebruikt mogen worden. Op deze manier kunnen eindgebruikers geen apparaten gebruiken die niet zijn toegelaten zoals bijvoorbeeld usb-sticks, externe harde schijven, usb-toetsenborden en dergelijke. Dit heeft als grote voordeel dat aanvallers zich niet doorheen het netwerk kunnen verplaatsen door usb-sticks te infecteren.

Device control wordt door alle bedrijven die onderzocht zijn aangeboden.

2.8 Application Control

Aanvallers gebruiken vaak applicaties die al op *endpoints* staan om zich binnen het netwerk verder te verspreiden. Om dit tegen te gaan kunnen beheerders een application control tool gebruiken om zo te vermijden dat bepaalde applicaties gebruikt kunnen worden. Wanneer dit wordt ingesteld met een blokkeer alles basisregel zorgt dit er ook voor dat aanvallers geen kwaadaardige applicaties kunnen uitvoeren die ze gedownload hebben nadat een *endpoint* geïnfecteerd werd. Hierdoor wordt er ook beschermd tegen onbekende kwaadaardige applicaties.

Application control wordt aangeboden door alle onderzochte bedrijven behalve Crowdstrike.

2.9 Credential management

Een van de eerste symptomen van een geïnfecteerd netwerk zijn logingegevens die gebruikt worden op ongebruikelijke plaatsen. Aangezien deze logingegevens niet noodzakelijk fout zijn is de kans dat een klassieke *endpoint protection* tool ze detecteert redelijk klein. Toch bestaat de kans dat een aanvaller een correcte username en wachtwoord heeft voordat er een aanval plaatsvindt. Dit kan bijvoorbeeld wanneer eindgebruikers hun logingegevens op een post-it bijhouden of door een succesvolle phishingmail.

In deze gevallen kan een credential management tool de indringer wel detecteren. Deze tool houdt bij welke credentials gebruikt worden op ongebruikelijke plekken in het netwerk en meldt deze. Op deze manier worden aanvallers met correcte logingegevens wel gedetecteerd.

2.9.1 Crowdstrike

Het enige bedrijf dat een tool aanbiedt die aan credential management doet is Crowdstike. Deze tool geeft beheerders de mogelijkheid om te zien waar administrator inloggegevens gebruikt worden in het netwerk. Ook geeft deze tool de mogelijkheid om te zien welke applicaties actief zijn in het netwerk en waar. [34]

2.10 Deception

Zodra indringers zich op het netwerk bevinden is het moeilijk om deze te detecteren, zeker als ze tijdens de initiële aanval toegang hebben gekregen tot een legitiem account. Een oplossing voor dit probleem is een tool die valstrikken plaatst in het netwerk. Dit soort tools worden deception tools genoemd.

Deception tools detecteren indringers door extra dingen toe te voegen aan het netwerk en deze dan te monitoren. Wanneer iemand verbinding maakt met één van de extra onderdelen van het netwerk kan met zekerheid gezegd worden dat dit een indringer is. Deze extra onderdelen kunnen bijvoorbeeld netwerkshares zijn maar sommige tools kunnen ook nep *endpoints* in het netwerk plaatsen waar indringers dan mee kunnen communiceren.

Dit soort tools heeft als grote voordeel dat aanvallers veel minder kunnen automatiseren. Indien een aanvaller toch automatisch het netwerk doorzoekt valt deze direct door de mand. Dit geeft het securitypersoneel een groot voordeel, want een aanvaller die zich niet automatisch kan verspreiden door er veel langer over om door het netwerk te reizen.

2.10.1 Symantec

Symantec is het enige onderzochte bedrijf dat een deception tool aanbiedt. Deze tool geeft beheerders de mogelijkheid om gecentraliseerd valse connecties, bestanden, inloggegevens en dergelijke aan te maken. Omdat gebruikers niet eens weten dat deze bestaan is het onmogelijk dat deze gebruikt worden voor legitieme doeleinden. Zodra er interactie is met het lokaas weten beheerders dus met zekerheid dat er een aanvaller op het netwerk zit en kunnen de besmette *endpoints* geïsoleerd worden. [35]

3 Conclusie

Om deze resultaten te illustreren worden deze weergegeven in een vergelijkingsmatrix. Hierdoor wordt er een objectief beeld gevormd van de gegevens en kunnen er gemakkelijker conclusies getrokken worden.

Tabel 12: Vergelijkingsmatrix researchonderdeel

Bedrijf	Carbon Black	Crowd Strike	Sophos	Trend Micro	Symantec	Microsoft
Threat Hunting	✓	✓	✓	✓	✓	✓
Phishing Training	✗	✗	✓	✓	✓	✓
E-mail filters	✗	✗	✓	✓	✓	✓
Encryptie*	✗	✗	✓	✓	✓	✗
E-mail encryptie	✗	✗	✓	✓	✓	✓
Data loss prevention	✗	✗	✓	✓	✓	✓
Device control	✓	✓	✓	✓	✓	✓
Application control	✓	✗	✓	✓	✓	✓
IT hygiëne	✗	✓	✗	✗	✗	✗
Deception	✗	✗	✗	✗	✓	✗

*Microsoft biedt wel harde schijf encryptie aan.

Het valt op dat in de vergelijkingsmatrix er 2 soorten bedrijven naar boven komen. Enerzijds zijn er bedrijven die gespecialiseerd zijn in EDR en die weinig andere tools aanbieden. Anderzijds zijn er bedrijven die proberen een zo volledig mogelijk aanbod te hebben.

Wat opvalt is dat er weinig onderzochte tools zijn die maar door enkele bedrijven worden aangeboden. De bedrijven die ervoor streven om hun aanbod zo volledig mogelijk te maken slagen hier dus ook grotendeels in.

We kunnen dus concluderen dat Carbon Black en Crowdstrike een beperkter aanbod hebben als de rest. Wat hierbij opvalt is dat dit ook de enige bedrijven waren met een commandline interventie mogelijkheid in het voorgaande onderzoek. Hun keuze om zich toe te leggen op enkel EDR en *endpoint protection* geeft hen dus op dat gebied een voorsprong.

Algemene conclusie

In dit eindwerk zijn enkele EDR-toepassingen met elkaar vergeleken op het gebied van performance, functionaliteiten en detecties. Ook is het volledige aanbod van de onderzochte bedrijven onder de loep genomen.

Uit dit onderzoek blijkt dat de onderzochte tools voornamelijk op vijf punten van elkaar verschillen. Namelijk de ondersteunde besturingssystemen, de integraties tussen de *endpoint protection* tool en de EDR-tool, de beschikbaarheid van de informatie, het platform waarop de tool beschikbaar is en het aanbod van het bedrijf.

Wat betreft de ondersteunde besturingssystemen ligt het grootste onderscheid tussen het al dan niet ondersteunen van Linux besturingssystemen. Enkel Carbon Black en Crowdstrike ondersteunen zowel Linux servers als Linux clients. Sophos ondersteund enkel Linux servers. Verder ondersteund Windows Defender ATP zowel clients als servers maar enkel via een externe partner. Opmerkelijk is dat de EDR-*suite* van Microsoft enkel de volledige functionaliteiten aanbiedt voor Windows 10 besturingssystemen. Oudere versies van Windows zijn dus niet volledig ondersteund.

Een ander onderscheid wat betreft de ondersteunde besturingssystemen is het al dan niet ondersteunen van mobiele *endpoints* die gebruik maken van Android of iOS. Hoewel alle bedrijven buiten Carbon Black een *endpoint protection suite* aanbieden voor deze besturingssystemen is Crowdstrike het enige bedrijf met een werkende EDR-toepassing voor mobiele *endpoints*.

Wanneer de integraties tussen de *endpoint protection suites* en de EDR-*suites* vergeleken worden is er maar 1 bedrijf wat uit de boot valt. Symantec is van alle onderzochte bedrijven het enige dat een aparte console heeft voor de EDR-toepassing.

Uit het onderzoek naar de beschikbaarheid van de informatie blijkt dat er een onderscheid is tussen tools die van elke gedetecteerde bedreiging een EDR-rapport voorzien en tools waar dit rapport aangevraagd moet worden. De enige onderzochte tools die enkel rapporten aanbieden na aanvraag zijn de Trend Micro en de Symantec tool. De EDR-toepassing van Symantec is wel in staat om deze rapporten na vaste intervallen te genereren.

De tools van Sophos en Microsoft bieden wel van elke gedetecteerde bedreiging een rapport aan. Het enige verschil tussen deze tools is dat Windows Defender ATP ook alle niet-relevante informatie die verzameld is beschikbaar maakt.

Wanneer het platform waarop de tool beschikbaar is vergeleken wordt blijkt al snel dat de meeste bedrijven zich focussen op een cloudbased tool. Enkel Symantec heeft geen tool die volledig cloudbased is. Verder zijn Carbon Black, Trend Micro en Symantec de enige bedrijven die nog een volledige *on-premise* tool aanbieden. Dit houd in dat enkel deze bedrijven in aanmerking komen wanneer er nood is aan een *on-premise* alternatief.

Tot slot leidt de analyse van het aanbod van de bedrijven tot de conclusie dat er twee soorten bedrijven zijn. Enerzijds zijn er Carbon Black en Crowdstrike die zich focussen op hun endpoint protection en EDR-toepassingen. Anderzijds zijn er de andere bedrijven die proberen een zo volledig mogelijk aanbod te hebben.

Bibliografie

[1] Carbon Black, „CB ThreatHunter | Advanced Threat Hunting & Incident Response | Carbon Black," Carbon Black, [Online]. Available: https://www.carbonblack.com/products/cb-threathunter/. [Geopend 23 04 2019].

[2] Carbon Black, „CB LiveOps | Real-Time Endpoint Query & Remediation | Carbon Black," Carbon Black, [Online]. Available: https://www.carbonblack.com/products/cb-liveops/. [Geopend 23 04 2019].

[3] Carbon Black, „CB ThreatSight | Managed Alert Monitoring And Triage | Carbon Black," Carbon Black, [Online]. Available: https://www.carbonblack.com/products/cb-threatsight/. [Geopend 23 04 2019].

[4] Carbon Black, „CB Defense | Next-Generation Antivirus | Carbon Black," Carbon Black, [Online]. Available: https://www.carbonblack.com/products/cb-defense/. [Geopend 26 02 2019].

[5] Secwise, „Home - Secwise," Secwise, [Online]. Available: https://www.secwise.be. [Geopend 24 02 2019].

[6] Secwise, „Cyber Security - Secwise," Secwise, [Online]. Available: https://www.secwise.be/cyber-security/. [Geopend 24 02 2019].

[7] Secwise, „Identity en access management - Secwise," Secwise, [Online]. Available: https://www.secwise.be/identity-en-access-management/. [Geopend 24 02 2019].

[8] Secwise, „Data *protection* - Secwise," Secwise, [Online]. Available: https://www.secwise.be/data-*protection*/. [Geopend 24 02 2019].

[9] Symantec, „Symantec - Global Leader In Next-Generation Cyber Security | Symantec," Symantec, [Online]. Available: https://www.symantec.com/. [Geopend 25 02 2019].

[10] CrowdStrike, „CrowdStrike - SaaS Endpoint Protection, Threat Intelligence, & Cloud Security," CrowdStrike, [Online]. Available: https://www.crowdstrike.com/. [Geopend 26 02 2019].

[11] Carbon Black, „Re-designing Linux Security: Do No Harm - Introduction | Carbon Black," Carbon Black, 15 11 2018. [Online]. Available: https://www.carbonblack.com/2018/11/15/re-designing-linux-security-do-no-harm-introduction/. [Geopend 28 02 2019].

[12] Trend Micro, „Trend Micro (BE) | Enterprise Cybersecurity Solutions," Trend Micro, [Online]. Available: https://www.trendmicro.com/en_be/business.html. [Geopend 26 02 2019].

[13] Sophos, „Sophos | Cybersecurity Evolved," Sophos, [Online]. Available: https://www.sophos.com/en-us.aspx. [Geopend 27 02 2019].

[14] CounterTack, „GoSecure Managed Detection and Response Services Powered by CounterTack Endpoint Protection Platform," CounterTack, [Online]. Available: gosecure.net. [Geopend 27 02 2019].

[15] Trend Micro, „Simulator | Phish Insight," Trend Micro, [Online]. Available: https://phishinsight.trendmicro.com/en/simulator. [Geopend 03 05 2019].

[16] Symantec, „Phishing Readiness | Symantec," Symantec, [Online]. Available: https://www.symantec.com/products/phishing-readiness. [Geopend 03 05 2019].

[17] Microsoft, „Attack Simulator in Office 365 | Microsoft Docs," Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator. [Geopend 03 05 2019].

[18] Sophos, „Sophos Email Security: Now Powered by Artificial Intelligence | Sophos," Sophos, [Online]. Available: https://www.sophos.com/en-us/products/sophos-email.aspx. [Geopend 06 05 2019].

[19] Trend Micro, „Email & Collaboration Security Solutions | Trend Micro," Trend Micro, [Online]. Available: https://www.trendmicro.com/en_be/business/products/user-*protection*/sps/email-and-collaboration.html. [Geopend 06 05 2019].

[20] Symantec, „email-security-cloud-en.pdf," Symantec, [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/data-sheets/email-security-cloud-en.pdf. [Geopend 06 05 2019].

[21] Microsoft, „Email Security - Microsoft Exchange Online Protection," Microsoft, [Online]. Available: https://products.office.com/en-us/exchange/exchange-email-security-spam-*protection*. [Geopend 06 05 2019].

[22] Sophos, „Full Disk Encryption | Always-On Enterprise Encryption Synchronizes Data in Real-Time | Sophos," Sophos, [Online]. Available: https://www.sophos.com/en-us/products/safeguard-encryption.aspx. [Geopend 07 05 2019].

[23] Trend Micro, „Endpoint Encryption | Trend Micro," Trend Micro, [Online]. Available: https://www.trendmicro.com/en_be/business/products/user-*protection*/sps/*endpoint*/*endpoint*-encryption.html. [Geopend 07 05 2019].

[24] Symantec, „Endpoint Encryption Powered by PGP Technology | Symantec," Symantec, [Online]. Available: https://www.symantec.com/products/*endpoint*-encryption. [Geopend 07 05 2019].

[25] Sophos, „Sophos Email Encryption - Blog - Sophos Central - Sophos Community," Sophos, [Online]. Available: https://community.sophos.com/products/sophos-central/b/blog/posts/sophos-email-encryption. [Geopend 07 05 2019].

[26] Trend Micro, „Email Encryption Solutions | Trend Micro," Trend Micro, [Online]. Available: https://www.trendmicro.com/en_ca/business/products/user-*protection*/sps/email-and-collaboration/email-encryption-*solutions*.html. [Geopend 07 05 2019].

[27] Symantec, „Desktop Email Encryption | Symantec," Symantec, [Online]. Available: https://www.symantec.com/products/desktop-email-encryption. [Geopend 07 05 2019].

[28] Symantec, „Gateway Email Encryption | Symantec," Symantec, [Online]. Available: https://www.symantec.com/products/gateway-email-encryption. [Geopend 07 05 2019].

[29] Microsoft, „Email encryption in Office 365 | Microsoft Docs," Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/office365/securitycompliance/email-encryption. [Geopend 07 05 2019].

[30] Sophos, „sophosdlpdsna.pdf," Sophos, [Online]. Available: https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosdlpdsna.pdf. [Geopend 07 05 2019].

[31] Trend Micro, „Integrated Data Loss Prevention, IDLP | Trend Micro," Trend Micro, [Online]. Available: https://www.trendmicro.com/en_hk/business/products/user-*protection*/sps/*endpoint*/integrated-data-loss-prevention.html. [Geopend 07 05 2019].

[32] Symantec, „Data Loss Prevention & Protection | Symantec," Symantec, [Online]. Available: https://www.symantec.com/products/data-loss-prevention. [Geopend 07 05 2019].

[33] Microsoft, „Overview of data loss prevention | Microsoft Docs," Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies. [Geopend 07 05 2019].

[34] Crowdstrike, „Network Security Monitoring - Falcon Discover | CrowdStrike," Crowdstrike, [Online]. Available: https://www.crowdstrike.com/*endpoint*-security-products/falcon-discover-network-security-monitoring/. [Geopend 07 05 2019].

[35] Symantec, „a-look-at-deception-en.pdf," Symantec, [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/white-papers/a-look-at-deception-en.pdf. [Geopend 13 05 2019].

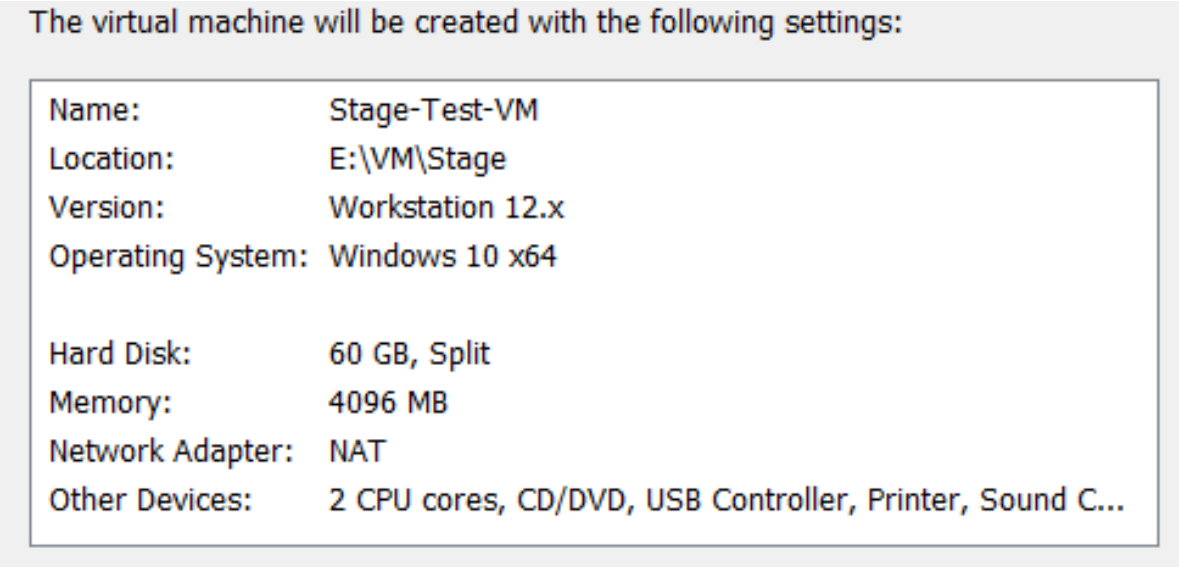
Bijlagen

A. Installatiegids Windows testmachine

B. Extra Windows Defender ATP feature

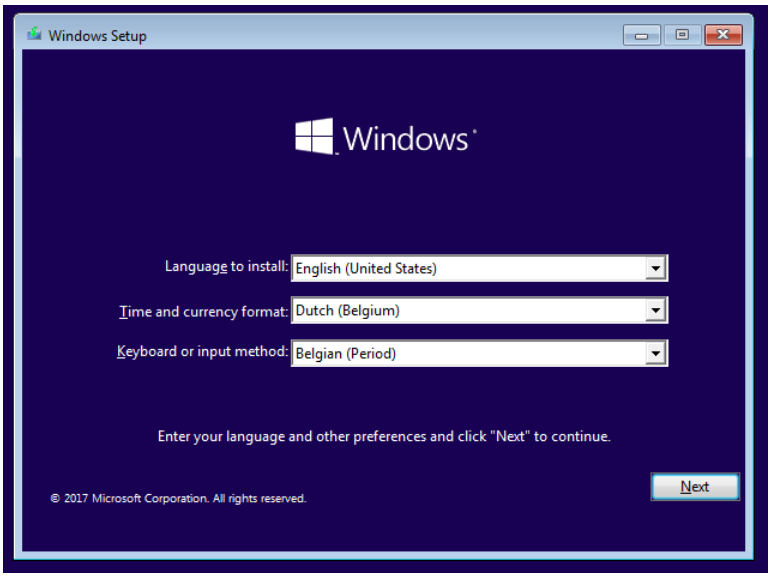
A. Installatiegids Windows testmachine

Voor de installatie van het besturingssysteem wordt er een virtuele machine (VM) aangemaakt in VMWare workstation. De instellingen van deze VM horen er uit te zien zoals te zien is in figuur 36. Na het aanmaken hoort onze VM geen besturingssysteem te hebben, één CPU met twee cores en 4 GB RAM. De overige instellingen behouden de standaardwaarden. Elke testmachine word “Stage-Test-VM” genoemd.



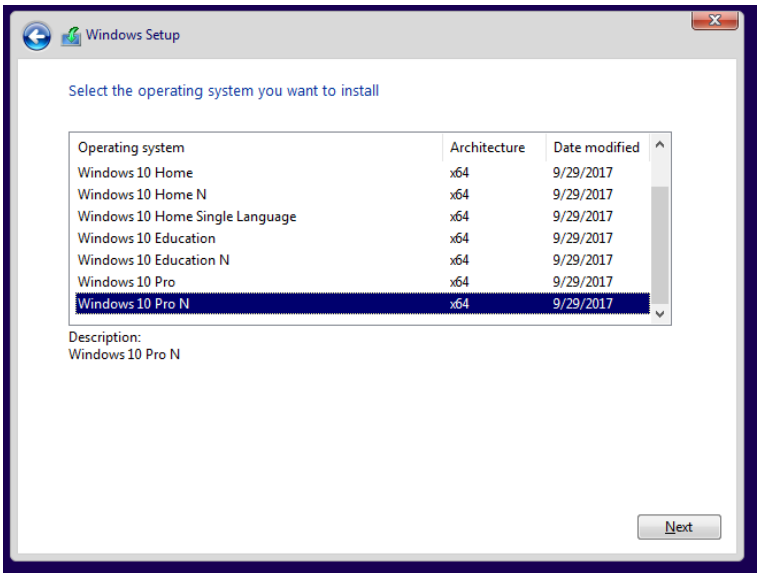
Figuur 36: Instellingen VM

Vervolgens wordt het besturingssysteem geïnstalleerd. De virtuele CD die gebruikt wordt om Windows mee te installeren wordt gemount door middel van VMWare Workstation. Het besturingssysteem wordt geïnstalleerd in het Engels maar de tijd- en toetsenbordinstellingen worden volgens Belgische normen ingesteld. De exacte instellingen zijn te zien in figuur 37.



Figuur 37: Instellingen taal

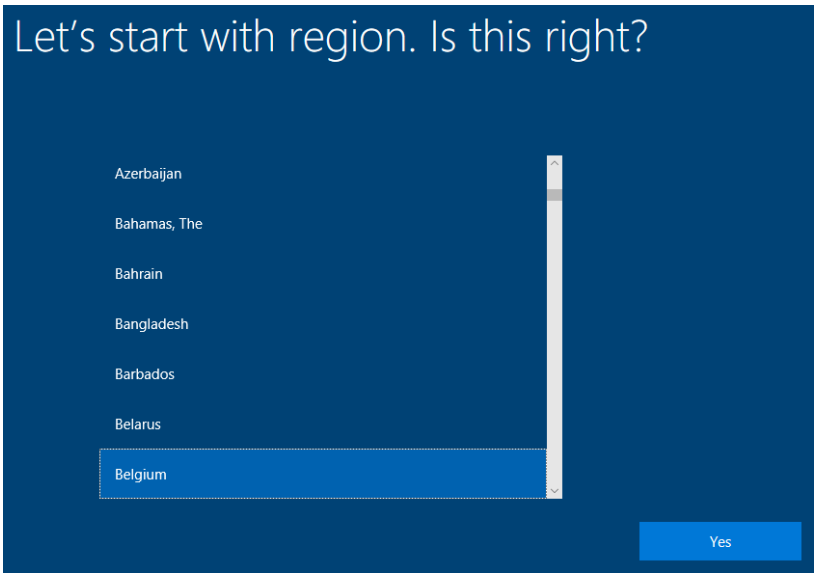
Wanneer er gevraagd wordt om een *product key* in te geven wordt gekozen voor de optie “I don’t have a product key”. Hierdoor kan er later gekozen worden uit een lijst van besturingssystemen die geïnstalleerd kunnen worden. Dit venster is te zien in figuur 38.



Figuur 38: Lijst besturingssystemen

Vervolgens wordt gekozen voor de optie om een gecustomiseerde installatie te doen. Hierdoor kan er gekozen worden om de volledige schijf te gebruiken voor Windows zonder dat er instellingen of bestanden bewaard worden.

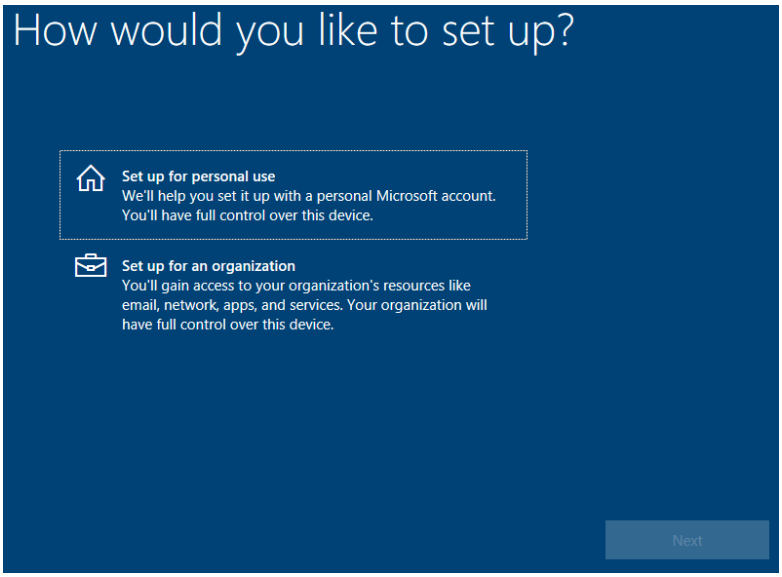
Tijdens het configureren van de gebruikersinstellingen wordt gekozen voor de optie om België als regio in te stellen zoals te zien is in figuur 39.



Figuur 39: Instellingen regio

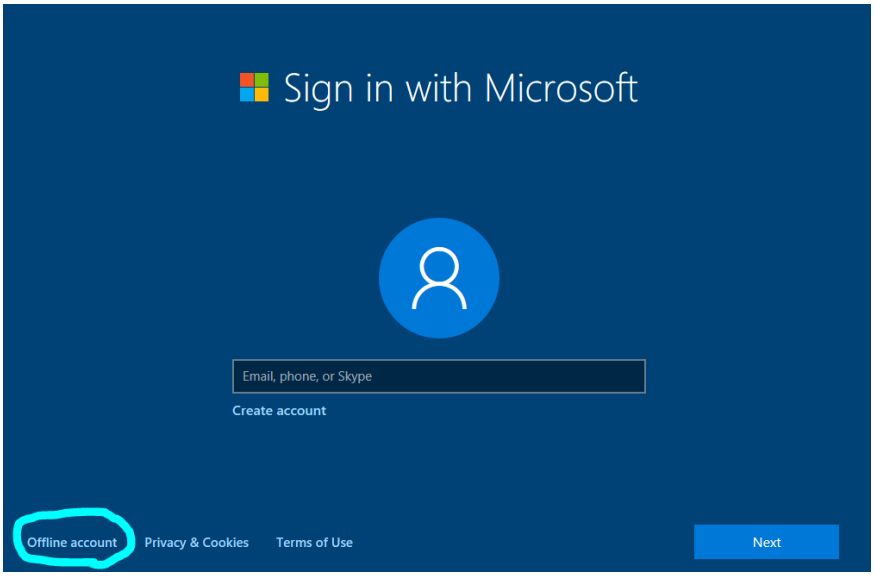
Ook de Belgische keyboard lay-out wordt bevestigd.

Vervolgens kan er gekozen worden om de computer in te stellen voor persoonlijk of professioneel gebruik. Voor deze tests wordt de keuze gemaakt om de computer in te stellen voor persoonlijk gebruik. Dit scherm wordt verder geïllustreerd in figuur 40.



Figuur 40: Instellingen persoonlijk gebruik

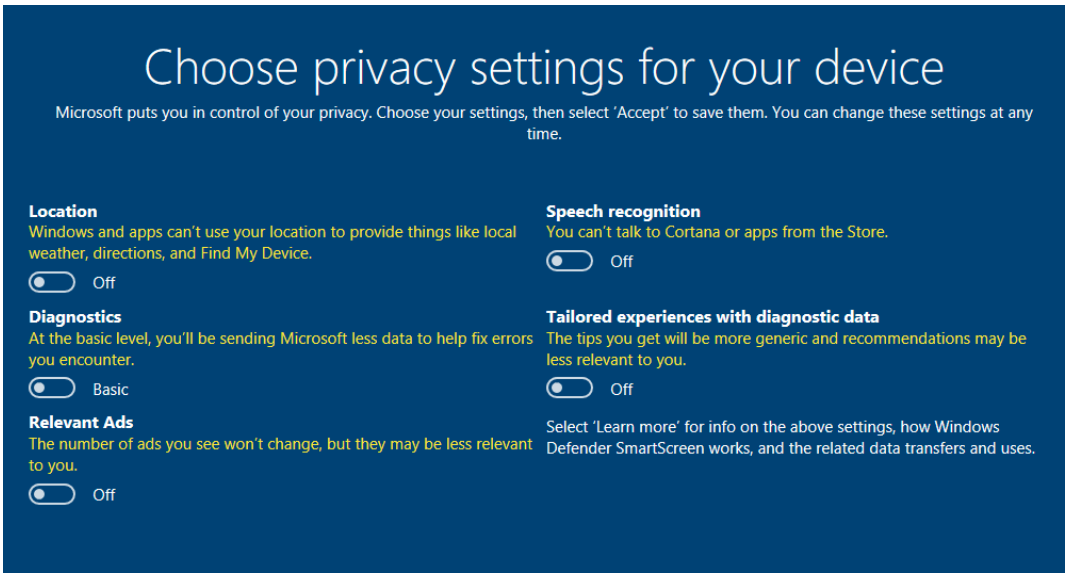
Op het volgende scherm wat te zien is in figuur 41 wordt gekozen om een lokaal account in te stellen.



Figuur 41: Instellingen offline account

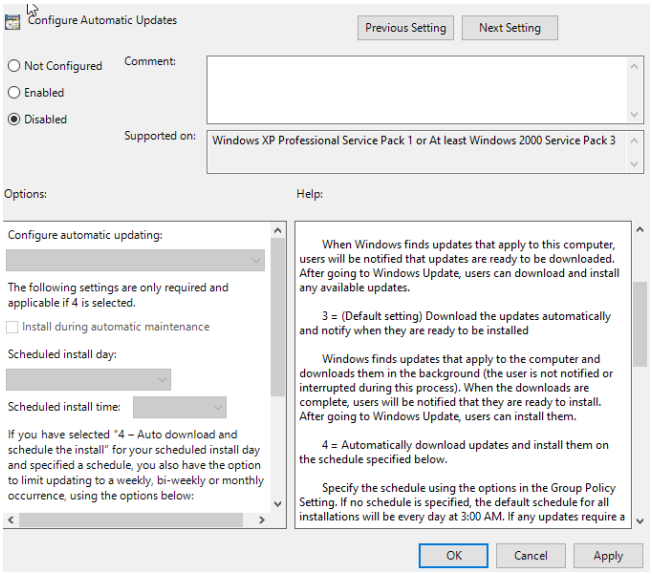
De inloggegevens die voor deze tests gebruikt werden waren Test als gebruikersnaam en Test123 als paswoord.

Om storingen tijdens de tests te vermijden werden de privacy instellingen zo beperkend mogelijk ingesteld. De exacte instellingen zijn te zien in figuur 42.



Figuur 42: Instellingen privacy

Nadat het besturingssysteem volledig geïnstalleerd is wordt met behulp van gpedit.msc de automatische updates uitgeschakeld. De policy instellingen zijn te zien in figuur 43. De policy zelf is terug te vinden onder "Computer Configuration/Administrative Templates/Windows Components/Windows Update/Configure Automatic Updates"



Figuur 43: Instellingen automatische updates

B. Extra Windows Defender ATP feature

Informatica staat niet stil en na afloop van het onderzoek maar voor de publicatie van dit eindwerk heeft Microsoft ook een Live commandline voorzien in de ATP suite. Omdat deze functie pas beschikbaar was nadat alle evaluaties afgelopen waren wordt deze functie niet opgenomen in de evaluatiematrices. Maar omwille van de volledigheid van dit eindwerk wordt deze besproken in deze bijlage.

De live commandline functie biedt beheerders de kans om connectie te maken met een endpoint en hierop commando's uit te voeren. Op deze manier kunnen services beëindigd worden, bestanden gedownload voor onderzoek en dergelijke. Hierdoor kunnen beheerders ook vanop afstand ingrijpen op endpoints die mogelijk geïnfecteerd zijn.

Een van de geavanceerde functionaliteiten van deze functie is het uitvoeren van powershell scripts. Hierdoor kunnen bovenop de standaard commando's beschikbaar in de tool ook alle powershell commando's uitgevoerd worden op endpoints.

OP het moment dat deze bijlage geschreven werd was deze functionaliteit enkel beschikbaar voor Windows 10 endpoints.