



Stageopdracht **Vergelijking SentinelOne & Microsoft Defender**

Reno Goeyvaerts & Robbe Sas | 2023-2024



INHOUDSTAFEL

Inleiding.....	4
De oplossingen.....	6
Microsoft defender XDR.....	6
SentinelOne XDR.....	6
Onderzoek.....	8
SKU's & Features.....	8
Microsoft Defender XDR.....	9
SentinelOne XDR.....	10
Management.....	10
Microsoft Defender XDR:.....	11
SentinelOne XDR:.....	11
Integraties.....	12
Microsoft Defender XDR.....	12
SentinelOne XDR.....	14
S1 RangerAD.....	15
Functionaliteiten:.....	15
Defender for identity.....	16
Functionaliteiten.....	16
Vergelijking.....	17
Deployment.....	17
Microsoft Defender XDR.....	17
SentinelOne XDR.....	18
Vergelijking.....	18
Testing.....	19
Soorten testen.....	19
SentinelOne.....	19
Intune.....	21
SentinelOne control panel.....	27
Sentinels.....	27
Endpoints.....	28
Manual en Pinned groups.....	30
Dynamic groups.....	30
Endpoint details window.....	32
General.....	32
Cloud.....	33
App inventory.....	33
Tasks.....	34
Updates.....	34
Tags.....	34
Actions.....	35
Agent actions.....	35
Endpoint actions.....	35
Response.....	36
Remote shell.....	36
Run script.....	38
Tags.....	40
Policy.....	40

Protection mode.....	40
Detection engines.....	41
Agent.....	42
Deep Visibility.....	43
Binary vault.....	44
STAR Custom Rules.....	45
Blocklist.....	45
Exclusions.....	46
Network control.....	46
Device control.....	47
Upgrade policy.....	48
Incidents.....	49
Threats.....	49
Threat overview window.....	51
Threat Indicators.....	52
Notes.....	53
XDR.....	53
Threat Explore view.....	54
Threat timeline view.....	56
Action Button.....	56
Alerts.....	58
Identity.....	59
Events.....	60
Ranger AD.....	60
AD exposures.....	61
Azure exposures.....	63
Remediation History.....	63
Identity endpoints.....	63
Activity.....	63
ThreatPath.....	64
Identity Endpoints.....	65
Policy Enforcement Status.....	66
Configuration.....	66
Identity policies.....	66
Active Directory.....	67
System.....	68
Startup Wizard.....	68
Reports.....	69
Visibility (Singularity data lake).....	69
Enhanced + legacy view.....	69
query library.....	74
Process graph.....	77
Event Count.....	77
Event Table.....	78
Indicators.....	78
STAR CUSTOM RULES.....	79
Applications.....	82
Inventory.....	83
Policy.....	84
Singularity marketplace.....	84
Catalog.....	85
Installed integrations.....	85

Alien Labs OTX Enrichment.....	86
Collector configurations.....	88
Ingestion Integrations.....	88
Microsoft Azure AD.....	88
Microsoft: O365.....	91
VirusTotal Threat Enrichment.....	99
Alien labs OTX Sandbox.....	101
Automation.....	101
Tasks.....	101
Script Library.....	102
Reports.....	102
Activity.....	104
API.....	106
Microsoft Defender XDR.....	109
Security Baseline.....	110
Attack Surface Reduction.....	112
Device Control.....	112
Attack Surface Reduction Rule.....	113
Microsoft Defender Control Panel.....	113
Hoofd dashboard.....	113
Alerts en Incidents.....	114
Activity log.....	115
Alert Management.....	116
Automatic Investigation.....	116
Threat Hunting.....	117
Community Queries.....	117
Custom Queries.....	118
Submissions.....	119
Deep Analysis.....	120
Werking Deep Analysis.....	121
Device Response Actions.....	122
Live Response.....	123
Werking Live Response.....	124
Collect Investigation Package.....	127
Werking Investigation Package.....	127
Restrict App Execution.....	130
werking Restrict App Execution.....	130
Isolate Device.....	131
Werking Device Isolation.....	132
Cloud Apps.....	133
Cloud Discovery.....	133
Cloud App Catalog.....	134
Cloud Apps Policies.....	134
Monthly Security Report.....	138
Email.....	138
Investigation.....	139
Explorer.....	139
Attack Simulation Training.....	140
Policy & Rules.....	146
Audit.....	146
Indicators.....	149
Configuratie Indicator URLs/Domains.....	149

Integrations.....	153
GitHub integration.....	153
API.....	160
Multi-tenant.....	161
Assignments.....	161
Demo.....	163
MalwareBazaar.....	163
EDR-Testing-script.....	165
Besluit.....	165
EDR.....	166
Threat Hunting.....	166
Integraties.....	166
Documentatie.....	166
Deployments.....	166
Algemene vergelijking.....	167
Bronnen.....	167

INLEIDING

Meer en meer bedrijven kiezen ervoor om hun IT-infrastructuur en security te laten beheren door externe dienstverleners. Hierdoor is het niet nodig om een volledig intern IT-team in te zetten, maar kan er toch worden voldaan aan alle vereisten op het gebied van infrastructuur en security. VanRoey biedt een dergelijke **managed service** aan voor haar klanten. Een van de diensten die zij aanbieden is het opzetten van een **XDR**-oplossing, waarbij XDR staat voor Extended Detection and Response. Dit is de opvolger van EDR, een bekendere detectie- en responsoplossing. EDR monitort alle endpoints, stuurt meldingen en voert acties uit bij het detecteren van potentieel gevaar.

XDR gaat echter verder dan EDR, omdat het hele bedrijf in de gaten houdt. Dit omvat niet alleen endpoints, maar ook aspecten zoals het netwerk, identity management, cloud-workloads, e-mails en andere belangrijke aspecten. Aangezien er verschillende XDR-platformen beschikbaar zijn, is het voor VanRoey van belang om de beste oplossing te bieden aan haar klanten, zodat zowel VanRoey als de klant tevreden zijn.

Om hier een antwoord op te krijgen, zullen we twee van deze platformen onderzoeken, testen en vergelijken: **SentinelOne** en **Microsoft Defender**. Beide zijn prominente spelers in het XDR-landschap. Met ons onderzoek hopen we een duidelijk beeld te schetsen van wat beide platformen te bieden hebben, zodat de meest geschikte oplossing kan worden aangeboden aan de klanten.

Zowel voor het onderzoek, testing en vergelijking gedeelte zal er voor elk van deze delen een apart onderdeel binnen deze documentatie voorzien worden. Hierdoor zal er een duidelijke scheiding tussen de theoretische en de praktische uitvoering gemaakt worden.

DE OPLOSSINGEN

Om een beter inzicht te krijgen in wat beide spelers nu juist te bieden hebben, zullen we in dit hoofdstuk een beschrijving geven van de oplossingen die SentinelOne en Microsoft Defender bieden op het gebied van Extended Detection and Response (XDR).

MICROSOFT DEFENDER XDR

Microsoft Defender XDR (Extended Detection and Response), ook bekend als Microsoft 365 Defender, is een XDR-platform dat een service biedt voor onderzoek en respons op cyberdreigingen. Het biedt native bescherming over endpoints, IoT-apparaten, hybride identiteiten, e-mail en samenwerkingsools, en Cloud toepassingen met gecentraliseerde zichtbaarheid, krachtige analyses, en automatische respons van cyberaanvallen. Dit platform helpt bedrijven om zich te beschermen tegen geavanceerde cyberdreigingen door middel van auto-herstelcapaciteiten voor veelvoorkomende problemen en schaalbaarheid van het beveiligingsteam met XDR-geautomatiseerde disruption.

Microsoft Defender XDR bestaat uit verschillende componenten en producten die samenwerken om een grote hoeveelheid aan beveiligingsdiensten te bieden:

- **Microsoft Defender for Endpoint**
 - Biedt preventieve bescherming, detectie na een breuk, geautomatiseerd onderzoek en reactie voor eindpunten
- **Microsoft Defender for Identity**
 - Beheert en beveilt hybride identiteiten en vereenvoudigt toegang voor medewerkers, partners en klanten
- **Microsoft Defender for Office 365**
 - Biedt e-mailbeveiliging en bescherming van documenten en samenwerkingsools
- **Microsoft Defender for Cloud Apps:**
 - Biedt zichtbaarheid, controle over gegevens en detectie van cyberdreigingen voor cloud services en apps
- **Microsoft Defender Vulnerability Management:**
 - Biedt continue zichtbaarheid van assets, intelligente risicobeoordelingen en ingebouwde repair tools om kritieke kwetsbaarheden en configuratiefouten te identificeren en aan te pakken

Deze componenten werken samen om een unified XDR-ervaring te bieden, waarbij alerts worden gecoördineerd en geanalyseerd om de volledige omvang en impact van een bedreiging te bepalen, en om automatisch actie te ondernemen om de aanval te voorkomen of te stoppen. Dit helpt beveiligingsteams om effectief te reageren op geavanceerde cyberdreigingen en hun incident respons te versnellen.

SENTINELONE XDR

SentinelOne XDR, ook bekend als Singularity XDR, is een geavanceerd cybersecurityplatform dat ontworpen is om organisaties te beschermen tegen verschillende cyberdreigingen, waaronder malware, ransomware en geavanceerde persistente bedreigingen (APTs). Het platform gebruikt machine learning en andere geavanceerde analytische technieken om in real-time beveiligingsgegevens te analyseren en patronen en gedragingen te identificeren die mogelijk een beveiligingsbedreiging kunnen aangeven. Wanneer een bedreiging wordt gedetecteerd, kan het platform automatisch een

reactie activeren, zoals het quarantainen van een apparaat of het versturen van een waarschuwing naar beveiligingspersoneel.

SentinelOne XDR bestaat uit verschillende componenten en diensten die zijn ontworpen om een breed scala aan beveiligingsdiensten te bieden:

- **Endpoint**
 - Het belangrijkste product is een beveiligingsplatform dat endpointbeveiliging, EDR (Endpoint Detection and Response), en geautomatiseerde automated threat response combineert in één oplossing
- **Cloud:**
 - SentinelOne biedt een reeks features en diensten aan om organisaties te beschermen tegen cyberdreigingen in de cloud. Het platform omvat functies die specifiek zijn ontworpen om cloud omgevingen te beschermen, zoals cloud-native endpointbeveiliging en EDR, evenals cloud-forensische mogelijkheden, cloud incidentrespons en cloud threat hunting.
- **Identity:**
 - Het platform biedt ook beveiligingsmogelijkheden gericht op identiteit gerelateerde cyberdreigingen, inclusief identiteit gebaseerde threat hunting

SentinelOne XDR onderscheidt zich door zijn gebruik van geavanceerde AI-technologieën en een multi-vector aanpak om cyberdreigingen te detecteren en te neutraliseren. Het platform is ontworpen om de tijd die een aanval in beslag neemt naar bijna nul te verminderen door geautomatiseerde responsfuncties te bieden, zoals waarschuwingen, het doden van processen, het quarantainen van bestanden en zelfs het terugdraaien van een aanval om gegevens te herstellen.

ONDERZOEK

Zoals hierboven vermeld lijken beide producten enorm hard op elkaar. Daarom is het toch belangrijk om hier de verschillen in te zoeken. Deze verschillen zullen uiteindelijk de beslissende factor zijn voor vele klanten bij het maken van een definitieve keuze.

In dit hoofdstuk gaan we onderzoek doen naar de volgende onderwerpen:

1. **SKU's & features**
 - a. Vergelijking en beschrijving van de verschillende SKU's die door beide oplossingen worden aangeboden
 - b. Analyse van de functies die in elke SKU zijn inbegrepen
2. **Management**
 - a. Vergelijking en beschrijving van de managementconsoles van beide oplossingen
 - b. Beoordeling van de gebruiksvriendelijkheid en functionaliteit van de consoles
3. **Deployment**
 - a. Vergelijking en beschrijving van de deployment methode van beide oplossingen
 - b. Beoordeling van de flexibiliteit en schaalbaarheid van de deployment opties
4. **Testing**
 - a. Beoordeling van de effectiviteit van beide oplossingen in het detecteren en blokkeren van bedreigingen
 - b. Vergelijking en beschrijving van features en integraties in een testomgeving
5. **S1 Ranger AD**
 - a. Analyse van de features en mogelijkheden van SentinelOne Ranger AD
6. **Defender for identity**
 - a. Analyse van de features en mogelijkheden van Microsoft Defender for Identity
7. **Integratie**
 - a. Vergelijking en beschrijving van de integratiemogelijkheden van beide oplossingen

SKU's & FEATURES

Bij het vergelijken van Microsoft Defender en SentinelOne is het essentieel om de specifieke SKU's (Stock Keeping Units) en functies van beide platforms te overwegen. Een SKU is een unieke identificatiecode voor een specifiek product of dienst binnen een inventaris. In het geval van cybersecurity-oplossingen zoals Microsoft Defender en SentinelOne, vertegenwoordigen verschillende SKU's verschillende prijzen, functie sets en licentievoorwaarden. Deze vergelijking helpt organisaties om te begrijpen welke oplossing het beste past bij hun unieke behoeften, budget, en de complexiteit van de cyberdreigingen waartegen ze willen beschermen.

Microsoft Defender XDR

Er worden voornamelijk drie pakketten verkocht, voorzien van verschillende functionaliteiten voor verschillende doelgroepen. Deze zijn: Business Premium, E3 en E5. Het meest gekozen pakket is het Microsoft Business premium pakket. Deze wordt vooral aangekocht voor bedrijven onder de 300 werknemers. Deze is dan ook het goedkoopst in vergelijking met de rest.

Defender heeft twee verschillende pakketten. Zij bieden het P1 en het P2 pakket. Daarom is het ook van belang om te kijken welk van de Microsoft Licenties welk Defender pakket inhoudt. P1 focust vooral op real-time detection en P2 vooral op threat explorer.

ABONNEMENT FEATURES	MICROSOFT BUSINESS PREMIUM	MICROSOFT E3	MICROSOFT E5
Prijs	€380/jaar	€380/jaar	€700/jaar
P1 Defender Support	P1 (requires E3 add-on)	P1	P1 & P2
EDR	✓	✓	✓
Role based access control	✓	✓	✓
API	✓	✓	✓
XDR-integration		✓ (requires E5 add-on)	✓
Multi-tenant Management (requires XDR)		✓	✓
Threat hunting (requires XDR)		✓	✓
Automated investigations & remediation			✓
Datarentatie	30 days	30 days	30 days

SentinelOne XDR

SentinelOne biedt drie verschillende pakketten aan die de klant een XDR-platform kunnen bieden. Deze zijn namelijk SentinelOne Singularity Complete, Commercial en Enterprise.

ABONNEMENT FEATURES	SINGULARITY CONTROL	SINGULARITY COMPLETE	SINGULARITY COMMERCIAL	SINGULARITY ENTERPRISE
Prijs	€73,63	€147,43	€209,99	Inquire with SentinelOne
EDR	✓	✓	✓	✓
Multi-Tenant Management	✓	✓	✓	✓
Role based access control	✓	✓	✓	✓
SDK	✓	✓	✓	✓
API	✓	✓	✓	✓
XDR		✓	✓	✓
Threat-hunting		✓	✓	✓
Data Retention		14 days	30 days	30 days
Identity threat detection and response			✓	✓
Network and Vulnerability Management				✓

SentinelOne doet aan dataretentie. Naarmate het pakket je selecteert, hoe langer je aan data retentie kan doen. SentinelOne biedt dan hierboven op nog eens de mogelijkheid om aan ransomware rollback te doen voor windows machines. Dit stelt organisaties in staat hun gecodeerde bestanden te herstellen naar de staat van vóór de aanval, waardoor de effecten van een ransomware-aanval effectief worden ongedaan gemaakt. Als SentinelOne de geëncrypteerde bestanden niet kan herstellen, betaalt SentinelOne \$1.000 per geëncrypteerde machine, tot een maximum van \$1 miljoen.¹

Verder is er zowel een API als een SDK beschikbaar. De documentatie hier rond is terug te vinden in de management console. De API beschikt over meer dan 300 functies.

MANAGEMENT

Centraal beheer van XDR-instellingen is cruciaal voor MSSP's (Managed Security Service Providers) om de beveiliging van hun klanten efficiënt en effectief te beheren. Hieronder bespreken we de mogelijkheden voor centraal beheer van XDR-instellingen voor de twee verschillende oplossingen.

¹ 'faq', sentinelone.com

Microsoft Defender XDR:

- ***Centrale console***
 - Biedt een centrale console voor het beheer van XDR-instellingen voor alle aangesloten tenants.
- ***Beheer van Defender-producten***
 - Beheer Defender for Endpoint, Defender for Office 365 en Defender for Cloud Apps vanuit één console.
- ***Beveiliging Baselines***
 - Implementeer en beheer beveiliging baselines voor verschillende workloads en omgevingen.
 - Bevat ingebouwde baselines voor verschillende operating systems, workloads ..
- ***Integratie met Azure***
 - Integreert met Azure Security Center voor een gecentraliseerd beveiligingsbeheer.
 - Maakt gebruik van Azure Sentinel voor geavanceerde analyse en threat hunting
- ***Multi-tenant***
- ***Multi-cloud platform support***

SentinelOne XDR:

- ***SentinelOne Management Console***
 - Beheer XDR-instellingen, agents en threat detection vanuit één centrale console.
 - Real-time overzicht van de security status van alle endpoints.
- ***Policy Engine***
 - Definieer en implementeer gedetailleerde Security policies voor verschillende groepen en apparaten.
- ***Hunting & Response***
 - Gebruik de console om proactief te zoeken naar bedreigingen en te reageren op incidenten.
 - Bevat geavanceerde tools voor threat hunting en incident response.
- ***Integraties***
 - Integraties voor management mogelijk door Singularity marketplace zoals Siem, Soar, ticketing ...
 - Integratie met Microsoft platformen voor SSO en data ingestion.
- ***Multi-tenant***
- ***Multi-cloud platform support***

FEATURES	MICROSOFT DEFENDER XDR	SENTINELONE XDR
Centrale console	Beschikbaar	beschikbaar
Meerdere tenants	Ondersteuning voor meerdere tenants	Ondersteuning voor meerdere tenants
Beheer van Defender-producten	ja	nee
Security Baselines	ja	nee
Integratie met Azure	ja	ja
Policy Engine	nee	ja
Threat Hunting & Response	beperkt	geavanceerd (visibility + data lake)
Integratie met Soar	beperkt	mogelijk door Singularity Marketplace
API-integratie	Beperkt	Uitgebreide mogelijkheden
Role-based access control (RBAC)	Beperkte mogelijkheden	Granulaire beperkingen
Whitelisting en blocklisting	Aanwezig	Aanwezig
Rapportage	Aangepaste rapporten en dashboard voor MSSP's	Standaard Rapporten en customiseerbare dashboards

INTEGRATIES

Hier bespreken we de integratiemogelijkheden van Microsoft Defender XDR en SentinelOne XDR. We vergelijken beide producten op basis van de functionaliteiten van de integratie, voordelen en nadelen met betrekking tot de integratiemogelijkheden met diverse tools en platformen.

Microsoft Defender XDR

Microsoft Defender XDR biedt integratiemogelijkheden met verschillende tools en platforms, zowel Microsoft made of 3rd party made, om uw IT-omgeving extra te beveiligen. Hieronder bespreken we enkele voorbeelden:

- ***Microsoft Intune***

De integratie van Microsoft Intune met Microsoft Defender XDR versterkt de beveiliging van uw organisatie door MDM-functionaliteit (Mobile Device Management) te combineren met geavanceerde threat detection and response.

Functies:

- *Security policies afdwingen zoals:*
 - Attack surface reduction
 - Antivirus configuration
 - Firewall rules
 - Security Baselines
- *Voorwaardelijke toegang*

Intune kan voorwaardelijke toegang inschakelen op basis van de beveiligingsstatus van een apparaat dat wordt gerapporteerd door Defender for Endpoint (deel van Defender XDR).

- *Apparaat compliance*

Intune kan apparaten markeren als niet-compliant als ze niet voldoen aan de vereisten van Defender for Endpoint.

- *Partner Catalog*

Defender biedt ondersteuning naar 3rd-party applicaties. Hiervoor zijn alle ondersteunde partners opgeliist onder "Partner Catalog" binnen het Defender portaal. Deze zijn onderverdeeld in Technology partners en Professional services. Binnen deze subcategorieën is er nog een opsplitsing gemaakt naargelang de functionaliteit van de integratie. De Partner Catalog zelf zorgt niet voor de integratie, maar zal u doorverwijzen naar de pagina met de nodige informatie en uitleg over de integratie.

Functies:

- *Technology partners*

Hier worden alle technologische integraties in opgeliist. In volgende categorieën biedt Microsoft Defender de mogelijkheid om je omgeving op een bredere manier te beveiligen:

- *SIEM*
- *SOAR*
- *BAS*
- *Threat intelligence*
- *Network/DNS security*
- *Identity*
- *...*

- *Professional services*

Dit kan je vergelijken met Technology partners, maar hier wordt geen integratie met een technologische tool gemaakt. Er zal een integratie worden gemaakt met een externe service die kan helpen de omgeving te beveiligen door een bepaalde taak binnen Microsoft Defender over te nemen. Volgende soorten services worden aangeboden:

- *Manage*
- *Respond*

- *Protect*
- *Evolve*
- *Educate*

SentinelOne XDR

Ook kan er op verschillende manieren een integratie vanuit SentinelOne gemaakt worden. SentinelOne doet dit op een net iets andere manier dan Microsoft Defender dit doet. Hieronder meer uitleg hierover.

- ***Singularity Marketplace***

SentinelOne biedt zelf heel wat integratiemogelijkheden binnen het platform. Dit noemen zij Singularity Marketplace. Met Singularity Marketplace kan je het XDR-platform uitbreiden. De marketplace telt tot op heden 75 partners die integratiemogelijkheden ondersteunen, waarvan 17 premium partners. Deze partners worden erkend en ondersteund door SentinelOne zelf. Deze partners zorgen ervoor dat SentinelOne kan geïntegreerd worden met onder andere SIEM-platformen, SOAR-platformen, Threat Intelligence, Cloud Security-platformen, e-mailplatformen en veel meer.

- ***Entra ID***

Ook is er de mogelijkheid om Entra ID te integreren binnen SentinelOne, om deze integratie te kunnen gebruiken heb je de P2 subscription van Entra ID nodig. Hiermee kan identiteitsbeheer verenigd worden in het XDR-platform van SentinelOne. Met naadloze integratie kunt u SentinelOne Singularity XDR verbinden met Microsoft Entra ID om identiteitsbeleid af te dwingen en automatisch op bedreigingen te reageren.

Functies:

- Forced password reset
- Sessie beëindigen
- Blokkeer de toegang voor compromised gebruikers
- Beperkte toegang voor compromised gebruikers identiteiten
- Makkelijke verbinding tussen Singularity XDR en Entra ID

- ***Intune***

Ook is er ondersteuning binnen SentinelOne zelf voor Intune, om deze integratie te kunnen gebruiken heb je een P2 subscription nodig van Intune. Dit gebeurt binnen de Singularity Marketplace. Hierin geeft Microsoft, een van de partners, de mogelijkheid om volgende acties uit te voeren:

- Reboot
- Retire
- Wipe
- Etc.

S1 RANGERAD

Ranger AD is een krachtige add-on voor SentinelOne Singularity XDR die uw organisatie beschermt tegen identiteitsbedreigingen. In de hedendaagse digitale wereld zijn identiteiten waardevolle doelen voor hackers. Ranger AD helpt u uw Active Directory (AD) en Entra ID te beveiligen tegen geavanceerde aanvallen.

Functionaliteiten:

Ranger AD biedt een uitgebreide set functionaliteiten die uw netwerkbeveiliging aanzienlijk verbeterd:

- **Detectie van identiteits bedreigingen:**
 - Continuous Scanning van on-prem AD of Entra ID op potentiële vulnerabilities
 - Risicobeoordeling:
 - Ranger AD beoordeelt elk account op basis van verschillende factoren, zoals:
 - Gebruikersrechten
 - Accounts met hoge privileges, zoals beheerdersaccounts, vormen een hoger risico.
 - Aanmeldingsgeschiedenis
 - Accounts met verdachte aanmeldingsactiviteit, zoals frequente aanmeldingen vanuit onbekende locaties, worden gemarkerd als kwetsbaar.
 - Gevoelighed van data
 - Accounts die toegang hebben tot gevoelige data, zoals financiële informatie of klantgegevens, vormen een hoger risico.
 - Identificatie van vulnerable accounts op elk privilege level
 - Vroegtijdige detectie van aanvallen die gericht zijn op identiteitsdiefstal en misbruik van accounts
 - **Machine learning**
 - Ranger AD maakt gebruik van machine learning om verdachte accounts te identificeren. Dit omvat:
 - **Identificatie van anomalieën**
 - Machine learning kan patronen in gebruikersgedrag identificeren en accounts detecteren die zich afwijkend gedragen
 - **Predictive analysis**
 - Machine learning kan voorspellen welke accounts een hoger risico lopen om gecompromitteerd te worden
 - **Reactie op identiteit incidenten:**
 - Acties om verdachte activiteiten te blokkeren en accounts te beveiligen kunnen automatisch of handmatig gebeuren
 - Het beperken van de impact van een identiteits breuk door snelle isolatie of deactivatie van accounts
 - **Verbeterde beveiliging van identiteitsinfrastructuur:**
 - Versterking van on prem AD en Entra ID door het identificeren van configuratiefouten
 - Implementatie van best practices voor identiteitsbeheer om het risico op aanvallen te verkleinen

DEFENDER FOR IDENTITY

Microsoft Defender for Identity zorgt voor het beveiligen van de identiteiten binnen het Defender XDR verhaal. Het is een cloud-based oplossing dat zowel lokale Active Directory- als cloud identiteiten kan beveiligen. Defender for Identity zal geavanceerde bedreigingen die op uw organisatie zijn gericht kunnen identificeren, detecteren en onderzoeken.

Functionaliteiten

Microsoft Defender for Identity biedt een assortiment aan belangrijke functionaliteiten om de beveiliging van de netwerkomgeving van een organisatie te versterken:

- **Identiteits bedreigingen detecteren**
 - Real time analyse en detectie
 - Aanvallen zoals kwaadwillige authenticaties, laterale beweging van aanvallers binnen het netwerk en andere verdachte activiteiten detecteren
 - **Risicoscores:** Op basis van de hierboven vermelde analyse worden risicoscores toegekend aan gebruikers. Verdachte handelingen, ongebruikelijke inlogmomenten en zo voort kunnen leiden tot een stijging in deze score
- **Machine learning**
 - Gebruikt voor geavanceerde aanvallen
 - Ongebruikelijke activiteiten en aanvalspatronen detecteren
- **Evaluatie en rapportage**
 - Inzicht geven op gedetecteerde bedreigingen door middel van de ernstfactor
 - Waarschuwingen voor verdachte activiteiten
- **Beveiligingsmaatregelen**
 - Op basis van gedragsanalyse en risicobeoordeling kan Microsoft Defender for Identity automatisch adaptieve beveiligingsmaatregelen activeren, zoals het blokkeren van verdachte aanmeldpogingen
- **Advanced hunting opties**
 - **Hunting op identiteits bedreigingen:** Defender for Identity biedt geavanceerde hunting opties om te zoeken naar potentiële bedreigingen. Security analysts kunnen hunten op specifieke indicators of compromis (IOC's)
 - **Identificatie van onbekende bedreigingen:** Defender for Identity kan onbekende bedreigingen identificeren door afwijkend gedrag te analyseren en machine learning-modellen te gebruiken
- **Microsoft environment**
 - Makkelijke integratie met andere Microsoft-beveiligingsoplossingen
 - Microsoft Defender for Endpoint, Microsoft Cloud App Security en Microsoft Defender for Office 365

Vergelijking

FEATURES	SENTINELONE RANGER AD	MICROSOFT DEFENDER FOR IDENTITY
Detectie	Continue scanning - Machine learning	Realtime analyse - Machine learning
Identificatie van kwetsbare accounts	gebasseerd op risicobeoordeling	gebasseerd op risicobeoordeling
Reactie	Automatische/handmatige acties - Beperken impact break - Herstellen accounts	Adaptieve beveiligingsmaatregelen
Verbetering	Versterken AD & Entra ID - Best practices - Beveiligingshouding	Integratie met Microsoft-beveiliging
Hunting	/	Geavanceerde hunting - IOC's & afwijkend gedrag
Beheer	Gering tot matig	Matig tot hoog

DEPLOYMENT

Als het gaat om de implementatie van oplossingen bij de klant, is het van cruciaal belang om de verschillende implementatiemogelijkheden te begrijpen en welke aspecten van de implementatie ze ondersteunen.

Het is essentieel om niet alleen de beschikbare implementatiemethoden te begrijpen, maar ook om rekening te houden met factoren zoals de complexiteit van de implementatie, de vereisten van de klant, en de integratie met bestaande systemen en processen. Bovendien moeten eventuele beperkingen of uitdagingen bij de implementatie worden geïdentificeerd en aangepakt om een soepele en succesvolle implementatie te garanderen.

Microsoft Defender XDR

- **Agentless**
 - Microsoft Defender XDR is een agentless oplossing, wat betekent dat er geen software op uw apparaten hoeft te worden geïnstalleerd. Dit maakt de implementatie eenvoudig en snel, en het vermindert de overhead op uw apparaten.
- **Automatische onboarding**
 - De onboarding van Microsoft Defender XDR start automatisch zodra een Defender-service is geactiveerd. Dit maakt de implementatie eenvoudig en snel, en het vermindert de kans op fouten.
- **Aanpassingsmogelijkheden**
 - Basisconfiguratie is automatisch, verdere aanpassingen via Microsoft Defender-portal, aanpassingen kunnen met Intune gepushed worden.

SentinelOne XDR

- **Agent**
 - Vereist installatie van een agent op elke endpoint.
- **Handmatige of automatische implementatie**
 - Flexibele implementatie via handmatige installatie of tools zoals group policy of MDM.
- **Configuratie**
 - U kunt gedetailleerde policies instellen voor verschillende groepen apparaten.
 - Configureer datacollectie instellingen.

We kunnen Intune gebruiken om SentinelOne Agents te installeren op de endpoints. Hiervoor gebruiken we de Intune content prep tool om de msi van SentinelOne gebruiksklaar te maken binnen Microsoft Intune. Aan de hand van onze SentinelOne site token kunnen wij dan automatisch met Intune SentinelOne agents deployen op machines en deze in verbinding stellen met het SentinelOne platform.

Vergelijking

FEATURES	MICROSOFT DEFENDER XDR	SENTINELONE XDR
Agent	/	agent
Implementatie	Automatisch	Handmatig of automatisch
Aanpassingsmogelijkheden	Beperkt (via Microsoft Defender-portal en Intune)	Flexibel (gedetailleerde policies per apparaatgroep, configuratie van datacollectie)
Offlinefunctionaliteit	beperkt	Volledig functioneel

TESTING

Het doel van de "Testing" fase is om de effectiviteit van Microsoft Defender XDR en SentinelOne Singularity XDR te beoordelen in het detecteren en blokkeren van bedreigingen. We zullen beide producten in een testomgeving implementeren en ze onderwerpen aan een reeks tests om hun functionaliteit te vergelijken. We zullen voor beide oplossingen ook de integratiemogelijkheden testen.

SOORTEN TESTEN

We zullen de volgende testen uitvoeren:

- **Detectietesten**
 - We zullen beide producten testen tegen een set bekende bedreigingen om te zien hoe goed ze deze kunnen detecteren.
- **Blokkeertesten**
 - We zullen beide producten testen tegen een set bekende bedreigingen om te zien hoe goed ze deze kunnen blokkeren.
- **Gebruiksgemaktests**
 - We zullen de gebruiksvriendelijkheid van beide producten testen om te zien hoe makkelijk ze te gebruiken zijn.
- **Integratietesten**
 - We zullen bestaande integraties van beide producten testen om te zien hoe makkelijk en goed deze zijn in te stellen en werken.

We zullen het hiernaast ook hebben over de configuraties die we hebben uitgevoerd bij beide producten en de instellingen die we hebben gebruikt voor Intune om onder andere de SentinelOne Agent automatisch te installeren.

SENTINELONE

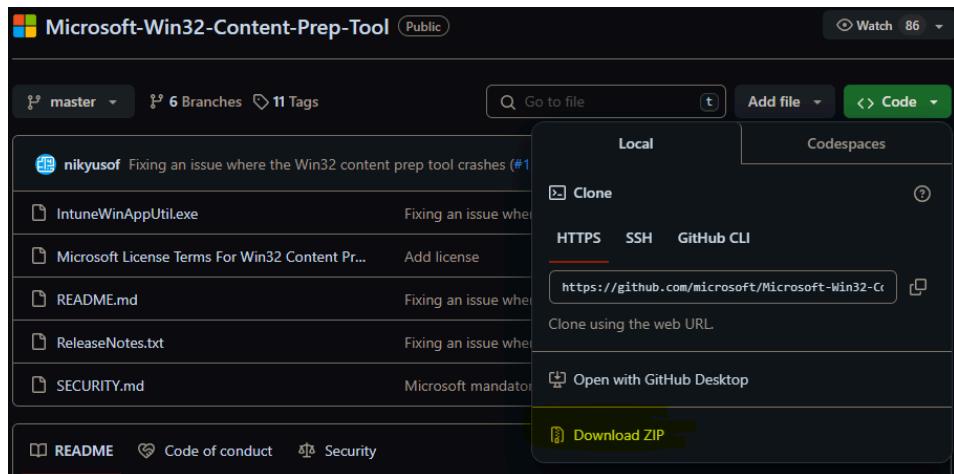
Om SentinelOne te kunnen implementeren in omgeving moeten we eerst de SentinelOne agents installeren op de machines. Dit doen we door gebruik te maken van Intune en co-pilot deployments. Vooraleer we hieraan kunnen starten hebben we eerst de gepaste agent gedownload op het SentinelOne platform gebaseerd op de OS van onze machines.

Nadat we deze hebben gedownload, hebben we gebruikgemaakt van de [Microsoft-Win32-Content-Prep-Tool](#).

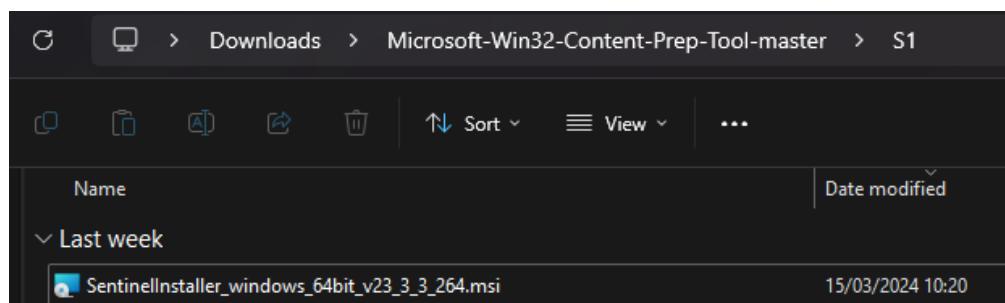
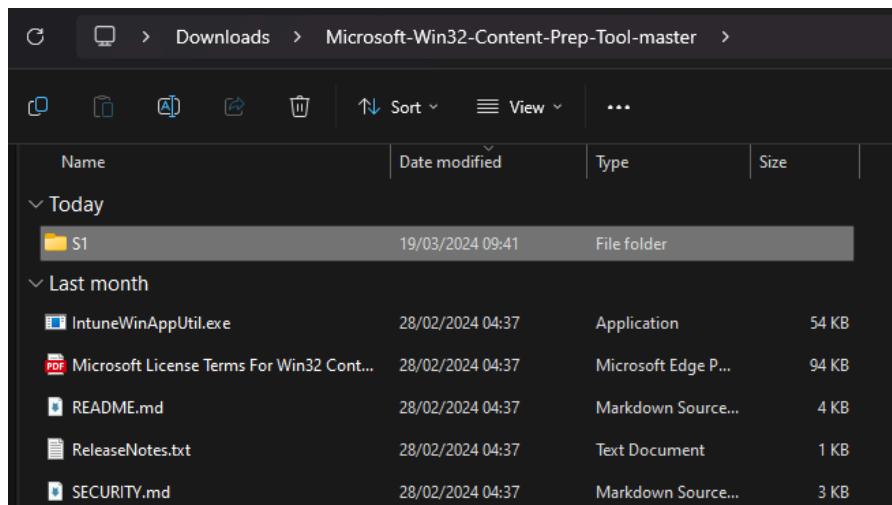
Dit zorgt ervoor dat we de Msi file die we downloaden wordt omgezet naar een. Intunewin bestand.

Dit doen we door de volgende stappen te ondernemen:

1. Eerst downloaden we de bestanden die op de website staan die hierboven gelinkt is:



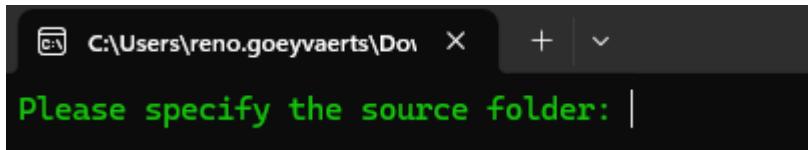
- Vervolgens unzippen we de zip folder en plaatsen we de SentinelOne agent file in een folder die in de unzipped zip folder zit



- Vervolgens klikken we de IntuneWinAppUtil.exe om het omzettingsproces te starten.

IntuneWinAppUtil.exe	28/02/2024 04:37	Application	54 KB
----------------------	------------------	-------------	-------

Na het klikken op de EXE wordt er een CMD-scherm geopend die er als volgend uitziet:



```
Please specify the source folder: |
```

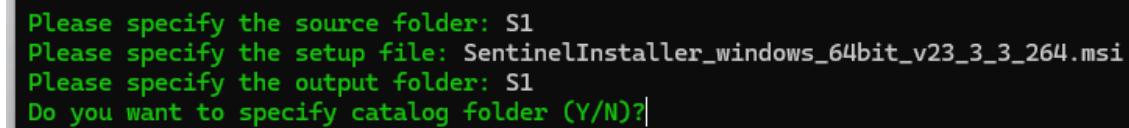
Hierin plaatsen we de volledige file path van de file, in dit geval S1

Na op enter te duwen, worden we geprompt voor de naam van het bestand in dit geval is dit SentinelInstaller_windows_64bit_v23_3_3_264.msi



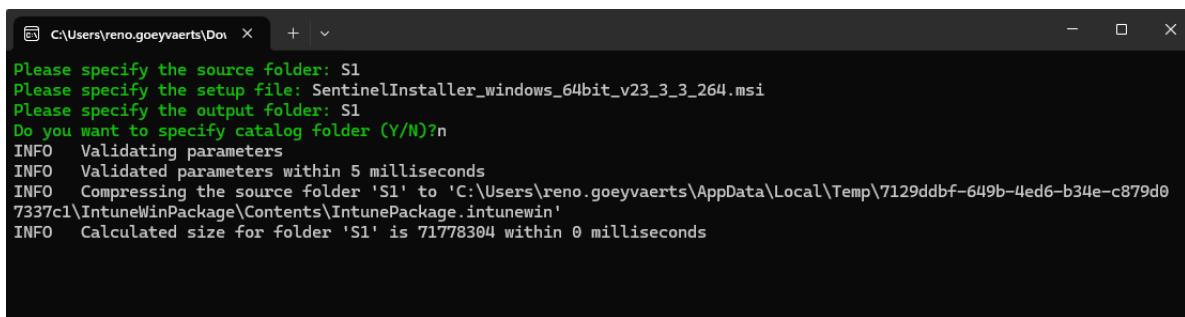
```
Please specify the source folder: S1
Please specify the setup file: SentinelInstaller_windows_64bit_v23_3_3_264.msi
Please specify the output folder: S1
```

Na nog eens op enter geduwd te hebben, worden we geprompt voor de destination folder. Hier kiezen we opnieuw voor S1 en drukken we op enter we krijgen dan dit te zien:



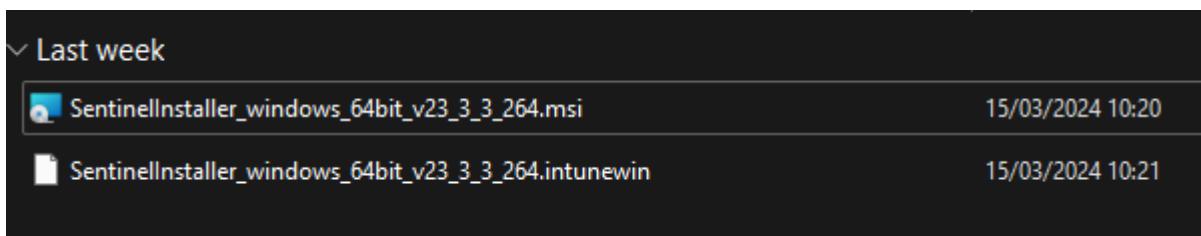
```
Please specify the source folder: S1
Please specify the setup file: SentinelInstaller_windows_64bit_v23_3_3_264.msi
Please specify the output folder: S1
Do you want to specify catalog folder (Y/N)?|
```

Nu typen we "N" en drukken we opnieuw op enter en dit start het conversieproces



```
Please specify the source folder: S1
Please specify the setup file: SentinelInstaller_windows_64bit_v23_3_3_264.msi
Please specify the output folder: S1
Do you want to specify catalog folder (Y/N)?n
INFO  Validating parameters
INFO  Validated parameters within 5 milliseconds
INFO  Compressing the source folder 'S1' to 'C:\Users\reno.goeyvaerts\AppData\Local\Temp\7129ddbf-649b-4ed6-b34e-c879d07337c1\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO  Calculated size for folder 'S1' is 71778304 within 0 milliseconds
```

Als het klaar is wordt het CMD-venster automatisch gesloten en kan je gaan kijken in de S1 folder of de file aanwezig is:



Intune

Nu we de agent voorbereid hebben voor de Intune deployment. Kunnen we starten met de configuratie voor de SentinelOne agent Deployment.

We begeven ons in het Intune admin center naar het apps onderdeel van het dashboard:

The screenshot shows the Microsoft Intune admin center interface. On the left, there is a navigation sidebar with various service icons: Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The 'All services' icon is highlighted. In the center, the title 'Apps | Overview' is displayed above a search bar. Below the search bar is a sidebar with links: Overview, All apps, Monitor, By platform, Windows, iOS/iPadOS, macOS, and Android. The 'All apps' link is highlighted.

We klikken nu op all apps en krijgen we volgend scherm te zien:

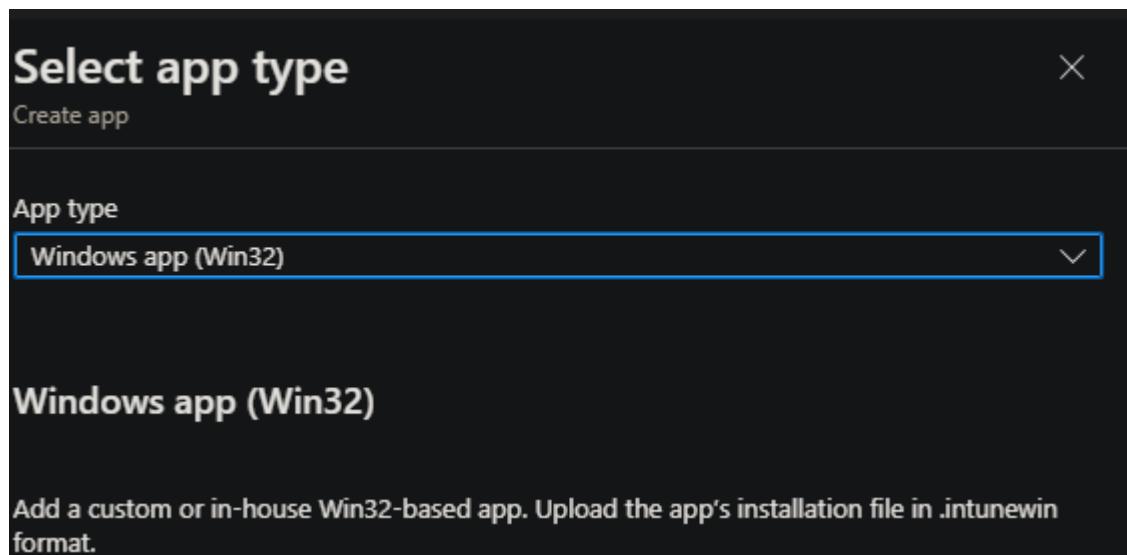
The screenshot shows the 'Apps | All apps' page. At the top, there is a search bar and several action buttons: Add, Refresh, Filter, Export, and Columns. Below the search bar is a search input field labeled 'Search by name or publisher'. A table lists three applications: 7-zip (Windows app (Win32)), Brave Browser (Windows app (Win32)), and Excel (Web link). The 'All apps' link in the sidebar is highlighted.

Name	Type
7-zip	Windows app (Win32)
Brave Browser	Windows app (Win32)
Excel	Web link

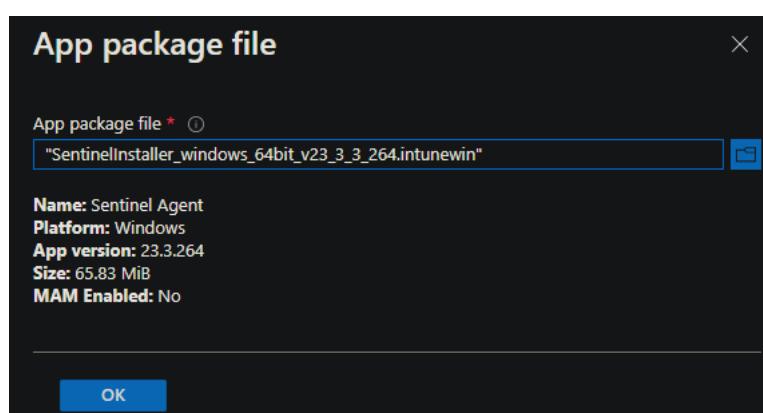
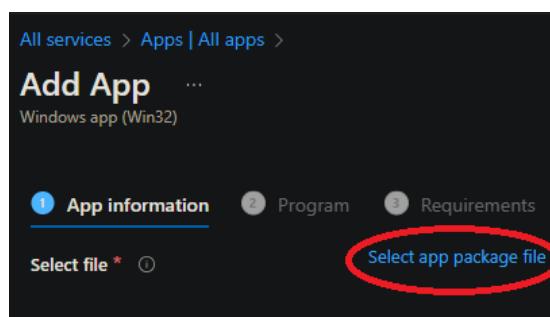
Hierna klikken we op de add knop

The screenshot shows the 'Apps | All apps' page again. The 'Add' button, which has a red circle around it, is located at the top right of the screen next to the other action buttons. The sidebar on the left is identical to the previous screenshot.

We krijgen het Select app type panel aan de rechterkant van het scherm we kiezen hiervoor de win32 app.



We klikken op select onderaan het panel en gaan naar het add app scherm waarin we het hiervoor gemaakte .Intunewin bestand zullen kiezen.



Hierna klikken we op ok en krijgen we het volgende scherm te zien:

The screenshot shows the 'App information' tab of a configuration interface. The 'Select file' field contains the path 'SentinelInstaller_windows_64bit_v23_3_3_264.intunewin'. The 'Name' field is set to 'Sentinel Agent Demo'. The 'Description' field contains 'Sentinel Agent'. The 'Publisher' field is set to 'SentinelOne'. The 'App Version' field shows '23.3.264'. The 'Category' dropdown is set to '0 selected'. There are buttons for 'Yes' and 'No' under 'Show this as a featured app in the Company Portal'. Fields for 'Information URL' and 'Privacy URL' both have placeholder text 'Enter a valid url'. Below these are fields for 'Developer', 'Owner', and 'Notes', each with an empty input box. At the bottom is a 'Select image' button.

Hierin kunnen we de publisher, owner en nog andere dingen beschrijven. Wij hebben bij Publisher SentinelOne ingevuld en zijn dan verdergegaan met de wizard door onderaan het scherm op next te klikken. We krijgen nu het program scherm te zien in de configuratie van de app.

The screenshot shows the 'Program' tab of the configuration interface. It includes fields for 'Install command' (containing 'msiexec /i "SentinelInstaller_windows_64bit_v23_3_3_264.msi" SITE_TOKEN=eyJ...'), 'Uninstall command' (containing 'msiexec /x "{4CE2629F-7EBF-4084-A629-571BC2FF21DF}" /qn'), 'Installation time required (mins)' (set to '60'), 'Allow available uninstall' (set to 'No'), 'Install behavior' (set to 'System'), and 'Device restart behavior' (set to 'No specific action').

We voegen aan het install commando ook nog de site token toe zodat wanneer de agent geïnstalleerd is deze direct aan de site wordt toegevoegd.

Je kan de Site token vinden op het SentinelOne dashboard > Site > Site Info

De commands voor de install en uninstalls worden automatisch ingevuld omdat de originele file een MSI-bestand was, we hebben de settings gebruikt die in bovenstaande foto te zien zijn. Als dit gebeurd is klikken we opnieuw op next. We komen nu terecht op de requirements page voor de app hier stellen we 2 dingen in, namelijk:

- Operating system architecture
- Minimum Operating system

The screenshot shows the 'Requirements' tab selected in a Microsoft Store app configuration interface. It displays two settings: 'Operating system architecture' set to '64-bit' and 'Minimum operating system' set to 'Windows 10 1607'. A descriptive text above the settings reads: 'Specify the requirements that devices must meet before the app is installed.'

We klikken vervolgens weer op next, we komen nu aan bij de detection rules. Deze rules worden gebruikt om te checken of de app effectief wel geïnstalleerd is.

The screenshot shows the 'Detection rules' tab selected. It includes a section header 'Configure app specific rules used to detect the presence of the app.' and a button 'Manually configure detection rules'. Below this, there's a table with columns 'Type' and 'Path/Code', showing the message 'No rules are specified.' and a '+ Add' button.

We kiezen voor "Manually configure detection rules" en daarna op add, we krijgen een nieuw panel te zien aan de rechterkant van het scherm namelijk Detection Rule.

The screenshot shows the 'Detection rule' dialog box. It has a field 'Create a rule that indicates the presence of the app.' and three configuration sections: 'Rule type' (set to 'MSI'), 'MSI product code' (containing the value '{4CE2629F-7EBF-4084-A629-571BC2FF21DF}'), and 'MSI product version check' (with 'Yes' selected).

We kiezen als rule type voor MSI en de product code wordt automatisch ingevuld, de product version check laten we op "No" staan en klikken we onderaan het panel op ok.

Configure app specific rules used to detect the presence of the app.

Rules format * ⓘ

Type Path/Code

MSI {4CE2629F-7EBF-4084-A629-571BC2FF21DF} ...

Nu zie je de zojuist gemaakte rule verschijnen, we drukken hierna op next.

De 2 volgende configuratie delen: Dependencies en Supersedence slagen we over omdat de agent niets specifiek nodig heeft. We komen nu aan bij assignments waar we de groep van users en devices gaan specificeren die de agent geïnstalleerd krijgen.

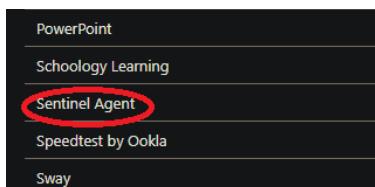
Required ⓘ

Group mode	Group	Filter mode
<input type="button" value="⊕ Included"/>	SentinelOne enjoyers	None

+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ

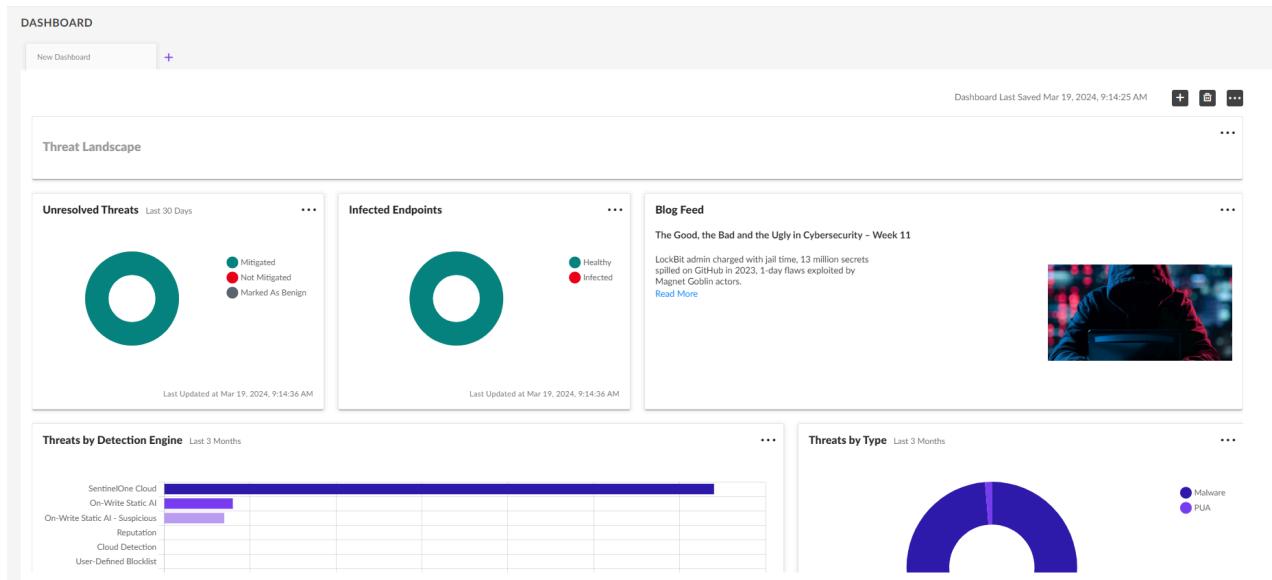
Nadat we dit hebben ingevuld klikken we voor de laatste keer op next en kom je op het review+create scherm waarin je je configuratie nog kan nakijken voor je de app maakt. Je klikt hier onderaan het scherm op create en dat is de laatste stap.

Je kan nu bij apps gaan kijken of de app ertussen staat.



SentinelOne control panel

Wanneer we inloggen op het SentinelOne platform worden we verwelkomd door het dashboard:

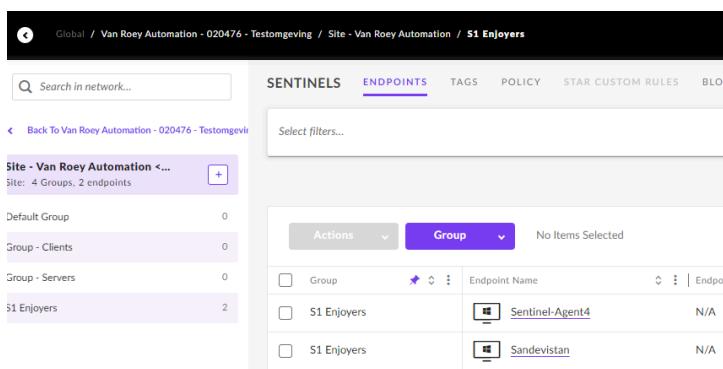


Deze dashboards kan je zelf samenstellen zodat het dashboard de data toont die belangrijk is voor jou.

Sentinels

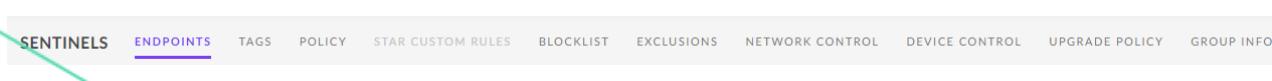


We klikken nu op Sentinels en dan krijgen we dit scherm te zien:



Hierin zien we de verschillende groepen binnen de site waarin we de endpoints kunnen plaatsen, hierdoor kunnen we een onderscheid maken in het implementeren van security policies op endpoints, door dit toe te passen kan men devices quarantainen of dergelijke.

We hebben binnen Sentinels een aantal tabs waarin we configuraties kunnen maken voor de group of site.



Endpoints

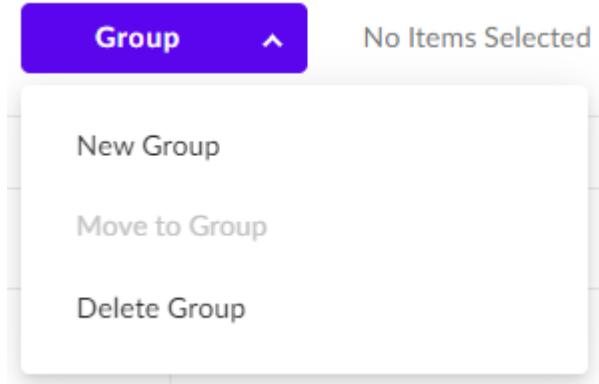
In deze tab van de Sentinels balk zien we alle endpoints die een SentinelOne agent heeft.

Actions		Group		No Items Selected		3 Endpoints		50 Results		Columns		Export	
	Group	Endpoint Name	Endpoint Tags	Account	Site	Last Logged In User	Domain	Console Visible IP					
<input type="checkbox"/>	S1 Enjokers	 Sandevistan	N/A	Van Roey Automation - 0204...	Site - Van Roey Automation	Norman	WORKGROUP	172.201.220.186					
<input type="checkbox"/>	S1 Enjokers	 NetRunner	N/A	Van Roey Automation - 0204...	Site - Van Roey Automation	N/A	WORKGROUP	20.229.116.149					
<input type="checkbox"/>	S1 Enjokers	 LPT-5CG0116GNV	N/A	Van Roey Automation - 0204...	Site - Van Roey Automation	otto	WORKGROUP	84.196.167.72					

Hier zien we informatie over desbetreffende endpoints, de info die je kan vinden in deze tabel is:

- Group
- Naam
- Last logged user
- IP
- Agent version
- Health status
- Device type
- OS
- System specs (CPU, RAM)
-

In deze tab kan je device groups maken, verwijderen en devices van groep veranderen.



We kiezen voor new group en komen we op dit scherm terecht:

ADD NEW GROUP

Group Name

*Group Name
Group Name...

Group Description
Enter Description...

Next

Hier geven we de groep een naam en eventueel een beschrijving (dit is niet verplicht van S1) als je hiermee klaar bent, klik je op next en krijg je volgend scherm te zien:

ADD NEW GROUP

Group Type

Manual Group
Select the endpoints that go in this Group. Endpoints move automatically from this Group to a Dynamic Group if they match a Dynamic Group filter.

Dynamic Group
Create an endpoint filter for this Group. All endpoints that match the filter automatically move to this Group, except for endpoints in Pinned Groups.

Pinned Group
Select the endpoints that go in this Group. Endpoints are pinned to this Group and do not automatically move to other Groups.

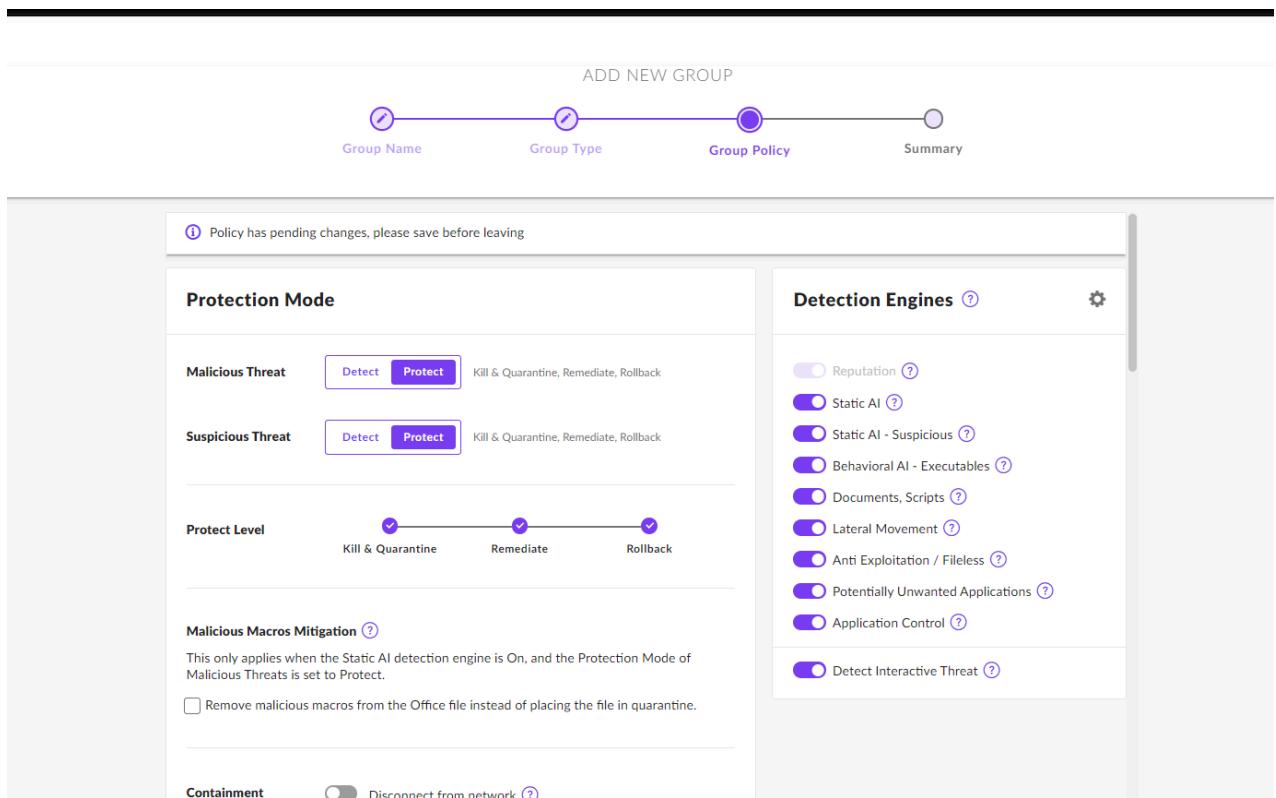
Next

Hier kunnen we kiezen wat voor group we maken, de keuze bestaat uit:

- **Manual group**
 - Kan worden gebruikt als normale groep of verzamelpunt tot de endpoints de filter van de dynamic group matchen.
- **Dynamic group**
 - Voor deze groep moet je een filter maken, alle endpoints die matchen met deze filter worden automatisch in deze groep geplaatst behalve de endpoints die in de pinned group staan.
- **Pinned group**
 - Deze groep is hetzelfde als de Manual group, alleen kunnen de endpoints in deze groep niet naar een dynamic group gaan.

Manual en Pinned groups

Voor zowel de Manual als de Pinned groups is de verdere configuratie hetzelfde, na het kiezen van één van deze twee group soorten klik je op next en krijg je het volgende scherm te zien:

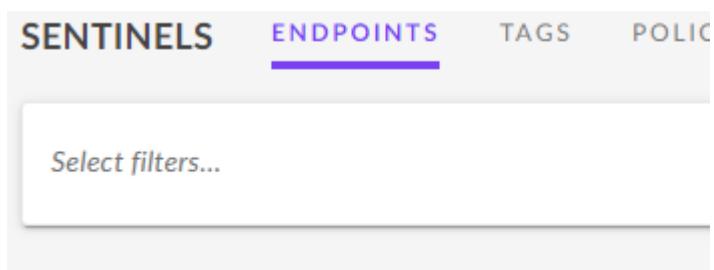


In dit scherm kan je de security configuratie doen die ook in de policy tab kan binnen Sentinels. De diepgaande uitleg over de opties kan je vinden onder de policy titel hieronder. Als je de settings hebt gekozen die je wilt implementeren, mag je naar onder scrollen op de pagina en klikken op create group en dan is de group klaar.

Dynamic groups

De configuratie van de dynamic groups is hetzelfde als die van de andere groups. We moeten alleen voor het configureren van de policies een group filter instellen. Dit doen we nog in de endpoint tab voor we een nieuwe group aanmaken.

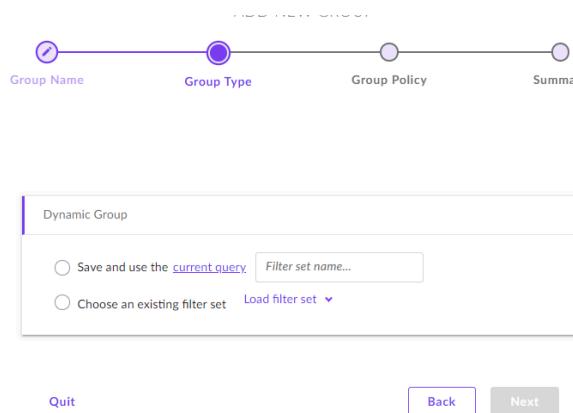
We klikken dan op select filters:



Hier kiezen we één van de filters uit die past bij jouw plan:

The screenshot shows a complex search and filter interface. On the left, there are two search boxes: 'Free text search' (Endpoint Name) and 'Search By Tag' (Has Tag). Below these are dropdown menus for 'Select a key' and 'Select a value', with an option to '+ Add to Filter'. The main area contains several filter categories with their counts: OS (Windows 3, macOS 1, Linux 1, Windows Legacy 1), Version (23.3.264 3), Type (Desktop 2, Laptop 1, Other 1, Server 1, Kubernetes Node 1, Storage 1), Domain (WORKGROUP 3), Memory (1 - 256), CPU count (1 - 64), and Core (1). There are 'Apply' buttons for each category and a 'View More Filters' link.

Wanneer je een filter hebt gekozen, klik je terug op: Group -> New group -> geef de groep een naam en klik op next -> Dynamic group en klik next. Je krijgt het volgende scherm te zien:



Hier kan je kiezen voor:

- **Save and use the current query**
 - Dit is de filter die we hiervoor hebben geselecteerd
- **Choose an existing filter set**
 - Door deze optie te selecteren kan je een al bestaande query kiezen

Wanneer je kiest voor de eerste optie kan je door op current query te klikken nog nakijken wat de query juist inhoudt. Dat ziet er ongeveer zo uit:

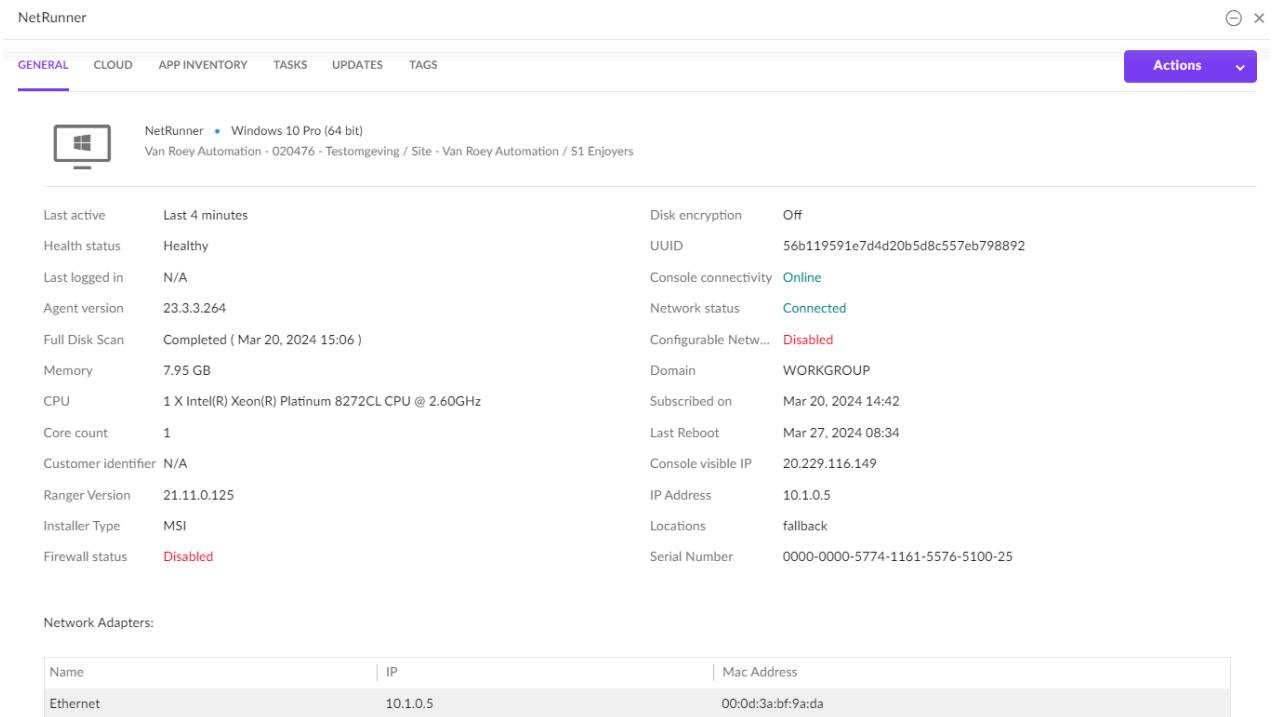
The screenshot shows a 'Current query preview' modal. It displays a single item under the 'Type' section: 'Laptop'. At the bottom is a 'Close' button.

Als de filter klopt, kan je een naam kiezen en hierna op next klikken. De verdere configuratie is dezelfde als die van Manual en Pinned groups.

Als je wilt werken met een bestaande filter kan je op load filter set klikken, dan op de filter die je wilt en vervolgens op next. De rest van de config is dezelfde als die van Manual en Pinned groups.

Endpoint details window

Als we op een van de namen van de endpoints klikken, komt er in de rechteronderhoek van het scherm een tab:



The screenshot shows the 'NetRunner' endpoint details window. At the top, there's a header with tabs: GENERAL (which is selected), CLOUD, APP INVENTORY, TASKS, UPDATES, and TAGS. To the right of the tabs is an 'Actions' dropdown menu. Below the header, there's a summary section with a Windows icon and the text: 'NetRunner • Windows 10 Pro (64 bit)', 'Van Roey Automation - 020476 - Testomgeving / Site - Van Roey Automation / S1 Enjoyers'. The main content area is divided into two columns. The left column contains: Last active (Last 4 minutes), Health status (Healthy), Last logged in (N/A), Agent version (23.3.3.264), Full Disk Scan (Completed (Mar 20, 2024 15:06)), Memory (7.95 GB), CPU (1 X Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz), Core count (1), Customer identifier (N/A), Ranger Version (21.11.0.125), Installer Type (MSI), and Firewall status (Disabled). The right column contains: Disk encryption (Off), UUID (56b119591e7d4d20b5d8c557eb798892), Console connectivity (Online), Network status (Connected), Configurable Netw... (Disabled), Domain (WORKGROUP), Subscribed on (Mar 20, 2024 14:42), Last Reboot (Mar 27, 2024 08:34), Console visible IP (20.229.116.149), IP Address (10.1.0.5), Locations (fallback), and Serial Number (0000-0000-5774-1161-5576-5100-25). Below this, there's a section titled 'Network Adapters:' with a table:

Name	IP	Mac Address
Ethernet	10.1.0.5	00:0d:3a:bf:9a:da

In deze tab vinden we allerlei informatie over de endpoint in kwestie.

General

In de general tab binnen het endpoint details window krijgen we een algemeen overzicht van de volgende zaken:

- Endpoint health
- Network
- Hardware status
- Last active
- Ip address
-

Cloud

In deze tab wordt voor endpoints die in AWS, Azure, Google cloud of kubernetes zitten, metadata getoond van deze endpoint.

NetRunner

GENERAL	CLOUD	APP INVENTORY	TASKS	UPDATES	TAGS
<hr/>					
 Microsoft Azure					
Account ID	5e592aa9-cfd4-4c01-8fb0-074e8e32a210				
Location	westeurope				
Resource Group	test-rg				
Instance ID	080360ce-1b9f-4e49-a3b8-512838b40536				
Image	win10-22h2-pro-g2				
Tags					
Instance Size	Standard_D2s_v3				

Zo kunnen we informatie zien zoals de region in Azure, de Resource group en de OS image.

App inventory

In deze tab zien we alle apps die op de endpoint geïnstalleerd zijn sinds de laatste scan.

GENERAL	CLOUD	APP INVENTORY	TASKS	UPDATES	TAGS	Actions
<hr/>						
Name		Installed Date		Size	Version	Publisher
.NET Framework		N/A		0.00 B	4.8	Microsoft
DirectX 12		N/A		0.00 B	12	Microsoft
Internet Explorer 11		N/A		0.00 B	11	Microsoft
MDAC		N/A		0.00 B	6.3	Microsoft
MSXML		N/A		0.00 B	3.0	Microsoft
MSXML		N/A		0.00 B	6.0	Microsoft
Microsoft 365 Apps for enterprise - en-us		03/20/24		0.00 B	16.0.17328.20184	Microsoft Corporation
Microsoft Edge		03/20/24		0.00 B	122.0.2365.92	Microsoft Corporation
Microsoft Edge WebView2 Runtime		03/20/24		0.00 B	122.0.2365.92	Microsoft Corporation
Microsoft Intune Management Extension		03/20/24		18.19 MB	1.76.152.0	Microsoft Corporation
Microsoft Office Click to Run - Monthly		N/A		0.00 B	16	Microsoft
Microsoft Office Click to Run 2016		N/A		0.00 B	16	Microsoft
Microsoft OneDrive		03/20/24		307.26 MB	24.040.0225.0003	Microsoft Corporation
Microsoft Visual Studio Tools for Office		N/A		0.00 B	10	Microsoft
Sentinel Agent		03/20/24		247.82 MB	23.3.264	Sentinel Labs, Inc.
Windows Media Player		N/A		0.00 B	12.0	Microsoft

Hier kunnen we volgende informatie zien van maximum 150 geïnstalleerde apps:

- Name
- Installed date

- Size
- Version
- Publisher

Tasks

In deze tab kunnen we al tasks zien die zijn geactiveerd vanuit de actions dropdown button, zoals agent-updates of script executions.

Task Name	Description	Status	Initiated by	Initiated time
Remote Script	Get Services	Completed	Reno Goeyvaerts	Mar 27, 2024

Updates

In deze tab kunnen we alle updates zien die vanuit SentinelOne zijn gepushed om de meest recente protection capabilities en updates te garanderen voor de endpoints.

Name	Category	ID	Applied at
Agent Anti Tamper	Security Update	DriverBlockWin241-2.1	2024-03-20T13:44:24.674000Z

Tags

In deze tab kunnen we de verschillende tags zien van de endpoints als deze er zijn.

No Tags Are Applied on This Endpoint

Manage Endpoints Tags

Actions

Binnen actions hebben we een grote keuze aan “actions” die we kunnen kiezen om uit te voeren op de endpoint waarvan je het Endpoint details window hebt openstaan. Er zijn verschillende categorieën van actions die hieronder zullen besproken worden.

Agent actions

Hieronder zie je de mogelijke acties op agent niveau, je kan de endpoint naar een andere site moven, de tags beheren, agent naar een andere control panel migreren, ... enzovoort.

Manage Tags

Edit Customer Identifier

Move to Another Site

Decommission

Show Passphrase

Revoke Token

Randomize UUID

Migrate Agent

Confirm Local Upgrade

Endpoint actions

Hieronder zie je de mogelijke actions op endpoint niveau, je kan de endpoint rebooten, je kan een bericht sturen naar de endpoint in kwestie, agent uninstall accepteren, ... enzovoort.

Reboot



Shut Down

Uninstall

Approve Uninstall

Reject Uninstall

Send Message



Response

Hieronder zie je de response actions die gebruikt kunnen worden wanneer een device compromised is, je kan de endpoint van het netwerk halen, een script runnen, ... enzovoort.

Disconnect from Network

Reconnect to Network

File Fetch

Remote Shell



Clear Remote Shell Session

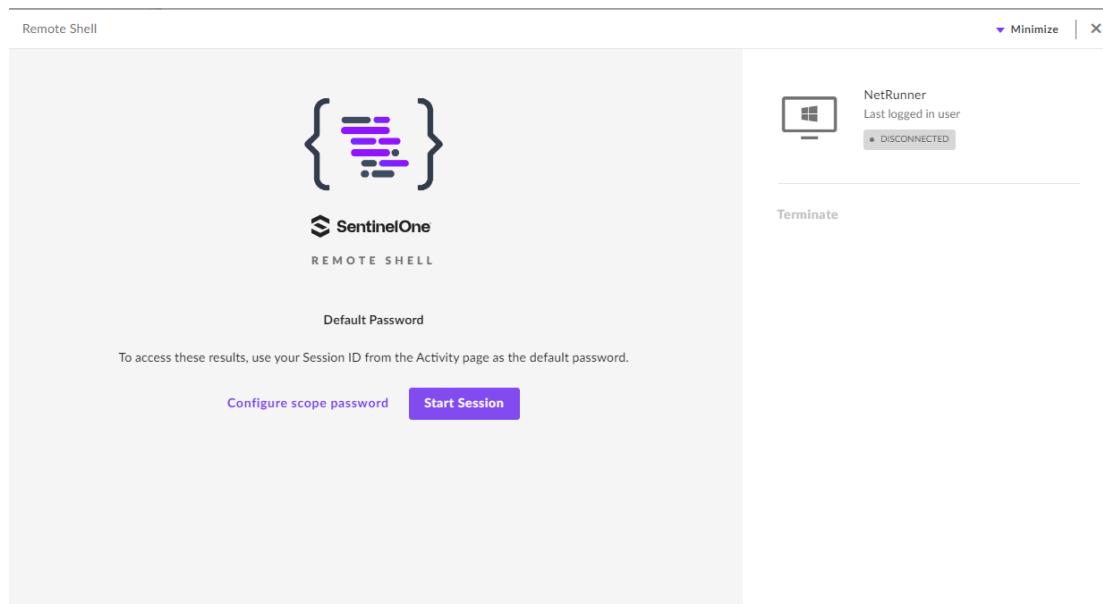
Run Script



Forensics Collection

Remote shell

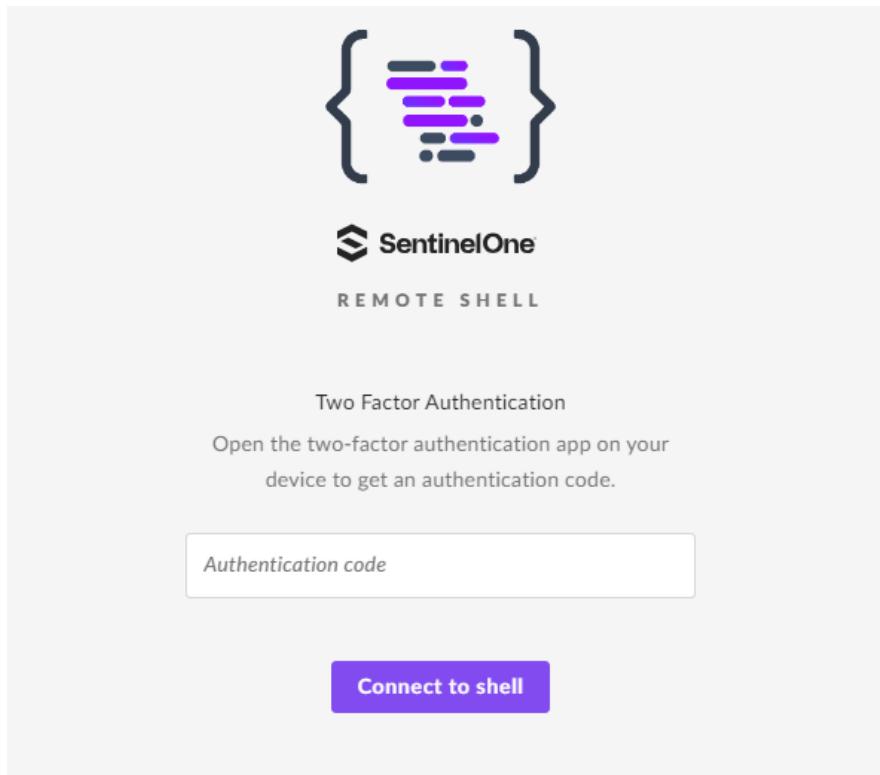
Met de remote shell action kunnen we een remote shell opstarten via het SentinelOne control panel enkel en alleen als je MFA hebt ingesteld, wanneer we hierop hebben geklikt krijgen we dit scherm:



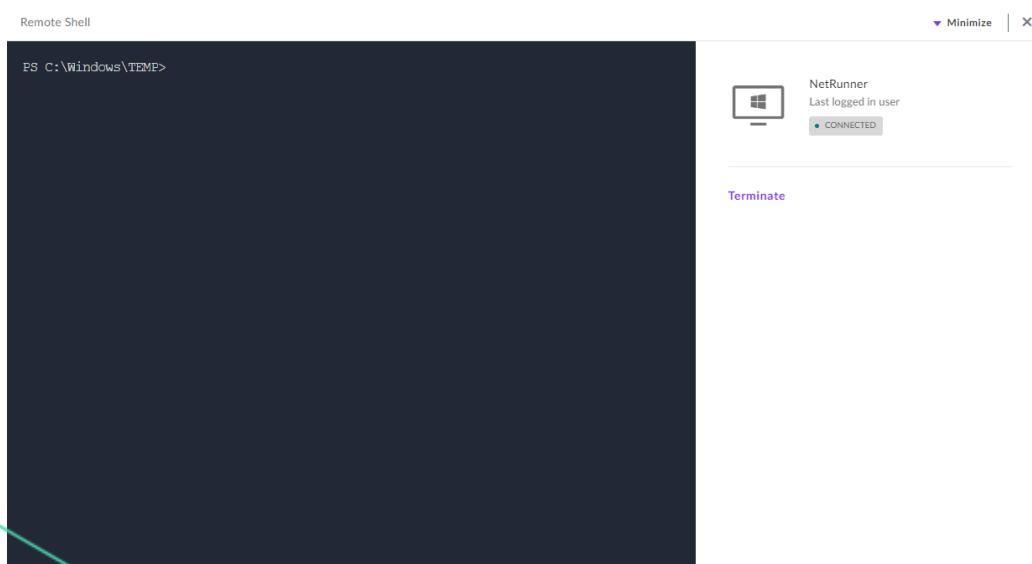
We kunnen hier kiezen tussen:

- **Configure scope password**
 - hier kunnen we het default password aanpassen dat je nodig hebt om de remote shell te starten.
- **start session**

Wanneer we klikken op start session worden we geprompt voor een MFA-code:



Als je deze hebt ingevuld kan je op connect to shell klikken en wordt de remote shell connection met de endpoint in kwestie gestart.



Remote shell heeft geen native command limitations buiten de commands die de agent services zouden stoppen.

Hier zijn de commands per os die je niet kan uitvoeren per OS:

- **Windows**
 - load
 - reload
 - unload
 - bind
- **macOS**
 - stop
- **Linux**
 - control disable
 - control enable
 - control stop
 - control uninstall
 - control upgrade
 - model prune
 - providers perf ebpf toggle
 - resource memory
 - all commands with set
 - all commands with clear

Run script

Wanneer we klikken op run script bij response actions krijgen we volgend scherm te zien:

Script Configuration ×

SCRIPT SELECTION INPUT / OUTPUT TASK CONFIGURATION SUMMARY

SCRIPT SELECTION

OS Type: All 20 scripts 10 Results

Task Name	Script Type	Version	OS Type	Author	Script ID	Initiated Time
Find File by Drive	Data Collection	1.0.0	Windows	SentinelOne	1644061329919...	Mar 19, 2023 09:5...
Get Services	Data Collection	1.0.0	Windows	SentinelOne	1349755395467...	Feb 6, 2022 08:23:...
Get Security Even...	Data Collection	1.0.0	Windows	SentinelOne	1164312724478...	May 26, 2021 12:4:...
Get USB Media	Data Collection	1.0.0	Windows	SentinelOne	1164312722590...	May 26, 2021 12:4:...
Get Scheduled Tas...	Data Collection	1.0.0	Windows	SentinelOne	1164312722121...	May 26, 2021 12:4:...

◀ 1 2 ▶

In dit scherm kunnen we een script kiezen dat wordt uitgevoerd op de endpoint in kwestie. Meer uitleg over de verschillende beschikbare scripts vindt u onder “automation”. Als je een script hebt gekozen en op next hebt gedrukt krijg je volgend scherm te zien:

The screenshot shows a step-by-step wizard with four tabs: Script Selection, Input / Output (highlighted in blue), Task Configuration, and Summary. The Input / Output tab contains two sections: Input and Output. The Input section has a note: "No Input. This script runs automatically without user interaction." The Output section has a dropdown menu labeled "Select".

Ik kies in dit geval voor SentinelOne Cloud en klik daarna op next, dan krijg je volgend scherm te zien:

The screenshot shows the Task Configuration screen. It includes sections for Task Parameters (Task Description: "Get Services", Script Execution Timeout: "3600 Seconds"), Execution Scheduling (Task Scheduling: "Select Date"), and a "Execution Scheduling" button.

In dit scherm kunnen we de Script Execution TimeOut definiëren dat bepaalt hoe lang het script mag proberen te runnen voor het script failed. We kunnen ook instellen wanneer het script wordt uitgevoerd. Na je de gewenste instellingen hebt

gekozen klik je op next en krijg je volgend scherm te zien:

The screenshot shows the 'SCRIPT CONFIGURATION' interface in four steps: SCRIPT SELECTION, INPUT / OUTPUT, TASK CONFIGURATION, and SUMMARY. The SUMMARY step is active, displaying the following details:

ENDPOINTS	
Total Endpoint	OS Type
1	Windows

SCRIPT				
Script Name	Script Type	Version	Author	Initiated Time
Get Services	Data Collection	1.0.0	SentinelOne	

INPUT	OUTPUT

At the bottom are buttons for 'Cancel', 'Submit & Add Another', and a large blue 'Submit' button.

In dit scherm kan je de gekozen instelling nog een keer nakijken voor je de script deployment submit, als alles in orde is klik je op submit en word je script uitgevoerd.

Tags

Tags kunnen worden gebruikt om endpoints te organiseren en te categoriseren. U kunt tags gebruiken om:

- Endpoints groeperen op basis van functies, afdeling of locatie.
- Endpoints te identificeren die mogelijk kwetsbaar zijn voor een bepaalde bedreiging.
- Endpoints te volgen die zijn geüpdatet met een nieuwe patch.

Network rogues

Network Rogues helpt u **onbeschermd apparaten** (zoals laptops zonder de SentinelOne-agent) op uw netwerk te vinden en te beheren.

Network Rogues scant uw netwerk om:

- Deze "rogue"-apparaten te **identificeren**
- Informatie te verstrekken voor **beheer** (besturingssysteem, IP-adres, MAC-adres)
- U te helpen **devices die geen SentinelOne installed hebben** in uw SentinelOne-agent-implementatie te zien

Dit verbetert uw beveiliging door:

- Het **attack surface** te verkleinen met minder onbeschermde apparaten
- U te helpen voldoen aan **security regulations**
- U **betere zichtbaarheid** te geven in uw netwerkapparaten

Om op deze apparaten de SentinelOne agents te installeren hebben we Ranger AD nodig.. De vereisten die nodig zijn om dit te kunnen doen zijn:

- ***General Requirements:***
 - Management Console Permissions: Admin (Manage Credentials, Deploy) or IT/IR (Deploy) role.
 - Web Browser: Chrome, Firefox, Safari, or Edge (Explorer not supported).
 - Network Access: Allow access to SentinelOne Management Console URLs on port TCP-443 (details vary based on location).
- ***Windows Requirements***
 - Recommended: Active Directory (AD) environment.
 - Communication Protocol: WinRM (Ports 5985 & 5986 open).
 - Fallback Authentication: NTLM (PSRemoting enabled on Deployer if used).
 - Optional Authentication: WMI (Ports 135 open, DCOM configured).
 - Package Copying: Admin\$ share available, SMB enabled on targets.
 - Agent Version: 4.6 SP2 or higher (version 21.6+ recommended).
 - Deployment Selection: Don't mix 32-bit and 64-bit devices in a single flow (separate packages).
- ***Linux Requirements***
 - Communication Protocol: SSH (Port 22 open).
 - Agent Classification: Automatically classified as Servers (change with sentinelctl management type).
 - Deployment Selection: Don't mix DEB and RPM package targets in a single flow.
- macOS Requirements:
 - Communication Protocol: SSH (Port 22 open).
 - Full Disk Access: Required for SentinelOne components (configure in MDM software).

Policy

De policy tab definieert hoe de agent de endpoints beschermt, monitort, en welke acties hij onderneemt als er een malicious of suspicious file is gedetecteerd.

Protection mode

Binnen deze settings definiëren we hoe SentinelOne moet reageren binnen een groep of site dit gebeurt door de volgende instellingen.

Protection Mode

Malicious Threat **Suspicious Threat**

Protect Level

Malicious Macros Mitigation (i)

This only applies when the Static AI detection engine is On, and the Protection Mode of Malicious Threats is set to Protect.

Remove malicious macros from the Office file instead of placing the file in quarantine.

Containment Disconnect from network (i)

In dit deel van Policy definiëren we hoe de agent moet reageren op malicious en Suspicious threats, hier zijn 2 mogelijkheden namelijk Detect of protect. De protect optie heeft 3 protect levels:

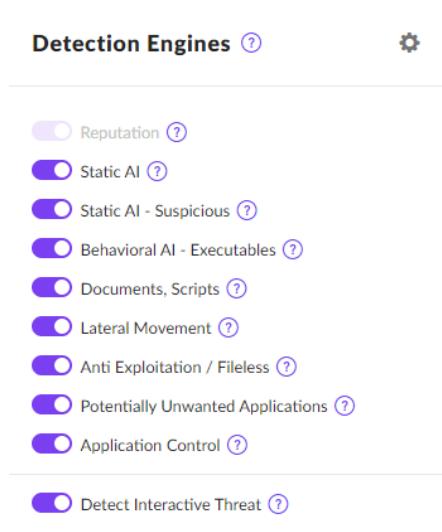
- **Kill & Quarantine**
 - Deze setting gaat alle processen die te maken hebben met de file stopzetten en deze file quarantainen.
- **Remediate**
 - Deze setting gaat aangepaste files door de “aanval” of malicious file herstellen.
- **Rollback**
 - deze setting wordt gebruikt wanneer er bijvoorbeeld een ransomware attack heeft plaatsgevonden om terug te gaan naar een bepaalde snapshot van voor de attack.

Er zijn nog 2 andere settings die je kan implementeren namelijk: Malicious macro's mitigation en containment.

Malicious macro's mitigation gaat de macro's uit het officedocument halen in plaats van het document te quarantainen zodat het document nog “gebruikt” kan worden. Containment zorgt ervoor dat wanneer er een malicious file gedetecteerd wordt op de endpoint dat alle netwerk connecties worden verbroken behalve deze met het SentinelOne management panel.

Detection engines

SentinelOne maakt gebruik van geavanceerde detectie engines om endpoints te beschermen tegen een breed scala aan bedreigingen. Deze geavanceerde technologieën analyseren het gedrag van processen, bestanden en netwerkactiviteit om verdachte activiteiten te identificeren en te signaleren.



De detectie van deze bedreigingen gebeurt door machine learning en AI, deze detecteren:

- Malicious en suspicious files die op de schijf worden geschreven
- Malicious activities die zich plaatsvinden op de machine
- onregelmatigheden in documenten en files
- Lateral movement
- web en command line exploits
- Malicious sub-processen die getriggerd worden bij het starten van een app
- Intrusion

Agent

In het agent panel binnen policy vinden we security settings en Agent UI terug.

Security settings heeft volgende mogelijkheden:

- **snapshots**
 - Saves windows agents VSS snapshots
- **Scan new agents**
 - Start een full disk scan bij elk nieuwe endpoint
- **Logging**
- **Anti Tamper**
 - Deze setting zorgt ervoor dat end-users of malware de agent niet kunnen uitschakelen of verwijderen.
- **Suspicious driver blocking**
 - Zowel voor windows signed als unsigned drivers.

We kunnen ook instellen wat de end-user ziet van de agent ui door deze settings:

- **het zien van ui en tray icon**
- **notificaties van suspicious events**

- *warnings voor agents errors*
- *de maximale leeftijd van events die getoond worden in de ui*
- *het tonen van blocked devices*
- *het tonen van quarantined files*

Deep Visibility

Deep Visibility

Deep Visibility Configuration

Collect this Deep Visibility data

<input checked="" type="checkbox"/> Process	?	<input checked="" type="checkbox"/> File	?	<input checked="" type="checkbox"/> URL	?	
<input checked="" type="checkbox"/> DNS	?	<input checked="" type="checkbox"/> IP	?	<input checked="" type="checkbox"/> Login	?	
<input checked="" type="checkbox"/> Registry Keys	8/8	?	<input checked="" type="checkbox"/> Scheduled Tasks	5/5	?	
<input checked="" type="checkbox"/> Command Scripts	?	<input checked="" type="checkbox"/> Cross Process	4/4	?	<input checked="" type="checkbox"/> Behavioral Indicators	?
			<input checked="" type="checkbox"/> Driver Load			

Data Masking [?](#) Focused File Monitoring [?](#)

Automatically install Deep Visibility browser extensions

! Do not select if your organization uses Google Workspace (formerly G Suite) to manage browser extensions
This overrides other browser extensions deployed with Google Workspace. If your organization uses Google Workspace to deploy browser extensions, deselect this option and deploy the SentinelOne browser extension in the same way you deploy other extensions.
This option requires Windows Agent 4.7+.

In het Deep Visibility panel binnen policy kan er geconfigureerd worden wat voor soort data er naar het data lake wordt gestuurd. We kunnen kiezen uit:

- **Processes**
 - Gecreëerde en aangepaste processen worden gelogd
- **DNS**
 - Dns connections worden gelogd
- **Registry Keys**
 - Events dat registry keys: toevoegen, aanpassen of verwijderen worden gelogd
- **Command Scripts**
 - Verzamelt powershell en andere CMD-scripts
- **File**
 - Gecreëerde, verwijderde en aangepaste files worden gelogd
- **IP**
 - Inkomende en uitgaande connecties worden gelogd
- **Scheduled Tasks**
 - Data van scheduled tasks wordt gelogd
- **Cross Process**
 - Events tussen processen worden gelogd
- **URL**

- Verzameld de bezochte websites
- **Login**
 - Login gerelateerde events worden gelogd
- **Behavioral Indicators**
 - Data van suspicious behavior en techniques wordt verzameld en georganiseerd
- **Driver Load**
 - Load op drivers wordt gelogd

We hebben hiernaast nog 2 andere opties namelijk

- **Data Masking**
 - Als je deze setting aanzet, zullen de paden van zip, pdf en office documenten gemaskeerd worden.
- **Focused File Monitoring**
 - Er wordt focus gelegd op het verzamelen van binaries en files die vermoedelijk active content bevatten.

Binary vault

De SentinelOne Binary Vault is een feature van SentinelOne die automatisch verdachte bestanden uploadt naar een beveiligde cloudopslag voor verdere analyse. Dit helpt met:

- **Onbekende bedreigingen detecteren**
 - Door middel van machine learning-algoritmen
 - Malware analyse en het begrijpen van hun kenmerken
- **Versneld onderzoek**
 - Gecentraliseerde opslag
 - File sharing

Binary Vault

Enable Automatic File Upload	<input type="checkbox"/> Enable Automatic File Upload ?
<hr/>	
Exclude Path	<input type="button" value="New Path"/>
<hr/>	
Exclude File Type	<input type="button" value="New File Type"/>
<hr/>	
Maximum file size Upload (Max 250MB)	<input type="text" value="250"/> MB
<hr/>	
Total Upload per Agent per day (Max 500MB)	<input type="text" value="500"/> MB
<hr/>	
Offline cache size (Max 2048MB)	<input type="text" value="2048"/> MB

Als laatste zijn er nog 2 settings:

More Options

Decommissioning Auto decommission after (30) days offline [?](#)

Remote Shell Enable Remote Shell

Decommissioning: dit zorgt ervoor dat als er een bepaalde geconfigureerde tijd geen interactie is geweest tussen de user en SentinelOne management console, de agent uit het SentinelOne management panel wordt gezet.

Remote shell: Deze setting bepaalt of je via de management console een remote shell kan starten.

STAR Custom Rules

STAR CUSTOM Rules is een krachtige tool die u kan helpen uw omgeving te beschermen tegen bedreigingen aan de hand van gecustomiseerde regels. Deze regels kunnen gebruikt worden voor:

- *Extra rules toe te voegen aan het bestaande security profiel*
- *Hunting*

Deze rules kunnen gemaakt worden met specifieke filters die kunnen gebaseerd zijn op volgende criteria:

- *Bestandsnamen en locaties*
- *Procesnamen en features*
- *Netwerkactiviteit*
- *Windows registry settings*

Wanneer er een bedreiging wordt gedetecteerd kunnen er automatisch acties ondernomen worden namelijk:

- *Blokkeren*
- *Quarantainen*

Blocklist

De SentinelOne Blocklist is een krachtige functie die endpoints beschermt tegen bekende bedreigingen. Het is een lijst met SHA-1 hashes van malware, ransomware en andere kwaadaardige bestanden die SentinelOne automatisch blokkeert.

Hoe werkt de Blocklist?

- *SentinelOne berekent de SHA-1 hash van elk bestand op een endpoint.*
- *De hash wordt vergeleken met de Blocklist.*
- *Als de hash overeenkomt met een hash op de Blocklist, wordt het bestand geblokkeerd.*
- *We kunnen handmatig hashes toevoegen of verwijderen van de Blocklist.*
- *We kunnen SentinelOne automatisch hashes laten toevoegen aan de Blocklist op basis van threat intelligence.*

Exclusions

Exclusions werkt hetzelfde als de blocklist maar in plaats van blokken gaan we bestanden en processen uitsluiten van scans en detectie.

Dit kan handig zijn in de volgende situaties:

- ***False positives***
 - Als een legitiem bestand of proces ten onrechte wordt gedetecteerd als een bedreiging, kunt u het toevoegen aan de Exclusions-lijst om te voorkomen dat het in de toekomst wordt geblokkeerd.
- ***Prestatieverbetering***
 - Als u merkt dat SentinelOne scans uw endpoints vertraagt, kunt u bepaalde bestanden of processen die geen bedreiging vormen uitsluiten van de scans.

Hoe exclusion configureren:

- *Je kan Exclusions configureren via de SentinelOne-console.*
- *Je kan Exclusions toevoegen op basis van:*
 - Bestandspad
 - Je kan een specifiek bestand of een map uitsluiten.
 - SHA-1 hash
 - Je kan een specifiek bestand uitsluiten op basis van de SHA-1 hash.
 - Procesnaam
 - Je kan een specifiek proces uitsluiten op basis van de naam.

Network control

Is een functie die het netwerkverkeer van uw endpoints zal beschermen tegen bedreigingen. Dit gebeurt door een breed scala aan functies die:

1. ***Netwerkverkeer te controleren***
 - We kunnen regels configureren om inkomende en uitgaande netwerkverbindingen te beheren.
 - We kunnen specifieke poorten en protocollen blokkeren.
 - We kunnen afwijkende netwerkactiviteit detecteren en monitoren.
 - We kunnen endpoints die zijn geïnfecteerd met malware of ransomware isoleren van het netwerk.
 - We kunnen automatisch verdachte netwerkactiviteit blokkeren.
 - We kunnen bedreigingen opsporen en hun oorsprong achterhalen
2. ***Bedreigingen te isoleren en te neutraliseren***
 - We kunnen endpoints die zijn geïnfecteerd met malware of ransomware isoleren van het netwerk.
 - We kunnen automatisch verdachte netwerkaktiviteit blokkeren.
 - We kunnen bedreigingen opsporen en hun oorsprong achterhalen.

The screenshot shows a software interface for managing firewall rules. At the top, there are tabs for 'Firewall' and 'Network Quarantine', with 'Firewall' selected. Below the tabs is a search bar with placeholder text 'Select filters...'. Underneath the search bar are buttons for 'New rule', 'Actions', and 'Reorder rules', along with a message 'No Items Selected'. A red circular icon with a white exclamation mark indicates that 'Firewall Control is off'. To the right, there are buttons for '50 Results', 'Columns', 'Export', and 'Import'. Below these controls is a table header with columns: Name, Tags, Status, Scope, Description, OS, Application, Direction, Protocol, Local Host, Local Port, and Remote. In the center of the screen is a large search icon with a magnifying glass and an 'X'. Below the icon, the text 'No results found' is displayed.

Device control

Device Control is een essentiële tool voor organisaties die hun endpoints willen beschermen tegen bedreigingen. Het biedt een uitgebreide set functies om uw endpoints te beveiligen.

Met device control kan je de volgende dingen instellen:

1. Toegang tot apparaten te beheren:

- We kunnen bepalen welke apparaten toegang hebben tot uw endpoints.
- We kunnen specifieke typen apparaten, zoals USB-sticks of externe harde schijven, blokkeren.
- We kunnen gedetailleerde rapporten genereren over apparaat gebruik.
- Het blokkeren of toestaan van apparaten kan gebeuren op USB, bluetooth en thunderbolt

2. Gevoelige data te beschermen:

- We kunnen voorkomen dat gevoelige data wordt gekopieerd naar onbevoegde apparaten.
- We kunnen versleuteling afdwingen voor externe apparaten.
- We kunnen dataverlies via onbevoegde kanalen voorkomen.

The screenshot shows a software interface for device control. At the top, there is a navigation bar with tabs: SENTINELS, ENDPOINTS, TAGS, POLICY, STAR CUSTOM RULES, BLOCKLIST, EXCLUSIONS, NETWORK CONTROL, and DEVICE CONTROL. The 'DEVICE CONTROL' tab is selected. Below the navigation bar is a search bar with 'USB' selected and a placeholder 'Select filters...'. Underneath the search bar are buttons for 'New rule', 'Actions', and 'Reorder rules', along with a message 'No Items Selected'. A table below shows a single row of data for a USB device. The columns are: Interface, Rule Name, Class, Vendor ID, Product ID, and Scope. The data row shows: USB, Test, Any, 0781, Any, and Group. There is also a checkbox column with an unchecked box next to the USB entry.

Om een device control rule toe te voegen klikken we binnen het device control panel op New Rule en krijgen we volgend scherm:

New Rule

Rule name **Field required**

Interface

Rule Type

Scope Van Roey Automation - 020476 - Testomgeving -> Site - Van Roey Automation -> \$1 Enjoyers

Action Allow Block

Continue **Cancel**

Hier kunnen we een aantal dingen bepalen:

- **Rule Name**
- **Interface**
 - Bluetooth
 - Thunderbolt
 - USB
- **Rule Type**
 - Bluetooth
 - Hardware identifiers
 - Bluetooth version
 - Thunderbolt
 - Vendor ID
 - USB
 - Vendor ID
 - Class
 - Serial ID
 - Product ID
 - Action
 - Allow Read & Write
 - Allow Read Only
 - Block

Upgrade policy

De upgrade policy is een flexibel beleid dat ervoor zorgt dat de endpoints hun SentinelOne agent up-to-date is. We kunnen volgende dingen instellen binnen deze tab:

- **Auto upgrade**
 - Agent Version
 - Update timing
 - Dit wordt nog eens onderverdeeld in 2 opties
 - Effective Immediately

- According to maintenance window
- Affected Endpoints
 - Dit wordt nog eens onderverdeeld in 2 opties
 - All endpoints in scope
 - Filter by Endpoint tags
- Maintenance Window
 - Maximum concurrent Downloads
 - Maintenance Windows settings
 - Local Upgrade Authorization
- Live Updates
- Local Upgrade
 - Let's user upgrade the agents themselves

Incidents



We klikken nu op Incidents en krijgen het volgende scherm te zien:

INCIDENTS											THREATS		ALERTS							
Last 3 Months			Select filters...																	
Threat Actions											Analyst Verdict		Incident Status		Group by Hash					
Status	Threat Details	AI Confidence Level	Analyst Verdict	Incident Status	Endpoints	Reported Time	Detecting Engine	Initiated By	Classification	Agent Version On De	Group by Hash	No Items Selected	92 Threats	100 Results	Columns	Export				
<input type="checkbox"/>	8c3aa4bd129381932b8c11740c3414af892...	Suspicious	True positive	Unresolved	Sandevistan	Mar 22nd 2024 • 09:49:11	On-Write Static AI - ...	Agent Policy	Malware	23.3.3.264	<input type="checkbox"/>									
<input type="checkbox"/>	test.sct	Malicious	True positive	Unresolved	Sandevistan	Mar 22nd 2024 • 08:21:15	SentinelOne Cloud	Agent Policy	Malware	23.3.3.264	<input type="checkbox"/>									
<input type="checkbox"/>	SOAPhound.exe	Malicious	True positive	Unresolved	Sandevistan	Mar 22nd 2024 • 08:21:15	SentinelOne Cloud	Agent Policy	Malware	23.3.3.264	<input type="checkbox"/>									
<input type="checkbox"/>	SRAKEWF6.exe	Malicious	True positive	Unresolved	NetRunner	Mar 22nd 2024 • 08:21:13	SentinelOne Cloud	Agent Policy	Malware	23.3.3.264	<input type="checkbox"/>									

Threats

In de threats tab van incidents kan je alle incidents zien die gebeurd zijn op de verschillende endpoints binnen je site, in de tabel zien we enkele begrippen:

- **Threat Mitigation Status:**
 - er zijn 2 statussen mogelijk
 - Mitigated
 - De bedreiging is gedetecteerd en de bedreiging is geneutraliseerd
 - Not mitigated
 - De bedreiging is gedetecteerd maar er zijn nog geen verdere stappen ondernomen
- **Threat Details:**
 - Dit is de naam van de malicious of suspicious file die het incident heeft getriggerd
- **Ai Confidence Level:**

- Dit is de karakteristiek van de file die gedetecteerd is door de ai, hier zijn 3 mogelijkheden:
 - Malicious
 - Suspicious
 - N/A
- ***Analyst verdict:***
 - dit is de beoordeling van de bedreiging
 - True positive
 - Undefined
 - False positive
- ***Incident Status:***
 - dit indiceert of er al acties ondernomen zijn voor deze alert, deze worden door het securityteam zelf aangepast, er zijn 3 mogelijke statussen:
 - Resolved
 - Unresolved
 - In progress
- ***Endpoints:***
 - Dit geeft aan op welke endpoint het incident heeft plaatsgevonden
- ***Reported Time:***
 - De datum en tijd dat het incident heeft plaatsgevonden
- ***Detection Engine:***
 - Dit geeft aan welke engine de malicious of suspicious file heeft gedetecteerd, hier zijn een aantal van de mogelijke engines:
 - SentinelOne Cloud
 - On-write Static AI
 - On-write Static AI - Suspicious
 - User-Defined Blocklist
 - Behavioral AI
 - Documents, scripts
 - potentially unwanted application
 -
- ***Initiated by:***
 - dit geeft aan wat de remediation heeft getriggerd, hier zijn een aantal mogelijkheden:
 - Agent Policy
 - Full Disk scan
 - Deep visibility command
 - Threat intelligence
 - Cloud detection
 - On-demand scan
 - Custom rule
 - ...
- ***Classification:***
 - Dit is wat voor malicious file het was die de threat notification heeft getriggerd

- Malware
- PUA
- *Agent version on detection*
- *Agent version*
- *File hash*
- *Completed action*
- ...

Threat overview window

Wanneer we klikken op een willekeurig event komen we op het volgende scherm terecht:

The screenshot shows a detailed threat analysis interface. At the top, there's a summary bar with threat status (MITIGATED), AI confidence level (MALICIOUS), analyst verdict (True Positive), incident status (Unresolved), mitigation actions taken (KILLED 200/200, QUARANTINED 0/6, REMEDIATED 419/419, ROLLED BACK 58/58), and reporting information (Identified Time: Mar 29, 2024 08:40:32, Reporting Time: Mar 29, 2024 08:40:33).

NETWORK HISTORY

Event	Date	Description
First seen	Mar 29, 2024 08:40:33	Only 1 time on the current endpoint
Last seen	Mar 29, 2024 08:40:33	1 Account / 1 Site / 1 Group

THREAT FILE NAME: EDR-Tester.bat

Detail	Value
Path	\Device\HarddiskVolume4\Users\Ronin\Downloads\EDR_Tester-master\E...
Command Line Arguments	/C "C:\Users\Ronin\Downloads\EDR_Tester-master\EDR-Tester.bat"
Process User	NetRunner\Ronin
Publisher Name	N/A
Signer Identity	N/A
Signature Verification	NotSigned
Originating Process	explorer.exe
SHA1	c3cd221e01fd60bb65902a2dffaad7766e41278d

ENDPOINT

Detail	Value
Real-time data about the endpoint:	NetRunner Van Roey Automation - 020476 - Testomgeving / Site - Van Roey Automation / S1 Enjoys
Console Connectivity	Online
Full Disk Scan	Completed at Mar 20, 2024 15:06:18
Pending reboot	No
Number of not mitigated threats	0
Network Status	Connected

CLOUD

Detail	Value
At detection time:	Van Roey Automation - 020476 - Testomgeving / Site - Van ...
Scope	Windows 10 Pro 19045
OS Version	23.3.244
Agent Version	Protect
Policy	N/A
Logged In User	56b119591e7d4d20b5d8c557eb79882
Domain	WORKGROUP
IP v4 Address	10.10.0.5
IP v6 Address	fe80::9050:7f1:1060:473e
Console Visible IP Address	20.229.116.149
Subscription Time	Mar 20, 2024 14:42:17

THREAT INDICATORS (22)

VirusTotal Threat Enrichment

Behaviour Summary

Latest Analysis Stats:

- Unsupported: 16
- Malicious: 19
- Undetected: 41

Associated Attack Techniques: [T1078, T1047, T1064, T1126, T1055, T1497, T1056, T1518, T1010, T1082, T1016, T1059, T1222, T1564]

File report:

- md5: 8f4b2cc3f35faba7a27b67b54a6a8a93
- sha256: b277e7ef32e780f4e2ecf2b3643024fd7c3d0d33140aba08908c3c0
- sha1: c3cd221e01fd60bb65902a2dffaad7766e41278d
- Magic: DOS batch file, Unicode text, UTF-8 text, with CRLF line terminators
- First submission date: 07-07-2022 13:38:31
- Last analysis date: 02-23-2024 07:46:45

More Details: <https://www.virustotal.com/gui/file/c3cd221e01fd60bb65902a2dffaad77>

Alien Labs OTX Enrichment

Hier kunnen we heel wat informatie zien zoals:

- *wanneer het malicious / suspicious bestand gezien is*
- *hoe vaak dit al gedetecteerd is op het device, site en in de groep*
- *File locatie*
- *Process user*
- *SHA1*
- ...

Hiernaast kunnen we deze ook downloaden en deze een wachtwoord geven, als je dit wachtwoord ook hebt ingevuld in de configuratie van de alien labs sandbox integratie zal deze integratie de file in een sandbox loslaten en kan je in de notes een melding zien als dit klaar is.

 Reno Goeyvaerts • Apr 05, 2024 13:19:52

[Alien Labs OTX Sandbox] File Uploaded
<https://otx.alienvault.com/indicator/file/8061e13eae1d3057d292f30147c47>

Hiernaast heb je een panel met 2 tabs van het endpoint details window:

ENDPOINT		CLOUD
Real-time data about the endpoint:		At detection time:
	NetRunner Van Roeij Automation - 020476 - Testomgeving / Site - Van Roeij Automation / S1 Enjokers	Scope OS Version Agent Version Policy Logged In User UUID Domain IP v4 Address IP v6 Address Console Visible IP Address Subscription Time
Console Connectivity	Online	N/A
Full Disk Scan	Completed at Mar 20, 2024 15:06:18	Windows 10 Pro 19045
Pending reboot	No	23.3.264
Number of not mitigated threats	0	Protect
Network Status	Connected	56b119591e7d4d20b5d8c557eb798892
		WORKGROUP
		10.1.0.5
		fe80::9050:c7f:1060:473e
		20.229.116.149
		Mar 20, 2024 14:42:17

Er is ook een panel aan de rechterkant van je scherm aanwezig waarop je de 3 volgende onderwerpen kan terugvinden:

- ***Threat Indicators***
- ***Notes***
- ***XDR***

Threat Indicators

Bij threat indicators kan je zien waarom de file als een threat werd gezien door SentinelOne, hieronder zie je enkele dingen die SentinelOne detecteert in de file:

- ***abnormaliteiten***
- ***hiding/stealthiness***
- ***Mitre attack techniques and strategies***
- ***Star Custom Rules***

Custom Rules	
file creation	
View Rule	View Alerts
Malware	
Executed suspicious shell command	
MITRE : Execution [T1059.007]	
Evasion	
Process wrote to a hidden file section	
MITRE : Defense Evasion [T1564.004][T1027][T1480.001]	
Process tampered with the Event Viewer logs	
MITRE : Defense Evasion [T1070.001][T1562.001][T1562.002]	
The windows event log has been cleared	
MITRE : Defense Evasion [T1070.001][T1562.001][T1562.002]	
Process executed with non-standard resource type	
MITRE : Command and Control [T1132]	
MITRE : Defense Evasion [T1027][T1480.001]	
Interpreters were chained together in execution	
MITRE : Defense Evasion [T1218][T1202]	
MITRE : Execution [T1059]	
Lolbins were chained together in execution	
MITRE : Defense Evasion [T1218][T1202]	

Notes

Notes kunnen door andere gebruikers van het SentinelOne platform geplaatst worden bij een threat of kan door integraties erbij geplaatst worden om volgende dingen weer te geven:

- *De status*
- *het resultaat*

XDR

Hier kunnen we de verschillende XDR applications zien die geïnstalleerd zijn via de Singularity marketplace en hun acties op de threat als deze er zijn:

HREAT INDICATORS (22) NOTES (4) XDR(3)

All XDR Applications (3) C

VirusTotal Threat Enrichment
Mar 29, 2024 08:40:38

Behaviour Summary

Verdicts: CLEAN
Verdict Confidence: 5%

Latest Analysis Stats:

- Unsuspected: 16
- Malicious: 19
- Undetected: 41

Associated Attack Techniques: [T1078; T1047; T1064; T1136; T1055; T1497; T1056.002; T1518.001; T1010; T1082; T1016; T1059; T1222; T1564.001]

File report:

- md5: 8f4b2cc3f35faba7a27b67b54a6a8a93
- sha256: b277e7ef32e780f4e2ecf2b3643026fd7c3d0d33140aba08908c3c0
- sha1: c3cd221e01fd60bb65902a2dffad7766e41278d
- Magic: DOS batch file, Unicode text, UTF-8 text, with CRLF line terminators
- First submission date: 07-07-2022 13:38:31
- Last analysis date: 02-23-2024 07:46:45

More Details:
<https://www.virustotal.com/gui/file/c3cd221e01fd60bb65902a2dffad776>

Threat Explore view

In dit scherm kunnen we al de activiteiten van de malicious of suspicious file zien voor deze is tegengehouden door SentinelOne:

Threats / EDR-Tester.bat

OVERVIEW EXPLORE TIMELINE Actions

Thread Status: MITIGATED | AI Confidence Level: MALICIOUS | Analyzed Verdict: True Positive | Incident Status: Unresolved

Mitigation Actions taken: KILLED: 200/200 QUARANTINED: 0/0 REMEDIATED: 499/499 ROLLED BACK: 0/0

Identified Time: Mar 29, 2024 08:40:32
Reporting Time: Mar 29, 2024 08:40:33

Processes

NetRunner

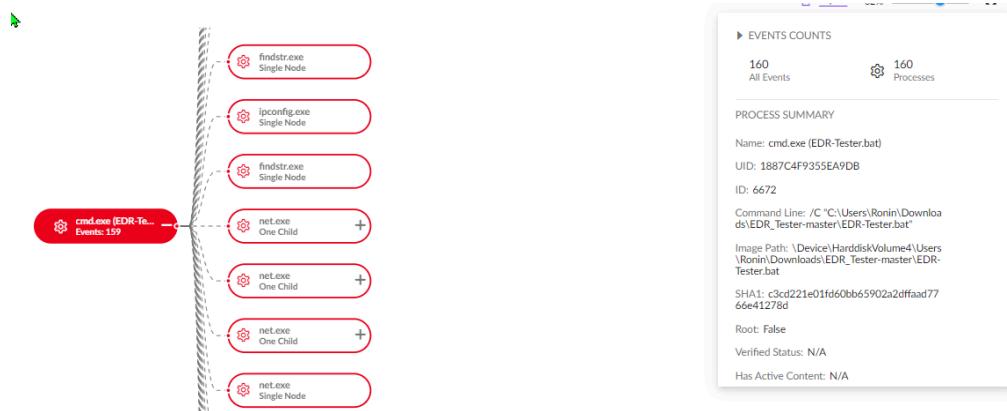
Search Process

Process	Pid	Date
cmd.exe (EDR-Te...)	6672	Mar 29, 2024 08:36:52
conhost.exe	1972	Mar 29, 2024 08:36:53
findstr.exe	10048	Mar 29, 2024 08:36:54
systeminfo.exe	2056	Mar 29, 2024 08:36:54
findstr.exe	8692	Mar 29, 2024 08:36:56
systeminfo.exe	8248	Mar 29, 2024 08:36:56
findstr.exe	7700	Mar 29, 2024 08:36:58

PROCESS TREE TIMELINE

START: Mar 29, 2024 08:36:52 END: Mar 29, 2024 08:40:31

We kunnen op de processen klikken en hier details zien van het geselecteerde proces:



We kunnen ook zien welke processen het hoofdproces heeft getriggerd. Naast de schematische voorstelling van de processen kunnen we ook alle events zien die de threat heeft veroorzaakt en filteren op wat voor type event het is:

Showing all events for the current threat						
	All Events	555	Files	80	Network Actions	3
Object Type	Event Type	Time	Attribute			
process	Process Creation	Mar 29, 2024 08:36:52	Target Process Root False	Target Process Name cmd.exe (EDR-Tester.bat)	Source Process Name N/A	Has Active Content N/A
process	Process Creation	Mar 29, 2024 08:36:53	Target Process Root True	Target Process Name conhost.exe	Source Process Name cmd.exe (EDR-Tester.bat)	Has Active Content true
indicators	Behavioral Indicators	Mar 29, 2024 08:36:54	Indicator Name Remote Memory Free	Indicator Description N/A	Target Process Name svchost.exe	Target Process UID 357C4F9355EA9DB
indicators	Behavioral Indicators	Mar 29, 2024 08:36:54	Indicator Name Remote Memory Allocation	Indicator Description N/A	Target Process Name findstr.exe	Source Process Name systeminfo.exe
process	Process Creation	Mar 29, 2024 08:36:54	Target Process Root True	Target Process Name cmd.exe (EDR-Tester.bat)	Source Process Name cmd.exe (EDR-Tester.bat)	Source Process UID 1887C4F9355EA9DB
indicators	Behavioral Indicators	Mar 29, 2024 08:36:54	Indicator Name Remote Memory Allocation	Indicator Description N/A	Target Process Name systeminfo.exe	Target Process UID 187C4F9355EA9DB
process	Process Creation	Mar 29, 2024 08:36:54	Target Process Root True	Target Process Name cmd.exe (EDR-Tester.bat)	Source Process Name cmd.exe (EDR-Tester.bat)	Source Process UID 1887C4F9355EA9DB
indicators	Behavioral Indicators	Mar 29, 2024 08:36:54	Indicator Name Remote Memory Free	Indicator Description N/A	Target Process Name explorer.exe	Target Process UID E07BC4F9355EA9DB
indicators	Behavioral Indicators	Mar 29, 2024 08:36:55	Indicator Name Remote Memory Free	Indicator Description N/A	Target Process Name svchost.exe	Source Process Name systeminfo.exe
indicators	Behavioral Indicators	Mar 29, 2024 08:36:55	Indicator Name Remote Memory Free	Indicator Description N/A	Target Process Name svchost.exe	Target Process UID 357C4F9355EA9DB
indicators	Behavioral Indicators	Mar 29, 2024 08:36:55	Indicator Name Remote Memory Free	Indicator Description N/A	Target Process Name svchost.exe	Source Process Name systeminfo.exe
indicators	Behavioral Indicators	Mar 29, 2024 08:36:55	Indicator Name Remote Memory Allocation	Indicator Description N/A	Target Process Name findstr.exe	Target Process UID 228C4F9355EA9DB
process	Process Creation	Mar 29, 2024 08:36:56	Target Process Root True	Target Process Name cmd.exe (EDR-Tester.bat)	Source Process Name cmd.exe (EDR-Tester.bat)	Source Process UID 1887C4F9355EA9DB
indicators	Behavioral Indicators	Mar 29, 2024 08:36:56	Indicator Name Remote Memory Allocation	Indicator Description N/A	Target Process Name systeminfo.exe	Target Process UID 2187C4F9355EA9DB
process	Process Creation	Mar 29, 2024 08:36:56	Target Process Root True	Target Process Name cmd.exe (EDR-Tester.bat)	Source Process Name cmd.exe (EDR-Tester.bat)	Source Process UID 1887C4F9355EA9DB

Threat timeline view

In dit scherm kunnen we een timeline zien van de genomen acties van SentinelOne om de malicious file te stoppen maar ook die van de threat zelf:

The screenshot shows a threat timeline view with the following details:

- Threat Status:** MITIGATED | **AI Confidence Level:** MALICIOUS | **Analyst Verdict:** True Positive | **Incident Status:** Unresolved
- Mitigation Actions taken:** KILLED (200/200), QUARANTINED (6/6), REMEDIATED (419/419), ROLLED BACK (58/58)
- Identified Time:** Mar 29, 2024 08:40:32 | **Reporting Time:** Mar 29, 2024 08:40:33
- Event Timeline:** Includes filters for Notes, Mitigation, Endpoint, Blocklist, Exclusions, Analyst Verdict, Incident Status, External Ticket Status, Threat Status, Fetch Threat File, and XDR Actions.
- Events:**
 - Mitigation (Mar 29, 2024 08:40:35): The management user Reno Goeyvaerts issued a quarantine command to threat EDR-Tester.bat on agent NetRunner. [Show More...](#)
 - Mitigation (Mar 29, 2024 08:40:35): The management user Reno Goeyvaerts issued a kill command to threat EDR-Tester.bat on agent NetRunner. [Show More...](#)
 - Mitigation (Mar 29, 2024 08:40:34): A reboot is required for the endpoint NetRunner to complete the remediate mitigation process on the threat EDR-Tester.bat. [Show More...](#)
 - Mitigation (Mar 29, 2024 08:40:34): The agent NetRunner successfully quarantined the threat: EDR-Tester.bat. [Show More...](#)
 - Threat Status (Mar 29, 2024 08:40:34):

Er kan op verschillende onderwerpen gefilterd worden, hier zijn enkele voorbeelden:

- **Notes**
- **Mitigation**
- **Analyst Verdict**
- **Threat status**
- ...

Action Button

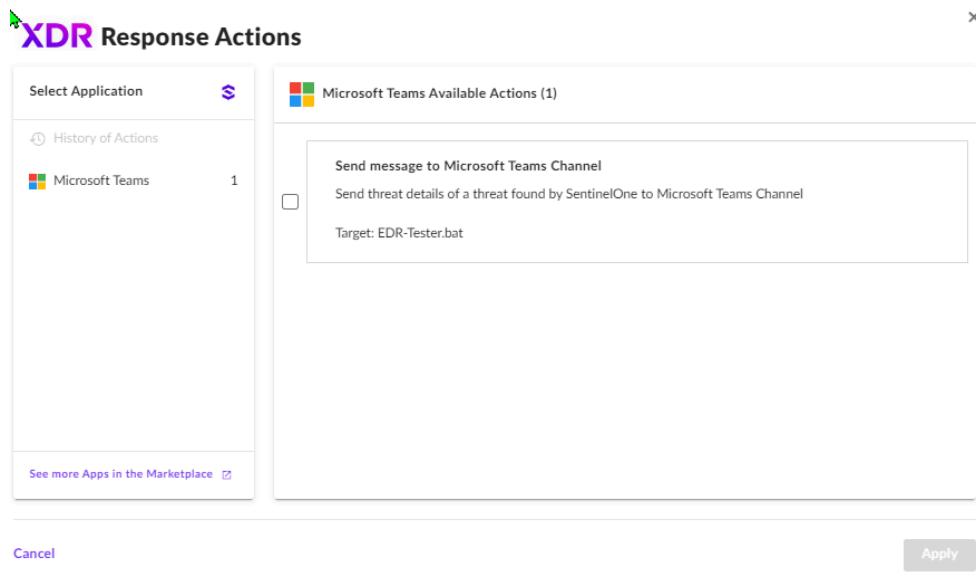
The screenshot shows an action button panel with the following details:

- OVERVIEW** | **EXPLORE** | **TIMELINE** | **Actions** | **⚙️**
- Actions:** Mitigation Action, XDR Response Actions, Run Script, Forensics Collection, Add To Blocklist, Add To Exclusions, Unquarantine, Disconnect.

In het threats panel hebben we rechts van boven ook nog een action button hier kunnen we volgende acties met ondernemen:

- **Mitigation actions:**
 - Kill

- Quarantine
- Remediate
- Rollback
- Met onze policy settings gebeurt dit automatisch
- **XDR response actions**
 - Dit zijn acties van integraties die uitgevoerd kunnen worden



- **Run Script**
 - heeft dezelfde mogelijkheden als in het action menu van de endpoint details window
- **Add to blocklist**
 - Deze actie gaat de file hash aan de blocklist toevoegen zodat de file direct wordt geblokkt/ in quarantaine gezet als deze gedetecteerd wordt.
- **Add to exclusions**
 - Deze actie gaat de file hash toevoegen aan de exclusion list waardoor de file niet in quarantaine wordt gezet als deze gedetecteerd wordt.
- **Unquarantine**
- **Disconnect**

Alerts

Alerts worden gegenereerd door STAR Custom Rules die later in het document aan bod komen. Hieronder zie je de alerts tab:

	Actions	Rule Name	Severity	Detected At	Endpoint Name	Event Type	Source Process Name	Source Process Image P...	Analyst Verdict
▼	Q	File creation	High	Mar 29, 2024 08:42:44	NetRunner	FILECREATION	certutil.exe	C:\Windows\System32\certutil...	Undefined
▼	Q	File creation	High	Mar 29, 2024 08:38:05	NetRunner	FILECREATION	7zG.exe	C:\Program Files\7-Zip\7zG.e...	Undefined
▼	Q	File creation	High	Mar 29, 2024 08:38:05	NetRunner	FILESCAN	N/A	N/A	Undefined

In de alerts tabel zien we volgende begrippen:

- **Actions**
- **Rule Name**
- **Severity**
- **Detected at**
- **Endpoint name**
- **Event type**
- **Source Process Name**
- **Source Process Image Path**
- **Analyst Verdict**
- **Incident Status**
- **Source process**

wanneer we op een van de alerts klikken kunnen we volgende details zien:

SOURCE PROCESS PARENT DETAILS	SOURCE PROCESS DETAILS	TARGET FILE DETAILS	ENDPOINT DETAILS
Name: explorer.exe Image Path: C:\Windows\explorer.exe User: NetRunner\Ronin Start Time: Apr 5, 2024 08:35:52 Command Line: C:\Windows\Explorer.EXE Integrity Level: high Publisher: MICROSOFT WINDOWS	Name: 7zG.exe Image Path: C:\Program Files\7-Zip\7zG.exe User: NetRunner\Ronin Start Time: Apr 5, 2024 10:41:42 Command Line: "C:\Program File\7-Zip\7zG.exe" x -o"C:\Users\Ronin\Downloads\" -a#7zMap24401:190-7:Event31456 Integrity Level: high	Path: C:\Users\Ronin\Downloads\b1861d123e1d10057d29230147c4763380f16cd1697d953676211c1a68635.exe Old Path: N/A ID: 82C0C8F9355EA9DB SHA1: e739a57348bf5af2c0865e766980e6b1c239ba3 SHA256: 8061d13e0e1c0057d29230147c4763380f16cd1697d953676211c1a68635	Endpoint Name: NetRunner Endpoint OS Type: windows Endpoint OS Name: Windows 10 Pro Endpoint OS Revision: 19045 Agent UUID: 56b119591e7d4d20b5d8c557eb798892 Agent Version: 23.3.264

CUSTOM RULE		View Custom Rule	GENERAL DETAILS	
Name	file creation		Detected At	Apr 5, 2024 10:42:21
Description	N/A		Reported At	Apr 5, 2024 10:42:31
Scope	account		Event Type	FILEMODIFICATION
Query Language	1.0		DV Event ID	01HTPPQZ0S1989NQY5X26
Query	TgtFileExtension In AnyCase ("iso", "lnk", "txt", "csv", "exe", "dock", "pdf", "doc", "jpeg", "zip", "bat", "elf") AND (TgtFilePath In Contains ("\\AppData\Local\Temp", "\\Downloads") AND (TgtFilePath Does Not Contain "Downloads.lnk" AND			
			Alert ID	1921643462910720028
			Source	STAR
			Hit Type	Events

- **SOURCE PROCESS PARENT DETAILS**
- **SOURCE PROCESS DETAILS**
- **TARGET FILE DETAILS**
- **ENDPOINT DETAILS**
- **CUSTOM RULE**
- **GENERAL DETAILS**

Identity



Wanneer we klikken op identity worden we verwezen naar een nieuwe tab waarop terecht komen op het identity dashboard. Hier kunnen we dingen zien zoals:

- Time-based attacks
- Top 5 suspicious Endpoints
- Ranger AD summary
- MITRE Tactics and attacks
- Recent events
- ...

The screenshot shows the Identity dashboard with the following data points:

- # of Detections: 2
- # of MITRE ATT&CK Techniques: 1
- # of MITRE ATT&CK Tactics: 4
- # EPs Under Risk: 0
- MITRE Tactics**: Initial Access (2), Execution (0), Persistence (2), Privilege Escalation (2), Defense Evasion (2), Credential Access (0), Discovery (0), Lateral Movement (0), Collection (0).
- Time-based Attacks**: A chart showing 0 attacks from 0 to 3.
- Identity**: Total Installed Endpoints (1), Suspicious (0), Offline (0).
- Suspicious Endpoints by Features**: No Data Available.
- Suspicious Events by Policy**: No Data Available.
- Event Summary**: Ranger AD (Very High risk).
- Recent events**: Default Admin Account Usage (an hour ago - AD\administrator) and Default Admin Account Usage (2 hours ago - AD\administrator).

Wanneer we klikken op analysis krijgen we de dropdown menu te zien:

The Analysis dropdown menu includes the following options:

- Events
- Ranger AD
- Identity Endpoints

Events

In deze pagina kunnen we alle events zien die matchen met bepaalde MITRE techniques, tactics en Categories.:

The screenshot shows the 'Events' section of the interface. At the top, there are three tabs: 'Dashboard', 'Analysis' (which is selected), and 'Configuration'. Below the tabs, there's a 'Events' section header. The main area contains several search filters: 'Free text search' (Ranger AD), 'Feature' (Ranger AD), 'Product' (Ranger AD), 'Service' (ACTIVE DIRECTORY), 'Category' (Recon), 'MITRE Technique' (Valid Accounts), and 'MITRE Tactic' (Persistence, Privilege Escalation, Defense Evasion, Initial Access). There are also dropdowns for 'Time' (Month), 'Severity' (Medium), and 'Log Type' (Unacknowledged). A summary table at the bottom shows one event: 'Default Admin Account Usage (Defense Evasion) (2)' from 'Features' under 'ACTIVE DIRECTORY' last seen 'an hour ago' with a first sighting '2 hours ago'.

Ranger AD

Na het klikken op Ranger AD komen we terecht op het Ranger AD dashboard waarin we volgende dingen kunnen zien:

- Test results
 - Deze score verschijnt pas als de analyse klaar is na de install van de Ranger AD Connector
- AD health
- Domains assessed
- Users
- Computers
-

The screenshot shows the 'Ranger AD' dashboard. At the top, there are tabs: 'Dashboard' (selected), 'Analysis' (which is currently active), and 'Configuration'. Below the tabs, there are four main sections: 'Test Results' (Health 78%, LOW RISK), 'Active Directory Health' (two stacked bar charts for 18 Apr and 19 Apr showing health levels: Very High, High, Medium, Low), 'Domains Assessed' (1 Domain Controller Unprotected), 'Users' (2 Security Groups Unprotected), 'Computers' (1 Computer Unprotected), and 'Most Vulnerable Assessments' (a grid of five items: Default Permission Changes on Domain Partition, Security Hardening Recommendations for Domain Controllers, Recent Changes to Default Domain Policy or Default Domain Controllers Policy, Default Administrator Account Hardening, Accounts with Risky User Account Control Parameters, and Protected Users Group Not Created or Not Used).

We hebben nog 3 andere tabbladen die we kunnen kiezen namelijk:

- AD exposures
- Azure exposures
- Remediation history

AD exposures

Wanneer we op AD exposures klikken krijgen we een opsomming van alle vulnerable configurations van de AD te zien, aan de hand van het severity level wordt er ook een remediation voorgesteld.

The screenshot shows the 'AD Exposures' tab selected in the top navigation bar. The main content area displays a table of vulnerabilities. Each row contains the following columns: Detection Name, Affected Domains, Vulnerable Objects, Severity, Score, Last 5 runs, and a Remediate button. The first row, 'Default Permission Changes on Domain Partition', is expanded to show more details. The 'Details' button in the last column of each row also has a dropdown arrow.

Detection Name	Affected Domains	Vulnerable Objects	Severity	Score	Last 5 runs	Remediate
Default Permission Changes on Domain Partition	1 out of 1 vulnerable	1 ↗ View	Very High	0%	>Last 5 runs	Remediate
Accounts with Never Expiring Passwords	1 out of 1 vulnerable	1 ↗ View	High	0%	Last 5 runs	Remediate
Regular Users Can Add New Computers into the AD Domain	1 out of 1 vulnerable	2 ↗ View	Medium	0%	Last 5 runs	Details
Domain Controller with Print Spooler Enabled (PrintNightmare)	1 out of 1 vulnerable	1 ↗ View	Very High	0%	Last 5 runs	Details
Recent Changes to Default Domain Policy or Default Domain Contro...	1 out of 1 vulnerable	2 ↗ View	Very High	0%	Last 5 runs	Details
Security Hardening Recommendations for Domain Controllers	1 out of 1 vulnerable	17 ↗ View	Very High	0%	Last 5 runs	Details
LDAP Unsigned Connections Allowed	1 out of 1 vulnerable	1 ↗ View	Very High	0%	Last 5 runs	Details

Wanneer we klikken op de remediate of Details knop van een van deze vulnerabilities krijgen we volgend scherm te zien:

The screenshot shows the 'Remediation' details page for the 'Default Permission Changes on Domain Partition' vulnerability. The top section displays the name, MITRE ATT&CK ID, severity (Very High), score (3.16%), and objects affected (1). A 'Remediate Now' button is prominently displayed. Below this, tabs for Summary, Remediation, Additional Information, and Objects are visible. The 'Additional Information' tab is selected, showing sections for Description, Known Attack Tools, and References. The 'Description' section states: 'A compromised user account with modified access to the domain partition in a forest can create new objects or make changes that propagate to newly created objects in AD. Inappropriate permissions can result in a DCSync attack leading to a full domain compromise.' The 'Known Attack Tools' section lists 'Bloodhound' and 'Powerview'. The 'References' section links to 'Active Directory Access Control List - Attacks and Defense'.

Hier krijg extra informatie over de vulnerability zoals:

- De attack tools voor deze vulnerability
- De impact op de security score
- Referenties

Maar ook de theoretische uitleg van de remediation:

Remediate Using Automated Script

0.00% of customers remediate this exposure. Detected at 100.00% of all customer deployments

3.16% Improve Score 0 Customers Used 0 Total number of Objects Remediated

Summary
Remove discovered standard user accounts from the ACLs of the domain partition.

Side Effects
If a service account was added to the domain partition's ACL to perform a particular function, it should be reevaluated. If necessary, it can be removed and replaced with a group for monitoring purposes.

Preparation for Remediation
Review the standard accounts that were detected in the domain partition's ACL. If they are standard user accounts and have no need for the permissions they've been granted, they should be removed immediately. If they are service accounts and have a legitimate need, they can be added to a group and the group can be added to the ACL. Monitor this group for changes.

Manual Remediation Steps
Verify the users and permissions reported by Ranger AD for the domain partition.
Check the security descriptor on Active Directory.
Open Active Directory Users and Computers MMC (Windows > Run > DSA.MSC).
Right-click the domain name and select properties.
In the Security tab, verify and remove the non-privileged users reported by Ranger AD.

Remediation Reference Articles
[BloodHound 1.3 – The ACL Attack Path Update – waldo.com](#)

Wanneer we klikken op remediate now krijgen we volgend scherm te zien:

Dashboard Analysis Configuration

Improve Protection - Exposures Ranger AD > Improve Protection > Exposures Cancel Next

Select-Objects **Remediate Using Script**

View by Exposures Need help on how to use Select-Objects? [Click here](#)

Severity Exposures Domain Object Type Account Status

All (1) Filtered (1) Filtered All All

Detection Name: Default Permission C... Domains: sentineluan.com Search here or type column name Clear all

All Exposures

Default Permission Changes on Domain Partition [1 of 1 objects] Score contribution (3.16%)

Hier kunnen we kiezen voor welke vulnerabilities een script moet worden gegenereerd. Wanneer je de vulnerabilities hebt gekozen die je wilt remediaten klik je op next en kom je op volgend scherm terecht:

80.54% ↑ Score will improve by 3.16% (from 77.39%) 1 View exposures 1 Exposures Selected 1 Objects Selected Generate script Modify Selected Exposures and Objects

Protect using Remediation Script

Remediation Script

Step 1: Download Remediation Script

- Download the zip file which contains script and JSON
- Download Remediation Script
- Current Version: NA
- Uncompress the zip file

Step 2: Execute the script

- Execute in Domain administrator context or launch PowerShell in Administrator Context as different user and run the below command
- Start-Process powershell -Cred...
- Provide tenant credentials
- Wait for the script to finish execution

View Summary

Protect using ADSecure-EP

Endpoint

ADSecure-EP protects against reconnaissance attacks on your AD infrastructure.

Hides real assets and inserts deceptive assets. Also blocks suspicious commands.

Choose which Endpoint Protection policies in the next screen.

Protect Entities →

hier kan je het script laten genereren of gebruik maken van de ADSecure-EP.

Azure exposures

In deze tab van Ranger AD kan je de Entra ID vulnerabilities zien als je een Tenant hebt gelinkt aan de SentinelOne control panel. Deze feature werkt exact hetzelfde als de AD Exposures behalve dat de Azure Exposures geen Remediation actions heeft.

Ranger AD						
Dashboard		AD Exposures		Azure Exposures		
Remediation History						
<input type="checkbox"/> Show Filters	Status	(Vulnerable)				
<input type="checkbox"/> Group By	Acknowledged	Sort By				
Detection Name	No	Severity				
Total Count: 19						
<input type="checkbox"/> Detection Name • Standard Users Allowed to Create Apps Details	Detection Source Azure AD	Vulnerable Objects 1 ↑ View CSV	Severity Very High	Run Time a day ago	Summary 1 out of 1 vulnerable	...
<input type="checkbox"/> Detection Name • Restrict Access to Azure Portal with conditional access Details	Detection Source Azure AD	Vulnerable Objects 1 ↑ View CSV	Severity High	Run Time a day ago	Summary 1 out of 1 vulnerable	...
<input type="checkbox"/> Detection Name • Users Are Allowed to Consent to Applications Details	Detection Source Azure AD	Vulnerable Objects 1 ↑ View CSV	Severity Medium	Run Time a day ago	Summary 1 out of 1 vulnerable	...
<input type="checkbox"/> Detection Name • Standard Users Allowed to Invite External Users Details	Detection Source Azure AD	Vulnerable Objects 1 ↑ View CSV	Severity Very High	Run Time a day ago	Summary 1 out of 1 vulnerable	...
<input type="checkbox"/> Detection Name • Privileged Users without Multi-Factor Authentication (MFA) Details	Detection Source Azure AD	Vulnerable Objects 1 ↑ View CSV	Severity Very High	Run Time a day ago	Summary 1 out of 1 vulnerable	...
<input type="checkbox"/> Detection Name • Azure AD Tenant without User Risk Policies enabled Details	Detection Source Azure AD	Vulnerable Objects 1 ↑ View CSV	Severity High	Run Time a day ago	Summary 1 out of 1 vulnerable	...
<input type="checkbox"/> Detection Name • Azure AD Tenant without Sign-In Risk Policies enabled Details	Detection Source Azure AD	Vulnerable Objects 1 ↑ View CSV	Severity High	Run Time a day ago	Summary 1 out of 1 vulnerable	...

Remediation History

In deze tab zie je alle Remediation actions die ondernomen zijn en wat hun status is:

Actions +							Search...
Exposures		Type	Status	Time	Details	Actions	Columns
<input type="checkbox"/>	1 Objects and 1 Exposures	Remediation	Ready To Download	39 minutes ago	Details	Script	Report

Identity endpoints

Wanneer we op deze optie klikken krijgen we volgende opties:

Activity

ThreatPath

Managed Endpoints

Policy Enforcement Status

Activity

De ADSecure-EP module verzamelt en stuurt AD-queries voor rapportage, het interval voor de rapportage kan ook worden geconfigureerd.

ThreatPath

Deze feature geeft een algemene view van alle exposures binnen het netwerk:

Er zijn verschillende tabs binnen ThreatPath die extra informatie geven over verschillende onderwerpen:

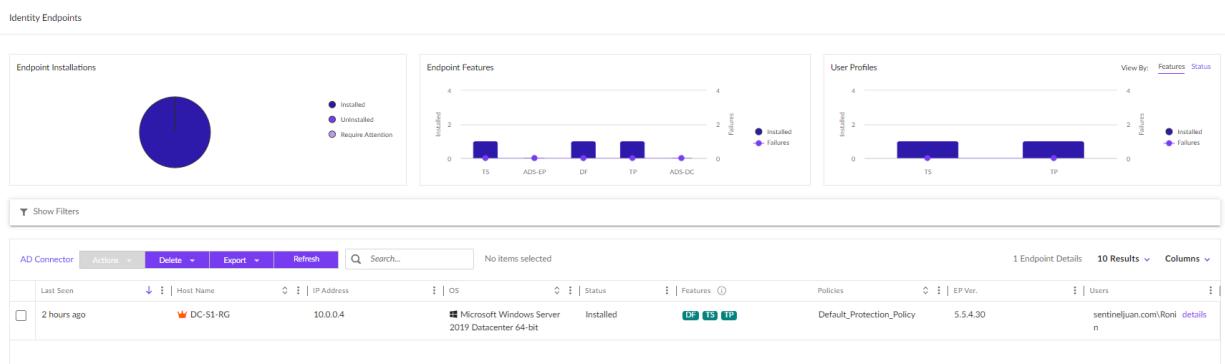
- **Active Directory**
 - hier kunnen we volgende dingen zien:
 - Accounts
 - Permissions
 - Stale Accounts
 - No Password Expiry
 - Group memberships
- **Endpoint Exposures**
 - Exposures worden onderverdeeld in volgende categorieën:

- Local Admin Accounts
- Local Service Accounts
- Same Password
- **Lateral Movement Paths**
 - Deze movement paths kunnen we zien voor:
 - Privilege Account Access
 - AWS
 - SSH
 - RDP Saved Credentials
 - RDP Memory Credentials
 -
- **TOP 5 Credentials**
- **Paths Discovered vs Remediations**

Identity Endpoints

In deze tab zie je al de endpoints die een ad connector hebben en hier kunnen we een aantal details van zien namelijk:

- **Host Name**
- **IP Address**
- **Os**
- **Status**
- **Features**
 - Deflect
 - Threatstrike
 - Threatpath
 - ADSecureEP
 - AdSecureDC
- **Policies**
- **EP version**
- **Linked user**



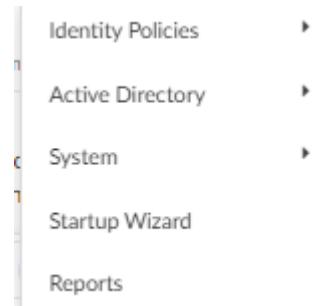
Policy Enforcement Status

Op deze pagina kunnen we alle transacties en statussen zien die enforced zijn door de Endpoint protection policies:

The screenshot shows a web-based interface titled "Policy Enforcement Status". At the top, there are navigation links: "Analyses > Endpoints > Policy Enforcement Status". A message below the title states: "This page lists out all the transactions and their status as enforced by the Endpoint Protection Policies. You can click on the 'Actions' button to change the status of transaction(s)." Below this is a search bar with fields for "Show Filters", "Time", "Month", and "Clear all". There are also buttons for "Actions", "Delete", and "Refresh". The main area has a header with columns: "Hostname", "Username", "Events", "Status", "Last Activity Time", and "Connector". A message at the bottom center says "No results found" next to a magnifying glass icon.

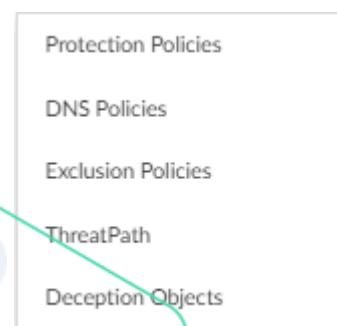
Configuration

Wanneer we klikken op configuration krijgen we volgende opties te zien:



Identity policies

Wanneer we op Identity policies klicken krijgen we de volgende opties te zien:

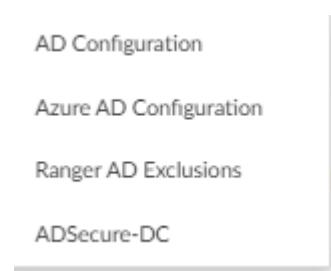


Hier kunnen we kiezen uit volgende onderwerpen:

- **Protection Policies**
 - zijn een set van regels die Singularity Identityfeatures configureren
- **Dns Policies**
- **Exclusion policies**
- **ThreatPath**
- **Deception Objects**
 - Dit is een feature binnen Identity die u instelt om de functies van identity te configureren in het de protection policy

Active Directory

Wanneer we op Active Directory klikken krijgen we de volgende opties te zien:



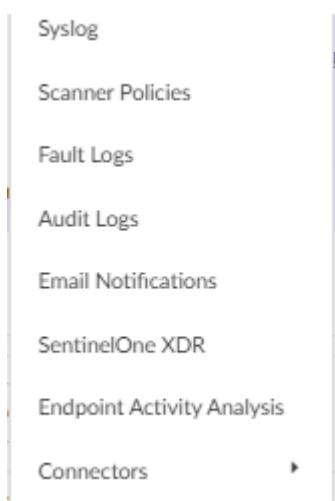
Hier kunnen wede volgende configuraties in doen:

- **AD Configuration**
 - hier moeten we volgende informatie over de AD doorgeven na de connector geïnstalleerd:
 - DC FQDN
 - Username
 - Password
 - Domain Name
 - LDAP Encryption Method
 - LDAP
 - LDAPS
 - WinRM Encryption Method
 - Over HTTP
 - Over HTTPS
 - Referral
 - Ranger AD
 - Enable threat Detection
 - Include all domains
 - Access over Trust

- **Azure AD Configuration**
 - Link met Entra ID gebeurt in settings → integrations → Azure Tenant
- **Ranger AD Exclusions**
- **ADSecure-DC**
 - monitor de nodige protocollen

System

Wanneer we op System klikken krijgen we de volgende opties te zien:



Hier kunnen we de volgende dingen configureren:

- **Syslog**
 - Identity Cloud biedt de mogelijkheid om syslogprofielen in te stellen. Deze profielen worden gebruikt om gebeurtenissen, foutlogs en auditlogs door te sturen naar syslogservers in uw netwerk.
- **Scanner Policies**
 - Dit gebruik je om scanners binnen je netwerk te monitoren maar niet geen alerts te laten genereren
- **Fault Logs**
- **Audit Logs**
- **Email Notifications**
- **SentinelOne XDR**
 - Maakt het mogelijk om de data die vergaard wordt binnen Identity naar het data lake wordt gestuurd
- **Endpoint Activity Analysis**
- **Connectors**
 - Okta
 - Duo

Startup Wizard

Binnen deze feature kan je volgende dingen configureren/ ondernemen:

- AD Security
- Identity Security
- De Ranger AD connector installeren
- De AD server toevoegen
- ID Policies toe

Reports

Met Identity Cloud kunt u rapporten genereren die informatie bevatten over uw omgeving. U kunt rapportprofielen instellen waarmee u bepaalt:

- Het type rapport: Welke gegevens wilt u in het rapport zien?
- De inhoud: Welke specifieke informatie moet worden opgenomen?
- De planning: Wilt u het rapport handmatig genereren of automatisch volgens een schema?

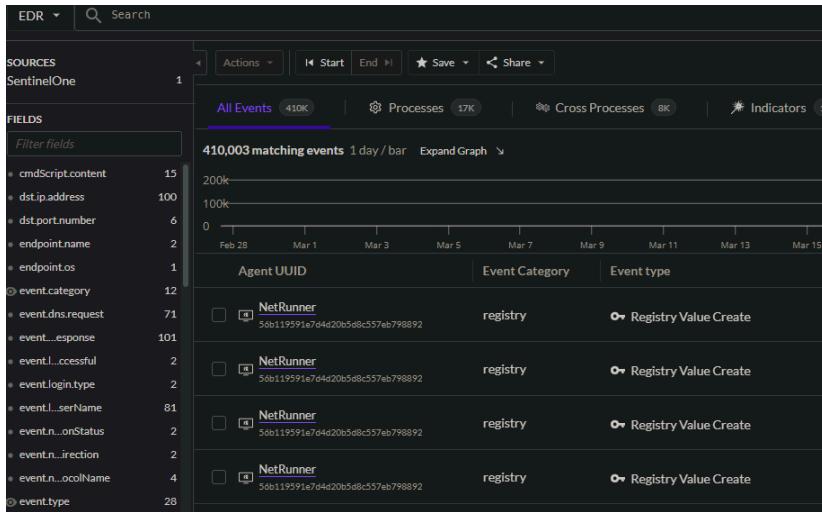
Visibility (Singularity data lake)



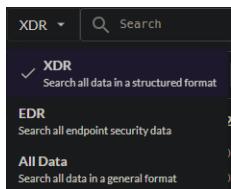
Als we klikken op Visibility komen we op het Singularity Data lake. Singularity Data lake is een locatie voor het verzamelen en transformeren van logs en Security data. We kunnen al deze data en logs bevragen en bewerken tijdens hunting naar de oorzaak van aanvallen of malware Deployments. We kunnen ook door middel van API's meer data ingesten voor een beter beeld te krijgen van wat er zich afspeelt binnen de omgeving.

Enhanced + legacy view

Hieronder zie je een screenshot van het Singularity data lake in de enhanced view, deze geeft de data weer zoals SIEM oplossingen dit doen. Dit kan wel wat verwarring veroorzaken door de hoeveelheid informatie die in een oogopslag te zien is.

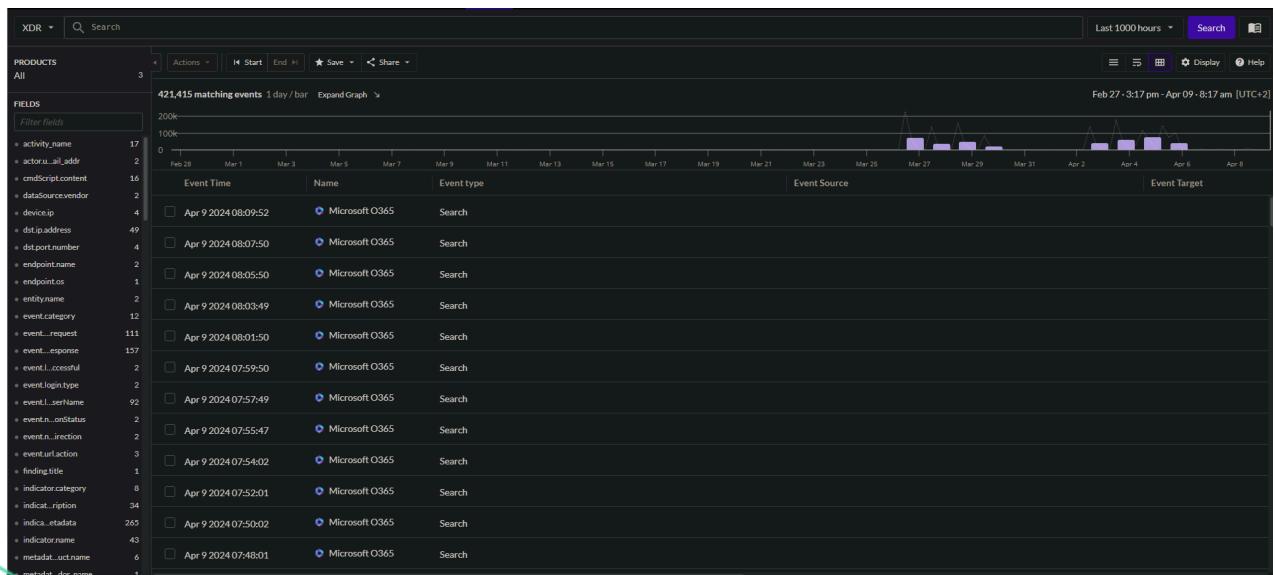


In de advanced visibility kunnen we kiezen tussen 3 views namelijk:



- **XDR**
 - Laat gestructureerde security data gecollecteerd door SentinelOne agents en integraties zien.
- **EDR**
 - Laat gestructureerde security data gecollecteerd door SentinelOne agents zien.
- **All data**
 - Laat data zien gecollecteerd door SentinelOne agents, de SentinelOne collector en integraties

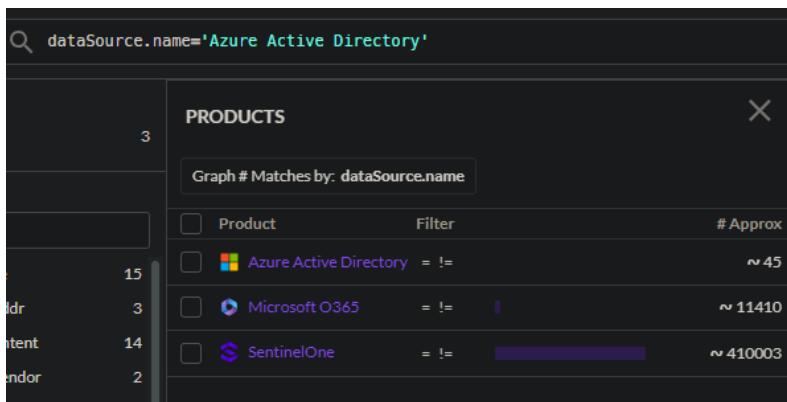
Wanneer we op XDR klikken krijgen we het volgende scherm te zien:



We zien hier ook een products tab, binnen deze tab kunnen filteren tussen de verschillende afkomsten van de data in dit geval:

PRODUCTS		
Graph # Matches by: dataSource.name		
Product	Filter	# Approx
 Azure Active Directory	= !=	~45
 Microsoft O365	= !=	~11410
 SentinelOne	= !=	~410003

Als we op een van deze namen klikken komt dit automatisch in de search field te staan.

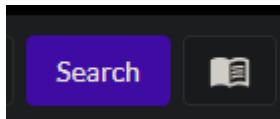


The screenshot shows a search bar at the top with the query `dataSource.name='Azure Active Directory'`. Below the search bar is a table titled "PRODUCTS" with the same data as the previous table, showing matches for Azure Active Directory (~45), Microsoft O365 (~11410), and SentinelOne (~410003).

Hiernaast kan je ook binnen fields filteren op specifiek data:

Filter fields	Value	Filter	# Approx
activity_name	Search	= !=	~6000
actor.u...il_addr	MDCRegulatoryComplianceAssessments	= !=	~3000
cmdScriptContent	MDCAssessments	= !=	~800
dataSource.vendor	Validate	= !=	~300
device.ip	Aggregate	= !=	~100
dstIp.address	Logon	= !=	~100
dst.port.number	Update	= !=	~90
endpoint.name	Set-Mailbox	= !=	~60
endpoint.os	Delete	= !=	~30
entity.name	UserLoginFailed	= !=	~30
event.category	ListColumnCreated	= !=	~30
event.dns.request	Add service principal.	= !=	~30
event.d...esponse	Install-DataClassificationConfig	= !=	~30
event.l...ccessful	MailItemsAccessed	= !=	~30
event.login.type	Update service principal.	= !=	~30
event...erName			
event.n...onStatus			
event.n...irection			
event.url.action			
finding.title			
indicator.category			

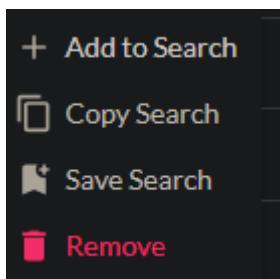
Om query's op te slaan in deze view van visibility moet je op de Search library knop naast de search knop:



dan krijg je volgend scherm te zien:

Recent	Saved	Shared	SentinelOne
Last Executed	Query	Actions	
> Apr 8 14:17	dataSource.name='Microsoft O365'		
> Apr 5 11:39	dataSource.name='Azure Active Directory'		
> Apr 5 11:39	dataSource.name='Microsoft O365'		
> Apr 5 11:38	dataSource.name='Microsoft O365'		
> Apr 5 08:47	dataSource.name='Microsoft O365' and event.type =◆...		
> Apr 5 08:38	dataSource.name='Microsoft O365'		
> Apr 5 08:38	dataSource.name='Microsoft O365'		
> Apr 4 15:01	dataSource.name='Azure Active Directory'		
> Apr 4 14:10	dataSource.name='Azure Active Directory'		
> Apr 4 09:11	src.process.parent.user='NetRunner\Ronin'		

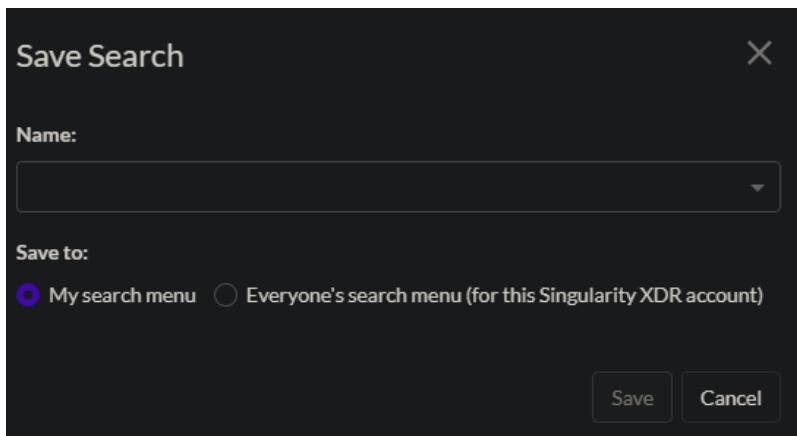
Hier zie je alle reeds gebruikte query's, als je een van deze wilt opslaan moet je klikken op de 3 puntjes naast de query's, je krijgt volgend schermpje te zien:



Hier heb je de mogelijkheid om:

- *De query aan je huidige search toe te voegen*
- *Deze query te kopiëren*
- *Deze query op te slaan*
- *Deze query uit de zoekgeschiedenis te verwijderen*

Wanneer je op save hebt geklikt krijg je volgend scherm te zien:



Hier kan je:

- *De query een naam geven*
- *kiezen wat voor soort query het wordt*
 - Een persoonlijke
 - Een gemeenschappelijke

Als alles goed gelukt is en we klikken op saved binnen de search library krijg je je saved query te zien:

The screenshot shows the 'Saved' tab in the search library. A table lists a single saved query named 'LOGIN'. The table columns are 'Name', 'Actions', 'Time Range', 'Query Filter', and 'View'. The 'Actions' column shows a magnifying glass and three dots icon. The 'Time Range' is 'Last 1000 hours'. The 'Query Filter' is partially visible as 'dataSource.name='Microsoft O365' and event.type ='Lo...'. The 'View' is 'XDR'.

SentinelOne biedt ook een legacy view aan die een iets simpeler beeld geeft van de data, dit kan je op onderstaande foto zien.

query library

The screenshot shows the Microsoft Sentinel interface in the 'Hunting' tab. At the top, there are three tabs: 'VISIBILITY', 'HUNTING' (which is selected), and 'STAR CUSTOM RULES'. Below the tabs is a search bar with the query: '(EndpointName Contains "Net..." AND SrcProcStorylineId = "F75CC2..." AND TgtFileExtension In AnyCase ("..."))'. There are buttons for 'New', 'Load Query', and 'Save New Query'. A '+' button is also present. The main area is titled 'Main Query' and includes filters: 'Events' (selected), 'Last 48 Hours', 'Max Results: 2000', and 'Loading Mode: Priority Fields'. Below these filters, a single query is listed: '1 Start Hunting...'. To the left of the main area, there is a sidebar with sections: 'Getting started with PowerQueries', 'Basic Event Queries' (which is expanded to show 'Advanced Event Queries', 'S1 Research Queries', and 'Recent Queries'), and a list of eight basic event queries:

- Events from all agents from the last hour
- All the Windows-related processes that ran in my sites in the last 24 hours
- All Registry activity in my sites from the last hour
- All network activity in my sites from the last hour
- All the file-related activities in 'Temp' folder, in my sites from the last hour
- A non-Windows process writes files to the temp directory
- Rundll or Regsvr executes a script
- Bat or cmd files are dropped directly to a temp folder

Je komt terecht in de Hunting tab van Visibility waarin je queries kan uitvoeren op de Singularity Data lake, zoals je in de foto hieronder kan zien, zijn er verschillende basis event queries die al voor je klaar staan.

This screenshot is identical to the one above, showing the Microsoft Sentinel interface in the 'Hunting' tab. It displays the same navigation bar, search bar, and list of basic event queries on the right side of the main area.

We klikken vervolgens op "All network activity in my sites from the last hour", we krijgen volgend scherm te zien:

The screenshot shows the SentinelOne interface under the 'HUNTING' tab. A query is running: 'EndpointName Contains "LPT..."'. It has found 436 results. The results table lists various events, including IP connects from endpoints like 'Sandevestan' and 'NetRunner' to IP addresses such as 'WindowsAzure...' and 'WaAppAgent.exe'. The table includes columns for Endpoint Name, Object Type, Event Type, Event Time, Source Process, and Source Process Command Line.

We kunnen door deze query al het verkeer zien dat het netwerk verlaat vanuit onze endpoints, op deze manier kunnen we eventuele verdachten netwerkactiviteit vinden en deze verder onderzoeken. Deze query behoort tot de Basic event queries er zijn nog 2 andere types van queries die SentinelOne aanbiedt in de query library namelijk:

- ***Advanced Event queries***
- ***S1 research queries***

De advanced Event queries kunnen worden gebruikt in threat hunting.

The screenshot shows the 'Advanced Event Queries' section of the query library. It lists several pre-defined queries:

- LOLBins command processors masquerade under a different name and path
- Rundll or Regsvr run content from a remote server
- Suspicious Powershell with base64 in the commandline
- LaZagne Search, returns number of events matched by endpoint and process, and percentage of total events by each process/endpoint tuple. (PQ)
- New unsigned DLL is dropped in the Windows directory (possible DLL hijack attempt)
- SpoolSrv Exploit (PQ)

Hier zie je verschillende queries die je kan runnen op het data lake om te checken of er threats gerelateerd aan deze queries hebben plaatsgevonden binnen jouw netwerk.

Als laatste hebben we ook nog de S1 research queries, deze queries zijn van het SentinelOne research team. In deze collectie zijn er queries die kunnen gebruikt worden voor het opsporen van IOC's(Indicators of compromise).

The screenshot shows a sidebar with categories: Getting started with PowerQueries, Basic Event Queries, Advanced Event Queries, S1 Research Queries, and Recent Queries. The main area displays a list of hunting queries:

- Hunting query for suspected exploitation of unpatched Windows privilege escalation flaw (CVE-2021-36934)
- Hunting query for suspected SolarWinds (Serv-U) activity - process creation
- Hunting query for suspected SolarWinds (Serv-U) activity - C2 communication
- Kaseya Ransomware Detection
- Hunting query for suspected PrintNightmare exploit attempts
- NTDS Copy
- Removal of indicators on Host
- Suspicious data compression

We kunnen natuurlijk ook zelf queries schrijven hieronder zie je een voorbeeld waar we filteren op de endpoint naam, Source process name en eventtype. We krijgen dan volgend resultaat te zien :

The screenshot shows a search results page with the following parameters:

- PowerQuery: New
- Events: 22.03.2024 15:00:00 To 22.03.2024 15:10:00
- Max Results: 2000
- Loading Mode: Priority Fields

Search query: 1 (EndpointName Contains "LPT-SCG0116GNV" and SrcProcName Contains "powershell.exe" and EventType = "Command Script")

The results table shows 18 results for Command Scripts:

Endpoint Name	Object Type	Event Type	Event Time	Source Proc.	Source Proc. ID	Source Process Command Line	Source	
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:05:13	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:05:13	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:05:13	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:05:13	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:05:13	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:06:22	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:06:22	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:06:22	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO
LPT-SCG01...	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:06:22	powershell.exe	False	76BB046ED09B75B2	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"	MICRO

Hierin zien we binnen de aangegeven tijdspanne al de events die voldoen aan de voorwaarden van de query, we kunnen op het pijltje aan de linkerkant van een van de events klikken, zien we meer informatie over het event zoals details over de processes en welk command is uitgevoerd.

The screenshot shows a detailed view of an event from the previous search result:

Event details:

- Endpoint Name: LPT-SCG01...
- Object Type: COMMAND_SCRIPT
- Event Type: Command Script
- Event Time: Mar 22, 2024 15:06:22
- Source Proc.: powershell.exe
- Source Proc. ID: False
- Source Process Command Line: 76BB046ED09B75B2 "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"

Details for the event:

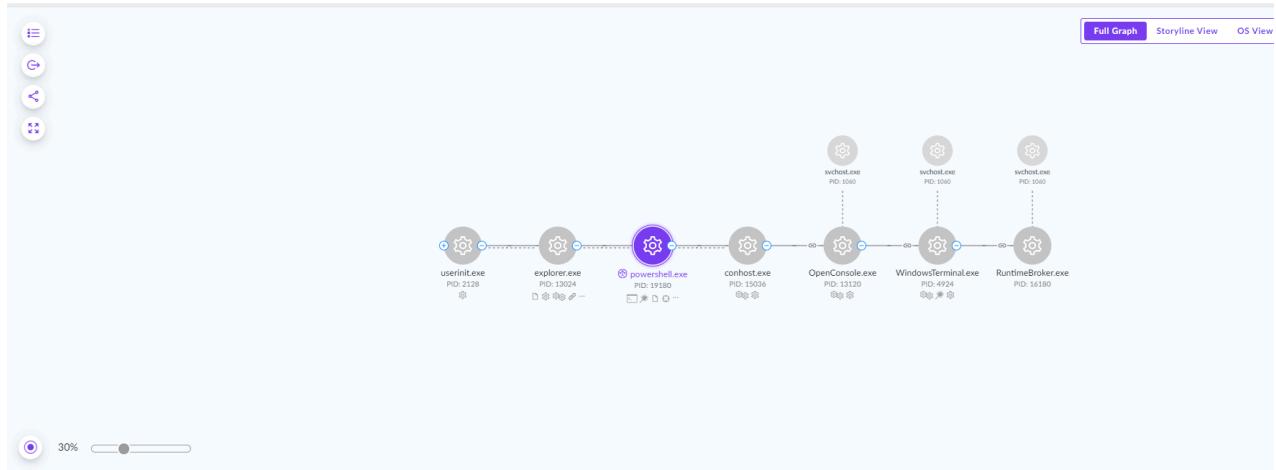
SOURCE PROCESS PARENT DETAILS		SOURCE PROCESS DETAILS		COMMAND SCRIPT DETAILS	
Name	explorer.exe	Name	powershell.exe	Command Script	curl https://secure.elcar.org/elcar.com.txt -o myfil...
Storyline ID	0553036ED09B75B2	Storyline ID	76BB046ED09B75B2	Application Name	PowerShell_C:\Windows\System32\WindowsPo... Show More
Start Time	Mar 22, 2024 14:19:40	Command Line	"C:\Windows\System32\WindowsPowerShell\v1...		
Image Path	C:\Windows\explorer.exe	User	AzureAD\otto		
Unique ID	0453036ED09B75B2	Start Time	Mar 22, 2024 15:05:12		
Image SHA1	a4e4e2bc502e4ab249b219da357d1aad163ab175	Image Path	C:\Windows\System32\WINDOWSPOWERSHEL...		
		PID	19180		
		Unique ID	75BB046ED09B75B2		

We kunnen na het testen van deze query ook de query opslaan, dit doe je door op de save new query knop te klikken:

 [Save New Query](#)

Process graph

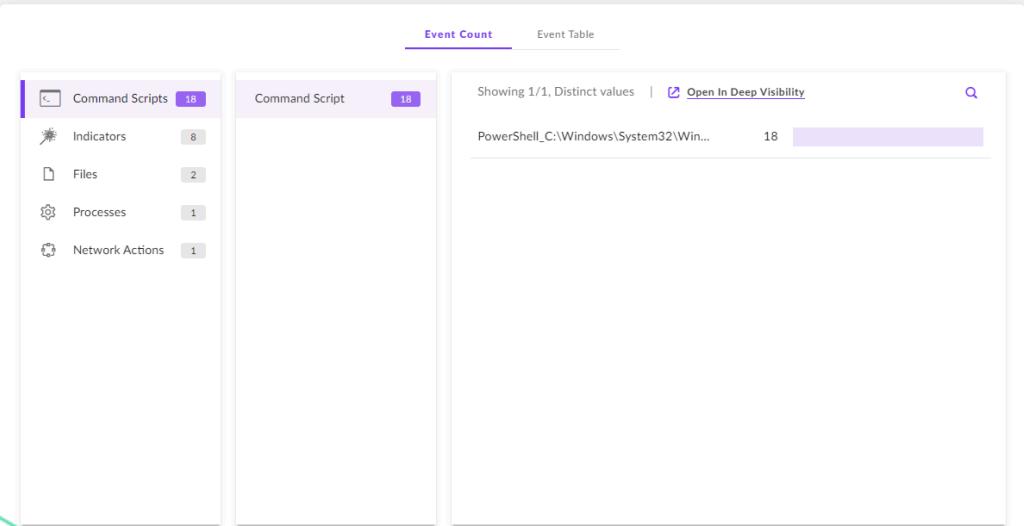
Als we op Explorer.exe of powershell.exe klikken krijgen we volgend scherm te zien:



In de afbeelding hierboven zie je de Process Graph, deze wordt gebruikt voor het bekijken wat de connectie is tussen het hoofdproces(selected node) waar je op hebt geklikt, in dit geval powershell.exe en de andere processen. Je kan dit bekijken vanuit het storyline standpunt, OS standpunt of de combinatie van allebei. Wanneer we naar onder scrollen op deze pagina zien we Event count en Event table.

Event Count

Event count is een gedetailleerde lijst van events die de selected node heeft veroorzaakt, er wordt gefilterd op event type en hoe vaak het event voorkomt. We kunnen ook filteren op de verschillende objecttypes, dit zie je aan de linker kant van het panel.



The screenshot shows the Event Count interface. On the left, there is a sidebar with categories: Command Scripts (18), Indicators (8), Files (2), Processes (1), and Network Actions (1). The main area has tabs for 'Event Count' (selected) and 'Event Table'. The 'Event Count' tab displays a table with one row: 'PowerShell_C:\Windows\System32\Win...' with a count of 18. There is a link 'Open In Deep Visibility' next to it. The 'Event Table' tab is currently inactive.

Event Table

Event Table is een gedetailleerde lijst van events die de selected node heeft veroorzaakt in hetzelfde formaat als de hunting tab van visibility. We kunnen ook filteren op de verschillende objecttypes, dit zie je aan de linker kant van het panel.

Endpoint Name	Source Process StoryLine ID	Object Type	Event Type	Event Time
LPT-5CG01...	0553036ED09B75B2	PROCESS	Process Creation	Mar 22, 2024 15:05:12
LPT-5CG01...	76BB046ED09B75B2	INDICATORS	Behavioral Indicators	Mar 22, 2024 15:05:12
LPT-5CG01...	76BB046ED09B75B2	PROCESS	Process Creation	Mar 22, 2024 15:05:12
LPT-5CG01...	76BB046ED09B75B2	INDICATORS	Behavioral Indicators	Mar 22, 2024 15:05:13
LPT-5CG01...	76BB046ED09B75B2	INDICATORS	Behavioral Indicators	Mar 22, 2024 15:05:13
LPT-5CG01...	76BB046ED09B75B2	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:05:13
LPT-5CG01...	76BB046ED09B75B2	COMMAND_SCRIPT	Command Script	Mar 22, 2024 15:05:13

Indicators

Bij threat indicators kan je zien waarom de file als een threat werd gezien door SentinelOne, deze indicators worden dan ook al gelinkt aan MITRE Techniques and tactics.

INDICATORS
BEHAVIORAL INDICATORS
Evasion
PowershellAmsiBypass Detected bypassing AMSI using reflection in powershell MITRE: Defense Evasion [T1574] MITRE: [T1562.001] MITRE: Persistence [T1574] MITRE: Privilege Escalation [T1574]
General
ProcessStartedFromLnk Process started from shortcut file MITRE: Execution [T1204]
WinRMUsed WinRM was used MITRE: Lateral Movement [T1021.006]
N/A
NetworkShareDiscovery Identified attempt to get a listing of network shares on a system MITRE: Discovery [T1135] MITRE: [T1018] MITRE: Collection [T1119] MITRE: Defense Evasion [T1480.001]
PeripheralDeviceDiscovery Identified attempt to discover connected devices on system MITRE: Discovery [T1120]

STAR CUSTOM RULES

In de visibility tab hebben we naast Hunting ook Star Custom Rules maken; STAR CUSTOM Rules is een krachtige tool die u kan helpen uw omgeving te beschermen tegen bedreigingen aan de hand van gecustomiseerde regels. Hieronder ziet u een foto van de STAR CUSTOM RULES tab.

Name	Status	Severity	Generated Alerts	Description	Status Reason	Active Response	Expiration Mode	Expiration Date
File creation	Active	High	3		Rule was activated by ...	On	Permanent	N/A

Wanneer we hierop klikken worden we automatisch doorverwezen naar het Sentinels panel. In deze tab kunnen we Rules:

- **Maken**
- **Aanpassen**
- **Activeren**
- **Deactiveren**
- **Verwijderen**
- **Dupliceren**

Als we op het pijltje klikken naast de rule krijgen we meer informatie over de Rule.

Rule Details	Condition	Response
Rule Name: file creation Description: Rule Severity: High Rule Type: Permanent Expiration Date: N/A Rule ID: 1914355098467258050 Created by: reno.goeyvaerts@vanroey.be Created At: Mar 26, 2024 08:21:51	Scope Hierarchy: Account Query Language: \$SQL 1.0 Query Type: Events Query: TgtFileExtension In AnyCase ('iso', 'ink', 'txt', 'csv', 'exe', 'docx', 'pdf', 'doc', 'jpeg', ...)	Treat as a threat: Malicious Network Quarantine: Off

De dingen die we kunnen zien van de rules zijn:

- **De naam**
- **Severity**
- **Query**
- **Query type**
- **Response method**
- **....**

We zien ook op de Rule balk hoeveel alerts er al gegenereerd zijn door de Rule, als we hierop klikken komen we terecht op het incidents panel.

Name	Status	Severity	Generated Alerts
File creation	Active	High	3

The screenshot shows the 'ALERTS' tab selected in a navigation bar. A search bar at the top right contains the text 'Rule Name file creation'. Below the search bar, there are filters for 'Alert Actions', 'Analyst Verdict', and 'Incident Status', followed by a message 'No Items Selected'. A table lists three detected events:

	Actions	Rule Name	Severity	Detected At	Endpoint Name
▼	<input type="checkbox"/>	File creation	High	Mar 26, 2024 09:00:15	NetRunner
▼	<input type="checkbox"/>	File creation	High	Mar 26, 2024 08:41:17	NetRunner
▼	<input type="checkbox"/>	File creation	High	Mar 26, 2024 08:27:57	NetRunner

Zoals we hierboven kunnen zien zie je dan ook de rule name, endpoint naam en wanneer er een situatie heeft voorgedaan die de rule heeft getriggerd.

Als we een rule willen toevoegen kunnen we dit doen door op de new rule te klikken en krijgen we volgend scherm te zien:

The screenshot shows the 'Create Custom Rule' wizard with four steps: Rule Details, Condition, Response, and Summary. The current step is 'Rule Details'.

- * Rule Name:** An input field with a red border and placeholder 'Valid input required'.
- Description:** A text area with a character count of 0/100.
- Rule Severity:** A dropdown menu set to 'Low'.
- Rule Type:** Radio buttons for 'Permanent' and 'Temporary' (selected).
- Expiration Date:** A date picker set to 'Sep 25, 2024'.
- Note:** A small note: 'You can set the rule to expire any day within 6 months from today.'
- Next:** A button at the bottom right.

In dit scherm kunnen we de rule de volgende details geven:

- *De naam*
- *Description*
- *Rule severity (hoe ernstig de situatie is wanneer er een log match met deze rule)*
- *Rule type (Permanent or temporary)*

Als we deze velden hebben ingevuld kunnen we op next duwen, we krijgen volgend scherm te zien:

Create Custom Rule

Rule Details Condition Response Summary

Scope: Van Roey Automation - 020476 - Testomgeving / Please Select... ▾

Query Language: S1QL 1.0 ▾

Query Verification Edit query

Events
1 Start Hunting...

Back Next

In dit scherm kunnen we de query meegeven die de suspicious of malicious event gaat detecteren, we kunnen ook kiezen welke versie van S1QL we willen gebruiken en hoe groot de scope is van deze Rule.

Als je alles hebt geconfigureerd zoals je wilt klik je vervolgens weer op next en krijg je volgend scherm te zien:

Create Custom Rule

Rule Details Condition Response Summary

Active Response

When this rule matches a SentinelOne endpoint event, Storyline Active Response should:

Treat as a threat
If enabled, the Agent generates a threat from the alert and applies a selected policy.

Network Quarantine
If enabled, the system automatically quarantines the alerted endpoints.
You can reconnect the endpoints from the Sentinels page or Endpoint Details.

Back Next

In dit scherm kunnen we instellen wat er moet gebeuren wanneer er een event matcht met de rule. We hebben volgende opties:

- **Treat as threat**
 - Suspicious threat policy:
 - Behandelt mogelijk schadelijke bedreigingen met alerts, quarantaine of blocking.
 - Malicious threat policy:
 - Behandelt met zekerheid kwaadaardige bedreigingen met blocking, verwijdering of quarantaine.
- **Network quarantine**

Als je hier de gewenste Active response methode hebt gekozen, klik je op next en krijg je volgend scherm te zien:

Rule Details

Rule Name: fsqfq Rule Severity: Low Rule Type: Permanent
Expiration Date: No Expiration

Condition

Scope Hierarchy: Site Query Language: 1.0 Query Type: Events
Query: TgtFileExtension In AnyCase ("iso", "Ink", "txt", "csv") AND (TgtFilePath In Contains ("\\AppData\\Local\\Temp", "\\Downloads") AND (TgtFilePath Does Not Contain "Downloads.Ink" AND TgtFilePath Does Not Contain "Recent"))

Response

Treat as a threat: Suspicious Threat Policy

Activate rule immediately after saving

Back Save Draft

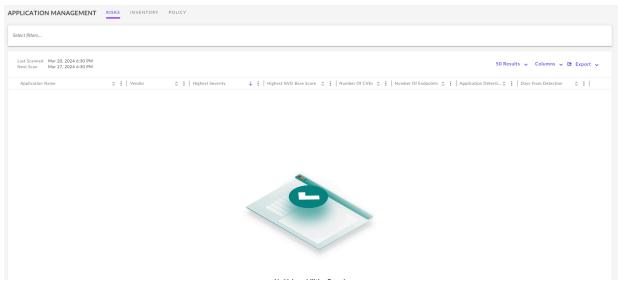
Dit scherm geeft je een overzicht van alle instellingen die je hebt gekozen zodat je deze nog kan nakijken voor je deze rule aanmaakt. We kunnen ook het vakje (Activate the rule immediately after saving) aanduiden zodat deze direct actief is na het creëren. Als alle settings kloppen voor jouw toepassing, kan je klikken op save draft en dan wordt deze rule gemaakt.

Applications



Application Management is een essentiële tool voor organisaties die hun applicatie security willen verbeteren en het beheer van hun applicatielandschap willen optimaliseren.

Als we hier op klikken komen we terecht in het application management panel waarin we risks (CVE's) kunnen zien die applications vormen op de agents.



Op dit scherm komen Risks tevoorschijn als deze er zijn.

Inventory

Wanneer we vanboven op inventory klikken krijgen we volgend scherm te zien:

APPLICATION MANAGEMENT				
RISKS				
INVENTORY				
Select filters...				
Scan Now Last Scanned: Apr 3, 2024 7:56 PM Next Scan: Apr 10, 2024 7:30 PM				
Name	Vendor	Number Of Versions	Number Of Endpoints	
7-Zip	Igor Pavlov	1	2	
Brave	Brave Software Inc	1	1	
DirectX 12	Microsoft	1	3	
Internet Explorer 11	Microsoft	1	3	
MDAC	Microsoft	1	3	
Microsoft 365 Apps for enterprise	Microsoft Corporation	1	2	
Microsoft Edge	Microsoft Corporation	2	3	
Microsoft Edge WebView2 Runtime	Microsoft Corporation	2	3	
Microsoft Intune Management Ext	Microsoft Corporation	2	3	
Microsoft Office Click to Run 2016	Microsoft	1	2	
Microsoft Office Click to Run - Mo	Microsoft	1	2	
Microsoft OneDrive	Microsoft Corporation	2	3	
Microsoft Update Health Tools	Microsoft Corporation	1	1	
Microsoft Visual Studio Tools for C	Microsoft	1	2	
Mozilla Firefox	Mozilla	1	1	
Mozilla Maintenance Service	Mozilla	1	1	

Hier zien we alle apps die aanwezig zijn op de verschillende endpoints binnen de site of group

Policy

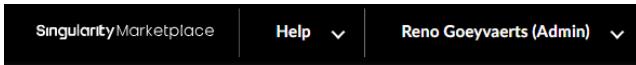
Wanneer we vanboven op policy klikken krijgen we volgend scherm te zien:

In dit scherm kunnen we volgende opties configureren:

- **Scan policy**
 - Vulnerability and Application scanning
 - Yes
 - No
- **Extensive Scan:**
 - geavanceerdere scan die betrouwbaardere resultaten geeft en heeft OS level vulnerability detection
 - Windows agents
 - Linux agents

Singularity marketplace

We kunnen naar de marketplace gaan door in de balk bovenaan het scherm op Singularity Marketplace te klikken:



Als we hierop klikken worden we naar een nieuw tabblad verwezen waarop volgend scherm te zien is:

The screenshot shows the Singularity Marketplace Catalog interface. At the top, there are tabs for 'Catalog' (which is selected), 'Installed integrations', and 'Collector configurations'. On the right, there are links for 'Reno Goevaerts' and 'Management console →'. Below the tabs, there's a search bar and filters for 'Capabilities', 'Vendors', and 'Categories'. The main area displays a grid of integration cards. Each card includes the vendor logo, name, and a brief description. The categories shown are Cloud Log, Ingestion, Threat Intel, IoT, Compliance, Email, Enrichment, and Partner Hosted.

Catalog

Hier zien we de catalog van alle ondersteunde integraties van SentinelOne, we kunnen filteren op de volgende categorieën:

- **Capabilities**
 - Automation
 - Enrichment
 - Ingestion
 - Sandbox
 - Alerts ingestion
 - partner hosted
- **Vendors**
 - Fortinet
 - Microsoft
 - Cisco
 - KnowBe4
 - Mandiant
 - AT&T Alien Labs
 - ...
- **Categories**
 - Zero Trust
 - ticketing
 - Sandbox
 - identity
 - threat intel
 - Siem
 - ...

Installed integrations

Wanneer we op installed integrations klikken krijgen we het volgend scherm te zien

The screenshot shows the 'Installed Integrations' section of the SentinelOne Catalog. It displays two integrations: 'Alien Labs OTX Enrichment' and 'Alien Labs OTX Sandbox'. The 'Alien Labs OTX Enrichment' card includes a description: 'Enrich threats with Alien Labs OTX intelligence'. The 'Alien Labs OTX Sandbox' card includes a description: 'Detonate threats from SentinelOne into Alien Labs OTX Sandbox for further analysis.' Navigation tabs at the top include 'Catalog', 'Installed integrations' (which is selected), and 'Collector configurations'.

Alien Labs OTX Enrichment

Hier zie je alle geïnstalleerde integraties en kan je door op een van de integraties te klikken, de instellingen van de integraties zien en eventueel wijzigen.

This screenshot shows the detailed view of the 'Alien Labs OTX Enrichment' integration. It includes the integration icon, name, vendor (AT&T Alien Labs), type (Threat Intel), and status (Installed). Below this, there's an 'Overview' section with a search bar, a scope dropdown set to 'Global / Van Roey Automation - 020476 - Testomgeving / Site - Van Roey Automation', and a 'View Logs' button. A note at the bottom indicates the last update was on March 15, 2024.

Als je klikt op view logs zie je alle achterliggende communicatie/ API calls van SentinelOne naar in dit geval Alien lab OTX.

This screenshot shows the 'View Logs' interface. It displays log entries for two successful API calls. The first entry is a 'Success (Status 200)' call made on March 27, 2024, at 08:47:10, with a trace ID of bf6eb70f-7371-48be-8884-3c6bd2e306c0. The second entry is another 'Success (Status 200)' call made on the same date and time. The interface includes a 'Scope of Access' dropdown and a 'C' icon for configuration.

Als je de integratie settings wilt bekijken of aanpassen kan je overal in het vak staan en klikken, voor de Alien Labs OTX Enrichment ziet dat er zo uit:

Simulation Mode

Run app in Simulation Mode (if checked, will ignore all other options)

Connection

API Token
.....

Response Actions

Options for triggering response actions (Note: URL Lookup and Hash Lookup Enrichments are automatic)

All Threats (Warning: Potentially disruptive to business operations) ▾

- Response Action: Kill
- Response Action: Quarantine
- Response Action: Remediate
- Response Action: Rollback
- Response Action: Disconnect from network
- Response Action: Add to Black list

Which scope to blacklist hash on?

Site ▾

We zien een aantal settings namelijk:

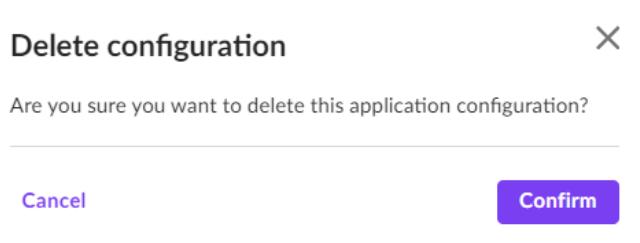
- **Simulation mode**
 - In het geval van alien labs kunnen we hier enrichments simuleren waardoor je kan zien hoe de integratie werkt
- **Connection**
 - API Token
- **Response actions**
 - Options for triggering response actions
 - no automated response
 - All threats
 - Malicious threats
 - When a threat is marked as a true positive
 - mogelijke response actions
 - Reponse action: kill
 - Reponse action: Quarantine
 - Reponse action: Remediate
 - Reponse action: Rollback
 - Reponse action: Disconnect from network
 - Reponse action: add to blacklist
 - Which scope to blacklist hash on
 - Global
 - Account
 - Site
 - Group

Deze settings zullen ook moeten ingesteld worden wanneer je de integratie installeert.

Om een integratie te verwijderen, klik je op het vuilbak icoontje.



Dit is het scherm dat je te zien krijgt als je op het vuilbakje klikt:



hier heb je de mogelijkheid om de deletion te cancellen of te confirmen.

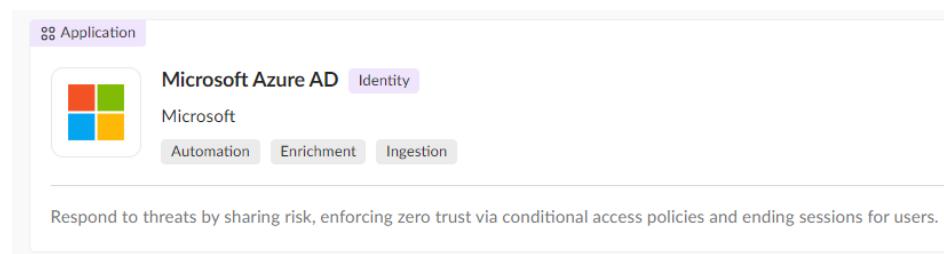
Collector configurations

De SentinelOne Collector (voorheen Scalyr agent) is een programma dat u op uw servers kunt installeren. Het verzamelt logs en systeemgegevens en uploadt deze naar SentinelOne. Deze nieuwe versie is makkelijk te installeren en beheren, en vereist weinig resources. De collector kan ook gebruikt worden voor de Docker containers of Kubernetes clusters.

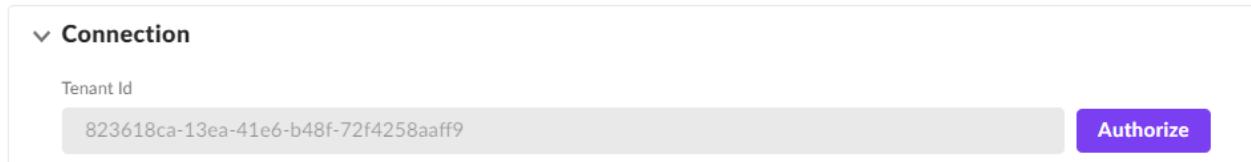
Ingestion Integrations

Op onze site binnen SentinelOne maken we gebruik van de Microsoft Azure AD en Microsoft: O365 integrations om de logs van het Microsoft platform naar SentinelOne te halen.

Microsoft Azure AD



Wanneer we de AD willen linken moeten we de connection met de tenant creëren. Dit doen we door op de paarse authorize button te klikken en de daaropvolgende stappen volgen.



Response actions hebben wij niet gebruikt omdat we veronderstellen dat het uitschakelen van accounts of iets dergelijks niet automatisch hoort te gebeuren.

We vullen de volgende velden in bij ingestion:

▼ Ingestion

A default parser for Azure AD data is used when you enable data ingestion. To use a different parser, enter the custom parser name.

Ingest Azure AD Threat Intelligence

Singularity Data Lake URL (Optional)

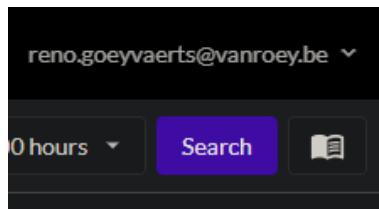
https://xdr.eu1.sentinelone.net/events?view=edr&theme=singularity&teamToken=6zXttBRpQqKoVkuBYaaXHA--

Singularity Data Lake API Token (Optional)

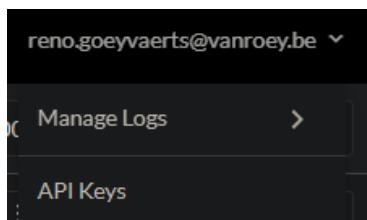
Use default parser (If checked, will ignore custom parser name)

Custom Parser Name (Optional)

De Singularity Data Lake API Token vind je in de Deep Visibility advanced view door op je account te klikken:



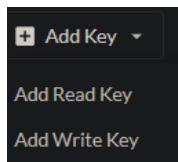
En vervolgens op API Keys:



Hier moet je kiezen voor een write Log Access Key:

Log Access Keys		
For 28906_1747875680273502021@s1.oem		
Key Value	Name	Access
*****Z/VKRe0-	AZURE AD	Write
*****NMJUYYs-	Initial key	Read
*****E3CvQUE-	app:azure-zero-trust-threats	Write
*****eugibd8-	app:microsoft	Write
*****0f/F9zg-	o365	Write

Je kan de initial key kiezen die ik in dit geval AZURE AD heb genoemd of zelf een key toevoegen door op Add Key te duwen en te kiezen voor Add Write key: :



Wanneer je deze key hebt ingevuld, klik je onderaan het scherm op install.

Om te kijken of de integratie werkt (wacht een aantal minuten) moeten we opnieuw naar Deep Visibility scherm wel bepaald naar de XDR view:

A screenshot of the Singularity Data Lake XDR view. The top navigation bar shows 'Singularity Data Lake' and 'Van Roey Automation - 020476 - Testomgeving'. The main area has tabs for 'XDR' and 'Logs'. A search bar is present. On the left, there are sections for 'PRODUCTS' (All, 3 items) and 'FIELDS' (Filter fields). The central area displays a summary: '23,013 matching events' over '5 minutes / bar', with an option to 'Expand Graph'. Below this, there's a large purple bar representing the event count.

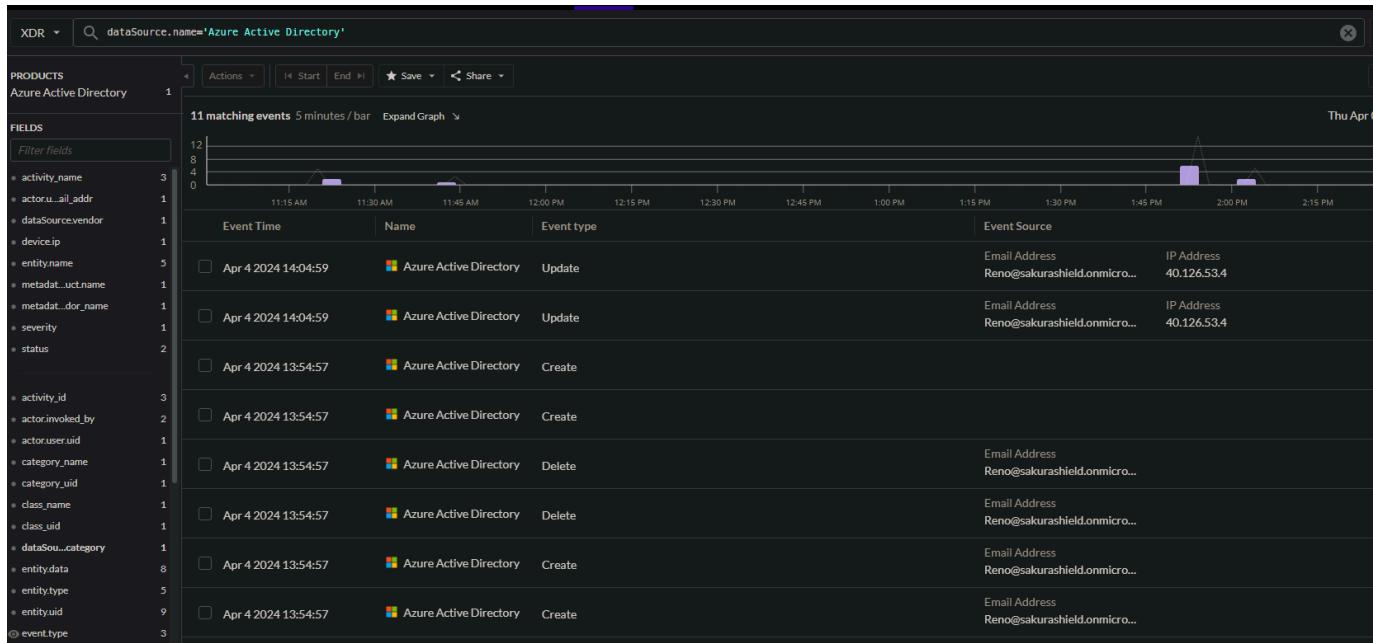
Je ziet de tab Products en klikt hierop, je krijgt volgende opties:

A screenshot of a 'PRODUCTS' modal. It shows a table with columns: Product, Filter, and # Approx. The products listed are: Azure Active Directory (~11), Microsoft O365 (~368), and SentinelOne (~22634). Each row has a checkbox next to it.

We kiezen voor Azure Active Directory:

A screenshot of the search bar. The filter input field contains the text 'dataSource.name="Azure Active Directory' in green. To the right of the search bar are buttons for 'Last 4 hours', 'Search', and a refresh icon.

We kunnen voor we zoeken naar de Active Directory logs nog de tijdspanne van de filter bepalen als dit gebeurd is klik je op search:



Microsoft: O365

Microsoft: O365 **Cloud Logs**

Microsoft

Ingestion

One-click collection of parsed Microsoft O365 logs

Om Office 365 logs in SentinelOne data lake te krijgen moet je een app registreren binnen Entra ID.
Je gaat naar het Entra ID panel binnen Azure en zoekt in het manage menu naar App Registrations

The screenshot shows the Microsoft Entra ID for workforce portal. At the top, there's a navigation bar with 'Home >' followed by the title 'VRA - Stage - Mic' and the subtitle 'Microsoft Entra ID for workforce'. Below the title is a sidebar with several sections: 'Overview' (indicated by a blue info icon), 'Preview features' (indicated by a plus sign icon), 'Diagnose and solve problems' (indicated by a wrench icon), 'Manage' (with a gear icon), and a list of items under 'Manage': 'Users' (person icon), 'Groups' (people icon), 'External Identities' (key icon), 'Roles and administrators' (person icon), 'Administrative units' (dotted box icon), 'Delegated admin partners' (key icon), 'Enterprise applications' (globe icon), 'Devices' (monitor icon), and 'App registrations' (grid icon). The 'App registrations' item is highlighted with a dashed blue border.

We klikken vervolgens op New registration:

The screenshot shows the 'App registrations' page. At the top, there's a header with several buttons: '+ New registration' (blue plus icon), 'Endpoints' (globe icon), 'Troubleshooting' (gear icon), 'Refresh' (refresh icon), 'Download' (down arrow icon), 'Preview features' (blue square icon), and a search bar. Below the header is a message box with an info icon: 'Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)'. Underneath the message box are three tabs: 'All applications' (gray), 'Owned applications' (underlined in blue), and 'Deleted applications' (gray). To the right of the tabs is a search bar with the placeholder 'Start typing a display name or application (client) ID to filter these r...' and a 'Add filters' button. A green cursor arrow points to the 'Owned applications' tab.

Hier kies je een naam en moet je geen andere dingen instellen.

Home > VRA - Stage - Microsoft S1/Defender | App registrations >

Register an application

Name
The user-facing display name for this application (this can be changed later).
o365

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (VRA - Stage - Microsoft S1/Defender only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the Microsoft Platform Policies [\[?\]](#)

Register

Nu kom je op het panel van de app, hier klikken we op client credentials:

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: test	Client credentials	: Add a certificate or secret
Application (client) ID	: fa09d2f9-c9bd-4016-a591-d204af85bb0f	Redirect URIs	: Add a Redirect URI
Object ID	: 07986e4c-caa0-49d5-b094-8857b200a14a	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 823618ca-13ea-41e6-b48f-72f4258aaff9	Managed application in ...	: test
Supported account types	: My organization only		

Hier klikken we op New client secret:

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
No client secrets have been created for this application.			

Je kan kiezen om de secret een description te geven maar dit moet niet, we klikken onderaan het panel op add:

Add a client secret

Description

Expires

De Value van de Secret kopieer je;

Certificates (0)	Client secrets (1)	Federated credentials (0)
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.		
+ New client secret	Description	Expires
	Password uploaded on Thu Apr 04 2024	10/1/2024
		Value ⓘ
		F068Q~itD85jfnB9XTK6E.Se3yFNEnW0st... Copy

Deze value plak je in het secret veld:

▼ Connection

* Tenant ID
823618ca-13ea-41e6-b48f-72f4258aaff9

* Application (Client) ID
bb626089-3253-4795-b83f-635d9bb59979

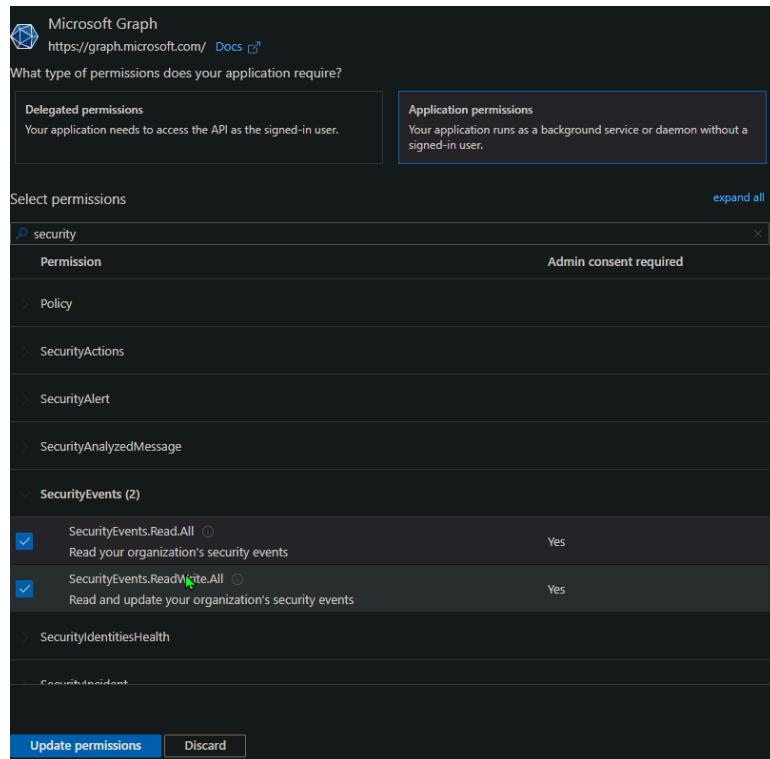
* Client Secret
.....

Nu gaan we terug naar het overview veld van de app en kopiëren we de Tenant ID en de Application Client ID ook:

^ Essentials	
Display name	: test
Application (client) ID	: fa09d2f9-c9bd-4016-a591-d204af85bb0f
Object ID	: 07986e4c-caa0-49d5-b094-8857b200a14a
Directory (tenant) ID	: 823618ca-13ea-41e6-b48f-72f4258aaff9

Vervolgens moeten we binnen de app de volgende stappen ondernemen:

1. *Klik aan de linkerkant op API Permissions.*
2. *Klik +Add a permission*
3. *Klik op Microsoft Graph, klik op Application permissions, selecteer dezelfde instellingen zoals in de screenshot*



4. *Klik vervolgens op Update permissions*
5. *Klik nu op Add a permission*
6. *Klik op de Office 365 Management APIs*



7. Klik op Application permissions, selecteer dezelfde instellingen zoals in de screenshot

The screenshot shows the 'Request API permissions' interface. At the top, there's a header with the title 'Request API permissions' and a close button. Below the header, there are two sections: 'Delegated permissions' and 'Application permissions'. The 'Delegated permissions' section is described as 'Your application needs to access the API as the signed-in user.' The 'Application permissions' section is described as 'Your application runs as a background service or daemon without a signed-in user.' Under the 'Select permissions' heading, there's a search bar with placeholder text 'Start typing a permission to filter these results'. A table lists permissions under categories: 'ActivityFeed (2)' and 'ServiceHealth (1)'. The permissions listed are:

Permission	Admin consent required
ActivityFeed.Read (Read activity data for your organization)	Yes
ActivityFeed.ReadDlp (Read DLP policy events including detected sensitive data)	Yes
ServiceHealth.Read (Read service health information for your organization)	Yes

At the bottom of the screen are two buttons: 'Add permissions' and 'Discard'.

8. Klik vervolgens op Add permissions

9. Als laatste moeten we nog klikken op Grant admin consent for

The screenshot shows the 'Configured permissions' page. The title is 'Configured permissions' and it states: 'Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. Click here to grant admin consent for all the permissions the application needs.' Below this, there are two buttons: '+ Add a permission' and 'Grant admin consent for VRA - Stage - Microsoft S1/Defender'.

Nu moeten we de Ingestion tab nog invullen:

▼ **Ingestion**

A default parser for Microsoft data is used when you enable data ingestion. To use a different parser, enter the custom parser name

- Ingest Microsoft Security Alerts
- Ingest Azure Active Directory Audit Exchange
- Ingest Exchange Audit
- Ingest SharePoint Audit Logs
- Ingest DLP Audit Logs
- Ingest Teams Audit Logs

Skylight URL (Optional)

Skylight API Token (Optional)

- Use default parser (If checked, will ignore custom parser name)

Custom Parser Name - Management API (Optional)

Custom Parser Name - Graph API (Optional)

Als dit allemaal gebeurd is kunnen we onderaan dit scherm op install klikken:

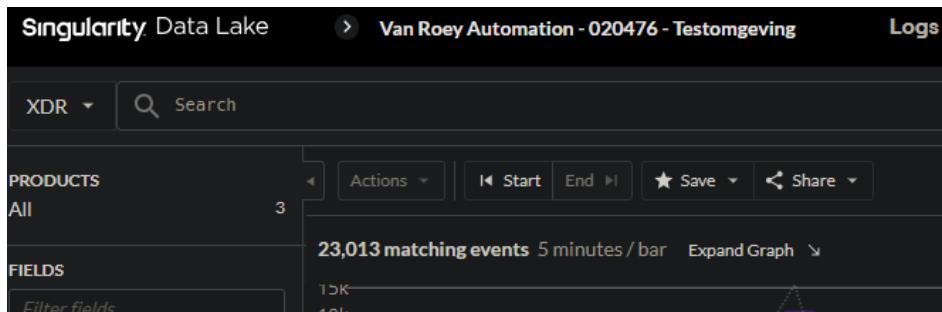
▼ **Connection**

* Tenant ID

* Application (Client) ID

* Client Secret

Om te kijken of de integratie werkt (wacht een tiental minuten) moeten we opnieuw naar Deep Visibility scherm wel bepaald naar de XDR view:



Je ziet de tab Products en klikt hierop, je krijgt volgende opties:

Product	Filter	# Approx
Azure Active Directory	= !=	~11
Microsoft O365	= !=	~368
SentinelOne	= !=	~22634

We kiezen voor Microsoft O365:

We kunnen voor we zoeken naar de Active Directory logs nog de tijdspanne van de filter bepalen als dit gebeurd is klik je op search:

Event Time	Name	Event type	Event Source
Apr 4 2024 16:19:49	Microsoft O365	Search	
Apr 4 2024 16:17:49	Microsoft O365	Search	
Apr 4 2024 16:16:03	Microsoft O365	Search	
Apr 4 2024 16:14:02	Microsoft O365	Search	
Apr 4 2024 16:12:01	Microsoft O365	Search	
Apr 4 2024 16:10:02	Microsoft O365	Search	
Apr 4 2024 16:07:59	Microsoft O365	Search	
Apr 4 2024 16:07:03	Microsoft O365	Update Service Principal	
Apr 4 2024 16:07:03	Microsoft O365	Update Application	
Apr 4 2024 16:06:00	Microsoft O365	Search	
Apr 4 2024 16:03:59	Microsoft O365	Search	

VirusTotal Threat Enrichment

Deze integratie is gelijk aan die van alienlab, de integratie geeft extra informatie over de threat en er kan ook ingesteld worden dat er vanaf een bepaalde reputation score response actions moeten genomen worden.

Global / Van Roey Automation - 020476 - Testomgeving / Site - Van Roey Automation X

Connection

* API Token

Response Actions

Options for triggering response actions (Note: Enrichment is automatic)

All Threats (Warning: Potentially disruptive, testing advised) ▾

VirusTotal reputation score above which response actions to be taken (-100 to 100)?
100

What is minimum number of VirusTotal 'malicious' votes above which response actions to be taken?
1

Response Action: Kill
 Response Action: Quarantine
 Response Action: Remediate
 Response Action: Rollback
 Response Action: Disconnect from network
 Response Action: Add to Black list

Which scope to blacklist hash on?
Site ▾

We zien een aantal settings namelijk:

- **Simulation mode**
 - In het geval van alien labs kunnen we hier enrichments simuleren waardoor je kan zien hoe de integratie werkt
- **Connection**
 - API Token
- **Response actions**
 - Options for triggering response actions
 - no automated response
 - All threats
 - Malicious threats
 - When a threat is marked as a true positive
 - mogelijke response actions
 - Reponse action: kill

- Reponse action: Quarantine
- Reponse action: Remediate
- Reponse action: Rollback
- Reponse action: Disconnect from network
- Reponse action: add to blacklist
- Which scope to blacklist hash on
 - Global
 - Account
 - Site
 - Group

Dit is hoe het eruit ziet in het threat details panel:

 **VirusTotal Threat Enrichment**
Apr 11, 2024 09:32:55

Behaviour Summary

Verdicts: MALWARE, STEALER, TROJAN, EVADER
Verdict Confidence: 84%

Latest Analysis Stats:

- Unsupported: 4
- Failure: 2
- Malicious: 34
- Undetected: 33

Associated Attack Techniques: ['T1047', 'T1036', 'T1562.001', 'T1497', 'T1027', 'T1027.002', 'T1003', 'T1056', 'T1552.002', 'T1012', 'T1518.001', 'T1057', 'T1018', 'T1016', 'T1083', 'T1082', 'T1114', 'T1005', 'T1573', 'T1571']

Note: 20/22 attack techniques listed above

File report:

- md5: dcaa4a1413159147caa274e74ea94977
- sha256: 19cf625d4d50e2104dd254bb8596a316dbe8dbbba51d92dd77f4c
- sha1: 329d6a499428bb158fb8d411f183d1ab42fc37b9
- Magic: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Alien labs OTX Sandbox

Deze integratie maakt ook gebruik van de Alien labs API token om de malicious of suspicious file naar hun sandbox te sturen om op deze manier een beeld te krijgen van wat voor impact de file zou hebben gehad op het systeem moest Sentinel hier niet tussen gekomen zijn.

Global / Van Roey Automation - 020476 - Testomgeving / Site - Van Roey Automation



* API Token

* Download Threat File Zip Password

Hier heb we 2 instellingen die we kunnen configureren:

- API token
- Threat file download password

Het password dat je hier invult moet hetzelfde password zijn dat je invult in het threat details window bij de threat download feature.

Automation



Deze functie binnen SentinelOne kan uw security-team helpen om efficiënter en effectiever te werken.

Wanneer je op automation hebt geklikt binnen het control panel krijgen we volgend scherm te zien:

The screenshot shows the 'AUTOMATION' tab selected in the top navigation bar. Below it, the 'TASKS' tab is active. The main area displays a table with one item. The columns include Task Name, Description, Initiated By, Initiated Time, Total In Current Scope, Completed, Failed, Pending, Pending User Action, and Expired. The single task listed is 'Remote Script' initiated by 'Reno Goeyvaerts' on 'Mar 27, 2024 10:56:43'. It has 1 completed action, 0 failed actions, 0 pending actions, and 0 pending user actions. The 'Completed' column shows a green checkmark icon.

Tasks

In de tasks tab die hierboven te zien is kan je de actions zien die zijn uitgevoerd op de endpoints. Je krijgt ook nog extra informatie te zien over de task namelijk:

- *Description*
- *Initiated by*
- *Initiated time*

- *Total in current scope*
- *Completed, failed, pending, expired*
- *Pending user action*
- *In progress, Scheduled, partially completed, Canceled*

Script Library

De Script Library bevat een breed scala aan scripts die u kunt gebruiken om uw endpoints efficiënter en effectiever te beheren. De library bevat scripts voor:

1. *Artifact collection*
 - a. Forensic file fetch
2. *Data collection*
 - a. Get Services
 - b. Get local services
 - c. Get Installed apps
 - d. Bash history
 - e. ...
3. *Action*
 - a. Download file
 - b. Start process
 - c. Disable Local user
 - d. Move File
 - e. ...

Reports



Deze functie binnen SentinelOne maakt het mogelijk om rapporten te genereren bestaand uit de 6 verschillende content mogelijkheden.

REPORTS										Load Report Task	
New Report Task	Delete Selection	No Items Selected								<input type="button" value="Load"/>	<input type="button" value="Report"/>
Date	Name	Scope	Site Name	Frequency	Interval	Status					
Mar 28, 2024	DANGER	Account	N/A	N/A	Last 30 days	Ready to download	<input type="button" value="Download PDF"/>	<input type="button" value="Download HTML"/>			

Wanneer we een Report willen genereren duwen we op de “New Report Task button” en krijgen we volgend scherm te zien:

The screenshot shows a configuration form for a new report task. At the top, there are fields for 'Report name *' (with placeholder 'Enter report name...') and 'Report content *' (with placeholder 'Select insight*'). Below these are sections for 'Frequency' (radio buttons for 'One-time report' and 'Scheduled report', with 'One-time report' selected) and 'Interval' (radio buttons for 'Last 30 days' and 'Manual', with 'Last 30 days' selected). A date selector dropdown is also present. At the bottom right are 'Next' and 'Quit' buttons.

Hier hebben we een aantal dingen die we kunnen instellen:

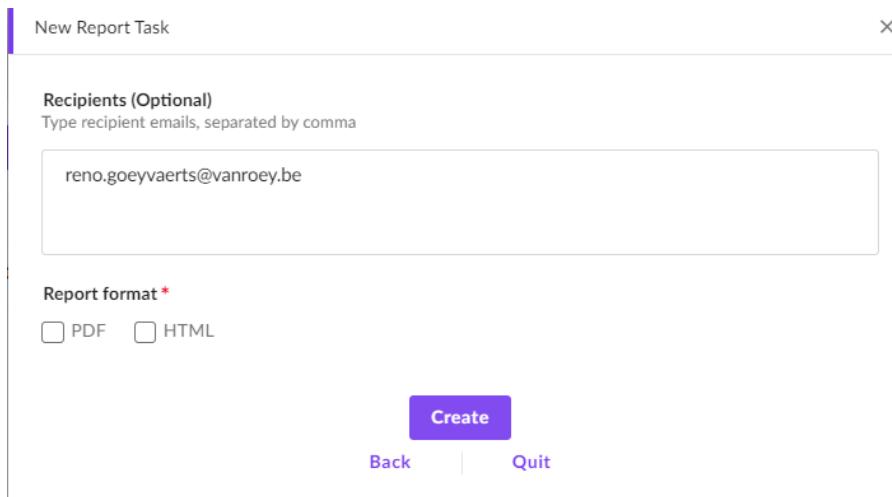
- **Report name**
- **Report content**
 - Executive Insights
 - Executive Insights by group
 - Mitigation and Response Insights
 - Application Insights
 - Threats Insights
 - Vigilance insights
- **Frequency**
 - One-time report
 - Scheduled report
 - Wekelijks op een gespecificeerde dag
 - Elke eerste dag van de maand

Wanneer we dit hebben ingesteld mag je op next duwen en krijgen we dit scherm te zien:

The screenshot shows the same configuration form as before, but with a 'Recipients (Optional)' section at the top. It includes a placeholder 'Enter email addresses...' and a 'Create' button at the bottom right.

Wanneer we dit leeg laten kunnen we gewoon op create duwen en wordt het rapport gemaakt.

Wanneer we een mailadres invullen krijgen we de volgende keuze voor het bestandsformaat van het rapport:



Als we een van deze formaten hebben gekozen kunnen we op create duwen en wordt het rapport gemaakt.



[You don't often get email from noreply@mailsender.sentinelone.net. Learn why this is important at <https://aka.ms/LearnAboutSenderIdentification>

A new report was generated at: Thu 28, Mar 2024 15:06:25.

Report Name: TEST

Report Period:

From: Tue 27, Feb 2024

To: Thu 28, Mar 2024

This report was originally created by: Reno Goeyvaerts You have received this email because the report creator added you to the recipients list.

Activity



Binnen activity kunnen we alle acties die binnen het SentinelOne platform gebeuren zien als logs en deze filteren op verschillende criteria.

Hieronder zie je de activity page:

The screenshot shows the Microsoft Defender XDR Activity Log page. At the top, there are several filter dropdowns: Malware, Mitigation, Threat Management, Exclusion, Operations, Administrative, and Detection Rules. Below these are two search input fields: 'User Email' and 'Endpoint Name'. The main area is titled 'Activity Log' and displays a list of events. Each event has a timestamp, a small icon, and a detailed log entry. For example, one event on Mar 28, 2024, at 16:00:18, is described as 'Application Microsoft: O365, ID: 1916023074749722968 : Application was disabled automatically by app platform because of error.' Another event on the same day at 16:00:18 shows an 'ERROR' message related to authentication. The log continues with more entries, including ones from March 29, 2024. At the bottom right of the log area, there is a page navigation bar with numbers 1 through 10.

Hierin kunnen we de volgende soorten filters en hun sub filtercriteria bekijken :

- **Malware**
 - Mitigated
 - Cloud marked as threat
 - New custom rule alert
 - Not mitigated
 - ...
- **Mitigation**
 - Kill
 - Network Quarantine
 - Remove Macro's
 - Rollback
 - ...
- **Threat management**
 - Confidence level change
 - Incident status
 - XDR actions
 - Notes
 - ...
- **Exclusion**
 - Cloud blocklist
 - Cloud hash exclusion
 - New / edit blocklist
 - Updated IDR exclusion
 - ...
- **Operations**
 - 2FA - Configured
 - Account administration

- Firewall traffic
- Live updates
- ...
- ***Administrative***
 - Agent decommissioned
 - System update
 - Uninstall
 - On-Demand disk scan
 - ...
- ***Detection Rules***
 - Detection rule: deleted
 - Detection rule: expired
 - Detection rule: edited
 - New detection rule
 - ...
- ***User Email***
 - Zoekveld
- ***Endpoint Name***
 - Zoekveld

API

De SentinelOne REST API stuurt verzoeken naar uw Management Server en reageert met gegevens die van de Agents komt of uit de management database heeft gehaald.

De API kan gebruikt worden om de hele omgeving binnen SentinelOne op een programmatische manier te beheren.

Voor API DOCS binnen de VanRoey kan u deze [link](#) gebruiken en als u wilt gebruik maken van een al op voorhand gemaakte requests kan u deze Postman collection gebruiken [link](#).

Om deze API te kunnen gebruiken heb je een API TOKEN nodig, deze kan jezelf genereren in het control panel.

Dit doe je door op je username te klikken wanneer je in het control panel bent:



Vervolgens te klikken op my user:

My User

Als we hierop hebben geklikt krijgen we volgend scherm te zien:

Reno Goeyvaerts

Actions

Full Name: Reno Goeyvaerts
Email: reno.goeyvaerts@vanroey.be
Created at: Mar 14th 2024
Role: Admin
API Token: N/A

Scope of Access

Van Roey Automation - 020476 - Testomgeving Admin

We klikken vervolgens op actions:

Actions

Edit User Details

Change My Password

Resend Onboarding Email

API Token Operations ▶

Clear Preferences

Vervolgens op API Token Operations:

Block API Token Generation

Allow API Token Generation

Generate API token

Wanneer je klikt op Generate API Token word je geprompt voor je 2FA code:

Authentication Required

x

You must re-authenticate to perform protected actions.

The authentication is valid for 30 minutes.

Two-Factor Authentication Code

[Cancel](#)

[Confirm Action](#)

Wanneer je deze hebt ingevuld krijg je volgend scherm te zien:

API Token for Reno Goeyvaerts

x

 This is the last time you can see this token.

API Token:

[REDACTED]

This API token will expire in 31 days, on May 2, 2024 08:55

 [Copy API Token](#)

[Close](#)

Je hebt nu de API Token voor je user en je kan nu gebruik maken van de SentinelOne API.

MICROSOFT DEFENDER XDR

Microsoft Defender implementatie vereist relatief weinig configuratie als er al gebruik wordt gemaakt van Intune. Dit wordt gedaan door middel van een service-to-service verbinding tussen Intune en Microsoft Defender.²

Om Microsoft Defender vervolgens in te stellen, zal je in Intune onder "Microsoft Defender for Endpoint" in "Endpoint Security" zorgen dat Intune het recht heeft om endpoint security configuration profiles aan/toe te passen.

Hier duid je ook aan dat Windows 10 en hoger geconnecteerd kunnen worden met Microsoft Defender for Endpoint.

The screenshot shows the Microsoft Intune admin center interface. On the left, there is a navigation sidebar with various options like Home, Dashboard, All services, Devices, Apps, and Endpoint security (which is highlighted with a red box). Below that are sections for Reports, Users, Groups, Tenant administration, and Troubleshooting + support. Under the Endpoint security section, there's a sub-section for Microsoft Defender for Endpoint (also highlighted with a red box). The main content area is titled "Endpoint security | Microsoft Defender for Endpoint". It includes a search bar, refresh, save, discard, and delete buttons. A note states: "The Microsoft Defender for Endpoint connector is active for Windows but a risk assessment is not included in a compliance policy for these platforms. To protect devices on these platforms, click here to set up a compliance policy with the Machine Risk Score settings configured in the Microsoft Defender for Endpoint section." Below this is a section titled "Endpoint Security Profile Settings" with a switch for "Allow Microsoft Defender for Endpoint to enforce Endpoint Security Configurations" which is set to "On" (highlighted with a red box). There are also sections for "Compliance policy evaluation" with switches for connecting Android, iOS/iPadOS, and Windows devices, all set to "On" (highlighted with red boxes). Other settings include "Enable App Sync (sending application inventory) for iOS/iPadOS devices" and "Send full application inventory data on personally owned iOS/iPadOS devices", both set to "Off".

In het Microsoft Defender portaal onder Instellingen > Endpoints > Enforcement scope duid je aan dat MDE de security instellingen uit Microsoft Intune gebruikt. De verbinding van Intune naar Microsoft Defender for Endpoint zorgt dat de apparaten automatisch op het Microsoft Defender portaal te zien zijn.

² 'Configure MDE in Intune', microsoft.com

Verder is er ook nog een Windows Autopilot Deployment profile aangemaakt. Hiermee wordt de deployment methode bepaald en kan de out-of-box-experience voor de eindgebruiker aangepast worden. Dit kan gedaan worden in Intune onder Devices > Windows > Windows Enrollment > Deployment profiles.

Security Baseline

In Intune onder endpoint security is er een aanpassing aangebracht binnen de security baseline. Onder Microsoft Defender for Endpoint baseline is er een nieuw profiel gemaakt. Hier wordt er verteld aan een specifieke groep gebruikers en

apparaten welke security configuratie er toegepast moet worden. Veel van deze instellingen zijn door Microsoft zelf al ingesteld. Wij zijn er nog is doorgaan en hier en daar wat zaken aangepast naar wat ons beter/interessant leek.

Security Baselines	Version
Security Baseline for Windows 10 and later	November 2021
Microsoft Defender for Endpoint Baseline	Version 6
Security Baseline for Microsoft Edge	Version 117
Windows 365 Security Baseline	November 2021
Microsoft 365 Apps for Enterprise Security Bas	Version 2306

Binnen deze baseline zijn er, zoals eerder vermeld, instellingen waar aanpassingen in gemaakt zijn. Volgende instellingen zijn ter beschikking binnen deze baseline:

- **Attack Surface Reduction Rules**
 - Hiermee wordt ervoor gezorgd dat de eindgebruiker een beperkter aanvalsoppervlak heeft. Dit wordt voornamelijk bereikt door bijvoorbeeld ervoor te zorgen dat verschillende functies binnen Microsoft Office-applicaties geblokkeerd worden. Ook wordt er een algemene netwerkbeschermingsregel ingesteld. Deze helpt eindgebruikers te beschermen tegen phishing-scams, kwaadaardige inhoud en dergelijke. Dit zijn slechts enkele voorbeelden; er worden nog meer maatregelen toegepast.
- **BitLocker**
 - Met BitLocker wordt ervoor gezorgd dat alle informatie die opgeslagen is, geëncrypteerd wordt.
- **Device Guard**
 - Device Guard biedt drie grote componenten: Configurable Code Integrity, VSM Protected Code Integrity en Platform and UEFI Secure Boot. Deze drie componenten werken samen om ervoor te zorgen dat alleen vertrouwde code wordt uitgevoerd vanaf het opstarten. Ze controleren of de boot binaries en firmware digitaal ondertekend zijn. Daarnaast worden belangrijke onderdelen van het systeem verplaatst naar een veilige omgeving voor extra bescherming tegen aanvallen.³
- **Device Installation**
 - Aan de hand van Hardware ID's kan je hier meegeven welke fysieke apparaten hier geïnstalleerd of niet geïnstalleerd mogen worden.⁴
- **DMA Guard**

³ 'W10 Device Guard & Credential Guard Demystified', Microsoft.com

⁴ 'Policy CSP - DeviceInstallation', microsoft.com

- DMA Guard is een extra laag voor beveiliging tegen kwaadaardige externe apparaten met DMA (Direct Memory Access). DMA Guard zorgt ervoor dat deze apparaten alleen toegang krijgen tot het geheugen dat voor hen is toegestaan.⁵
- **Firewall**
 - Hiermee worden algemene firewall instellingen doorgevoerd. Hiermee wordt het risico op netwerkbeveiliging dreigingen verminderd.
- **Microsoft Defender**
 - Microsoft Defender instellingen kunnen hier in geconfigureerd worden. Zaken zoals het scannen van gedownloade bestanden en ingeplande systeem scans kunnen hier aangepast worden.
- **Smart Screen**
 - Smart Screen is een beveiligingstoepassing dat door bepaalde diensten wordt gebruikt. Hieronder valt onder andere Microsoft Edge. Het houdt zich vooral bezig met het scannen van bestanden, apps, browsers en e-mails.

Attack Surface Reduction

Met Attack Surface Reduction (ASR) kunnen we de plaatsen waar een eindgebruiker van een bedrijf kan worden aangevallen verkleinen. Dit kunnen we doen door aan device control te doen en attack surface rules toe te passen.

Device Control

Met device control kunnen we aansluitbare apparaten beheren door deze te blokkeren of toe te laten. Deze apparaten kunnen gevvaarlijk zijn wanneer ze aangesloten zijn op een apparaat van een eindgebruiker, server of dergelijke systemen. Denk maar aan een USB drive die ongewilde programma's kan installeren. Om dit in te stellen kan je binnen Microsoft Intune naar Endpoint Security gaan en onder Attack Surface Reduction een nieuwe policy aanmaken.

Met zo'n device control policy is het mogelijk om bepaalde rechten van apparaten toe te staan of te blokkeren. Wij hebben ervoor gezorgd dat alle removable storage geen write rechten hebben op de endpoints. Ook kunnen er uitzonderingen gemaakt worden waarbij je deze rechten bij één bepaalde removable storage wel toelaat.

⁵ 'Policy CSP - DmaGuard', microsoft.com

Attack Surface Reduction Rule

Verder zijn er ook attack surface rules beschikbaar. Met deze regels is het mogelijk om specifieke kenmerken van malware of vergelijkbare bedreigingen te blokkeren. Zo kun je bijvoorbeeld de executierechten van obfuscated scripts uitschakelen of het booten in Windows safe mode onmogelijk maken. Deze instellingen kunnen geconfigureerd worden op dezelfde locatie binnen Intune waar Device Control is ingesteld.

The screenshot shows the Microsoft Intune admin center interface. On the left, there's a sidebar with various security features like Antivirus, Disk encryption, Firewall, Endpoint Privilege Management, Endpoint detection and response, App Control for Business (Preview), Attack surface reduction, Account protection, Device compliance, and Conditional access. The 'Attack surface reduction' option is highlighted with a red box. The main content area is titled 'Endpoint security | Attack surface reduction' and shows a 'Create a profile' dialog. In this dialog, under 'Platform', 'Windows 10, Windows 11, and Windows Server' is selected. Under 'Profile', 'Attack Surface Reduction Rules' is selected. Below this, there's a section titled 'Attack Surface Reduction Rules' with a description: 'Attack surface reduction rules target behaviors that malware and malicious apps typically use to infect computers, including: Executable files and scripts used in Office apps or web mail that attempt to download or run files Obfuscated or otherwise suspicious scripts Behaviors that apps don't usually initiate during normal day-to-day work'. At the bottom of the dialog, there are buttons for 'Create Policy', 'Refresh', and 'Export'.

Zelf hebben wij Attack Surface Rules toegevoegd. In deze regel worden heel wat eigenschappen die wij zelf al een aantal keer hebben zien terugkomen tijdens het zoeken naar malware. Vandaar dat het ons belangrijk leek om deze zaken zeker toe te voegen:

- | | |
|--|---------|
| ● <i>Block adobe reader creating child processes</i> | Blocked |
| ● <i>Block execution of obfuscated scripts</i> | Blocked |
| ● <i>Block win32 API-calls from office macros</i> | Blocked |
| ● <i>Block office applications from creating executable content</i> | Blocked |
| ● <i>Block credential stealing from the windows local security auth subsystem (default: block)</i> | Blocked |
| ● <i>Block Office applications from injecting code into other processes</i> | Blocked |
| ● <i>Block rebooting machine in Safe mode</i> | Blocked |
| ● <i>Use advanced protection against ransomware</i> | Blocked |
| ● <i>Block executable content from email client and webmail</i> | Blocked |

Microsoft Defender Control Panel

Hoofd dashboard

Het Defender-portaal van Microsoft biedt verschillende dashboards aan. Het hoofd dashboard wordt weergegeven wanneer je het portaal opent. Hier worden verschillende aspecten getoond, waaronder een algemene beveiligings score, apparaten/gebruikers die als risico worden beschouwd, recente incidenten en meer.

Alerts en Incidents

Daarnaast biedt het Defender Portaal tal van andere onderdelen. Sommige van deze onderdelen worden kort vermeld op het hoofd dashboard. Zo zijn er aparte vensters voor alerts en incidenten. Een incident kan worden beschouwd als een reeks alerts die hoogstwaarschijnlijk met elkaar in verband zijn gebracht.

The screenshot shows the Microsoft Defender Incidents page. At the top, there's a search bar and various navigation icons. Below the header, the title 'Incidents' is displayed, followed by a subtitle 'Most recent incidents and alerts'. There are buttons for 'Export', 'Search for name or ID' (with a calendar icon), '1 Week' (with a dropdown arrow), and 'Customize columns'. A 'Filter set' section includes a 'Save' button and an 'Add filter' button. The main area lists five incidents with the following details:

Incident name	Tags	Severity
Exploit incident on one endpoint	19	Medium
'CVE-2017-11882' exploit malware was prev...		Low
Possible CVE-2017-0199/CVE-2017-11882 vu...		Medium
Malware incident on one endpoint	18	Informational
'Crysan' backdoor was prevented on one en...	17	Low

Als er meer informatie over zo'n incident gevonden moet worden, kan er op een van de alerts geklikt worden. Zo kan men alle relevante informatie hierover zien. Dit omvat zaken zoals het betrokken apparaat en de gebruiker, maar ook de volledige geschiedenis die heeft geleid tot de aanwezigheid van deze alert op het dashboard.

Om een nog meer gedetailleerd scherm, dat alle samenhangende elementen van dit incident bevat, te verkrijgen. Kan er op de incidentnaam zelf geklikt worden. Hiermee opent volgend scherm:

The screenshot shows the Microsoft Defender interface for an incident. The title is "'Casdet' malware was prevented on one endpoint'. The left sidebar has icons for Home, Protection, Threats, Assets, Investigations, Evidence and Response, and Summary. The main area has tabs for Attack story, Alerts (1), Assets (1), Investigations (1), Evidence and Response (1), and Summary. The 'Alerts' tab is selected, showing one alert from March 25, 2024, at 8:46 AM, which is new and labeled 'Casdet' malware was prevented. This alert is associated with the endpoint 'desktop-q6vopv2'. To the right is an 'Incident graph' showing a node for 'desktop-q6vopv2' connected by a dashed line to another node, with file hashes visible below it. Below the graph are buttons for Communication and Association.

Onder "Attack story" kan je het event dat de alert heeft getriggerd op chronologische volgorde opnieuw afspeLEN.

Aangezien er bij dit voorbeeld maar één alert aangemaakt wordt binnen het incident is er ook maar één entry in de attack story. Verder zijn er aparte tabs waarop je de bijbehorende alerts, assets, onderzoek (later meer hierover) en bijbehorend bewijs, zoals bestanden die mogelijk malware bevatten, kunt vinden. In de laatste tab wordt alles opnieuw verkort samengevat om het grote beeld nogmaals te schetsen.

Activity log

Ook wordt er een activity log per incident bijgehouden. Hier wordt elke input voor dit incident opgeslagen. Moest er iemand de status van het incident veranderen naar "Resolved", dan wordt dit in de activity log gezet. Ook is er de mogelijkheid om opmerkingen te plaatsen, zodat er meer verduidelijking kan meegegeven worden.

The screenshot shows the 'Activity log' section of the Microsoft Defender interface. At the top, there's a header 'Content: Audits, Comments'. Below it is a list of audit events:

- A comment from 'Robbe@sakurashield.onmicrosoft.com' dated Mar 29, 2024 at 8:48 AM: 'Test comment - Heyo :))'
- A determination change from 'Not available' to 'Malware' on Mar 29, 2024 at 8:47 AM by User Robbe@sakurashield.onmicrosoft.com
- A classification change from 'Not Set' to 'True positive' on Mar 29, 2024 at 8:47 AM by User Robbe@sakurashield.onmicrosoft.com
- An incident assignment to 'Robbe@sakurashield.onmicrosoft.com' on Mar 29, 2024 at 8:47 AM by User Robbe@sakurashield.onmicrosoft.com
- A status change from 'Active' to 'Resolved' on Mar 29, 2024 at 8:40 AM by App API Action

Below the list is a toolbar with icons for Normal, Bold, Italic, Underline, Strikethrough, and others. A text input field labeled 'Add comment' is also present.

Alert Management

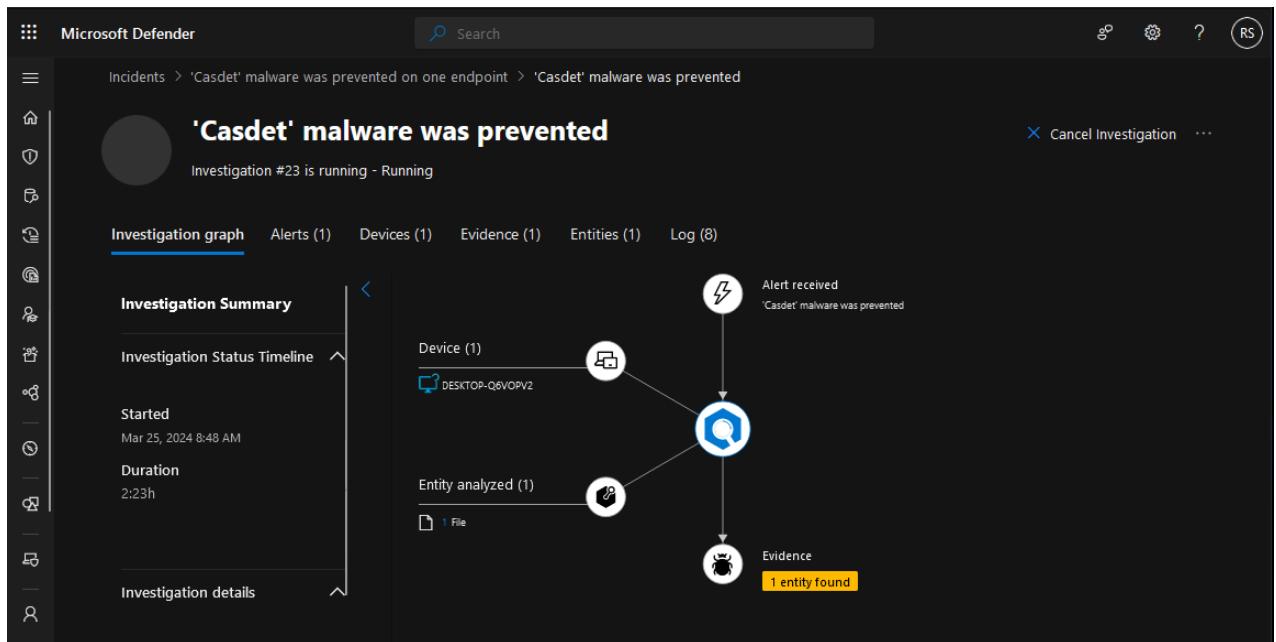
Wanneer er een nieuwe alert binnenkomt, dan kan deze gemanaged worden. Hierbij kunnen er allerlei gegevens worden meegegeven. Deze gegevens omvatten de alert status, de assigned user, de classification van de alert en eventuele commentaar. Elk van deze gegevens kunnen de volgende waarden verkrijgen:

- **Status**
 - New
 - Resolved
 - In progress
- **Assign to**
 - Assign uzelf of een andere gebruiker
- **Classification**
 - True positive
 - Informational, expected activity
 - False positive

Onder classification kan er specifiek aangeduid worden wat er dan bijvoorbeeld onder false positive, informational of true positive valt. Om hier een voorbeeld voor te geven kan je aanduiden of het ging om malicious user activity of een compromised account als het gaat over een true positive.

Automatic Investigation

Wanneer er een alert wordt aangemaakt binnen Microsoft Defender, wordt er ook automatisch een investigation op die alert uitgevoerd. Zo'n investigation ziet er als volgt uit:



Dit scherm heeft gelijkaardige functionaliteiten als het hiervoor besproken scherm van de incidenten, maar hier wordt bovenop nog extra analyses bij vrijgegeven. Terwijl alerts worden gemaakt en er een automatic investigation wordt uitgevoerd, wordt elk toepasselijk entry beoordeeld. Hieruit kunnen dan acties volgen die vervolgens ervoor zullen zorgen dat het eindsysteem beveiligd blijft. De beoordeling kan volgende output hebben:⁶

- Malicious
- Suspicious
- No threats found

Threat Hunting

Het portaal biedt ook de mogelijkheid om aan threat hunting te doen. Deze werkt aan de hand van queries die in KQL (Kusto Query Language) worden geschreven. Hiermee kunnen gebruikers bedreigingen opsporen en analyseren in de omgeving die wordt beschermd door Microsoft Defender. Door het schrijven en uitvoeren van deze queries kunnen verdachte activiteiten en patronen geïdentificeerd worden die mogelijk wijzen op een inbraak of een aanval. Threat hunting stelt gebruikers in staat om diepgaande analyses uit te voeren op endpoint gegevens, netwerkverkeer en andere bronnen om potentiële bedreigingen te kunnen vinden die anders mogelijk onopgemerkt zouden blijven. Hiermee kunnen organisaties hun beveiligingsmaatregelen versterken en snel reageren op potentiële bedreigingen, waardoor de kans op schade door cyberaanvallen wordt geminimaliseerd.

Community Queries

Microsoft Defender heeft een aantal kant en klare community queries die je kan gebruiken. Dit zorgt ervoor dat je gebruik kan maken van relatief moeilijke en tijdsabsorberende queries die al voor u zijn geschreven. Om hier een voorbeeld van te geven bestaat er een query dat de Microsoft Defender Antivirus Security Intelligence version, Engine version, Product

⁶ 'Overview of automated investigations', microsoft.com

version, Security Intelligence publish/build timestamp en de Security intel refresh timestamp opzoekt en nakijkt of deze up-to-date is per endpoint. De query en het uitvoeren van deze query ziet er als volgt uit:

The screenshot shows the Microsoft Defender Advanced hunting interface. On the left, there's a navigation pane with various categories like Lateral Movement, Network, Persistence, Privilege escalation, Protection events, Ransomware, TVM, and Troubleshooting. Under TVM, several queries are listed, including 'Detect CISA Alert' and 'devices_with_vuln...'. The main area is titled 'Advanced hunting' and shows a query editor with the following KQL code:

```

1 // This query will identify the Microsoft Defender Antivirus Security Intelligence version, Security Intelligence up to date value, ...
2 // This query was updated from https://github.com/Azure/Azure-Sentinel/tree/master/Hunting%20Queries/Microsoft%20365%20Defender/TVM%20
3 let expiringPublishDate = ago(8d);
4 DeviceTvmInfoGathering
5 | extend AvMode = iif(tostring(AdditionalFields.AvMode) == '0', 'Active', iif(tostring(AdditionalFields.AvMode) == '1', 'Passive', iif(
6 | extend AvIsSignatureUpToDateTemp = tostring(AdditionalFields.AvIsSignatureUpToDate), DataRefreshTimestamp= Timestamp,
7 AvIsPlatformUptodateTemp=tostring(AdditionalFields.AvIsPlatformUptodate),
8 AvIsEngineUptodateTemp = tostring(AdditionalFields.AvIsEngineUptodate),
9 AvSignatureDataRefreshTime = todatetime(AdditionalFields.AvSignatureDataRefreshTime),
10 AvSignaturePublishTime = todatetime(AdditionalFields.AvSignaturePublishTime),
11 AvSignatureVersion = tostring(AdditionalFields.AvSignatureVersion),
12 AvEngineVersion = tostring(AdditionalFields.AvEngineVersion),
13 AvPlatformVersion = tostring(AdditionalFields.AvPlatformVersion)
14 | extend AvIsSignatureUpToDate = iif((((isnull(AvIsSignatureUpToDateTemp)
15 or (isnull(AvSignatureDataRefreshTime))))
```

Below the query editor, there are tabs for 'Getting started', 'Results', and 'Query history'. The 'Results' tab is selected, showing a table with three items. The columns are: DeviceId, DeviceName, DataRefreshTimestamp, OSPlatform, AvMode, AvSignatureVersion, and AvIsSign. The data is as follows:

DeviceId	DeviceName	DataRefreshTimestamp	OSPlatform	AvMode	AvSignatureVersion	AvIsSign
5cc0833c94e5...	desktop-q6vopv2	Mar 22, 2024 2:07:21 PM	Windows11	Active	1.407.619.0	true
2773850802e5...	strong-vm	Mar 22, 2024 2:07:21 PM	Windows10	Active	1.407.619.0	true
c74643b48991...	werkend-balske2	Mar 22, 2024 2:07:21 PM	Windows10	Active	1.407.619.0	true

Custom Queries

Het gebruik van deze kant-en-klare queries kan enorm handig zijn, maar biedt niet altijd datgene waar iemand naar op zoek is. Vandaar is het ook mogelijk om eigen queries te schrijven in KQL en deze ook op te slagen. Voor testdoeleinden hebben we volgende query geschreven:

```

DeviceEvents
| where ActionType == "PowershellCommand"
| extend PowershellCommand=extractjson("$.Command", AdditionalFields, typeof(string))
| where PowershellCommand startswith "Invoke-WebRequest"
```

The screenshot shows the Microsoft Defender Advanced hunting interface. On the left, there's a sidebar with navigation icons and sections like 'PowerShell webrequest content', 'Schema', 'Queries' (which is selected), 'Shared queries', 'Suggested', 'My queries', 'Community queries', and 'Command and Control'. The main area has a search bar at the top. Below it, there's a 'Run query' button, a date range selector ('Last 7 days'), and options to 'Save', 'Share link', and 'Create detection rule'. A code editor window displays the following PowerShell-like query:

```

1 DeviceEvents
2 | where ActionType == "PowerShellCommand"
3 | extend PowershellCommand=extractjson("$.Command", AdditionalFields, typeof(string))
4 | where PowershellCommand startswith "Invoke-WebRequest"

```

Below the query editor, there are tabs for 'Getting started', 'Results' (which is selected), and 'Query history'. The results table shows one item found in 0:00:247, with a low priority (yellow). The columns are 'Timestamp', 'DeviceId', 'DeviceName', 'ActionType', and 'Int'. The single result row is: Mar 22, 2024 2:5... c74643b489913c7e9... werkend-bakske2 PowerShellCommand

Deze query zoekt in de log van apparaten naar PowerShell-commando's die beginnen met "Invoke-WebRequest". Dit commando wordt vaak gebruikt om web verzoeken te maken vanuit PowerShell. De query is handig voor het opsporen van mogelijk kwaadaardige activiteiten.

Voor testing-purposes werd telkens het volgende commando gebruikt: "(Invoke-WebRequest -Uri "<https://openphish.com/feed.txt>").Content"

We hebben wel gemerkt dat het gebruik van deze query enkel werkt voor powershell cmdlets die origineel vanuit powershell komen. Dit betekent dat wanneer het commando binnen lijn vier van bovenstaande query bijvoorbeeld gelijk is aan "curl", dan zal dit niet werken aangezien "curl" afkomstig is vanuit unix-based commandline tools en niet vanuit powershell zelf.

Submissions

Microsoft Defender biedt ook de mogelijkheid om e-mails, Teams-berichten, e-mailbijlagen, URL's, bestanden en door gebruikers gemelde gegevens door te sturen voor verder onderzoek. Deze verzoeken zullen door Microsoft zelf verwerkt en onderzocht worden. Dit kan bijvoorbeeld handig zijn als u iets heeft gevonden dat geen alert activeert, maar wat naar uw mening wel verdacht lijkt. Of andersom, een bestand dat volgens u volkomen veilig zou moeten zijn, maar dat voor één of andere reden gezien wordt als gevaarlijk.

Dit proces is zeer eenvoudig. Binnen "Actions & Submissions" onder "Submissions" wordt er de keuze gegeven om te kiezen tussen de mogelijke types van submissies die doorgestuurd kunnen worden. Moest er nu een bestand zijn doorgekomen waarvan u denkt dat deze wel gevaarlijk is, kan u via "Files" een nieuwe submissie aanmaken. Hiervoor drukt u op de "Add new submission" knop om deze nieuwe submissie aan te maken.

Submissions

Emails Teams messages Email attachments URLs **Files** User reported

Totals for past 30 days

Pending	Completed
0	0

Export **Add new submission** Refresh

Submission name	Submission ID

Hierna wordt een nieuw forum geopend met de vraag naar relevante gegevens die Microsoft nodig heeft vooraleer ze aan de analyse van het bestand kunnen beginnen. Hierin geef je dan vervolgens het bestand mee, de verwachte categorisering en hoe ernstig van belang de analyse is. Ten slotte is er ook de mogelijkheid om een extra beschrijving mee te geven.

Submit items to Microsoft for review

We will review and use your submission to update our detections. You'll be able to review our findings in the Submissions page. [Learn more about submissions.](#)

Select the submission type ^①

Files

// Render files with their respective remove buttons

No file uploaded

// File input component

Maximum file size is 500 MB. Use the password 'infected' to encrypt archive files.

NOTE: Submit only the specific files you want analyzed. Submitting an installer package or an archive with a large number of files may delay the analysis and cause your submission to be deprioritized.

This file should have been categorized as

Malware
 Unwanted Software
 Clean

Choose the priority

Low - bulk file or file hash submission
 Medium - standard submission
 High - need immediate attention (3 allowed per org per day)

Notes for Microsoft (optional)

Anything else you would like to add?

Deep Analysis

Zoals eerder werd aangehaald wordt er bij het aanmaken van een alert een automated investigation gestart. Hierbij worden heel wat gegevens verzameld. Binnen deze gegevens komen ook de bestanden te staan die met deze alert te maken hebben en eventueel extra bestanden die de automated investigation nog gevonden heeft. Deze bestanden worden gezien als "evidence". Op deze "evidence" kan er een deep analysis worden gestart. Hiermee kan het bestand in een beveiligde omgeving worden uitgevoerd. Hieruit wordt een rapport teruggegeven waar zaken zoals: de bezochte IP's,

uitgevoerde scripts en meer worden vermeld. Hierdoor krijgt men een bredere kennis over wat dit bestand inhoudt en mogelijk veroorzaakt kan hebben.

Niet zomaar elk bestand kan worden opgestuurd voor deep analysis. Het bestand met een portable executable (exe, dll bestand) zijn. Enkel hier kan er een correcte analyse op worden uitgevoerd.

Werking Deep Analysis

Om een bestand via deep analysis te analyseren ga je naar eerder welk alert. Dit alert gaat een automated investigation gestart hebben. Rechts kan je naar beneden scrollen om de details van de automated investigation te vinden. Om deze details te openen kan er op de investigation ID geklikt worden.

The screenshot shows the 'Automated investigation' details. It includes:

- Investigation ID:** 'Leonem' malware was prevented
- Investigation status:** Remediated
- Start time:** Apr 15, 2024 10:25:23 AM
- End time:** Apr 15, 2024 10:40:23 AM
- Duration:** 14:59m

Below this, there is a section titled 'Impacted assets' which is currently collapsed.

Onder "evidence" krijg je alle relevante bestanden te zien. Als tussen deze bestanden een portable executable zit en je hiervan meer informatie wilt kan je hierop klikken. Dit opent een extra venster rechts. Door op de drie bolletjes rechtsboven te klikken worden er meer opties getoond. Hiertussen zal "Deep analysis" staan.

The screenshot shows the file details for a file named **a40b613bca52ec196d6be4ac375d9076922b41c c4742c15a2ff1137bd6400eb7.exe**. The file was submitted for Deep analysis. The status is Success. The 'Deep analysis' option is highlighted with a blue border. Other options shown include:

- Open file page
- Manage indicator
- Download file
- Stop and Quarantine File
- Ask Defender Experts
- Manual actions
- Go hunt
- Deep analysis

Below the file name, there is a 'Detection' section showing VirusTotal detection ratio (43/70) and Malware detection (Trojan:Win32/Leonem.A).

Hier wordt de keuze gegeven door middel van een knop om dit bestand te submitten voor deep analysis.

The screenshot shows the Microsoft Defender Deep Analysis interface. At the top, it displays a file icon, the signer as 'Unsigned', and a size of '1.61 MB'. Below this, a navigation bar includes 'Overview', 'Incidents & Alerts', 'Observed in organization', 'File names', 'File content', and 'Deep Analysis' (which is underlined). A note below the navigation states: 'Submitting file to deep analysis collects the file from the device or from Microsoft sample store if the file already exists. Collecting the file can take up to 3 hours depending on file and device availability. The collected file is analyzed in a secured environment and a detailed report is created.' A blue 'Submit' button is located at the bottom left of this section.

De analyse zelf kan even duren. Microsoft claimt dat de analyse tot 15 minuten kan duren vooraleer deze tot een einde komt. Eens deze klaar is wordt er een rapport met alle gevonden activities, behavior, changes en meer die hiermee te maken hebben.

The screenshot shows the results page of the Microsoft Defender Deep Analysis. It starts with a green circular icon indicating 'Results available' and the text 'Latest available result: Apr 16, 2024 1:51 PM'. The 'Behaviors' section is expanded, showing a table for 'Environment Awareness' with one row:

Time	Process [PID]	Target	Details	Result
Apr 16, 2024 1:47 PM	[no name].exe [3332]	HKEY_LOCAL_MACHINE\System\CurrentCont...	BRWARR	Success

The 'Observables' section is collapsed, showing the message 'No dropped files or network communications were observed'. A blue 'Resubmit' button is located at the bottom left of this section.

Device Response Actions

In Defender is het mogelijk om bepaalde acties per device handmatig uit te voeren of te starten. Hierdoor kunnen bepaalde acties snel uitgevoerd worden op apparaten. Volgende acties kunnen handmatig gestart worden op individuele apparaten:

- Manage tags
- Initiate Automated Investigation
- Initiate Live Response Session
- Collect investigation package
- Run antivirus scan
- Restrict app execution
- Isolate device
- Contain device
- Consult a threat expert

- Action center

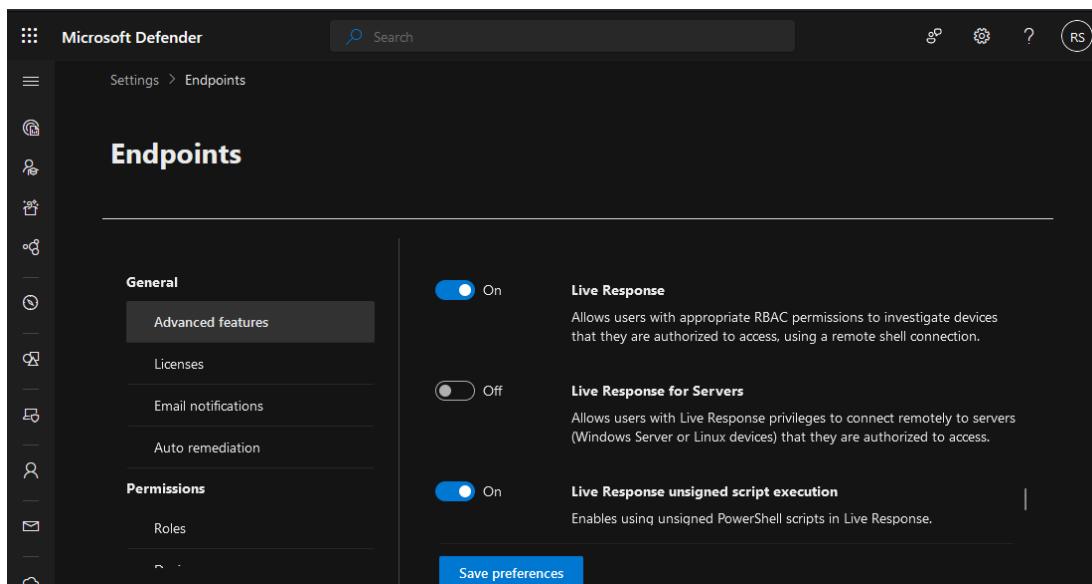
Dit zijn de mogelijkheden voor een P2 licentie van Defender. Bij een P1 licentie zijn er slechts vier acties mogelijk. Deze zijn namelijk:

- Run antivirus scan
- Isolate device
- Stop and quarantine a file
- Add an indicator to block or allow a file.

Aangezien de meeste van deze acties redelijk vanzelfsprekend zijn en vooral in de achtergrond zullen uitgevoerd worden zullen wij een aantal van deze acties testen en aanvullen met de nodige informatie.

Live Response

Een handige feature dat Microsoft Defender aanbiedt, is het gebruik van Live Response op endpoints. Hiermee kan er, aan de hand van een remote shell connectie, verbinding gemaakt worden met een apparaat vanop een afstand. Deze verbinding opent een command line interface waarbij een aantal commando's uitgevoerd mee kunnen worden. Deze lijken beperkt, maar zijn vrij krachtig. Zeker wanneer de mogelijkheid om unsigned powershell scripts uit te voeren aangezet wordt. Deze is niet verplicht en staat standaard ook af. De mogelijkheid om aan live response te doen staat standaard ook niet op. Om deze op te zetten ga je binnen het Defender portaal naar "Settings", onder Endpoints > Advanced features ga je drie instellingen terugvinden die gerelateerd zullen zijn aan live response.

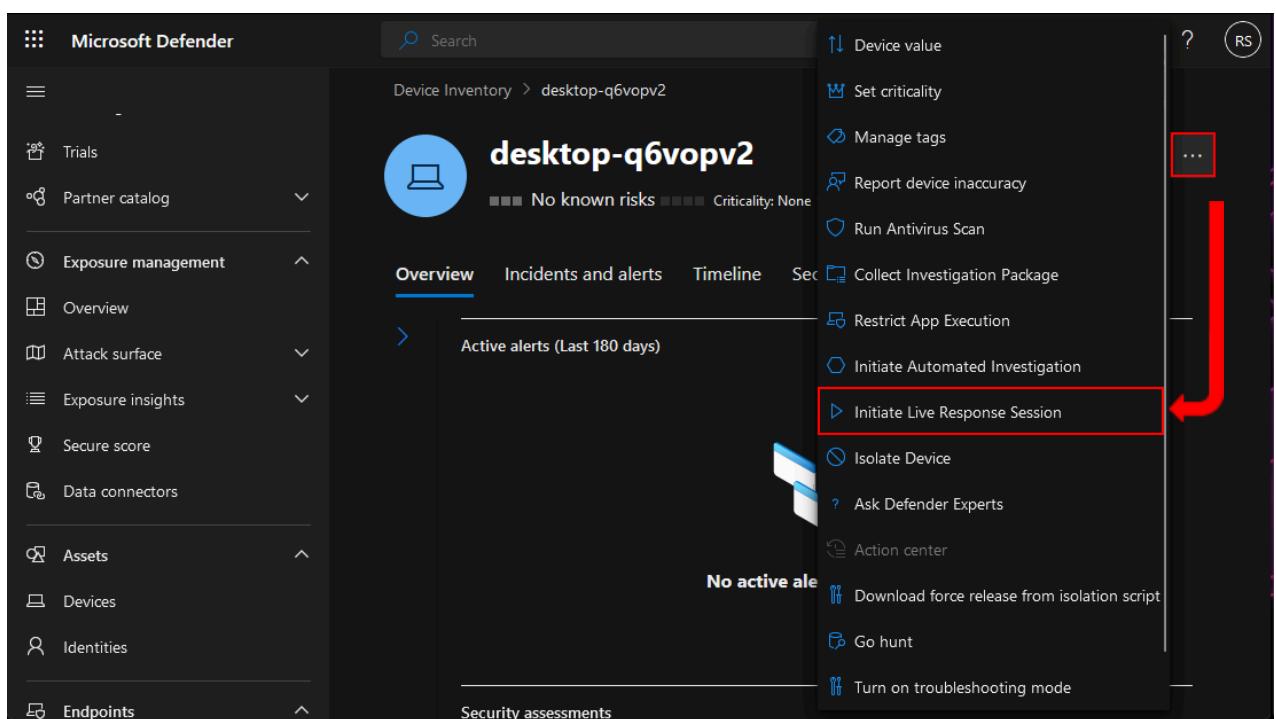


- *Live Response*
 - Hiermee wordt de live response functionaliteit aangezet. Zolang de gebruiker de nodige rechten heeft kan de gebruiker een remote shell connectie starten en commando's uitvoeren op dit apparaat.
- *Live Response for servers*

- Hiermee wordt de live response functionaliteit aangezet voor Windows servers en Linux apparaten. Zolang de gebruiker de nodige rechten heeft kan de gebruiker een remote shell connectie starten en commando's uitvoeren op dit apparaat.
- *Live Response unsigned script execution*
 - Hiermee wordt het mogelijk om powershell scripts, die naar de library zijn geüpload en niet gesigned zijn, uit te voeren binnen live response. Deze optie is niet altijd aangeraden, maar kan wel veel mogelijkheden bieden.

Werking Live Response

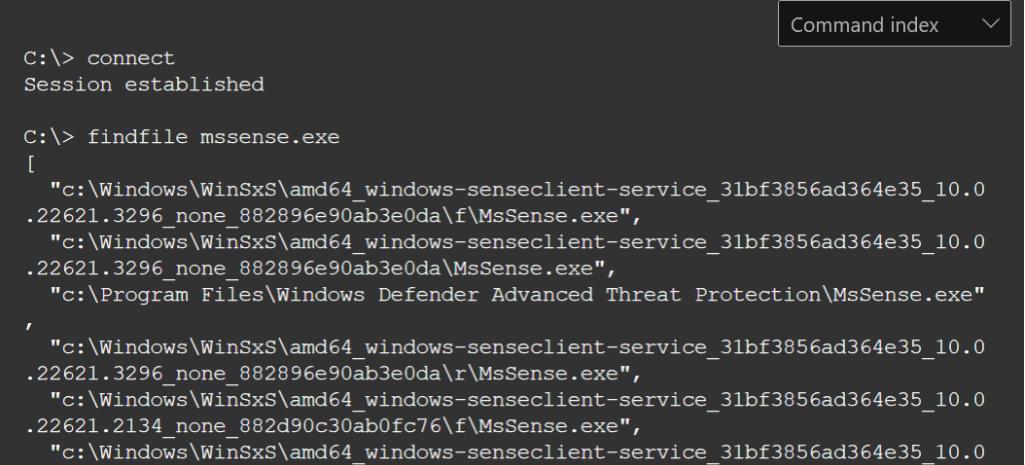
Om een live response sessie te starten ga je binnen het Microsoft Defender portaal naar devices. Je selecteert hier het apparaat waarvan je een live response sessie wilt starten. Rechtsboven klik je op de drie puntjes, hierdoor krijg je meer opties voor dit apparaat te zien. Tussen deze opties gaat de mogelijkheid staan om een live response sessie te kunnen starten.



De sessie wordt gestart en u krijgt de mogelijkheid om commando's via de remote shell in te geven. Voor meer informatie rond de commando's die ondersteund worden kan u "help" in de remote shell ingeven. Dit geeft een lijst met alle beschikbare commando's ondersteund met minimale uitleg over het commando. Twee handige commando's zijn bijvoorbeeld:

- *services*
 - Laat alle services zien op het apparaat. Handig om te kijken of hier services draaiend zijn die hier niet thuis horen.
- *findfile*
 - Doorzoekt het gehele apparaat naar de ingevoerde bestandsnaam.

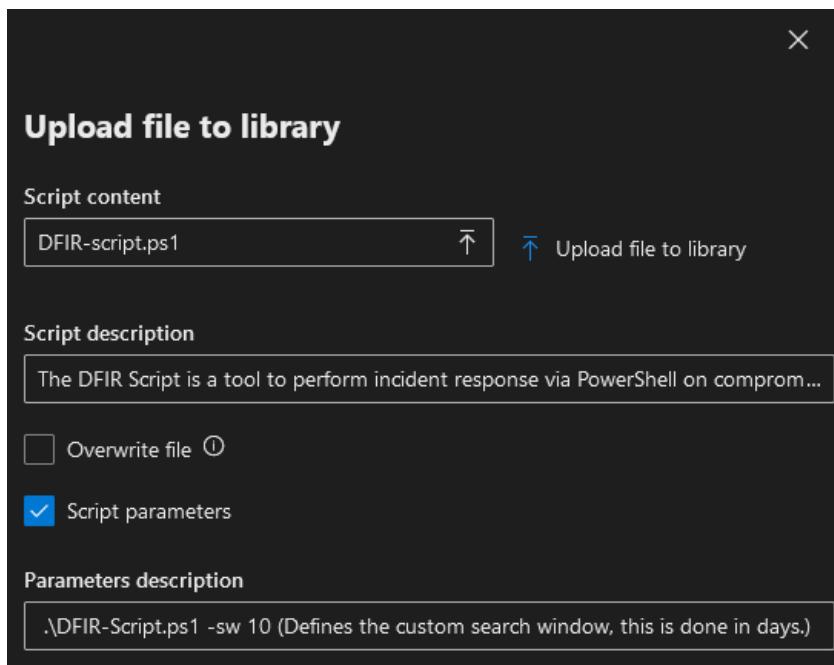
Het uitvoeren van één van deze commando's ziet er als volgt uit:



```
C:\> connect
Session established

C:\> findfile mssense.exe
[
  "c:\Windows\WinSxS\amd64_windows-senseclient-service_31bf3856ad364e35_10.0
.22621.3296_none_882896e90ab3e0da\f\MsSense.exe",
  "c:\Windows\WinSxS\amd64_windows-senseclient-service_31bf3856ad364e35_10.0
.22621.3296_none_882896e90ab3e0da\MsSense.exe",
  "c:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
,
  "c:\Windows\WinSxS\amd64_windows-senseclient-service_31bf3856ad364e35_10.0
.22621.3296_none_882896e90ab3e0da\r\MsSense.exe",
  "c:\Windows\WinSxS\amd64_windows-senseclient-service_31bf3856ad364e35_10.0
.22621.2134_none_882d90c30ab0fc76\f\MsSense.exe",
  "c:\Windows\WinSxS\amd64_windows-senseclient-service_31bf3856ad364e35_10.0
```

Als de optie “Live Response unsigned script execution” aanstaat in instellingen is het mogelijk om powershell scripts zelf te uploaden en uit te voeren binnen live response. Online hebben wij een zeer handige powershell script gevonden genaamd [DFIR-script](#). Dit script doet aan incident response door heel wat gegevens van het systeem op te zoeken en weg te schrijven in verschillende soorten bestanden en verschillende mappen die vervolgens in een zip worden gestoken. Vooraleer dit via live response kan uitgevoerd worden, moet dit script eerst geüpload worden naar de library. Dit kan gedaan worden door rechtsboven op “Upload file to library” te klikken. Hier kan het bestand geüpload worden, een descriptie krijgen en mogelijk een descriptie voor de parameters meegeven. Ook is er de optie om het bestand te “overwitten”. Dit wil zeggen dat als er al een script met dezelfde naam in de library zit, dan wordt deze vervangen.



Om na te kijken of deze correct is geüpload, kan je aan de hand van een commando alle geüploade scripts opvragen. Dit wordt gedaan met het “library” commando. Zoals u ziet staat deze ter beschikking voor ons om uit te voeren op het apparaat.

```
C:\> library
File name      Description
Parameters      Parameters
rs description
Uploaded by
=====
=====

DFIR-script.ps1 The DFIR Script is a tool to perform incident response via PowerShell on compromised devices with an Windows Operating System (Workstation & Server). Yes .\DFIR-Script.ps1 -sw 10 (Defines the custom search window, this is done in days.) Tue Mar 26 2024 14:02:11 GMT+0100 (Midden-Europees standaardtijd) Robbe@sakurashield.onmicrosoft.com

C:\> [ ]
```

Nu kan het script met het "run" comando uitgevoerd worden. In dit geval zou het comando er als volgt uitzien: "run DFIR-script.ps1". Het duurt even vooraleer dit script klaar is, maar na het uitvoeren van dit script zou er een zip in volgende map horen te zitten: C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads

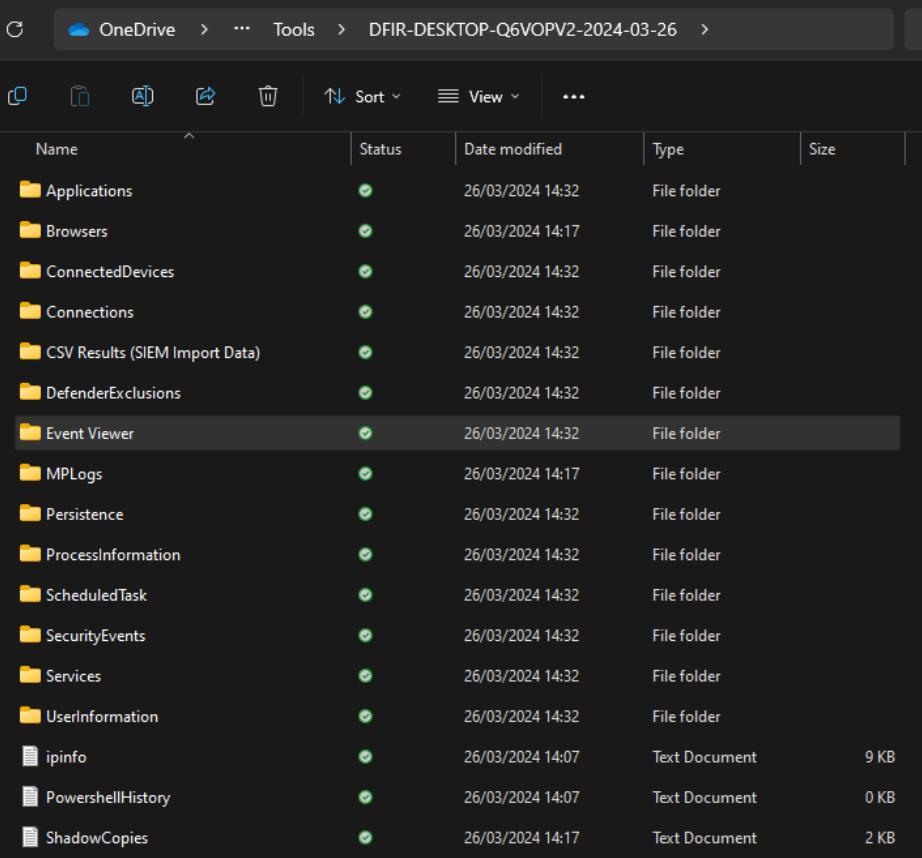
Dit bestand uit de machine halen met live respons kan opnieuw met een comando. Hiervoor gebruiken we het "getfile" comando. Dit comando zal de zip naar de lokale machine downloaden. Hierdoor kan er een analyse, aan de hand van de gegevens binnen de zip, gestart worden.

```
Command index ▾
C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads> ls
Path          Created           Modified          Size
---          ======           ======          =====
.             2023-09-13 16:03:49  2024-03-26 13:18:10  0
..            2023-09-13 16:03:49  2023-09-13 16:03:49  0
DFIR-DESKTOP-Q6VOPV2-2024-03-26
    true        false          false
    2024-03-26 13:07:25  2024-03-26 13:17:47  0
DFIR-DESKTOP-Q6VOPV2-2024-03-26.zip
    false        false          false
    2024-03-26 13:17:51  2024-03-26 13:18:09  32699703
OpenHandleCollector.exe.lock
    false        false          false
    2024-03-21 14:20:21  2024-03-21 14:20:21  0

C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads> getfile DFIR-DESK
TOP-Q6VOPV2-2024-03-26.zip
File download started

C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Downloads> [ ]
```

In deze zip zijn er zaken zoals recente applicatie installaties, powershell geschiedenis, gebruiker informatie, IP-informatie en veel meer. Zelfs Event viewer logs waren hierin terug te vinden.



The screenshot shows a file explorer window with the following navigation path: OneDrive > Tools > DFIR-DESKTOP-Q6VOPV2-2024-03-26. The main area displays a list of files and folders, each with a status icon (green checkmark), date modified, type (File folder or Text Document), and size. The 'Event Viewer' folder is currently selected.

Name	Status	Date modified	Type	Size
Applications	✓	26/03/2024 14:32	File folder	
Browsers	✓	26/03/2024 14:17	File folder	
ConnectedDevices	✓	26/03/2024 14:32	File folder	
Connections	✓	26/03/2024 14:32	File folder	
CSV Results (SIEM Import Data)	✓	26/03/2024 14:32	File folder	
DefenderExclusions	✓	26/03/2024 14:32	File folder	
Event Viewer	✓	26/03/2024 14:32	File folder	
MPLogs	✓	26/03/2024 14:17	File folder	
Persistence	✓	26/03/2024 14:32	File folder	
ProcessInformation	✓	26/03/2024 14:32	File folder	
ScheduledTask	✓	26/03/2024 14:32	File folder	
SecurityEvents	✓	26/03/2024 14:32	File folder	
Services	✓	26/03/2024 14:32	File folder	
UserInformation	✓	26/03/2024 14:32	File folder	
ipinfo	✓	26/03/2024 14:07	Text Document	9 KB
PowershellHistory	✓	26/03/2024 14:07	Text Document	0 KB
ShadowCopies	✓	26/03/2024 14:17	Text Document	2 KB

Collect Investigation Package

In hetzelfde venster waar er een live response sessie gestart kan worden, kan er ook een investigation package worden opgevraagd. Dit wordt vooral gedaan wanneer er vraag is naar de huidige status van het apparaat en als deze in een aanval terecht is gekomen kan er gekeken worden wat de aanvaller allemaal heeft uitgevoerd op dit apparaat.

Werking Investigation Package

Wanneer er op "collect investigation package" geklikt wordt voor een bepaald apparaat, opent er een pop-up met extra info en de vraag naar wat meer uitleg naar waarom dit uitgevoerd moet worden. Deze moet verplicht meegegeven worden anders kan de investigation package niet worden gedownload.

Collect investigation package from werkend-bakske2

This action will gather information about the device. Once completed, you can download and view the package.

Comment:

Heyo
This is a test :]

Confirm

Close

Als deze klaar is met het ophalen van de gegevens dan kan je door opnieuw onder hetzelfde venster binnen dat bepaalde apparaat op het Defender portaal naar action center gaan. Hier kan de investigation package gedownload worden.

Action center

ⓘ For submitted actions to take effect, device must be connected to the network.

Investigation package collection

Status

⬇ Package collection package available

ⓘ Package collection submitted

Heyo

This is a test :]

By Robbe@sakurashield.onmicrosoft.com on Apr 9, 2024 11:11:14 AM

De investigation package wordt gedownload als een zip-bestand. Bij het unpacken van de zip staan er verschillende mappen die bestanden bevatten gerelateerd aan die bepaalde map. Dit ziet er zo uit:

Name	Status	Date modified	Type	Size
Autoruns	✓	09/04/2024 09:26	File folder	
Installed Programs	✓	09/04/2024 09:26	File folder	
Network Connections	✓	09/04/2024 09:24	File folder	
Prefetch Files	✓	09/04/2024 09:26	File folder	
Processes	✓	09/04/2024 09:26	File folder	
Scheduled Tasks	✓	09/04/2024 09:23	File folder	
Security Event Log	✓	09/04/2024 09:23	File folder	
Services	✓	09/04/2024 09:24	File folder	
SMB Session	✓	09/04/2024 09:24	File folder	
System Information	✓	09/04/2024 09:24	File folder	
Temp Directories	✓	09/04/2024 09:23	File folder	
Users and Groups	✓	09/04/2024 09:24	File folder	
WdSupportLogs	✓	09/04/2024 09:23	File folder	
Forensics Collection Summary	✓	09/04/2024 09:26	Microsoft Excel C...	16 KB

Om een voorbeeld te geven wat er bijvoorbeeld in een van deze bestanden van de investigation package staat, zullen wij er een aantal laten zien.

- SystemInformation.txt

```

Host Name: Werkend-bakske2
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.19045 N/A Build 19045
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: N/A
Registered Organization: N/A
Product ID: 00331-10000-00001-AA578
Original Install Date: 3/14/2024, 10:37:38 AM
System Boot Time: 4/9/2024, 9:12:13 AM
System Manufacturer: Microsoft Corporation
System Model: Virtual Machine
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel® Family 6 Model 106 Stepping 6 GenuineIntel ~2793 Mhz
BIOS Version: Microsoft Corporation Hyper-V UEFI Release v4.1, 11/28/2023
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume3
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC) Coordinated Universal Time
Total Physical Memory: 4,045 MB

```

- QueryUser.txt

USERNAME	SESSIONNAME	ID	STATE	IDLE TIME	LOGON TIME
barry	rdp-tcp#1	2	Active		1 4/9/2024 9:21 AM

- Forensics Collection Summary.csv

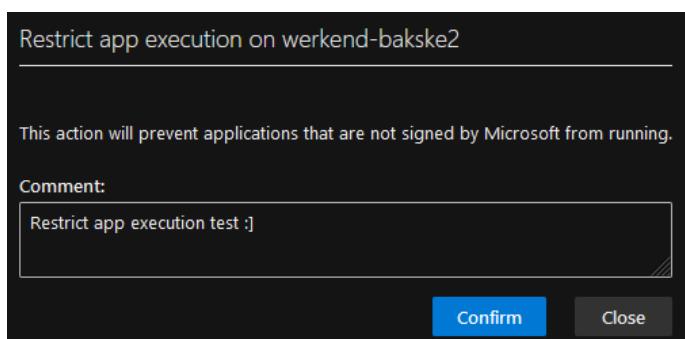
A1	Current Time	Command Name	Command Line	Status	hError
1	[2024-04-09T09:23:36Z]	WdSupportLogs	C:\Windows\system32\cmd.exe /C "%ProgramFile%Completed	Completed	0
2	[2024-04-09T09:23:40Z]	hkcu_Software_Microsoft_Windows_Explore	C:\Windows\system32\reg.exe QUERY "HKEY_USERS Completed	Completed	0
3	[2024-04-09T09:23:40Z]	hkcu_Software_Microsoft_Windows_Explore	C:\Windows\system32\reg.exe QUERY "HKEY_USERS Completed	Completed	0
4	[2024-04-09T09:23:40Z]	hkcu_Software_Microsoft_Windows_Explore	C:\Windows\system32\reg.exe QUERY "HKEY_USERS Completed	Completed	0
5	[2024-04-09T09:23:40Z]	hkcu_Software_Microsoft_Windows_Explore	C:\Windows\system32\reg.exe QUERY "HKEY_USERS Completed	Completed	0
6	[2024-04-09T09:23:40Z]	TempDirFiles	C:\Windows\system32\cmd.exe /C "dir /A /Q /S /T "C Completed	Completed	0
7	[2024-04-09T09:23:40Z]	TempDirFiles	C:\Windows\system32\cmd.exe /C "dir /A /Q /S /T "C Completed	Completed	0
8	[2024-04-09T09:23:40Z]	TempDirFiles	C:\Windows\system32\cmd.exe /C "dir /A /Q /S /T "C Completed	Completed	0
9	[2024-04-09T09:23:41Z]	ActiveNetConnections	C:\Windows\system32\netstat.exe -abno Completed	Completed	0
10	[2024-04-09T09:23:44Z]	ScheduledTasks	C:\Windows\system32\schtasks.exe /query /v /fo C: Completed	Completed	0
11	[2024-04-09T09:23:44Z]	UserInstalledPrograms	C:\Windows\system32\reg.exe QUERY "HKEY_USERS Completed	Completed	0
12	[2024-04-09T09:23:44Z]	UserInstalledPrograms	C:\Windows\system32\reg.exe QUERY "HKEY_USERS Completed	Completed	0
13	[2024-04-09T09:23:44Z]	UserInstalledPrograms	C:\Windows\system32\reg.exe QUERY "HKEY_USERS Completed	Completed	0
14	[2024-04-09T09:23:44Z]	Wow6432NodeInstalledPrograms	C:\Windows\system32\reg.exe QUERY "hklm\Software Completed	Completed	0
15	[2024-04-09T09:23:44Z]	InstalledPrograms	C:\Windows\system32\reg.exe QUERY "hklm\Software Completed	Completed	0
16	[2024-04-09T09:23:47Z]	LocalGroups	C:\Windows\system32\cmd.exe /C "for /f "delims=*" Completed	Completed	0

Restrict App Execution

Als er zeker sprake is van een aanval op een van de apparaten in een bedrijf. Kunnen alle applicaties (met een uitzondering voor Microsoft signed applicaties) volledig uit worden gezet. Hierdoor kunnen mogelijk gevaarlijke applicaties niet opstarten op het apparaat. Dit is een vrij drastische actie, maar nog steeds minder drastisch dan het volledige apparaat te isoleren.

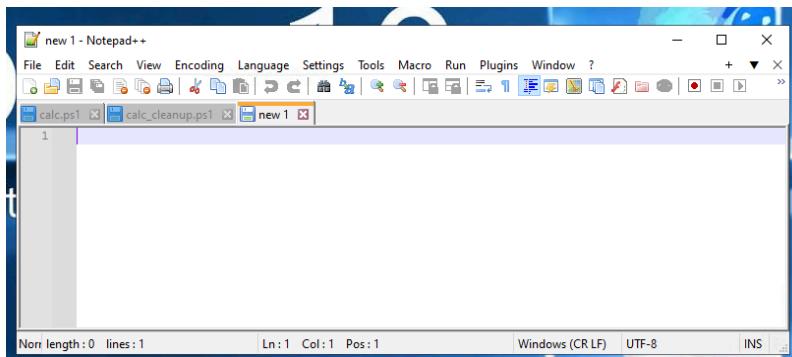
Werking Restrict App Execution

Om dit uit te voeren ga je opnieuw naar het apparaat en klik je rechtsboven op de drie bolletjes. Hier kan je "Restrict App Execution" aanduiden. Opnieuw ben je verplicht kort uit te leggen waarom deze actie uitgevoerd wordt.

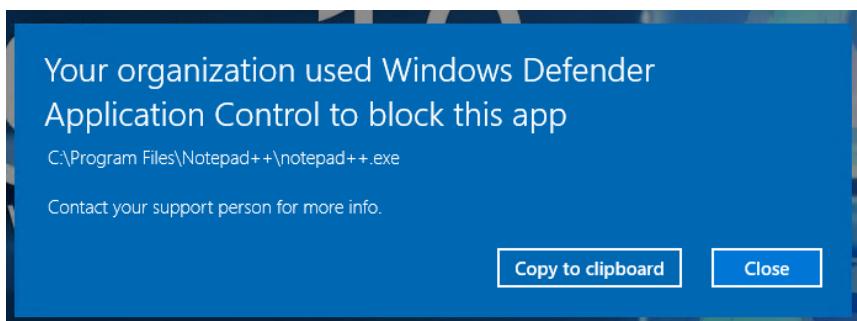


Ook hier zal de status ervan te vinden zijn op action center. Deze is ook opnieuw te vinden door op de voorgaande drie bolletjes te klikken.

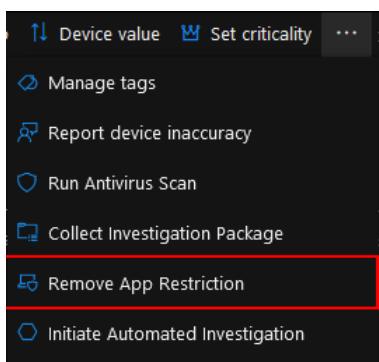
Vooraf was het mogelijk om op dit apparaat notepadd++ te openen en te gebruiken.



Na het uitvoeren van deze actie zal de volgende melding tevoorschijn komen wanneer je de applicatie probeert te openen.



Het opheffen van deze actie kan zeer gemakkelijk. In het Defender portaal ga je naar het apparaat dat de app restriction actie aan heeft staan. Door opnieuw gebruik te maken van de drie bolletjes bovenaan rechts zal je zien dat er nu "Remove app restriction" komt bij te staan.



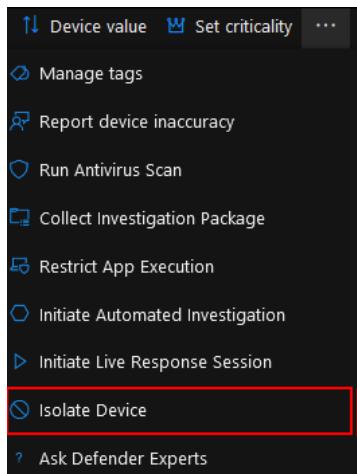
Hier zal er, zoals voorheen, opnieuw een beetje uitleg bijgezet moeten worden waarom deze actie gedaan wordt. Hierna kan opnieuw gebruik worden gemaakt van alle applicaties binnen het apparaat.

Isolate Device

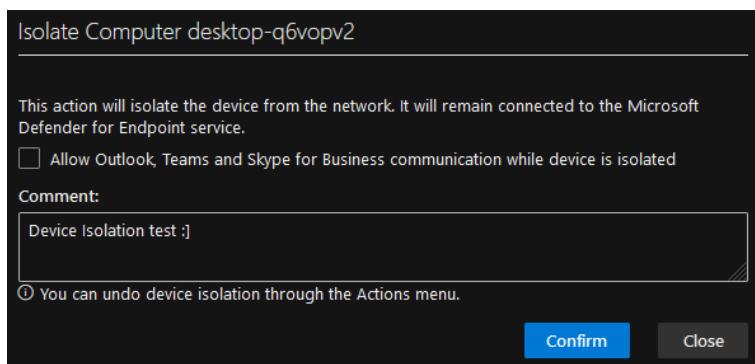
Een nog drastischere maatregel dan het restricten van applicatie-uitvoeringen is het isoleren van een apparaat. Wanneer dit wordt gedaan, wordt het gehele apparaat van het netwerk gekoppeld. De connectie met Defender blijft nog wel actief. Hierdoor kan het apparaat nog aan monitoring doen terwijl deze toch is geïsoleerd van het netwerk. Dit kan ervoor zorgen dat de aanvaller zwaar beperkt wordt in het soort acties dat hij kan ondernemen.

Werking Device Isolation

In het Defender portaal onder devices kan je kiezen voor welk apparaat je wilt isoleren. Als je op een van de apparaten hebt doorgeklikt, dan kan je, door rechtsboven op de drie bolletjes te klikken, kiezen voor “Isolate Device”.



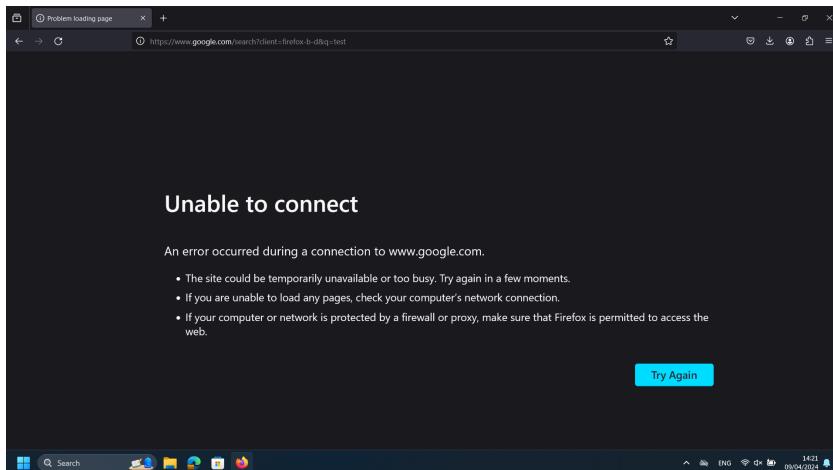
Hier opent een venster. In dit venster wordt een extra stukje uitleg gegeven over wat deze actie inhoudt. Ook wordt er de keuze gegeven om een uitzondering te maken voor Outlook, Teams en Skype. Hierdoor zullen deze applicaties werkend blijven tijdens de isolatie van het apparaat. Ten slotte zal er nog een kort stukje uitleg gegeven moeten worden over waarom je deze actie uitvoert.



Als een apparaat wordt geïsoleerd krijgt deze een melding aan wat zegt dat het apparaat geen netwerkconnectie meer zal krijgen.



Zoals er hier getoond wordt is het inderdaad niet meer mogelijk om een verbinding te maken met het internet.



Het apparaat uit deze isolatie komt overeen met het verwijderen van de applicatie restriction. Dit gebeurt ook via de drie bolletjes rechtsbovenaan in het device in het Defender portaal. Hier staat nu een nieuwe optie tussen genaamd "Release From Isolation". Voor dit wordt uitgevoerd moet ook hier uitgelegd worden waarom deze actie wordt uitgevoerd.

Cloud Apps

Met Microsoft Defender for Cloud Apps kan er beveiliging gebracht worden op SaaS niveau. Eerst werd dit geïntegreerd in Microsoft Purview. Hiermee kon er aan information protection op SaaS niveau gebeuren, maar nu is dit ook beschikbaar binnen Microsoft Defender XDR.

Cloud Discovery

Cloud Discovery kijkt door middel van uw traffic logs naar welke cloud apps er gebruik worden gemaakt. Deze krijgen op bepaalde factoren een rating. Deze rating zorgt voor een geschatte veiligheidswaarde.

Binnen Cloud Discovery zijn er meerdere overzichten waar erdoor gebladerd kan worden. Het eerste dat je te zien krijgt is een algemeen dashboard van Microsoft Defender for Cloud Apps. Hier wordt schematisch informatie getoond over bijvoorbeeld de risk levels van de cloud apps en welke gebruikers het meeste verkeer over deze apps hebben verstuurd/ontvangen.

Verder is er nog keuze uit Discovered Apps, Discovered resources, IP adressen, Users en Devices. De namen zijn voor het grootste deel vanzelfsprekend. Discovered Apps geeft een lijst terug met gebruikte apps binnen uw organisatie. Hier kan je bijvoorbeeld apps filteren op basis van hun risicoscore, waarbij een score van 10 staat voor goed beveiligd en een score van 0 voor een groot gevaar, of op basis van populariteit en gebruiks frequentie. Vervolgens is er nog de tab Cloud resources. Hier kan er meer diepgaande informatie van PaaS en IaaS resources getoond worden om hier een nog beter overzicht op te krijgen. Je kan hier de resources voor zowel AWS, Azure en Google Cloud terugvinden. Onder "IP addresses" kan je per IP-adres van elk endpoint de hoeveelheid traffic, upload en transaction zien. Dit kan ook gedaan worden onder de tabs Users en Devices.

Cloud App Catalog

Hier worden alle SaaS apps getoond. Hier zijn in totaal op het moment 32.731 apps in opgelijs. Ook hier kan er op verschillende manieren gefilterd worden, maar ook kan je hier per app ervoor kiezen om deze te sanctionen of unsanctionen.

- ***Sanctioned app:***
 - Dit wil zeggen dat de app goedgekeurd wordt en wordt ervaren als veilig voor gebruik. Ook kunnen er policies aangemaakt worden die specifiek uitgevoerd zullen worden voor de apps die als sanctioned gemarkerd zijn.
- ***Unsanctioned app:***
 - Unsanctioned apps zijn het omgekeerde van de sanctioned apps. Deze worden ervaren als gevaarlijk. Door de app op “unsanctioned” te zetten zal de applicatie niet automatisch geblokkeerd worden. Om deze te kunnen blokkeren zal er een block script gemaakt moeten worden of een andere gelijkaardige policy.

Cloud Apps Policies

Onder de policy tab van Cloud apps kunnen de policies aangemaakt en beheerd worden. Hier heb je de keuze om zeven verschillende soorten policies aan te maken: Activity policy, Cloud Discovery anomaly detection policy, File policy, App discovery policy, Access policy, Session policy en OAuth app policy.

Als voorbeeld stellen wij een app discovery policy in die alle nieuwe app discoveries, die een risico score lager dan één hebben, als unsanctioned zullen instellen. Dit doen we door naar “Policies” onder Cloud Apps te gaan en hier op “policy management” te klikken. Hier hebben we vervolgens de keuze om op “create policy” te klikken en dan op “app discovery policy”. Om deze filter in te stellen geven wij de basisgegevens mee zoals een naam en een beschrijving en stellen wij een filter in. Deze filter gaat als uitvoerende regel dienen die de policy gaat volgen. Hier kiezen we om dit te doen op basis van de risk score. Door middel van de slider geven we mee dat er een actie moet gebeuren tussen een waarde van nul en een.

Create app discovery policy

Cloud Discovery policies enable you to create alerts for new apps that are discovered in your organization.

Policy template *

No template

Policy name *

New apps with score eq to 1 or lower (unsanctioned)

Policy severity *



Category *

Cloud Discovery

Description

New apps with score equal to one or lower will be set as unsanctioned

Apps matching all of the following

X Risk score equals

Verder onderaan wordt er de keuze gegeven om een alert te maken en eventueel ook een e-mail te sturen wanneer dit gebeurt. In dit geval hoeft dit niet te gebeuren dus wordt dit uitgezet. Ook stellen we iets verder de actie in dat moet gebeuren. Hier stellen we in dat de app getagged moet worden als unsanctioned.

Alerts

Create an alert for each matching event with the policy's severity

Governance actions

Tag app as sanctioned

Tag app as unsanctioned

Tag app as monitored

Tag app with custom tag Select app tag

We secure your data as described in our [privacy statement](#) and [online service terms](#).

Create

Cancel

Als we ervoor willen zorgen dat de unsanctioned apps niet bezocht kunnen worden, kunnen er automatisch indicators worden aangemaakt hiervoor. Dit is een instelling die ervoor zorgt dat cloud apps en MDE geïntegreerd zijn met elkaar en hieruit indicators kunnen aanmaken. Om dit te doen moet er naar de instellingen binnen het Defender portaal worden gegaan en onder cloud apps kan er naar "Microsoft Defender for Endpoint" worden doorgeklikt. Hier zetten we "Enforce App Access" aan.

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint Integration

Enforce app access
Enabling this will Block access to apps that were marked as Unsanctioned and will deliver a Warning or Block message to users who attempt to run apps marked as Monitored.

Alerts
Configure the severity for signals sent to Microsoft Defender for Endpoint.

Informational

User warnings

Notification URL
Enter the redirect URL for warned users
Enter URL

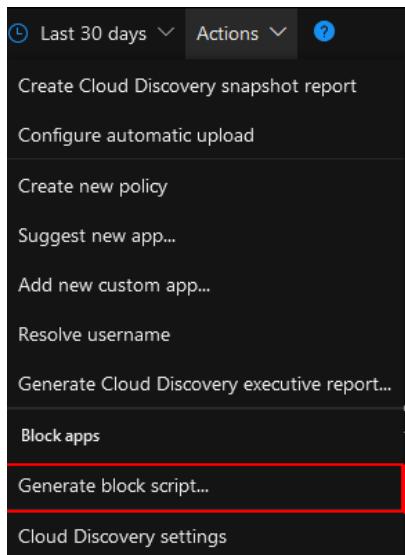
Bypass duration
Set the duration of the user bypass
hours

Save We secure your data as described in our [privacy statement](#) and [online service terms](#).

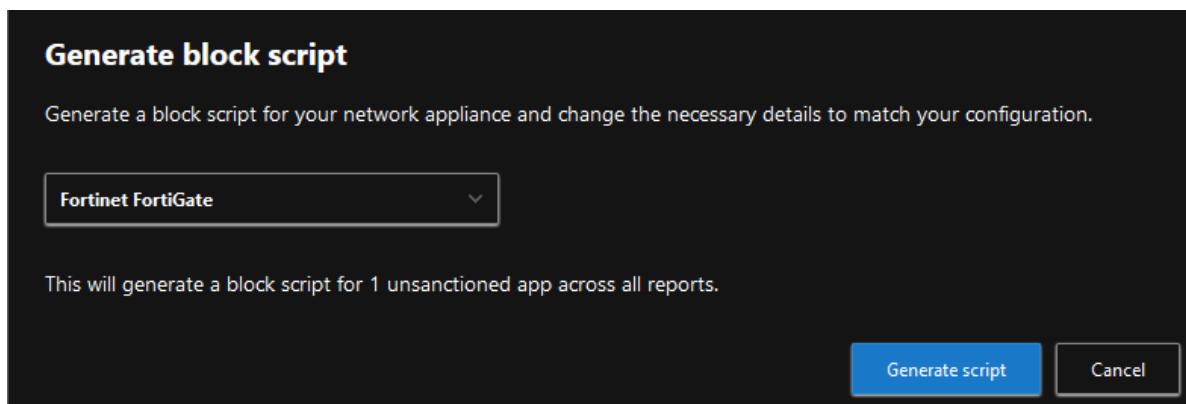
Hierna komen de bijbehorende url's ook bij in de indicator tab bij te staan. In dit geval zijn dit alle url's die gelinkt zijn aan youtube aangezien deze op "unsanctioned" staat.

<input type="checkbox"/>	googlevideo.com	YouTube	Block execution	Informational	All devices	Never	Unsanctioned cloud app acce
<input type="checkbox"/>	youtube-nocookie.com	YouTube	Block execution	Informational	All devices	Never	Unsanctioned cloud app acce
<input type="checkbox"/>	youtu.be	YouTube	Block execution	Informational	All devices	Never	Unsanctioned cloud app acce
<input type="checkbox"/>	youtube.co	YouTube	Block execution	Informational	All devices	Never	Unsanctioned cloud app acce
<input type="checkbox"/>	video.google.com	YouTube	Block execution	Informational	All devices	Never	Unsanctioned cloud app acce
<input type="checkbox"/>	youtube.com	YouTube	Block execution	Informational	All devices	Never	Unsanctioned cloud app acce

We kunnen dit nog een stapje verder nemen en een block script hiervoor laten genereren. Hiermee zullen alle apps, die nu automatisch als unsanctioned gezien worden wanneer ze een score dat gelijk is aan één of nul, in een ACL voor het meegegeven security apparaat terechtkomen. Ik heb bijvoorbeeld Youtube als "unsanctioned" ingesteld. Een block script maken kan niet in policy, maar dit wordt gedaan in Cloud Discovery. Rechtsboven kan er op "Actions" geklikt worden en hier vervolgens een nieuw block script gegenereerd worden.



Hier stellen we het security device in dat gebruikt wordt. In dit geval is dat Fortinet FortiGate.



Nadat we dit block script hebben aangemaakt. Zal een txt bestand gedownload worden waar de nodige config voor het aangeduide security device in staat. Voor de youtube webapp voor fortigate zal dit als volgt zijn:

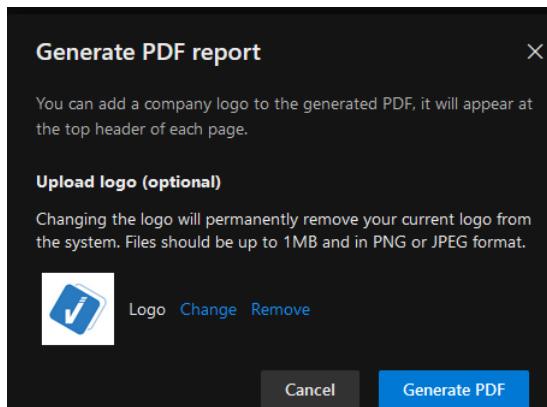
```
config webfilter urlfilter
    edit <ID>
        config entries
            edit 1
                set url youtube.com
                set type simple
                set action block
                set status enable
            next
            edit 2
                set url youtu.be
                set type simple
                set action block
                set status enable
            next
            edit 3
                set url youtube.co
                set type simple
                set action block
                set status enable
            next
            edit 4
                set url video.google.com
                set type simple
                set action block
                set status enable
            next
            edit 5
                set url googlevideo.com
                set type simple
                set action block
                set status enable
            next
            edit 6
                set url youtube-nocookie.com
                set type simple
                set action block
                set status enable
        end
    end
```

Monthly Security Report

Microsoft Defender biedt de mogelijkheid om een pdf bestand te downloaden dat een verslag bevat van de huidige Defender omgeving van ofwel de voorbije 30 dagen of de voorbije 90 dagen. Dit verslag bevat bijvoorbeeld de security score van de endpoints en vergelijkt dit met een bedrijf van een gelijke grootte of de hoeveelheid resolved incidents en alerts worden hier ook meegegeven.

Tijdens het maken van dit verslag kan er ook een bedrijfslogo toegevoegd worden. Deze wordt dan rechtsboven elk blad van het verslag geplaatst.

Het maken van zo'n verslag kan gedaan worden door eerst naar Reports te gaan. Hier kan er onder "Endpoints" op "Monthly security summary" geklikt worden. Bovenaan krijg je de keuze om dit in te stellen voor 30 dagen of 90 dagen. Het daadwerkelijk aanmaken van het verslag kan door rechtsboven op "Generate PDF report" te klikken. Hier krijg je dan ook de keuze om een bedrijfslogo in te stellen.



Email

Microsoft Defender XDR heeft een build-in functionaliteit waarbij de beheerders meer inzicht kunnen krijgen in het e-mailverkeer binnen de organisatie. Hierdoor krijgen zij een beter idee of er mogelijks gevraagde punten liggen op vlak van e-mails.

Investigation

Eerder werd er verteld hoe er een automatic investigation gestart wordt wanneer er een alert wordt aangemaakt. Microsoft Defender for Office 365 bekijkt de oorspronkelijke e-mail op bedreigingen en identificeert andere e-mailberichten die verband houden met de oorspronkelijke e-mail en mogelijk deel uitmaken van een aanval. Deze analyse is belangrijk omdat e-mailaanvallen zelden bestaan uit slechts één e-mail.⁷

Wanneer Automated investigation and response (AIR) is uitgevoerd op een alert, zullen alle relevante informatie van de investigation hier te vinden zijn indien er gebruik is gemaakt van e-mail binnen de aanval.

Explorer

Hier wordt er schematisch en aan de hand van ondersteunende grafieken zeer interessante informatie weergegeven. Hierdoor kan er een beter inzicht in het mailgebruik binnen de organisatie worden verkregen.

Je hebt de mogelijkheid om hier heel uitgebreid in te filteren. Om een voorbeeld te geven in hoeveel hier mogelijk in is, zijn dit een aantal filters die toegepast kunnen worden: sender address, recipient, sender domain, subject, malware family, impersonated domains, impersonated user, file type, email size en dit zijn maar enkele voorbeelden.

⁷ 'Email analysis in investigations for MDO365', Microsoft.com

The screenshot shows the Microsoft Defender for Office 365 Explorer interface. At the top, there are tabs for 'All email', 'Malware', 'Phish', 'Campaigns', 'Content Malware', and 'URL clicks'. A search bar at the top right contains the query 'Sender address Equal any of' followed by three entries: 'otto@sakurashield.onmicrosoft.com', 'robbe.sas@vanroey.be', and 'vanroey.be'. Below the search bar is a 'Save query' button. The main area has a header with tabs for 'Email', 'URL clicks', 'Top URLs', 'Top clicks', 'Top targeted users', 'Email origin', and 'Campaign'. It also includes 'Message actions', '5 items', 'Export', and 'Customize columns' buttons. The table below lists five items from the search results:

Date (UTC +02:00)	Subject	Recipient	Tags	Sender address	Sender domain
Apr 5, 2024 9:36 AM	2e testmail suspicious url	otto@sakurashield.onmicrosoft.com	-	robbe.sas@vanroey.be	vanroey.be
Apr 5, 2024 8:53 AM	RE: test mail clicked url logging	robbe.sas@vanroey.be	-	otto@sakurashield.onmicrosoft.com	sakurashield.onmicrosoft.com
Apr 5, 2024 8:52 AM	RE: test mail clicked url logging	robbe.sas@vanroey.be	-	otto@sakurashield.onmicrosoft.com	sakurashield.onmicrosoft.com

Attack Simulation Training

Nog een toffe functionaliteit binnen Microsoft Defender for Office 365 is het uitvoeren van attack simulations. Hierbij kan je aan de hand van templates een zelfgemaakte aanval opstellen voor de medewerkers om te kijken hoe zij hierop reageren. Ook is het mogelijk om hier vervolgens een gepaste training aan te koppelen moest de medewerker de simulatie aanval falen.

Een Attack Simulation Training starten is zeer eenvoudig, maar kan enorm helpen om een groter inzicht te krijgen voor het mailgebruik binnen de organisatie. Onder Email & collaboration in het Defender portaal kan je klikken op Attack Simulation Training. Hier krijg je alle ongoing simulaties te zien. Als je vervolgens op "Launch simulation training" klikt, begin je met het aanmaken van deze simulatie.

Eerst moet je meegeven welke aanvalstechniek je wilt uitvoeren. Je hebt hier keuzen uit:

- **Credentials harvest**
 - Aan de hand van een url word je doorverwezen naar een inlogpagina waar naar je gegevens wordt gevraagd.
- **Malware attachment**
 - In het bericht zal een attachment aan gelinkt zijn. Als deze geopend wordt zou er malware uitgevoerd kunnen worden.
- **Link in attachment**
 - Dit is een combinatie van de twee bovenstaande technieken. Hierbij wordt er een attachment
- **Link to malware**
 - Een url dat doorverwijst naar een file sharing site waar de malware zich bevindt.
- **Drive-by URL**
 - Hier wordt een url meegegeven naar een site die in de achtergrond probeert informatie van de gebruiker te stelen.
- **OAuth Consent Grant**
 - Hier maakt een aanvaller een Azure-toepassing die het doelwit vraagt om toestemming te verlenen voor toegang tot bepaalde gegevens.
- **How-to Guide**

- Met deze techniek kan een eenvoudige handleiding rechtstreeks naar eindgebruikers worden gestuurd met instructies over het uitvoeren van taken, zoals het rapporteren van een phishing mail.

Als voorbeeld wordt er gebruik gemaakt van credential harvesting

Select technique

Select the social engineering technique you want to use with this simulation. We've curated these from the MITRE Attack framework. Depending on your selection, you will be able to use certain types of payloads.



Credential Harvest

In this type of technique, a malicious actor creates a message, with a URL in the message. When the target clicks on the URL within the message, they are taken to a web site, the website often...

[View details of Credential harvest](#)



Malware Attachment

In this type of technique, a malicious actor creates a message, with an attachment added to the message. When the target opens the attachment,

Hierna geef je de simulatie een naam, beschrijving en hierop volgt het gebruikte template voor het bericht. Hier heb je keuze tussen heel wat templates. Verder kan je ook zien in welke taal dit bericht staat en wat de success rate van dit template is. Eentje met een hoge success rate is blijkbaar "Netflix account suspension". Het is mogelijk om meerdere aan te duiden en het is mogelijk om deze eerst naar uzelf te sturen.

Select payload and login page

Select payload for this simulation technique. You can create or collect your own payloads to add this list. Note that if you create a new payload, you will be redirected to a payload creation wizard. You can also map a login page for Credential Harvest or Link in Attachment technique to a payload from the preview tab.

[Global payloads](#)

[Tenant payloads](#)

[Send a test](#)

1 of 100 selected

Search

Filter

Payload Name	Language	Predicted Compromise Rate (%) ↓
<input type="checkbox"/> American express password reset	English	45
<input type="checkbox"/> Payroll work file sharing	English	42
<input type="checkbox"/> Tesco Bank account verification	English	41
<input type="checkbox"/> Expense report sharing	English	40
<input type="checkbox"/> DHL Shipment Confirmation	English	38
<input type="checkbox"/> Email Quarantined Notification	English	37
<input checked="" type="checkbox"/> Netflix account suspension	English	37

Verder wordt er gevraagd voor welke eindgebruikers deze simulatie van toepassing is. Hier kan je alle gebruikers aanduiden of specifiek een gebruiker aanduiden. In deze test wordt een gebruiker gebruikt.

Target users

Add existing users and groups or import a list of email addresses.

- Include all users in my organization
- Include only specific users and groups

[+ Add users](#) [Import](#)

① 1 user(s) or group(s) with valid and unique email addresses have been added.

[⟳ Refresh](#)

Name	Email
otto	otto@sakurashield.onmicrosoft.com

Ook kunnen er trainingen gekoppeld worden aan de simulatie. Stel voor dat een werknemer een email attachment heeft gedownload van een phishing mail dan kan hier een specifieke training aan gekoppeld worden. Je kan hier kiezen om zelf de training cursussen te kiezen of dit te laten doen door Microsoft Defender zelf en je kan een deadline instellen hiervoor.

Assign training

Select training preferences, assignment, and customize a landing page for this simulation.

Preferences

Select training content preference

Microsoft training experience (Recommended)

- Assign training for me (Recommended)

Let Microsoft assign training courses and modules based on a user's previous simulation and training

- Select training courses and modules myself

I want to select specific training courses and modules from Microsoft's catalog

Due Date

Select a training due date

7 days after Simulation ends

Ten slotte moet er nog een landing page gekozen worden. Moest de medewerker de simulatie falen, dan zal de werknemer op deze pagina terechtkomen. Hierdoor zal de werknemer te weten komen dat dit een simulatie is en de nodige informatie hierrond. Opnieuw biedt Microsoft een aantal templates aan waar je uit kan kiezen. Ook kan er een taal worden ingesteld en zelfs een company logo worden toegevoegd. Je kan de landing page previewen wanneer je op een van de namen van de templates klikt.

Microsoft Landing Page Template 4

Preview Details

Select language *

English

 Company logo

Uh oh! There was something phishy about that message \${DisplayName}...

You were just phished by your security team as part of an internal simulation.

A real attack could have put our organization and our customers at risk!

Take a few minutes to learn what you missed from this page and from the trainings that have been assigned to you.



Bij het lanceren van de simulatie zal de mail verstuurd worden naar de aangeduide gebruikers. Dit kan een aantal minuten duren vooraleer de simulatie daadwerkelijk start. De binnenkomende mail ziet er als volgt uit.

Please Verify Your Netflix Account

ⓘ Some content in this message has been blocked because the sender isn't in your Safe senders list. [I trust content from admin2@templatern.com.](#) | [Show blocked content](#)

N NETFLIX <admin2@templatern.com> To: otto Fri 4/5/2024 10:59 AM

Your account has been suspended

Dear client,
We've temporarily suspended your account due to some issues in the automatic verification process.

For this reason we suspended your account, until you verify all required information's and update your payment method. We will provide with all the steps you need to unlock your account. Please follow these instructions after you click on the button below.

[Update Your Details](#)

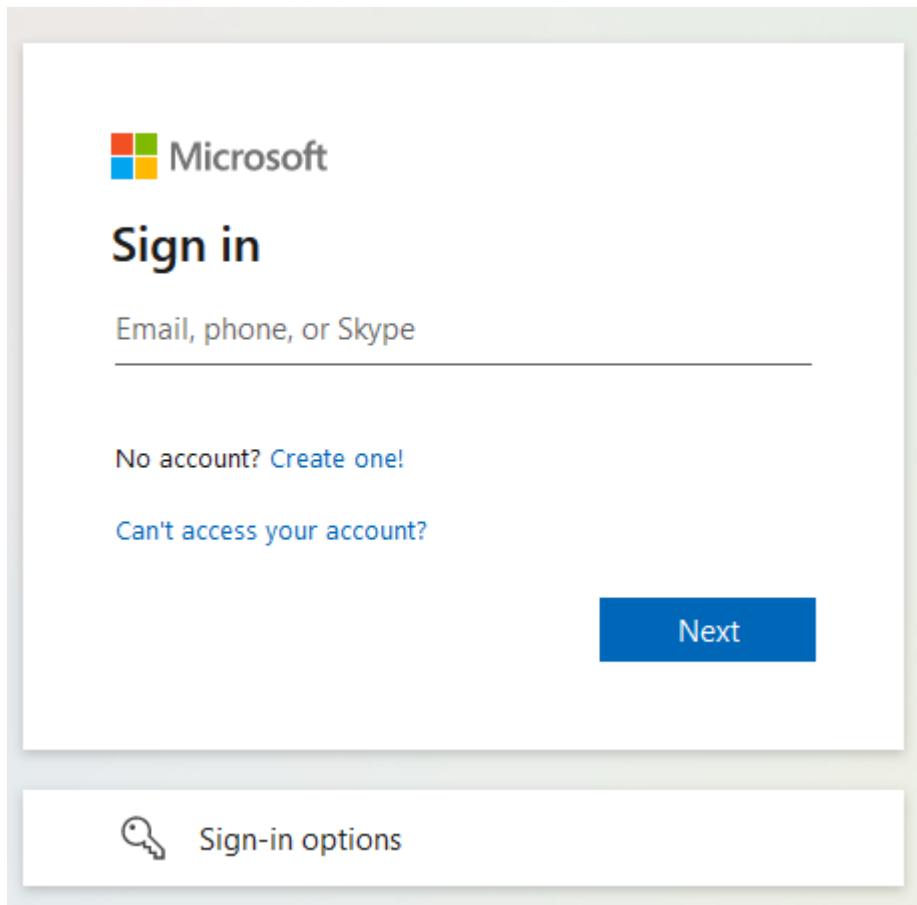
Follow these steps :

- Login to your account.
- Update your **Billing** information's
- Update your **Payment** method

If you do not verify your account, your account will be deleted permanently.
Please help us to clear your status and update your account.

Thanks,
Netflix

Alle soorten interacties die de gebruiker heeft met de mail worden doorgestuurd naar Defender. Hieronder valt onder andere: het openen van de mail, het openen van de url, het verwijderen van de mail, het ingeven van credentials, en meer. Bij het openen van de mail word je herleid naar een inlogpagina die vraagt naar je Microsoft gegevens.

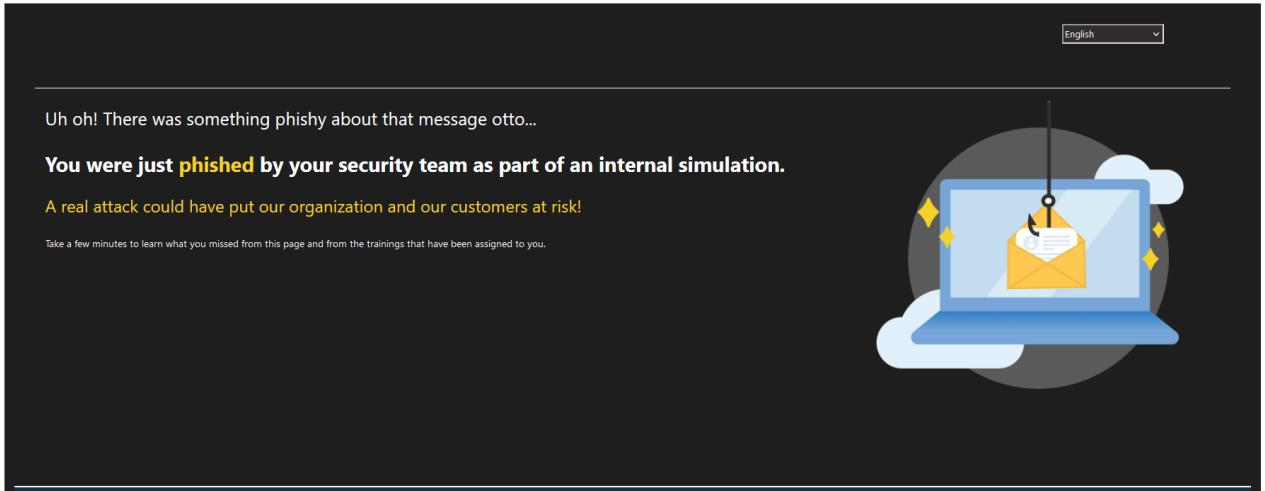


Deze lijkt op de originele pagina, maar wanneer er gekeken wordt zal je zien dat dit niet de officiële inlogpagina is.

<https://www.sharepointle.com/eur/823618ca-13ea-41e6-b48f-72f4258aaff>

Het domein sharepointle wordt niet beheerd door Microsoft, maar het domein SharePoint wel. Dit is een van de vele indicatoren die laten blijken dat dit een phishing mail is.

Na het ingeven van de gegevens, word je verwezen naar de eerder gekozen landing page.



Onderaan de site staat de verwijzing naar de training.

We've assigned you some training to learn how to avoid this in the future.

[Go to training](#) [Add to calendar](#)

Terug op het Defender portaal kan je het rapport van de simulatie opvragen. Onder de tab "Attack Simulation Training" worden alle simulaties opgelijst. Door simpelweg op de naam te klikken wordt het rapport ingeladen.

voorbeeld attack simulation

In progress Processing User Actions Social Engineering . Credential Harvest Delivery Platform : Email

[View Activity Timeline](#) [Refresh](#)

[Report](#) [Users](#) [Details](#)

Simulation Impact

100.00% users were compromised & 0% users reported

Category	Status
Compromised users	1 / 1
Users who reported	0 / 1

[View compromised users](#) [View users who reported](#)

All user activity

Action	Status
Clicked message link	1 / 1
Supplied credentials	1 / 1
Read message	1 / 1
Deleted message	0 / 1
Replied to message	0 / 1
Forwarded message	0 / 1
Out of office	0 / 1

Delivery Status

Action	Status
Successfully received message	1 / 1
Positive Reinforcement Message Delivered	0 / 0
Just Simulation Message Delivered	0 / 0

Training completion

0% users completed training

Action	Status
Mass Market Phishing ClickedPayload	0 / 1
Web Phishing Compromised	0 / 1

Policy & Rules

Binnen Microsoft Defender for Office 365 kunnen er policies aangemaakt worden die helpen de activiteiten binnen het bedrijf veilig te houden. Deze policies en rules zijn opgedeeld in drie categorieën:

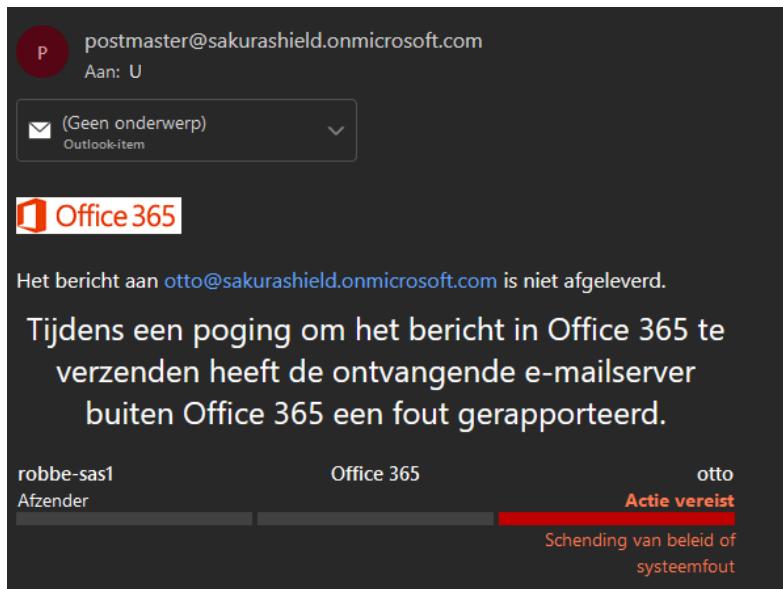
- **Threat policies**
 - Bepaalt hoe Microsoft Defender voor Office 365 omgaat met verdachte e-mails en bestanden.
- **Alert policy**
 - Bepaalt wie en hoe er wordt gewaarschuwd wanneer verdachte activiteiten worden gedetecteerd.
- **Activity alerts**
 - Bepaal welke activiteiten in Microsoft Defender voor Office 365 worden vastgelegd en gecontroleerd.

Binnen Threat policies heb je opnieuw drie verschillende subcategorieën. Deze zijn: Templated policies, Policies en Rules.

Wij hebben een nieuwe policy hierin gemaakt, een anti-malware policy om specifiek te zijn. Tijdens het maken van zo'n anti-malware policy geef je de policy een naam en duid je aan voor wie deze policy geldt. Dit kan door middel van users, groups en domeinen geselecteerd worden. Vervolgens geef je aan welke protectie instelling deze moet volgen. Wij hebben ervoor gekozen om bestanden met een bat extensie te rejecten. Hierna wordt er een non-delivery receipt (NDR) verstuurd naar de afzender. Malware zap is hier ook in aangeduid. Deze zorgt ervoor dat zelfs als het bestand aan is gekomen en achteraf blijkt dat deze malware bevat, deze alsnog quarantined wordt.

The screenshot shows the 'Protection settings' configuration page for an anti-malware policy. At the top, it says 'Configure the settings for this anti-malware policy'. Below that, under 'Protection settings', there is a checked checkbox for 'Enable the common attachments filter' with '.bat' selected. A link 'Select file types' is provided. Under 'When these file types are found', there are two radio buttons: one for 'Reject the message with a non-delivery receipt (NDR)' (which is selected) and one for 'Quarantine the message'. At the bottom, there is another checked checkbox for 'Enable zero-hour auto purge for malware (Recommended)'. The background of the screenshot is dark.

Als we een mail willen sturen dat een bat-bestand als attachment heeft, dan krijgen we volgende mail terug verzonden naar ons. Dit betekent dat de policy correct werkt.



Oorspronkelijke berichtdetails

Gemaakt op: 5/04/2024 12:34:47
Adres van afzender: robbe-sas1@outlook.com
Adres van geadresseerde: otto@sakurashield.onmicrosoft.com
Onderwerp: dit is een test

Foutdetails

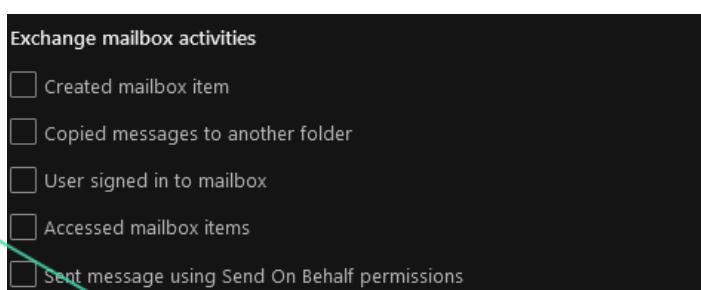
Fout: 550 5.0.350 One or more of the attachments in your email is of a file type that is NOT allowed by the recipient's organization.
Bericht geweigerd door: DUOP191MB2107.EURP191.PROD.OUTLOOK.COM

Meldingsdetails

Verzonden door: DUOP191MB2107.EURP191.PROD.OUTLOOK.COM

Audit

In het linkermenu binnen het Microsoft Defender portaal staat onderaan "audit". Met audit krijgen tenant administrators de mogelijkheid om naar activiteiten te zoeken. Het soort activiteiten kan enorm breed gaan. Er zijn meer dan 50 activiteit categorieën waar je uit kan kiezen en onder elk van deze categorieën kan er een specifieke activiteit gekozen worden. Om hier een voorbeeld van te geven zijn hier een aantal activiteiten voor exchange:



Het oplijsten van deze activiteiten kan voor meer inzicht zorgen binnen de Microsoft Defender omgeving. Stel voor een incident speelt plaats en iemand heeft deze op resolved gezet zonder dat je volledig zeker bent dat deze in werkelijkheid is opgelost. Dan kan je met audit gaan kijken wie dit heeft gedaan en eventueel navragen aan deze persoon of dit daadwerkelijk correct is. Hieronder laten we zien hoe je deze gegevens kunt opvragen.

Deze searchquery zorgt ervoor dat ik alle activiteiten van de aangegeven gebruiker opvraag tussen de tijdsperiode. Deze search zal gequeued worden en vervolgens starten. Het opvragen van deze gegevens kan even duren afhankelijk van hoe breed de zoekquery is.

Als deze klaar is, dan komt het resultaat onderaan te staan. Wanneer je hierop klikt word je doorverwezen naar een schema met de aangevraagde activiteiten van de gebruiker in die tijdsperiode.

Date (UTC)	IP Address	User	Record type	Activity	Item
Apr 4, 2024 8:4...		Robbe@sakurashield.on...	SecurityComplianceCenterEOPC...	Get-UnifiedAuditLogRe...	
Apr 4, 2024 9:0...		Robbe@sakurashield.on...	SecurityComplianceCenterEOPC...	Get-UnifiedAuditLogRe...	
Apr 4, 2024 8:4...		Robbe@sakurashield.on...	SecurityComplianceCenterEOPC...	New-UnifiedAuditLogR...	
Apr 4, 2024 2:2...		Robbe@sakurashield.on...	DataInsightsRestApiAudit	Search	
Apr 4, 2024 2:2...		Robbe@sakurashield.on...	DataInsightsRestApiAudit	Search	

Indicators

Door gebruik te maken van Indicators kan je het mogelijk maken om toegang tot bestanden die overeenkomen met een hash van een bekend, malicious bestand of bijvoorbeeld een url dat malware kan bevatten tegenhouden voor eindgebruikers. Indicators worden voor de volgende twee scenario's vooral gebruikt:

- Bekende IoC's
- Explicit toegestane bestanden/url's bij een False Positive

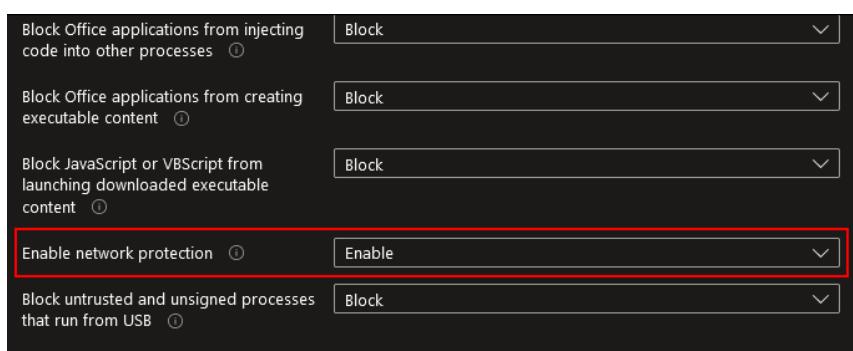
Binnen Microsoft Defender kan je een Indicator op vier verschillende soorten attributen toepassen. Deze zijn:

- File hashes
- Ip addresses
- URLs/Domains
- Certificates

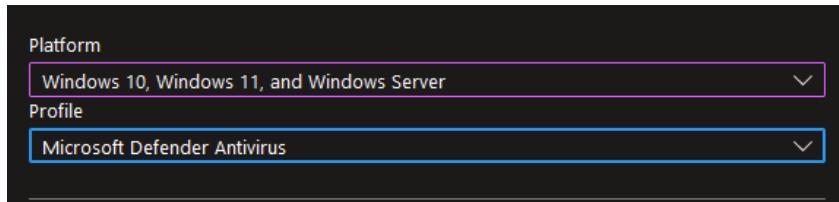
Om Indicators in te kunnen stellen wordt er verwacht dat er zowel configuratie binnen Intune wordt toegepast als binnen het Microsoft XDR portaal. Wij hebben vooral de focus gelegd op de requirements nodig om een indicator aan te maken voor een URL/Domain. Voor de andere Indicators kan de configuratie anders verlopen. Best om even hier de officiële documentatie voor te raadplegen.

Configuratie Indicator URLs/Domains

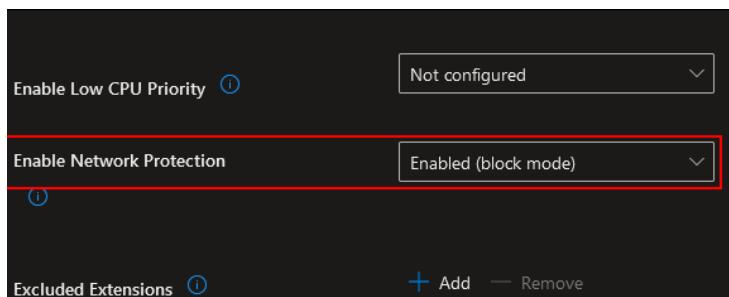
Zoals eerder vermeld is het maken van zo'n Indicator niet moeilijk, maar het opzetten van de juiste policies en instelling vereist iets meer aandacht. Als eerste moet "Network Protection" aan staan en op "block mode" staan. Hiervoor heb ik drie verschillende policies aangemaakt/aangepast. Als eerste moet er een aanpassing binnen de Security Baseline in Intune uitgevoerd worden. Dit kan door binnen Intune naar "Endpoint Security" te gaan en zo door te klikken naar "Security Baseline". Onder "Microsoft Defender for Endpoint baseline" kan je een nieuwe profile maken. Hier zorg je ervoor dat onder "Attack Surface Reduction Rules" de optie "Enable network protection" op "Enable" staat.



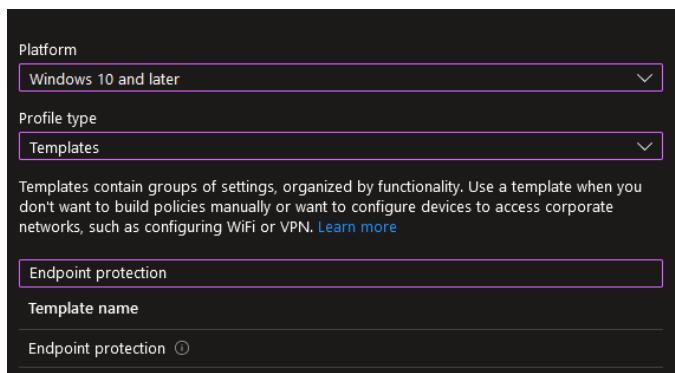
Hierna moet er binnen "Antivirus" in Intune onder "Endpoint Security" een nieuwe policy gemaakt worden. Om een nieuwe policy te maken geef je de volgende config mee.



Hierna stel je Network Protection in door deze als "Enabled (Block Mode)" in te stellen.



Nadat deze policy is aangemaakt, moet er nog een laatste policy worden aangemaakt. Dit gebeurt binnen Intune onder "Devices" >> "Windows" >> "Configuration Profiles". Hier kan een nieuwe policy worden aangemaakt. Dit doe je door de volgende configuratie mee te geven en hier het "Endpoint protection" template aan te duiden.



Hierop volgend stellen we "Network Protection" in door onder "Microsoft Defender Exploit Guard" naar "Network Filtering" te gaan.

The screenshot shows the Microsoft XDR portal interface. At the top, there are five tabs: Basics (green checkmark), Configuration settings (selected, blue outline), Assignments, Applicability Rules, and Review + create. Under Configuration settings, there are several sections: Microsoft Defender Application Guard, Windows Firewall, Microsoft Defender SmartScreen, Windows Encryption, Microsoft Defender Exploit Guard, Attack Surface Reduction, Controlled folder access, and Network filtering. A note below Network filtering states: "Block outbound connection from any app to low reputation IP/domain · This can be enabled in Audit/Block mode." Below this note is a "Learn more" link. At the bottom, there is a "Network protection" dropdown set to "Enable".

Als al deze policies zijn aangemaakt, moet er nog één instelling binnen het Microsoft XDR portaal worden aangezet. Om deze op te zetten ga je binnen het portaal naar instellingen. Hier ga je naar “Endpoints”. Onder advanced features moet de instelling “Custom network indicators” aanstaan.

The screenshot shows the "Custom network indicators" feature in the Microsoft XDR portal. It has a toggle switch labeled "On". Below the switch is a section titled "Custom network indicators" with the following text: "Configures devices to allow or block connections to IP addresses, domains, or URLs in your [custom indicator lists](#). To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform ([see KB 4052623](#)). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender for Endpoint data."

Nu alles gereed staat kan er eindelijk een indicator worden aangemaakt. Dit kan gedaan worden door eerst naar “settings” te gaan en door te klikken naar “Endpoints”. Links kan je kiezen voor “Indicators”. Wij stellen een indicator in voor een url, dus klikken we op URLs/Domains bovenaan. Door op “Add Item” te klikken openen we het configuratiescherm hiervoor. We geven de url mee waar we de toegang voor willen blokkeren. Als test url hebben wij gekozen om toegang tot “buienrader” te blokkeren. Ook kan er een Expiration Date worden ingesteld voor deze Indicator.

Indicator

Indicator details

Specify the url and the expiration date. [Learn more](#)

URL/Domain *

buienradar.nl

Indicator type Domain

Title *

block buienradar access

Description *

block buienradar access

Expires on (UTC)

Never

Custom

In het volgende scherm stellen wij een actie in dat moet worden uitgevoerd. Aangezien wij deze pagina willen blokkeren, kiezen wij voor "Block Execution". Verder is er ook nog de keuze om te kiezen tussen: allow, audit en warn.

Action

Response action -Select the action to take whenever this URL/Domain is found.

Allow

Audit

Warn

Block execution

Verder kan er ook een alert hieraan worden gekoppeld. Dit is binnen deze test niet van toepassing, dus slagen we deze over.

Dit zou alle nodige configuratie zijn om een indicator correct in te stellen. Denk er wel aan aangezien er net drie policies zijn aangemaakt, één instelling is aangepast en er een indicator is aangemaakt, kan dit wel wat tijd vereisen eens deze zullen werken. Als de eindgebruiker nu naar buienradar surft, zal de eindgebruiker de volgende popup zien.



This website is blocked by your organization.

Hosted by www.buienradar.nl

Contact your administrator for more information. [Visit the support page.](#)

[Go back](#)

Microsoft Security

Integrations

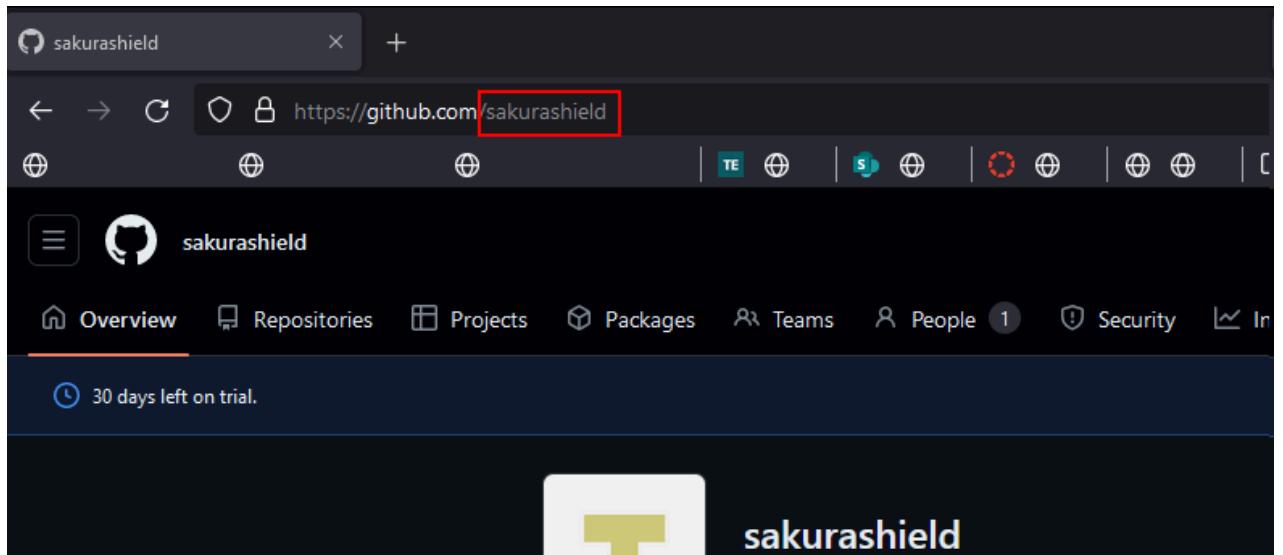
Zoals in het onderzoeksgedeelte van de documentatie is uitgelegd geeft Defender de mogelijkheid om een integratie met een van de partners op te zetten. Deze worden opgesplitst in technologische integraties en professionele services. Deze integraties opzetten wordt, in de meeste gevallen, gedaan door documentatie van de partner. Dit betekent ook dat de daadwerkelijke configuratie vaak buiten Microsoft Defender zal plaatsvinden.

GitHub integration

Defender heeft momenteel heel wat partners waarmee een integratie mogelijk is. Een van deze partners is GitHub. Om deze integratie op te kunnen zetten, moet er een GitHub enterprise cloud license aanwezig zijn. Wij maken gebruik van een 30-dagen free trial. Hierdoor zullen niet alle functionaliteiten van toepassing voor ons zijn, maar kunnen wij de integratie wel opzetten. Door GitHub Enterprise Cloud te verbinden met Defender for Cloud Apps krijgt u beter inzicht in de activiteiten van uw gebruikers en wordt bedreigingsdetectie voor afwijkend gedrag geboden. Volgende threats zullen voornamelijk van toepassing zijn:

- Compromised accounts and insider threats
- Data leakage
- Insufficient security awareness
- Unmanaged bring your own device (BYOD)

Om de verbinding tussen Defender en GitHub cloud enterprise op te zetten, is de organisatie login naam nodig. Deze kan worden teruggevonden in de url. Voor ons is dit gelijk aan "sakurashield".



Hierna zal er een nieuwe OAuth app opgezet moeten worden. Dit kan door binnen uw organisatie paneel in GitHub naar instellingen te gaan. Onder Developer settings zal er een pagina staan genaamd "OAuth Apps". Hier worden een aantal gegevens verwacht.

Register a new OAuth application

Application name *
Test-Intagration-Defender
Something users will recognize and trust.

Homepage URL *
https://oauth-sakurashield.com
The full URL to your application homepage.

Application description
Application description is optional
This is displayed to all users of your application.

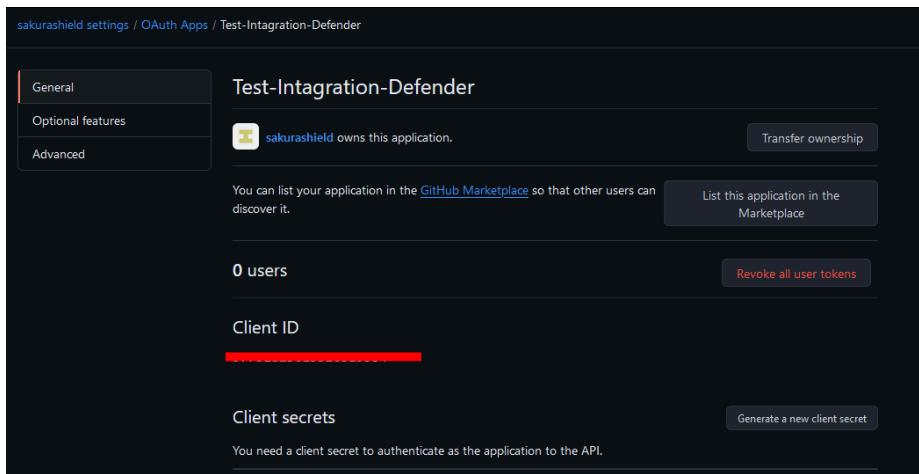
Authorization callback URL *
https://portal.cloudappsecurity.com/api/oauth/connect
Your application's callback URL. Read our [OAuth documentation](#) for more information.

Enable Device Flow
Allow this OAuth App to authorize users via the Device Flow.
Read the [Device Flow documentation](#) for more information.

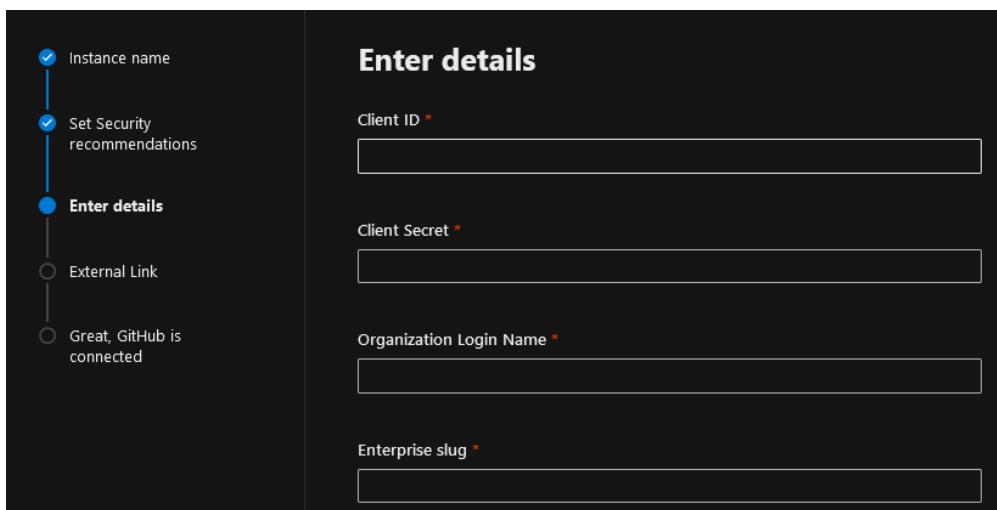
Register application **Cancel**

Voor alle veldjes kan er relatief vrij gekozen worden wat hier wordt in geplaatst. Enkel het veldje voor de "Authorization callback URL" moet deze waarde exact dezelfde url zijn. Nu deze OAuth app gemaakt is, hebben wij hier twee waarden

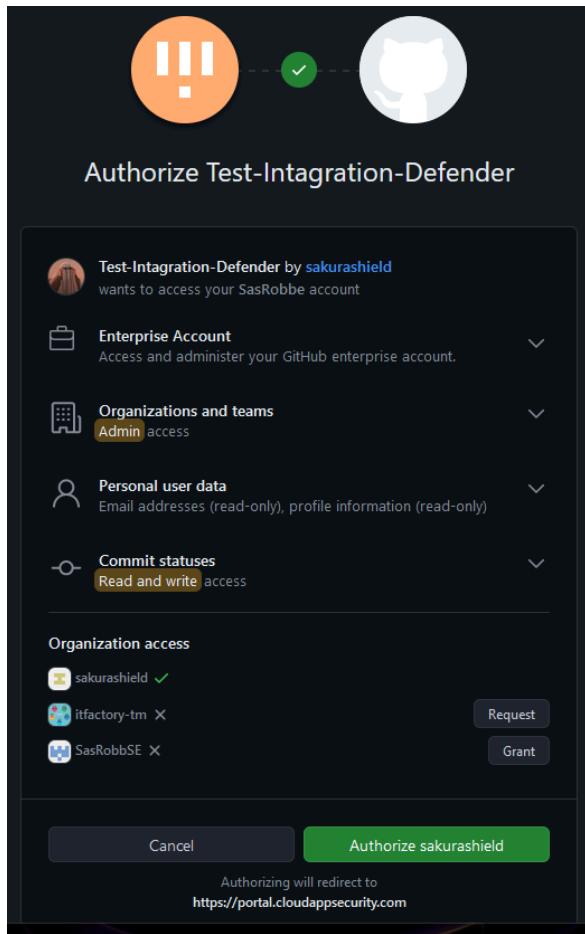
van nodig: client ID en client Secrets. Deze zijn te vinden op het scherm dat getoond wordt direct na het aanmaken van de app.



Nu kunnen we overgaan naar het Defender portaal om de link tussen de twee te leggen. Dit kan gedaan worden door naar instellingen te gaan. Onder cloud apps gaat u naar "App Connectors". Hier wordt de optie gegeven om een nieuwe app connector toe te voegen. We duiden hier GitHub aan en vullen vervolgens de nodige gegevens aan.



Ook moet er toestemming vanuit een administrator account vanuit de GitHub organisatie worden goedgekeurd.



Als de verbinding al succesvol is gekoppeld, is er toegang tot meer informatie van deze app. Je kan hier naartoe gaan door naar instellingen te gaan. Onder cloud apps gaat u naar "App Connectors". Hier zal GitHub integratie tussen staan. Als er op de naam geklikt wordt, opent er een dashboard. Op dit dashboard kunnen gegevens gevonden worden zoals active users en een activity chart.

Settings > Cloud apps > Integration_Test

Integration_Test Code hosting

SECURITY RECOMMENDATIONS

Dashboard Info Accounts Activity log Alerts

Overview

User activities by top frequent locations ⓘ



Je kan ook de verschillende accounts die gevonden zijn binnen deze integratie opvragen. Filteren is hier ook een optie. Dit maakt het makkelijker om specifieke gebruikers op te zoeken.

Dashboard Info Accounts **Activity log** Alerts

Filters: Advanced filters

User name: Select users ⏺ | Affiliation: Internal | External | Type: User | Account

Groups: Select user group ⏺ Show admins only

Export | 1 - 1 of 1 users and accounts | Hide filters | Table settings

User name	Affili...	Type	Email	Apps	Grou...	L...
Robbe Sas	Internal	Account	sasrobbe			Apr ...

Hiernaast is er ook een activity log. Hier worden alle activiteiten in opgelijsd die vanuit GitHub komen. Hier worden heel wat activiteiten naar doorgestuurd zoals: repo creations, repo deletions, renames, downloads en meer. Per log worden heel wat gegevens bijgehouden. Hieronder valt de gebruiker, het ip-adres, locatie en datum. Ook kan vanuit hier een policy worden gemaakt.

Queries: Select a query Advanced filters

User name: **Select users** Raw IP address: Activity type: **Select value**

Location: **Select countries/regions**

Show details Hide filters Table settings

Activity	User	IP a...	Location	Device	D
>Delete: folder sakurashie	sasrobbe	81.82.2...	Belgium	—	Apr 1...
>Delete: folder sakurashie	sasrobbe	81.82.2...	Belgium	—	Apr 1...
Delete: folder sakurashie	sasrobbe	81.82.2...	Belgium	—	Apr 1...
Create: folder sakurashie	sasrobbe	81.82.2...	Belgium	—	Apr 1...
Edit: permission repo.ch	sasrobbe	81.82.2...	Belgium	—	Apr 1...
Edit: permission repo.ch	sasrobbe	81.82.2...	Belgium	—	Apr 1...

Ten slotte kunnen de alerts, gemaakt door deze integratie, ook worden opgehaald. Deze alerts kan je via dit venster terugvinden of in het algemeen alert dashboard van Microsoft Defender.

Integration_Test Code hosting

SECURITY RECOMMENDATIONS

Dashboard Info Accounts Activity log **Alerts**

Filters: Advanced filters

Status: Category: **Select risk category** Severity: 

User name: **Select users** Policy: **Select policy**

Bulk selection Hide filters Table settings

Alert	Sta...	Res...	Sev...	Da...
 deleted multiple repos in github enterprise Q deleted multiple repos in g... ↗ Integration_Test ↗ Rob...	<input type="button" value="OPEN"/>	—		Me... 4/11/20...

Voor dit voorbeeld hebben wij een eigen policy aangemaakt dat een alert maakt. Deze policy zal een alert maken wanneer drie of meer folders verwijderd zullen worden binnen organisaties die geregistreerd staan binnen onze GitHub enterprise. Hier is ervoor gekozen om pas actie te voeren wanneer de activiteit drie keer binnen 30 minuten is gebeurd. Dan wordt er ook gelimiteerd dat deze activiteiten binnen dezelfde app moeten gebeuren en enkel unieke activiteiten gelden. De configuratie van de policy ziet er als volgt uit:

Create filters for the policy

Act on:

Single activity
Every activity that matches the filters

Repeated activity:
Repeated activity by a single user

Minimum repeated activities:

Within timeframe: minutes

In a single app

Count only unique target files or folders per user ⓘ

Hier wordt de filter ingesteld. Met deze filter kan de policy door de activity log kijken naar passende entries. In dit geval kijkt de policy naar delete activities uit onze GitHub enterprise genaamd "sakurashield". Rechts kan je kiezen om deze filters te testen door te klikken op "Edit and preview results". Hierdoor kan je zeker zijn dat de gebruikte filter werkt naargelang je wilt bereiken.

Activities matching all of the following

Activity type equals Delete

Activity objects Item equals sakurashield ⓘ

+ Add a filter

>Edit and preview results

Ten slotte geven we ook nog mee hoe de policy alerts aanmaakt en of er verdere acties moeten worden uitgevoerd. Hier kiezen we ervoor dat telkens wanneer deze policy wordt uitgevoerd er ook een alert zal gemaakt worden. Ook kan er gekozen worden om bijvoorbeeld de gebruiker opnieuw te laten inloggen wanneer dit gebeurt. Dit kan aangezet worden onder "Governance actions".

Alerts

Create an alert for each matching event with the policy's severity

Send alert as email ⓘ

Daily alert limit per policy

Send alerts to Power Automate
[Create a playbook in Power Automate](#)

Governance actions

All apps

Microsoft 365

This policy was modified 2 hours ago

Om deze policy te testen, zijn er drie nieuwe repositories aangemaakt die hierna gelijk weer verwijderd zijn. Dit zal drie nieuwe entries aanmaken in de activity log.

⌚	Delete: folder sakur	sasrobbe	81.82.243.152	Belgium	—	Apr 11, 2024 ...	⋮
⌚	Delete: folder sakur	sasrobbe	81.82.243.152	Belgium	—	Apr 11, 2024 ...	⋮
⌚	Delete: folder sakur	sasrobbe	81.82.243.152	Belgium	—	Apr 11, 2024 ...	⋮

Dit zal dan de policy moeten aanspreken aangezien deze drie entries binnen de 30 minuten zijn binnengekomen. Hierdoor zal er ook een alert aangemaakt worden.

The screenshot shows the Microsoft Defender interface with the 'Alerts' tab selected. At the top, there are filters for Status (OPEN), Category (Select risk category), Severity (Low, Medium, High), and User name (Select users). Below the filters are buttons for Bulk selection and Export. A dropdown menu labeled 'Alert' is open. One alert is highlighted with a red circle and icon. The alert details are as follows:

- Icon: Red circle with a white alert symbol.
- Message: deleted multiple repos in github enterprise
- Details: deleted multiple repos in g... Integration_Test Robbe Sas 81.82.243.152 Belgium

API

Microsoft Defender biedt een reeks API's die het mogelijk maken om de functionaliteiten van Microsoft Defender for Endpoint te integreren en te automatiseren in andere systemen en workflows. Hieronder vindt u een uitleg over de drie soorten API's die worden aangeboden:

- **Microsoft Defender for Endpoint API**
 - Dit is een gestructureerde API die toegang geeft tot gegevens en mogelijkheden van Microsoft Defender for Endpoint, zoals het onderzoeken van entiteiten en het uitvoeren van reacties op apparaten.
- **Raw Data Streaming API**
 - Deze API maakt het mogelijk om gebeurtenissen en waarschuwingen rechtstreeks te verzenden naar Azure Event Hubs of Azure Storage, hiermee kan er langdurige dataretentie voorzien worden. Het ondersteunt het streamen van gebeurtenissen via Advanced Hunting naar Event Hubs en/of Azure Storage Account.
- **SIEM API**
 - Hiermee kunnen detecties van Microsoft Defender XDR worden opgehaald met behulp van SIEM-oplossingen zoals Microsoft Sentinel, IBM QRadar en Splunk, waardoor incidenten en waarschuwingen kunnen worden gebruikt voor incident response.⁸

Vooraleer de API gebruikt kan worden, moeten er eerst een aantal stappen ondernomen worden. Deze stappen zijn als volgt:

⁸ 'Overview of management and APIs', Microsoft.com

- Maak een Microsoft Entra application
- Verkrijg een access token door middel van deze application
- Gebruik de verkregen token om Defender for Endpoint API te gebruiken

Multi-tenant

Microsoft Defender biedt de mogelijkheid om meerdere tenants te beheren via het Microsoft Defender multi-tenants portaal. Dit kan handig zijn voor managed security service providers (MSSP's) die de omgevingen van hun klanten beheren. Om een tenant toe te kunnen voegen heb je één van de twee benodigdheden nodig zodat deze beheerd kan worden via dit portaal. Dit is ofwel Granular delegated admin privilege (GDAP) of Microsoft Entra B2B authentication.

The screenshot shows the Microsoft Defender Multi-tenant portal interface. At the top, there is a navigation bar with icons for home, shield, and more, followed by the title "Microsoft Defender | Multi-tenant". A search bar and user profile are also present. Below the title, a sidebar on the left contains icons for tenant management, device inventory, threat hunting, and endpoint security enhancement. The main area is titled "Tenants" and displays the following statistics in large boxes:

Tenant	Exposed devices	Critical CVEs	High severity CVEs	Security recommendations
1	2	4	203	31

Below these stats, a table lists tenant details:

Tenant name	Exposure score ↓	Exposure change	Exposed de...	Recommendati...	Weaknesses	Critical C...
VRA - Stag...	34 (Medium)	▼ 13	2 / 3	31	272	4

Het portaal kan alles iets beperkter dan het originele Microsoft Defender portaal, maar kan wel alle belangrijke functionaliteiten die het zou moeten doen. Hier valt onder: alerts/incidents, Threat hunting, device inventory, endpoint security enhancement.

Assignments

Daarbovenop biedt nog een extra functionaliteit. Deze functionaliteit noemt "assignments", maar om dit aan te zetten moet men eerst in het Microsoft Defender portaal van die tenant onder de Microsoft Defender XDR instellingen "Multi-tenant content source" aanzetten.

The screenshot shows the Microsoft Defender XDR Settings interface. On the left, there's a sidebar with various icons and a navigation tree. The main area has a search bar at the top. Below it, the title 'Microsoft Defender XDR' is displayed. A horizontal line separates this from the settings area. The left side of the settings area has a 'General' section with several options: Account, Email notifications, Alert service settings, Permissions and roles, Streaming API, and Multi-tenant content source. The 'Multi-tenant content source' option is highlighted with a red box. Below this is a 'Rules' section. To the right, under 'Multi-tenant content source', there's a description: 'Allow multi-tenant administrators to use this tenant as a source of security content, including custom detections.' A toggle switch labeled 'Allowed' is set to 'On'. At the top right of the main area, there are several small icons.

Nu dit aanstaat kan er aan de hand van Detection Rules assignments over meerdere tenants gestuurd worden. Om meer specifieke resultaten te verkrijgen is het ook mogelijk om device groups mee te geven. Hiermee kan je een groep geselecteerde endpoints aanspreken om deze assignment op uit te voeren.

Verder is er ook een detection rule nodig om een assignment aan te maken. Deze kan gemaakt worden in het Microsoft Defender portaal onder hunting. In Advanced Threat Hunting kan er een nieuwe editor geopend worden door op het plusje te duwen. Hierin kan de Detection rule aangemaakt worden. Een van de detection rules dat wij hebben aangemaakt is de volgende:

The screenshot shows a 'Detection rule' editor window. It contains a code block with a numbered list of PowerShell-like commands. The first few lines are: 1 DeviceEvents, 2 | where Timestamp > ago(30d), 3 | where ActionType == "AntivirusDetection". The code continues with summarize and where clauses. The entire code block is numbered from 1 to 6.

Deze gaat tussen de device events van de afgelopen 30 dagen kijken naar antivirus detecties. Als de hoeveelheid van deze detecties groter is dan vijf, dan wordt er een actie aan het apparaat gekoppeld. De acties die uitgevoerd kunnen worden zijn:

- *Isolate device*
- *Collect investigation package*
- *Run antivirus scan*
- *Initiate investigation*
- *Restrict app execution*

Dit zijn de mogelijkheden als het gaat over devices. We kunnen ook aan de hand van andere zaken acties uitvoeren naargelang de detection rule, deze zijn: files, users en e-mails. Hieronder staan de bijbehorende acties:

- **Files**
 - Allow/Block
 - Quarantine file
- **Users**
 - Mark user as compromised
 - Disable user
 - Force password reset
- **Emails**
 - Move to mailbox folder
 - Delete e-mail

Na het aanmaken van de assignment waarbij je de assignment een naam geeft, er een detectie rule aan koppelt, de tenants aanduidt en eventuele device groups selecteert, ziet het er als volgt uit.

The screenshot shows the Microsoft Defender Multi-tenant interface. The top navigation bar includes 'Microsoft Defender | Multi-tenant', a search bar, and various icons. The main area is titled 'Assignments' with the sub-instruction 'Group similar tenants and apply relevant content with assignments.' Below this is a toolbar with 'Create assignment', 'Edit assignment', 'Remove assignments', 'Sync assignments', and a search bar. A table lists an assignment named 'Run AVscan on detected files'. The columns include 'Name', 'Applied to...', 'Content', 'Last sync ...', 'Last sync...', 'Last synced by', 'Created on', and 'Created by'. The entry shows 'Run AVscan on detected files' applied to '1 tenant' with '1 detection' and a status of 'Successful' (22-3-2024). It was created by 'Robbe@sakura...' on 22-3-2024 at 11:42:... and last synced by 'Robbe@sakura...' on the same date and time.

DEMO

Om de daadwerkelijke kracht van beide XDR-platformen te kunnen tonen en hier de verschillen in te kunnen vinden, is het belangrijk om een simulatie voor beide platformen uit te voeren. Hierdoor kunnen we zien welke alerts worden aangemaakt en wat er geblokkeerd wordt. Hieruit kunnen we vervolgens eigen conclusies trekken die zullen helpen bij de vergelijking tussen de twee producten.

MalwareBazaar

MalwareBazaar is een project gemaakt door abuse_ch. Hier worden verschillende soorten malware samples op geüpload. Dagelijks kan dit tot honderden samples zijn die door verschillende bronnen zijn geüpload. MalwareBazaar is community-driven en biedt vele verschillende soorten malware. Hiermee wilt abuse_ch ervoor zorgen dat het internet een veiligere plaats wordt.

Wij hebben doorheen onze stage hier verschillende keren malware samples gedownload. Wij vonden het belangrijk om dit meerdere keren en met verschillende samples te doen om zo een accuraat resultaat te verkrijgen.

Het downloaden van een malicious bestand via MalwareBazaar ziet er als volgt uit:

MALWARE bazaar by ABUSE.ch

- [Browse](#)
- [Upload](#)
- [Hunting](#)
- [API](#)
- [Export](#)
- [Statistics](#)
- [FAQ](#)
- [About](#)
- [Login](#)

Browse Database

See search syntax see below, example: tag:TrickBot

[Search](#)

Search Syntax [?](#)

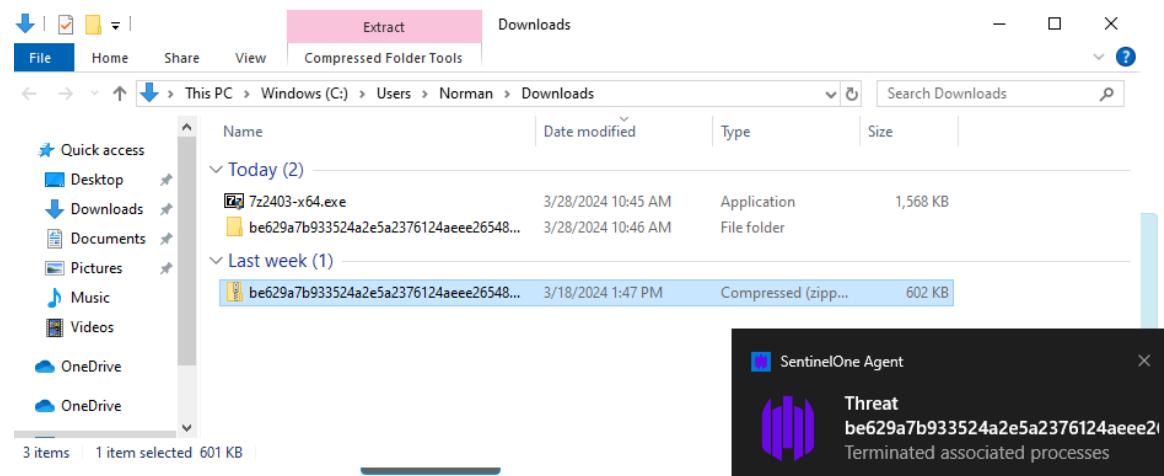
Search:

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2024-03-28 09:49	307815ae8a2bd9a92066...	dll		dll zgrAT	Anonymous	Cloud
2024-03-28 09:47	2c39793aae8f8966937d5...	exe	Neshta	exe Neshta	cocaman	Cloud
2024-03-28 09:47	8b256bc239fb12c41017...	zip	Neshta	Neshta zip	cocaman	Cloud
2024-03-28 09:46	c2ddcab49f620d41df9...	exe		32 exe	zbetchekin	Cloud
2024-03-28 09:41	99d42ee02b2d43170796...	exe	GCleaner	32 exe gcleaner trojan	zbetchekin	Cloud
2024-03-28 09:31	fe156159a26f8b7c140db...	lnk	Kimsuky	apt Kimsuky lnk	smica83	Cloud
2024-03-28 09:31	7b741ba5f5bfe5a6045f1...	lnk		lnk	cocaman	Cloud
2024-03-28 09:31	636a279a20a10b244241...		Guloader	Guloader Xxe	Anonymous	Cloud
2024-03-28 09:23	0412820e4dacf52180862...	exe	CoinMiner	CoinMiner exe	SecuriteInfoCom	Cloud

Zo ziet de database van MalwareBazaar eruit. Zoals je kan zien worden er vele verschillende soorten malware aangeboden en wordt de database zeer regelmatig geüpdatet. Wij stellen voor om niet de meest recente uploads te downloaden aangezien deze nog te nieuw kunnen zijn en dus mogelijk niet herkend kunnen worden door detectiesystemen.

Als je er één gekozen hebt, dan kan je de sample in de vorm van een geëncrypteerde zip-bestand downloaden. Om deze zip te kunnen openen, gebruiken wij 7-zip. Met 7-zip kunnen wij, aan de hand van het meegeleverde wachtwoord, het bestand unzopen op een van de endpoints.

Wij hebben het al eens meegemaakt dat Microsoft Defender soms het geëncrypteerde zip-bestand al detecteert en automatisch verwijdert. Ditzelfde is bij SentinelOne nog niet voorgekomen. Daarentegen is het detecteren van SentinelOne wel sneller in vergelijking met Microsoft Defender, dit duurt gemiddeld langer dan bij SentinelOne.



Hierboven ziet u de SentinelOne agent op een van de endpoints die het unzipped bestand detecteert. Het detecteren van het bestand ging enorm snel en het daarna automatisch verwijderen volgde er direct na. Ook het binnenkrijgen van de alert op het dashboard van SentinelOne gebeurde heel snel. Als wij ditzelfde doen op een endpoint dat gebruikt maakt van

Microsoft Defender, dan gaan dezelfde stappen, zoals hiervoor beschreven staan, ook uitgevoerd worden. Enkel gaat dit wat langer duren. Na het unzippen wordt het bestand pas na 1-2 minuten gedetecteerd en vervolgens automatisch verwijderd. De alert op het dashboard zien kan zelfs soms nog langer duren.

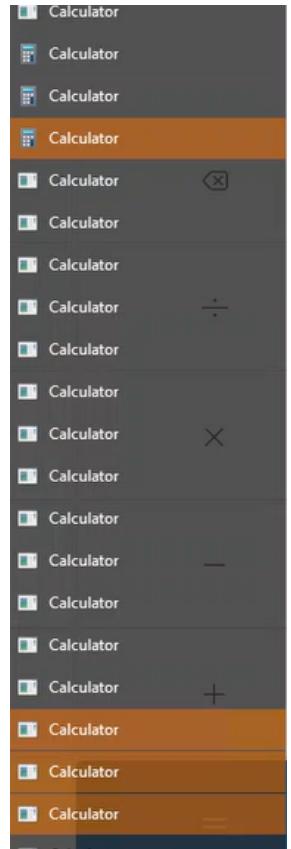
EDR-Testing-script

Hier wordt getest welke activiteiten een alert kunnen aanmaken. Wij gebruiken hiervoor een GitHub repo dat een bat-script bevat. Dit script voert een heleboel vaak gebruikte tools en technieken uit die een hacker min of meer ook zou uitvoeren. Hierdoor kunnen wij de nauwkeurigheid van ons XDR-systeem testen. Het gebruikte script en de technieken die dit script test, kunnen via [deze link](#) worden teruggevonden.

Op een endpoint dat beveiligd wordt met Microsoft Defender wordt de repo gedownload. Het unzippen zorgde voor een alert. Verder werd het niet gezien als malicious. Pas bij het uitvoeren van het script begonnen de alerts binnen te komen. De meeste testen openen de calculator app, maar in principe is het niet moeilijk om de uiteindelijke executie aan te passen naar iets dat wel schadelijk kan zijn.

Tegen het einde van het uitvoeren van de testscript stonden er een heleboel calc-applicaties open. Elk van deze openstaande applicaties is een aparte tool/techniek gebruikt door het script. In principe zou elke van deze openstaande applicaties voor een alert gezorgd moeten hebben.

Het Defender portaal heeft een nieuw incident geregistreerd, inclusief de bijbehorende waarschuwingen. In sommige gevallen hebben we overeenkomsten gevonden tussen deze waarschuwingen en de uitgevoerde technieken.



A screenshot of the Microsoft Defender portal. The main title is "Multi-stage incident involving Execution & Discovery including Ransomware on one endpoint". The "Alerts" tab is selected, showing three recent alerts: 1. "Mar 22, 2024 10:47 AM New 'Smokeloader' malware was detected" (werkend-bakske2). 2. "Mar 26, 2024 8:14 AM New Malware was detected in a zip archive file" (werkend-bakske2). 3. "Mar 26, 2024 8:14 AM New PowerSploit post-exploitation tool" (werkend-bakske2). To the right, there is an "Incident graph" visualization showing connections between nodes: "WERKEND-BAKSKE2" is connected to "3 IPs", "((o))", "6 URLs", and "91 Files". A "Manage incident" button is also visible.

Op SentinelOne hebben we hetzelfde geprobeerd. Bij het downloaden van de repo werd er gelijk al een alert aangemaakt en werden de bestanden van de endpoint verwijderd. Verder zijn we te weten gekomen dat het bat-bestand in de repo op zichzelf kan werken zonder de andere bestanden in de repo nodig te hebben. Met deze informatie hebben we de inhoud van het originele bat-bestand gekopieerd in een zelfgemaakte bat-bestand. Hierdoor werd het wel mogelijk om dit op de endpoint uit te voeren zonder dat dit verwijderd wordt door SentinelOne. Bij het uitvoeren was het mogelijk om een paar van de technieken uit te voeren, maar plots werd het volledige script gekilled en werd er een rollback gestart.

BESLUIT

EDR

De EDR van SentinelOne is beter, sneller en heeft geavanceerdere opties qua response en detection, de manier van alerts en threats tonen is simpeler en duidelijker dan die van Defender.

THREAT HUNTING

Beide platformen bieden de mogelijkheid om aan threat hunting te doen. Beide hebben ook gelijke functionaliteiten binnen threat hunting, maar kunnen niet volledig hetzelfde. Dit zorgt ervoor dat bepaalde zaken die bijvoorbeeld binnen SentinelOne zeer eenvoudig gaan, moeizamer of zelfs niet lukken binnen Microsoft Defender.

INTEGRATIES

SentinelOne biedt meer integraties aan dan Defender en deze zijn makkelijker toepasbaar, SentinelOne doet dit aan de hand van hun Singularity marketplace. Defender doet op een andere manier. In de Defender portaal staan automatisch al een aantal integraties van andere Microsoft portalen. Ook kunnen er integraties worden toegevoegd tussen de Microsoft Defender technology partners. Deze vereisen, in tegenstelling tot SentinelOne, wel wat manuele configuratie en kan niet binnen Defender zelf worden toegevoegd.

DOCUMENTATIE

Aangezien Microsoft Defender heel wat functionaliteiten binnen het portaal aanbiedt, is er de mogelijkheid dat bepaalde zaken niet duidelijk zijn en extra uitleg vragen. Op elke pagina staat een knop dat u doorverwijst naar een Microsoft Learn pagina. Deze pagina's zijn zo goed als altijd zeer volledig en up-to-date. Dit doet Microsoft zeer goed.

DEPLOYMENTS

SentinelOne maakt gebruik van een agent die wij deployen door middel van Intune, Defender for endpoint maakt gebruik van Intune voor het pushen van Defender policies naar de endpoints. Intune is soms traag in het pushen van deze policies, dit is iets wat SentinelOne niet heeft aangezien Intune alleen nodig is voor de installatie van de agent en de policy configuraties gebeuren door SentinelOne cloud.

ALGEMENE VERGELIJKING

Ons onderzoek heeft geleid tot een heleboel conclusies en meningen rond de twee XDR-oplossingen. Waaruit we kunnen constateren dat Defender XDR interessant is voor omgevingen die een nadruk leggen op het Microsoft ecosysteem en de beveiliging hiervan. Terwijl SentinelOne voor klanten bestemd is die hier geen nadruk op leggen en eerder op zoek zijn naar één van de betere opties op de markt rond security. Mensen die kiezen voor SentinelOne kiezen voor een XDR met geavanceerde detectie met snelle response, eenvoudige implementatie en beheer, flexibele integratie en . Aan de andere kant, mensen die kiezen voor Defender XDR kiezen voor een XDR die naadloze integratie met Microsoft 365, uitgebreide hoeveelheid aan functionaliteiten, kostenefficiëntie en betrouwbare ondersteuning biedt.

BRONNEN

Configure Microsoft Defender for Endpoint in Intune. (2024, 18 januari). Microsoft. Geraadpleegd op 19 maart 2024. van <https://learn.microsoft.com/en-us/mem/intune/protect/advanced-threat-protection-configure>

Deception Objects Overview. (2023, 02 november). Community SentinelOne. Geraadpleegd op 22 april 2024. van <https://community.sentinelone.com/s/article/000007832>

Email analysis in investigations for Microsoft Defender for Office 365. (2024, 2 april). Microsoft Learn. Geraadpleegd op 5 april 2024. van

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-analysis-investigations?view=o365-worldwide>

Extended Detection and Response. (XDR) (z.d.). Microsoft. Geraadpleegd op 5 maart 2024. van <https://www.microsoft.com/en-us/security/business/solutions/extended-detection-response-xdr>

FAQ. (2024, 26 februari). SentinelOne. Geraadpleegd op 5 maart 2024. van <https://www.sentinelone.com/faq/#sentinelone-integrations>

Indicators. (2024, 25 maart). Community SentinelOne. Geraadpleegd op 26 maart 2024. van <https://community.sentinelone.com/s/article/000006251>

Microsoft Defender XDR. (z.d.). Microsoft. Geraadpleegd op 5 maart 2024. van <https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-xdr>

Microsoft Sentinel documentation. (z.d.). Microsoft Learn. Geraadpleegd op 6 maart 2024. van <https://learn.microsoft.com/en-us/azure/sentinel/>

Overview of management and APIs. (2023, 27 september). Microsoft learn. Geraadpleegd op 2 april 2024. van <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/api/management-apis?view=o365-worldwide>

Policy CSP - DeviceInstallation. (2024, 18 januari). Microsoft. Geraadpleegd op 19 maart 2024. van <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-deviceinstallation#deviceinstallatior-n-allowinstallationofmatchingdevicesetupclasses>

Policy CSP - DmaGuard. (2024, 18 januari). Microsoft. Geraadpleegd op 19 maart 2024. van <https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-dmaguard#dmaguard-deviceenumerationpolicy>

Remote Shell. (2024, 25 maart). Community SentinelOne. Geraadpleegd op 29 maart 2024. van <https://community.sentinelone.com/s/article/000005095>

Rogues Overview. (2024, 25 maart). Community SentinelOne. Geraadpleegd op 30 april 2024. van <https://community.sentinelone.com/s/article/000006410>

Scanner Policies. (2024, 18 april). Community SentinelOne. Geraadpleegd op 22 april 2024. van <https://community.sentinelone.com/s/article/000007978>

Setting Up Credentials for Ranger Deploy. (2024, 25 maart). Community SentinelOne. Geraadpleegd op 30 april 2024. van <https://community.sentinelone.com/s/article/000006424>

Setup-xdr-tools. (2023, 14 december). Microsoft Learn. Microsoft Learn. Geraadpleegd op 5 maart 2024. van <https://learn.microsoft.com/en-us/security/operations/setup-xdr-tools>

ThreatPath Overview. (2024, 25 maart). Community SentinelOne. Geraadpleegd op 19 april 2024. van <https://community.sentinelone.com/s/article/000007785>

Use automated investigations to investigate and remediate threats. (2022, 22 december). Microsoft Learn. Geraadpleegd op 25 maart 2024. van <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automated-investigations?view=o365-worldwide>

Using the Endpoint Details Window. (2024, 25 maart). Community SentinelOne. Geraadpleegd op 27 maart 2024. van <https://community.sentinelone.com/s/article/000004948>

Using the Process Graph. (2024, 25 maart). Community SentinelOne. Geraadpleegd op 25 maart 2024. van <https://community.sentinelone.com/s/article/000006310>

What is Microsoft Defender XDR. (2023, 15 november). Microsoft Learn. Geraadpleegd op 5 maart 2024. van <https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide>

Windows 10 Device Guard and Credential Guard Demystified. (2021, 28 januari). TechCommunity Microsoft. Geraadpleegd op 27 maart 2024. van <https://techcommunity.microsoft.com/t5/iis-support-blog/windows-10-device-guard-and-credential-guard-demystified/ba-p/376419>

Working with Protection Policies. (2024, 18 april). Community SentinelOne. Geraadpleegd op 19 april 2024. van <https://community.sentinelone.com/s/article/000008002>