ZOLDER

MISP TO MICROSOFT SENTINEL

White Paper

1

Het thema cybersecurity is actueler dan ooit, zeker voor organisaties die voortdurend grote hoeveelheden bijzondere persoonsgegevens verwerken, zoals de zorg. Maar niet alleen de zorg krijgt te kampen met een toenemende complexiteit van cybersecurity. Dit geldt zeker ook voor andere (overheid)sectoren.

In een succesvolle cybersecuritystrategie is de uitwisseling van dreigingsinformatie tussen vertrouwde partners cruciaal. Hoe houd je daar als organisatie voldoende grip op en hoe richt je dat zo voordelig en effectief mogelijk in op ICT-gebied?

Het uitwisselen van dreigingsinformatie is een taak van het Nationaal Cybersecurity Centrum (NCSC) en zijn buitenlandse equivalenten. In Nederland wordt binnen het Landelijk Dekkend Stelsel (LDS) op gecontroleerde wijze dreigingsinformatie verspreid onder bepaalde doelgroepen.

Op technisch niveau is het Nationaal Detectie Netwerk (NDN) gerealiseerd, met als doel om de uitwisseling van dreigingsinformatie te automatiseren. Maar hoe koppelt een deelnemende organisatie die data aan de eigen ICT?

In veel gevallen wordt dreigingsinformatie beschikbaar gesteld via het MISP platform. Deze Whitepaper beschrijft hoe de data vanuit het MISP gekoppeld kan worden aan Microsoft Sentinel om zo signalen van verdacht gedrag in de kern van de kantoorautomatisering waar te kunnen nemen.

INHOUDSOPGAVE

1 INLEIDING & PROBLEEMSTELLING

In het Landelijk Dekkend Stelsel en het Nationaal Detectie Netwerk zijn diverse aanbieders van dreigingsinformatie actief, elk met een eigen doelgroep en werkwijze. In meerdere gevallen maakt de aanbieder gebruik van het Malware Information Sharing Platform (MISP) om de dreigingsinformatie als Cyber Threat Intelligence (CTI) beschikbaar te stellen.

1.1 Informatie uit MISP halen

Afnemers van dreigingsinformatie vanuit een MISP server, kunnen op MISP inloggen om die informatie te downloaden in diverse bestandsformaten, of een softwarekoppeling leggen met een MISP API om de informatie automatisch te verbinden aan de eigen beveiligingssystemen, zoals een Intrusion Detection Systeem (IDS) of Security Information and Even t Management (SIEM).

Voor een dergelijke koppeling zijn scripts nodig die de informatie kunnen interpreteren én op de juiste manier in het doelsysteem kunnen wegschrijven. Ook moeten dergelijke scripts regelmatig, bijvoorbeeld elke dag, worden gedraaid om de laatste CTI te verwerken, waarvoor enige ICT-infrastructuur nodig is.

1.2 Het probleem

De ontwikkeling van de scripts en het onderhoud van de ICT-infrastructuur is voor veel organisaties onbegonnen werk: te complex en (dus) te duur. Het gevolg? De doelgroep kan de waardevolle dreigingsinformatie alleen in rapportvorm tot zich nemen. Maar dat is om drie redenen onwerkbaar:

1. De organisaties beschikken gemiddeld genomen niet altijd over een securityteam om de dreigingsinformatie te interpreteren.
2. Het gaat om grote hoeveelheden dreigingsinformatie, die doorlopend wordt aangevuld.
3. Het doel, namelijk om snel te signaleren dat een bekende aanval wordt uitgevoerd, wordt gemist.

Dit alles kan ertoe leiden dat onvoldoende duidelijk is wat er moet gebeuren met bijvoorbeeld een door het Nationaal Detectie Netwerk geclassificeerd spambericht.

Kortom: ook al zijn er veel organisaties aangesloten bij het NDN en LDS, als de geautomatiseerde CTI-keten niet actief is vanwege bijvoorbeeld de grote complexiteit en/of te hoge kosten, dan bereikt de uitwisseling van dreigingsinformatie het doel niet. En dit vormt een niet te verwaarlozen bedreiging voor de cyberweerbaarheid van de Nederlandse maatschappij.

2

Oplossing

De koppeling van MISP met Microsoft Sentinel via een onderhoudsvriendelijke Azure Function.

2 GERICHTE OPLOSSING

2.1 De richting

Hoe valt een zodanige bedreiging voor cybersecurity in Nederland op te lossen? Om de gedeelde CTI effectief te benutten, kunnen organisaties die ook gebruik maken van Microsoft 365-cloud, de CTI-feed van hun aanbieder vanuit het MISP-platform koppelen aan Microsoft Sentinel.

Door de gedeelde dreigingsinformatie te kunnen vergelijken met de logging van Microsoft 365 wordt het mogelijk om in Microsoft 365 relevante alarmen en waarschuwingen in te stellen. Zo kan er bijvoorbeeld een melding worden ingesteld als iemand probeert aan te melden bij Microsoft Teams vanaf een IP-adres dat in MISP is geclassificeerd als kwaadaardig, of als een collega een e-mail ontvangt vanaf een eerder ontdekt spamadres.

In deze whitepaper beschrijven we hoe de koppeling van een MISP-server met Microsoft Sentinel gerealiseerd kan worden met een eenvoudige set-up die onderhoudsvriendelijk is en nauwelijks extra geld kost. Deze koppeling is initieel gebouwd door Zolder op verzoek van GGD GHOR Nederland, waarna besloten is de opgebouwde kennis publiek te delen.

2.2 Drie componenten

In deze set-up maken we gebruik van drie componenten:

1. MISP als de bron

2. Microsoft Sentinel als doelfunctie bij de afnemer

3. Een Azure Function om data vanuit de bron in het doel te krijgen.

Bij stap 3 komen een aantal specifieke knelpunten aan het licht. Immers, met Azure Functions is het mogelijk om dreigingsinformatie op een laagdrempelige maar onderhoudsvriendelijke manier in de praktijk te verwerken en toe te passen. Maar het neerzetten van Azure Functions vereist doorzettingsvermogen. Bovendien: wie controleert of het nog werkt? Wie bouwt precies de juiste KQL-queries? En wie volgt de alarmen op en hoe?

Voor organisaties zonder eigen security team (en misschien ook wel degene met), is het antwoord op deze vragen: Attic. Attic is een eenvoudig portaal, in de vorm van een mobiele app, waarmee organisaties toegang krijgen tot actuele securityinformatie, meldingen en aanbevelingen over eventuele problemen met de eigen digitale voorzieningen en hoe die aan te pakken en op te lossen. Attic wordt gekoppeld wordt aan de ICT-voorzieningen/applicaties in de Microsoft cloud. Hoe dit werkt, leest u in deze whitepaper.

3

Installatie

Installeren en configureren van de 3 benodigde componenten: MISP, Microsoft Sentinel en een Azure Function.

3 INSTALLATIE

3.1 Stap 1: MISP

Als afnemer van dreigingsinformatie heeft u toegang tot de MISP-server van uw aanbieder, die zij gebruiken om threat intelligence uit te wisselen. In sommige gevallen, wordt de MISP-server beschermd door een firewall, waardoor het nodig is dat u eerst het IP-adres doorgeeft van waar u de MISP-server wilt raadplegen.

MISP is daarna bereikbaar via een web-browser. Door aan te melden, kunt u de API sleutel die behoort bij uw account vinden.

In bijlage I treft u een handleiding voor verkrijgen van de API-sleutel.

3.2 Stap 2: Sentinel

Microsoft Sentinel fungeert binnen de Microsoft Cloud als een SIEM-tool, waar Microsoft365-abonnees gratis gebruik van kunnen maken. Een aantal cruciale logbronnen van Microsoft zelf zijn zonder extra kosten toe te voegen[1].

Heeft u Sentinel nog niet geactiveerd? Raadpleeg dan bijlage II bij deze whitepaper voor verdere instructies.

Kosten Microsoft Sentinel

Goed om alvast te weten is dat als u Microsoft Sentinel wilt inschakelen, u binnen de 'tenant' van de Microsoft-omgeving een Azure Subscription nodig heeft. Die Subscription zelf kost geen geld, maar configureert op welke wijze in Azure gemaakte kosten in rekening gebracht kunnen en mogen worden. Het is mogelijk om een test/trial subscription te registreren om de set-up eerst een maand kosteloos te testen.

Helaas is het kostenaspect van dataopslag in Sentinel een vrij complex verhaal. Het kan gaan over enkele euro's per maand maar de totale kosten zijn afhankelijk van een groot aantal factoren. Het voert te ver om dat ook in deze whitepaper uiteen te zetten.

Op de website geeft Microsoft uitleg bij het prijsmodel[2]. De kosten die gemoeid zijn met de Azure Function in volgende paragraaf zijn een stuk voorspelbaarder en daar zetten we dus ook wat ervaringscijfers voor uiteen.

Een manier om gecontroleerd uit te vinden wat de kosten voor Sentinel bedragen is door in de instellingen van de subscription de kosten te limiteren tot een acceptabel bedrag. Tevens kan een nieuwe subscription drie maanden in Trial worden geplaatst waardoor kosten niet in rekening worden gebracht. Zaak is dan wel om in die drie maanden het gebruik van Sentinel en deze MISP-koppeling al in doelsituatie actief te hebben om een goed beeld te krijgen van de verwachte kosten.

1) https://docs.microsoft.com/en-us/azure/sentinel/billing?tabs=commitment-tier#free-data-sources

2) https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/

3.3 Stap 3: Azure Function

Azure Functions dienen om geautomatiseerd zelfgeschreven scripts uit te laten voeren. Vroeger zou voor dat doel een server ingericht en onderhouden moeten worden. Het voordeel van Azure Functions is dan ook met name dat de onderliggende infrastructuur door Microsoft onderhouden wordt.

De complete set-up zoals we die nodig hebben, bestaat op hoofdlijnen uit de volgende Azure componenten:

1. **App Registration** – deze app krijgt de juiste rechten om data weg te schrijven in de ThreatIndicators tabel van Sentinel.
2. **Keyvault** – bevat de keys om geautomatiseerd te authenticeren bij de App Registration.
3. **Function** – bevat de scripts om in interval informatie uit MISP op te halen, te herschrijven naar bruikbare data en vervolgens via de App Registration in Sentinel te plaatsen.
4. **NAT Gateway** – (optioneel) maakt het mogelijk dat de function draait vanaf een vast IP-adres, zodat dit toegevoegd kan worden aan de allowlist van de firewall van MISP.

In bijlage III bij deze whitepaper treft u een uitgebreide step-by-step guide aan voor het gebruik van Azure Functions.

Kosten Azure Function

De kosten voor de Azure Function set-up kunnen we benaderen op basis van onze eigen ervaring in het derde kwartaal 2022. De genoemde bedragen zijn gemiddelden per maand en exclusief BTW.

Onderdeel	Kosten
Azure Function incl. Keyvault & Storage	€ 0,01
Premium Service Plan	€ 11,12
NAT Gateway	€ 27,94
Public IP	€ 3,10
Totaal	**€ 42,17**

De totale kosten in die periode van drie maanden bedroegen € 126,50. Dit is € 42,17 gemiddeld per maand, waarvan 99,7% gekoppeld aan de optionele configuratie die nodig is om een gefixeerd IP-adres aan de function te koppelen. Als MISP-publiek benaderbaar is, zullen de kosten verwaarloosbaar zijn.

3.4 Use Cases

Nu de dreigingsinformatie beschikbaar is in Sentinel, is het mogelijk om naar eigen inzicht rules te bouwen die alarm slaan als een match optreedt. Daarbij is belangrijk te beginnen met denken vanuit scenario's, ofwel use cases. Door namelijk eerst goed na te denken wanneer alarm geslagen moet worden, en vooral ook: wanneer niet, wordt vermeden dat een rule te vaak of onnodig triggert.

Een aantal voor de hand liggende use cases zijn beschikbaar in de GitHub waar ook de Function code geplaatst is: https://github.com/zolderio/misp-to-sentinel

Voorbeelden van KQL en verdere instructies, ook voor het maken van Sentinel Playbooks en Sentinel Rules, zijn te vinden in bijlage IV.

> *KQL is een krachtig hulpmiddel om data te onderzoeken en patronen te herkennen, afwijkingen te identificeren, statistische modellen te maken en meer.*

Kusto Query Language (KQL)

De use cases zijn geschreven in Kusto Query Language (KQL), de taal waarmee complexe Sentinel-zoekopdrachten worden geschreven. Ook het Microsoft Defender-portal werkt met KQL, dus het is geen overbodige luxe deze taal aan te leren.

Microsoft biedt hier zelf leermodule SC-200 voor aan: https://learn.microsoft.com/en-us/training/modules/analyze-results-kusto-query-language/

ZOLDER

De eenvoudige route: Attic Security

Hardening en monitoring voor Microsoft 365

Zoals we eerder al aangaven is Azure Functions onderhoudsvriendelijk en laagdrempelig, maar nog geen garantie voor een goedwerkend systeem. Met Attic biedt Zolder zorgorganisaties een oplossing: Attic is een unieke laagdrempelige optie om een Microsoft-omgeving te hardenen en te monitoren.

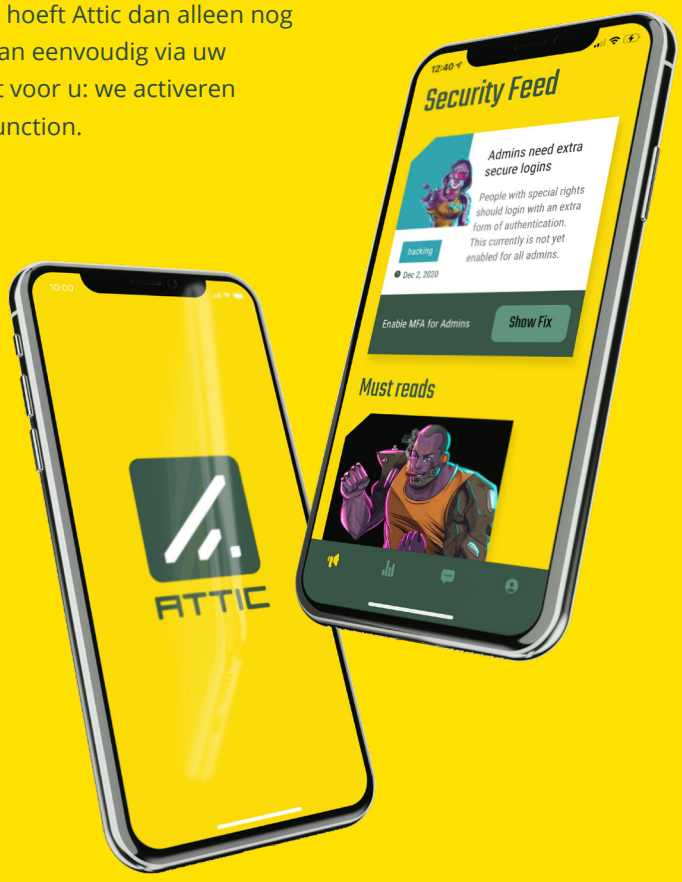
Attic detecteert niet alleen problemen, maar levert vaak ook direct de oplossing. Wanneer er een zwakte in Microsoft 365 wordt gedetecteerd, ontvangt u automatisch een melding. Als er een fix beschikbaar is, verhelpt u het probleem met een druk op de knop.

Daarvoor activeren wij onder andere Sentinel en optioneel kunnen we die verbinden aan een of meerdere MISP-bronnen. U hoeft Attic dan alleen nog maar te koppelen aan uw Microsoft-tenant. Dat kan eenvoudig via uw smartphone of webbrowser. Wij doen dan de rest voor u: we activeren Sentinel en zetten die in de lijst van onze Azure Function.

Attic kan ook prima draaien naast de bestaande relatie die u mogelijk al heeft met een andere Microsoft-partner, of zelfs als onderaannemer van die partner. Daarvoor hebben we Attic for MSP.

Interessant? Kijk dan eens op

atticsecurity.com



4

Conclusie

Onderhoudsvriendelijke set-up maakt de automatisering van uitwisseling van dreigingsinformatie bereikbaar voor de kleinste organisaties.

4 CONCLUSIE

De uitwisseling van dreigingsinformatie is een belangrijke factor in een landelijke cybersecuritystrategie. Zolang de dreigingsinformatie niet toegepast wordt in techniek, blijft het een ineffectieve maatregel.

Nu Microsoft cloud voor veel organisaties in het hart van de bedrijfsvoering staat, is dat misschien wel de belangrijkste IT-component om dreigingsinformatie op toe te passen.

Azure Functions bieden een zeer onderhoudsvriendelijke manier om dreigingsinformatie vanuit het Nationaal Detectie Netwerk in praktijk toe te passen. Het is een laagdrempelige, zo niet de laagstdrempelige, manier om het Landelijk Stelsel echt Dekkend te krijgen.

Dus elke organisatie met Microsoft 365 en een partner in het Landelijk Dekkend Stelsel, zonder actieve monitoring, zou deze configuratie moeten gaan bouwen.

Er is geen goede reden om het niet te doen, behalve het ontbreken van beschikbare kennis, maar dat lossen we graag voor u op via atticsecurity.com.

B

Bijlagen

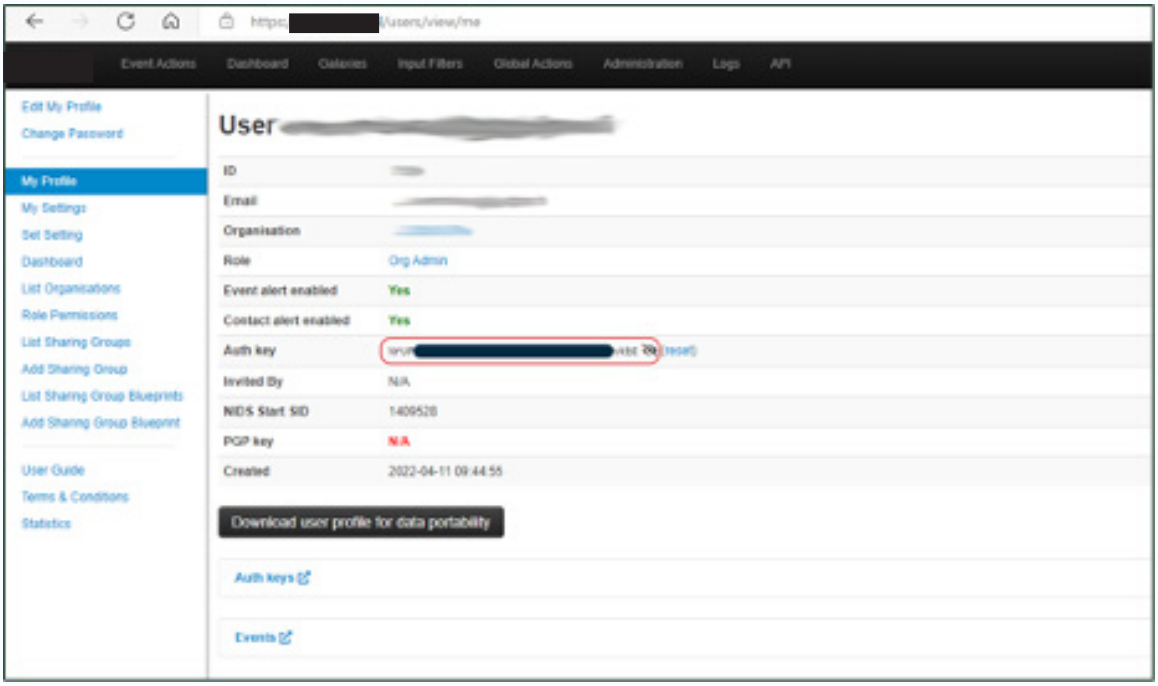
Onderhoudsvriendelijke set-up maakt de automatisering van uitwisseling van dreigingsinformatie bereikbaar voor de kleinste organisaties.

B1 BIJLAGE I : MISP API SLEUTEL

Open het webportal van de MISP server en log in.

Na het aanmelden kan de API-sleutel behorend bij uw account worden verkregen via Global Actions > My Profile, URL. Bijvoorbeeld: https://mispdomein.com/users/view/me

De sleutel vindt u in het veld Auth key. Klik op het oogje om de code zichtbaar te maken en te kopiëren. Sla dit op een veilige plaats op (bijvoorbeeld in een wachtwoordmanager) voor later gebruik.



B2 BIJLAGE II : MICROSOFT SENTINEL

B2.1 Sentinel Inschakelen

Om Microsoft Sentinel in te schakelen, is binnen de 'tenant' van de Microsoft omgeving, een Azure Subscription nodig. Die Subcription op zichzelf kost geen geld, maar configureert op welke wijze in Azure gemaakte kosten in rekening gebracht kunnen en mogen worden. Het is mogelijk om een test/ trial subcription te registreren om de setup eerst een maand kosteloos te testen.

Wanneer de subscription is gerealiseerd, kan Sentinel worden ingeschakeld.

1. Ga naar https://portal.azure.com
2. Zoek naar de service "Microsoft Sentinel"
3. Klik op Create om een nieuwe Sentinel instance te maken
4. Klik op Create a new workspace. Een workspace dient om logging te verwerking binnen Azure. Koppel de workspace aan de gewenste subscription. Maak een nieuwe resource group aan, geef de workspace een naam (bijv. Sentinel") en kies de regio voor de workspace (bijv. "West Europe")
5. Selecteer na het aanmaken van de nieuwe Workspace en klik op Add om de Sentinel instance te maken en openen.

B2.2 Gratis Logbronnen Koppelen

Let op: alleen de vermeldde Data Types binnen de betreffende Data Connectors zijn gratis te onboarden, voor alle andere data types geldt dit niet.

Data Connector	"Gratis" Data type
Azure Activity Logs	AzureActivity
Azure AD Indentity Protection	SecurityAlert (IPC)
Office 365	OfficeActivity (SharePoint)
	OfficeActivity (Exchange)
	OfficeActivity (Teams)
Microsoft Defender for Cloud	SecurityAlert (Defender for Cloud)
Microsoft Defender for IoT	SecurityAlert (Defender for IoT)
Microsoft 365 Defender	SecurityIncident
	SecurityAlert
Microsoft Defender for Endpoint	SecurityAlert (MDATP)
Microsoft Defender for Identity	SecurityAlert (AATP)
Microsoft Defender for Cloud Apps	SecurityAlert (Defender for Cloud Apps)

Als de Sentinel instantie draait, kunnen de logbronnen worden gekoppeld.

1. Open Microsoft Sentinel
2. Ga naar Data Connectors
3. Voeg de logbronnen toe die u relevant vindt uit bovenstaande lijst(en). Minimaal de 3 OfficeActivity logs, aangezien die data bevatten die goed te correleren is met de data vanuit MISP.

Na het activeren van de logbronnen zal het nog wat tijd duren voordat de data daadwerkelijk beschikbaar is in Sentinel. Dit kan als volgt worden gecontroleerd:

1. Ga in Sentinel naar Logs
2. Klik de eerste popups weg tot u in het Query scherm bent.
3. Type als query: OfficeActivity
4. Klik op Run
5. Als resultaten getoond worden, is de koppeling geslaagd. Herhaal deze stappen voor andere connectoren die gekoppeld zijn.

B2.3 Betaalde Logbronnen Koppelen

Naast bovenstaande gratis logbronnen is het mogelijk om allerlei andere logbronnen aan Sentinel te verbinden en het als volledige SIEM in te zetten, maar daar zijn dan wel kosten aan verbonden. Ten eerste kunnen sommige databronnen een licentie upgrade vereisen. Ten tweede rekent Microsoft kosten voor opslag van de logs.

Welke logbronnen precies relevant zijn, hangt af van de organisatie EN de beschikbare informatie in de MISP-koppeling. En zeker omdat er nu kosten kunnen ontstaan: bedenk eerst wat je precies wilt matchen of wat je precies met de logbron wilt doen en voeg geen bronnen toe die je niet nodig hebt.

Data Connector	Data Type	Levert Op
Azure Active Directory	SignInLogs	AzureActivity
Microsoft 365 Defender	EmailUrlInfo	Extra data types in de Microsoft 365 Defender connector, die vanuit de mailstroom in Exchange Online alle relevante data loggen die gematcht kan worden tegen de CTI vanuit MISP: EmailUrlInfo > Urls die in emails worden aangeboden kunnen gematcht worden tegen bekende kwaadaardige websites EmailEvents > emailadres, domein van emailadres, IP adres van zender, onderwerp, zijn allemaal aspecten die gelogd worden en te match zijn tegen CTI in MISP EmailAttachmentInfo > bestandsnamen en SHA256 filehashes om te matchen tegen bekende malware of anderszins kwaadwaardige bestanden
	EmailEvents	
	EmailAttachmentInfo	

B3 BIJLAGE III : AZURE FUNCTION

B3.1 App Registration aanmaken en configureren

1. Open Azure via https://portal.azure.com
2. Ga naar App registrations
3. Maak een nieuwe registratie aan
4. Geef een naam aan de nieuwe app registration, bijvoorbeeld “misp2sentinel”. De overige instellingen kunnen standaard blijven.
5. Klik na het aanmaken van de app registration in de overview pagina bij Client credentials op “add a certificate or secret”
6. Klik onder Client secrets op New client secret
7. Geef een beschrijving op, bijvoorbeeld “M2S Azure Function” en houdt de aanbevolen expiratieduur aan.
8. Kopieer de Value van de nieuwe Client Secret, deze moeten opgeslagen worden in een Azure Vault.

B3.2 Secret waarde samenstellen

Vanuit bovenstaande App Registration zijn 3 elementen nodig om in de Keyvault in het juiste format toe te voegen zodat het script goed kan werken met de app.

- **TENANT_ID** = de waarde die bij Directory (tenant) ID vermeld staat in App Registration overview.
- **APP_ID** = de waarde die bij Application (client) ID vermeld staat in App Registration overview.
- **APP_SECRET** = de waarde die gekopieerd werd in de laatste stap hierboven als Client Secret.

De samengestelde waarde die we nodig hebben om in de Keyvault op te slaan, is dan als volgt, waarbij de gemarkeerde delen vervangen dienen te worden door bovenstaande waardes:

```
{“<TENANT_ID>”: {“id”: “<APP_ID>”, “secret”: “<APP_SECRET>”} }
```

Het format van deze key waarde maakt het mogelijk om de Azure Function de Threat Intel data in meerdere Sentinel instances weg te schrijven. Dit is bijvoorbeeld handig indien er een testomgeving bestaat, of om andere redenen meerdere Sentinel installaties aanwezig zijn.

.

B3.3 Keyvault aanmaken en key opslaan

1. Ga in Azure naar Key vaults
2. Klik op Create key vault
3. Configureer de key vault naar wens, let vooral op de regio waarin deze wordt opgeslagen, normaliter “West Europe”
4. Klik na het aanmaken van key vault onder Objects op Secrets en maak een nieuwe secret aan
5. Vul de waardes in die hierboven zijn gekopieerd uit App Registration Secrets

- De naam van de key MOET “tenants” zijn.
- Als Secret Value de Secret waarde die hierboven is samengesteld.
- Overige waardes mogen standaard gelaten worden.

B3.4 Function aanmaken

Ga als volgt te werk om de Azure Function aan te maken.

1. Ga in Azure naar “Function App”
2. Klik op Create om een nieuwe Azure function aan te maken

- Geef een willekeurige naam aan de App
- Kies bij Publish voor Code, met Python als Runtime Stack. Let wederom op de Region (“West Europe”)
- OS kan Linux blijven
- Kies bij Plan type voor App service plan.
- Overige settings kunnen standard blijven, klik op Review + Create.

.

B3.5 Function Code plaatsen

1. Download allereerst de benodigde bestanden van GitHub: https://github.com/zolderio/misp-to-sentinel

2. Open config.py om de juiste waardes in te vullen

- misp_key = de API key die u eerdere in de voorbereidende fase vanuit de MISP web portal veilig heeft opgeslagen

- misp_domain = de URL waar de MISP draait

3. Ga in de Azure Function naar Functions en klik op Create

4. Kies voor het template Time trigger

5. Kies een naam voor de Function, bijvoorbeeld “m2s”

- Vul een schedule in op basis van CRON-syntax . Bijvoorbeeld dagelijks om 0:00 uur: “0 0 0 * * *”

- Klik op Create

6. Ga in de nieuwe functie naar Code + Test.

7. Upload de Function code

B3.6 Extra Set-up voor Statisch IP

MISP-servers worden soms beschermd door een firewall. Alleen geregistreerde IP-adressen mogen met de MISP-server verbinding maken. Daarom is het nodig dat de Azure Function wordt geconfigureerd om met MISP te verbinden over een vastgesteld IP-adres. Dit is mogelijk door de Function via een NAT Gateway te laten communiceren. Hoe dit te doen, is afgeleid van een Microsoft beschrijving , en gaat als volgt:

1. Ga in Azure naar Virtual networks
2. Klik op Create
    * Koppel het netwerk aan dezelfde resource group als de Azure Function
    * Geef een willekeurige naam op, bijvoorbeeld “m2s-vnet” en als regio weer West Europe
    * De rest van de instellingen kan standaard gelaten worden
3. Open de Azure Function en ga naar Networking
4. Klik bij Outbound Traffic op VNet Integration
5. Klik op Add VNet
    * Selecteer het zojuist aangemaakt Virtual Network en het default subnet, daarna op Create
6. Ga in Azure naar Public IP addresses
7. Klik op Create
    * Kies een naam voor het IP-adres, bijvoorbeeld “m2s-publicip”
    * Koppel het ip-adres aan dezelfde resource group als de Azure Function
    * De rest van de instellingen kan standaard gelaten worden
8. Onder overview kan het gereserveerde IP-adres gevonden worden, sla dit op om door te geven aan de aanbieder
9. Ga in Azure naar NAT gateways
10. Klik op Create
    * Koppel de NAT gateway aan dezelfde resource group als de Azure Function
    * Geef een willekeurige naam op, bijvoorbeeld “m2s-nat”, als regio weer West Europe
    * Ga naar volgende stap: Outbound IP
    * Selecteer bij Public IP addresses het zojuist aangemaakte Public IP. Laat Public IP prefixes ongeselecteerd
    * Ga naar volgende stap: Subnet
    * Selecteer bij Virtual Network het eerder aangemaakt vnet
    * Kies default als subnet
    * Ga naar Review + Create en klik op Create

11. Open de Azure Function
12. Verifieer onder Networking dat bij Outbound Networking Features de NAT Gateway nu ingeschakeld is. Het enige wat nu nog moet gebeuren is dat al het verkeer over de gateway gestuurd moet worden.
13. Ga naar in het linkermenu naar Configuration
14. Klik onder Application Settings op New application setting
    * Name = WEBSITE_VNET_ROUTE_ALL
    * Value = 1
    * Klik OK
15. Klik op Save om de configuratie op te slaan

Geef het IP-adres door aan de aanbieder van de MISP server, zodat zij het aan de allowlist van hun firewall kunnen toevoegen.

B3.7 Validatie

Nadat de aanbieder bevestigd heeft het IP-adres te hebben toegevoegd, zal eerstvolgende middernacht de Function de dreigingsinformatie succesvol in Sentinel moeten kunnen importeren. Vanaf de ochtend daarna kan dit worden gevalideerd in Sentinel.

1. Open in Azure de service Microsoft Sentinel

2. Klink aan de linkerkant op Threat Intelligence

3. Hier moet een overzicht ontstaan met duizenden indicatoren, met als bron “SecurityGraph”

B3 BIJLAGE IV : VOORBEELDEN

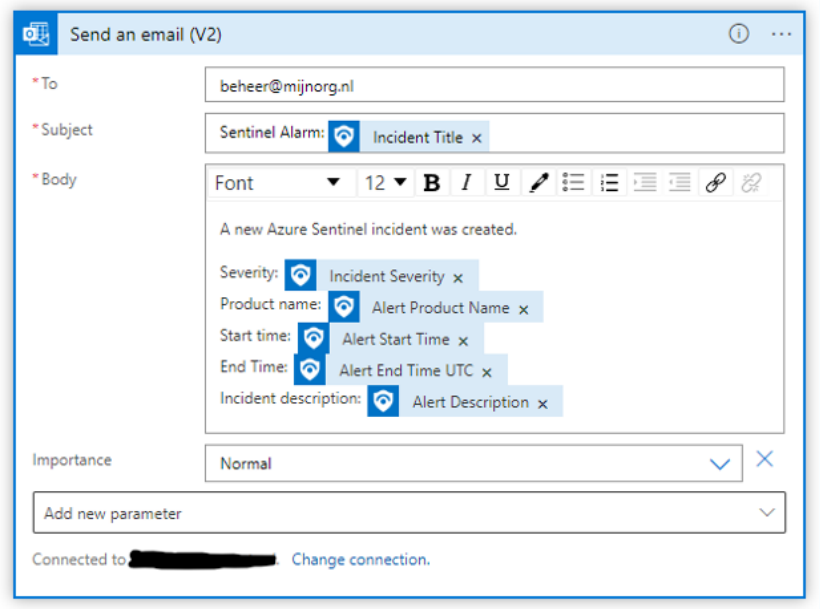
B4.1 Voorbeelden Sentinel Rules in KQL

Beschrijving	"Gratis" Data type
Identificeer Office-activiteit vanuit een kwaadaardig IP-adres	let TI=ThreatIntelligenceIndicator | where TimeGenerated > ago (24h) | where NetworkSourceIP != "" | summarize by NetworkSourceIP;OfficeActivity | where TimeGenerated > ago (5m) | where ClientIP in (TI)
Identificeer e-mails met kwaadaardige URL's	let TI=ThreatIntelligenceIndicator | where TimeGenerated > ago (24h) | summarize by Url;EmailUrlInfo | where TimeGenerated > ago (5m) | where Url in (TI) | join (EmailEvents) on NetworkMessageId | join (ThreatIntelligenceIndicator) on Url | where TimeGenerated2 > ago (24h)
Identificeer e-mails afkomstig van kwaadaardige afzenders	let TI=ThreatIntelligenceIndicator | where TimeGenerated > ago (24h) | where EmailSenderAddress != "" | summarize by EmailSenderAddress;EmailEvents | where TimeGenerated > ago (5m) | where SenderFromAddress in (TI) | where EmailDirection == "Inbound" | join (ThreatIntelligenceIndicator) on $left.SenderFromAddress == $right.EmailSenderAddress | where TimeGenerated1 > ago (24h)
Identificeer e-mails met kwaadaardige bijlagen	let TI=ThreatIntelligenceIndicator | where FileHashType == "SHA256" | where TimeGenerated > ago (24h) | summarize by FileHashValue; EmailAttachmentInfo | where TimeGenerated > ago (5m) | where SHA256 in (TI) | join (EmailEvents) on NetworkMessageId | join (ThreatIntelligenceIndicator) on $left.SHA256 == $right.FileHashValue | where TimeGenerated2 > ago (24h)

B4.2 Sentinel Playbook

Playbooks zijn automatische handelingen die Sentinel kan initiëren bijvoorbeeld naar aanleiding van een alarm. Dat kan een ontzettende complexe lijst aan handelingen zijn, denk aan het resetten van wachtwoorden of uitschakelen van accounts. Maar in zijn simpelste vorm dient een playbook om een e-mail te ontvangen als een rule triggert. Om rules goed te kunnen configureren, moet eerst het playbook worden ingesteld.

1. Ga in Sentinel onder Configuration naar Automation
2. Klik op Create en kies voor Playbook with incident trigger
3. Geef de Playbook een willekeurige naam, bijvoorbeeld “mail-me”
4. Ga naar de laatste stap en klik op Create and continue to designer
5. Voeg in de Logic App Designer een nieuwe actie toe, en kies voor Office 365 Outlook, dan Send an email
6. Nu moet waarschijnlijk een koppeling gelegd worden met een mailbox om emails namens die box te kunnen verzenden. Deze mailbox wordt dus de afzender van alarmmails, wat een reden kan zin om hier een service account voor aan te maken in de tenant.
7. Vul de Ontvanger(s) van de alertmail, het Onderwerp en de Body van de e-mail in. Daarbij kan gebruik gemaakt worden van variabelen vanuit het incident. Bijvoorbeeld:



8. Klik op Save

Dit playbook ofwel deze logic app kan nu aan alle Sentinel Rules worden gekoppeld waarvan we een e-mail willen ontvangen indien deze triggert.

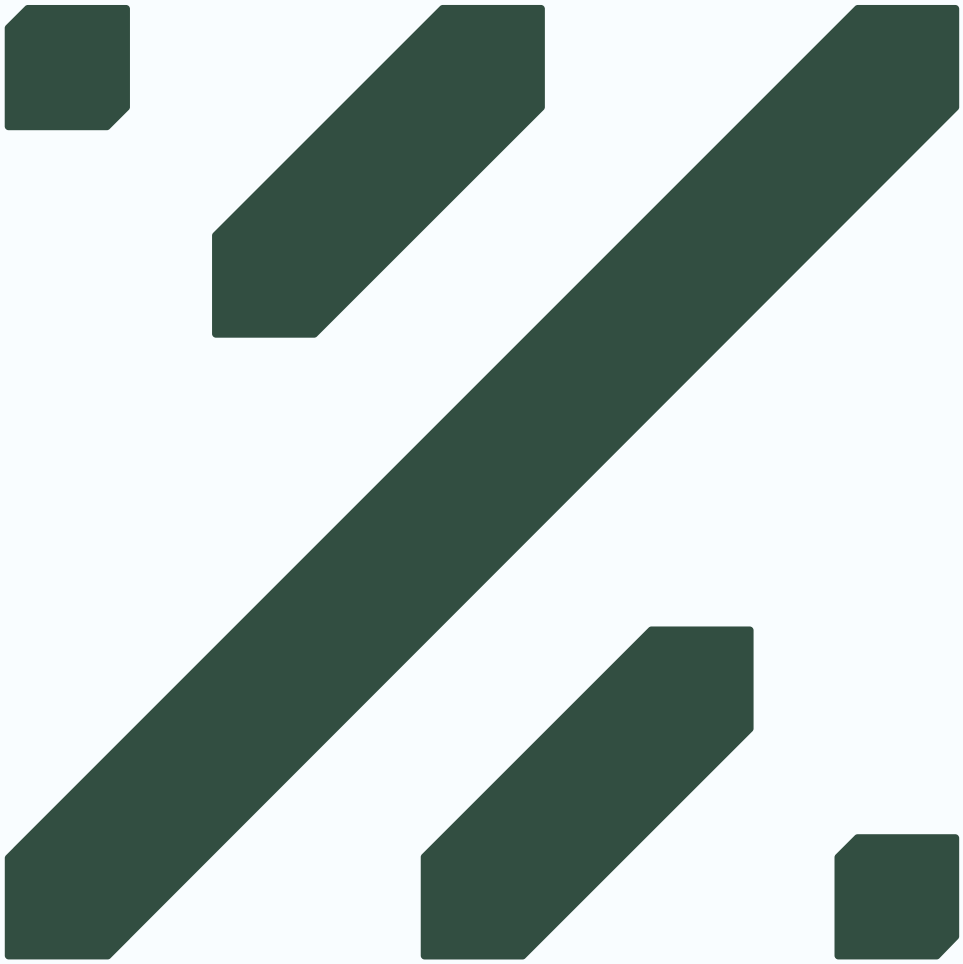
B4.3 Sentinel Rule Maken

1. Open in Azure de service Microsoft Sentinel
2. Ga naar Analytics
3. Klik op Create en kies voor Scheduled query rule
4. Geef een naam naar keuze op en ga naar de volgende stap: Set rule logic
5. Plaats in het veld Rule Query de KQL syntax
6. Bepaal hoe vaak de rule moet worden uitgevoerd
7. Ga naar de volgende stap: Incident settings
8. Ga naar de volgende stap: Automated response
9. Maak een nieuwe automation rule aan door op Add new te klikken
   * Geef de rule een willekeurige naam
   * Kies bij Actions voor Run Playbook
   * Selecteer het playbook dat zojuist is aangemaakt
   * Klik op Apply
10. Ga naar de laatste stap: Review en klik op Create

B4.3 Validatie

Om te valideren of rules en playbooks goed werken, zou u een rule kunnen maken die u bewust kunt triggeren. Bijvoorbeeld een rule die triggert wanneer u een e-mail ontvangt met bepaalde waarde in het subject.

Maar er moet nog wel wat uit te vinden blijven, dus die gaan we niet uitschrijven voor u. Succes!



ZOLDER

applied security research

zolder.io
+31168799850