TLP:GREEN

LOGMANAGEMENT EN SIEM DESIGN GUIDE

Monitoring & Detectie – Security Log Management & Analytics

Best Practice 1.0

Complexiteit document
Gemiddeld 

Samenwerken maakt

DIGITAAL VEILIGER

VSSR

Inhoudsopgave

Voorwoord

De Rijksoverheid verwerkt grote hoeveelheden gevoelige informatie en is daarmee een interessant en gewild doelwit. Cybercriminelen en statelijke actoren zoeken naar kwetsbaarheden om zich zo toegang te verschaffen tot de supplychain, netwerken, systemen en (gevoelige) informatie.

De wereld van cyberdreigingen verandert snel en vraagt om gezamenlijke inspanning om weerbaar te zijn waarbij een Security Operations Center (SOC) een belangrijke schakel vormt. Dit vraagt om samen te werken aan breder toegepaste én verbeterde SOC-dienstverlening. Het programma Versterken SOC Stelsel Rijk (VSSR) is opgezet om hieraan bij te dragen.

Een belangrijk onderdeel van SOC-diensten zijn de monitoring- en detectiediensten. Deze zijn erop gericht om een veelheid aan loggegevens en andere (meta-)datastromen afkomstig van de IT-infrastructuur, randapparatuur, bedrijfsapplicaties en andere dataverwerkingen in een organisatie te analyseren, aggregeren en correleren. Monitoring en detectiesystemen kunnen op basis hiervan verdachte gedragingen detecteren en alarm slaan.

Om een SOC effectief en doelmatig in te zetten is het noodzakelijk dat er een aantal onderwerpen binnen een organisatie zijn ingericht. VSSR levert diverse producten die rijksorganisaties ondersteunen bij het inrichten van een SOC en de daarvoor benodigde randvoorwaarden.

Een essentieel aspect van een goed functionerend Security Operations Center is het effectief beheren van securitylogs. Dit document biedt een uitgebreide handleiding voor de architectuur en implementatie van securitylogmanagement. Hierbij is expliciet gekozen om als uitgangspunt de producten van Microsoft te nemen. De toegepaste principes zijn, echter, niet Microsoft-specifiek en kunnen generiek worden ingezet.

Achtergrond	Doelgroep
VSSR levert verschillende kennisproducten. Dit document maakt onderdeel uit van een set van miniproducten die rijksorganisaties helpt om een aantal SOC operationele randvoorwaarden in te richten.	Versterken SOC Stelsel Rijk (VSSR) biedt met dit document handvatten voor SOC-Leads, SOC-Analisten, (SOC- en Security)Architecten, SIEM- en security engineers.

1 Documentgegevens

1.1 Documenthistorie

Versie	Datum	Omschrijving
V1.0	23-07-2025	Initiële versie

1.2 Referenties

Document	Link
VSSR-kennisdocumenten	VSSR (rijksapplicaties.nl)

1.3 Definities

Ter verduidelijking van de terminologie en begrippen die in dit document worden gebruikt is er een verzameling van definities te vinden op Woordenboek - Cyberveilig Nederland.

Term	Definitie
Verbose netwerk	Een 'verbose network' (of in het Nederlands: 'uitgebreid netwerk') verwijst naar een netwerk dat gedetailleerde informatie en logs genereert, waardoor je meer inzicht krijgt in het netwerkverkeer en de processen die erop plaatsvinden

2 Introductie tot securitylogmanagement

2.1 Inleiding

In het licht van toenemende cyberdreigingen en strengere wet- en regelgeving is het goed inrichten van een Security Operations Center (SOC) cruciaal. Een belangrijk basisonderdeel hiervan is securitylogmanagement. Securitylogmanagement kan op verschillende manieren worden ingevuld maar ligt altijd aan de basis van de verder in te richten detectie en respons. Dit document biedt een handleiding voor het implementeren van securitylogmanagement op basis van de Microsoft-productlijn.

Het voeden van securitylogmanagement en SIEM-oplossingen is afhankelijk van actieve beveiligingsoplossingen en passieve logcomponenten binnen het ICT-landschap die belangrijke detectie- en audit-logdata doorsturen. Deze verschillende aanleverbronnen worden in dit document verder uiteengezet om te zorgen dat een SOC en de logmanagement- en/of SIEM-oplossing wordt voorzien van de juiste logdata.

Voor de invulling van de dit document is gekozen om de Microsoft Product Suite als uitgangspunt te nemen. Microsoft is een gevestigde naam in de markt, met oplossingen zoals Microsoft Office en het Windows-besturingssysteem die al jarenlang de standaard vormen binnen organisaties. Met de ontwikkelingen van de afgelopen jaren is ook de Cloud niet meer weg te denken. Waar organisaties voorheen hun ICT-oplossingen voornamelijk zelf hostten, wordt tegenwoordig steeds vaker gebruikgemaakt van SaaS-oplossingen zoals Microsoft 365, maar ook van diverse andere derde partijen. Daarnaast hebben veel organisaties zelf ontwikkelde applicaties die gehost worden op hun eigen infrastructuur, zowel op locatie als in de Cloud.

Deze veelzijdigheid brengt veel flexibiliteit, maar ook complexiteit met zich mee, met name op het gebied van beveiliging. Microsoft biedt dan ook een breed scala aan beveiligingsoplossingen die aansluiten op verschillende infrastructuren en dreigingsscenario's. Elke oplossing heeft specifieke aansluitvoorwaarden en richt zich op een bepaald beveiligingsdoel. Omdat Microsoft een breed bereik aan producten heeft, wordt dit productlandschap hier dan ook genomen om verdere inrichting van een aantal basis SOC-oplossingen in het kader van securitylogmanagement uiteen te zetten.

Voor een SOC is het essentieel om te begrijpen welke Microsoft security-componenten nodig zijn om specifieke dreigingen te detecteren en mitigeren. Veel van deze oplossingen zijn bovendien inbegrepen bij licenties die veel Rijksoverheid-organisaties al bezitten, zoals Microsoft 365 E3 of E5. Dit document biedt een overzicht van het Microsoft security-ecosysteem en helpt SOC-teams inzicht te geven in hoe deze oplossingen effectief ingezet kunnen worden binnen hun beveiligingsstrategie en hoe vervolgens op basis van deze keuzes de juiste data naar de logmanagementoplossing gebracht kan worden.

2.2 Doel en reikwijdte

Het doel van dit document is om organisaties op weg te helpen bij het inrichten van de meest gangbare Microsoft securityproducten samen met de Microsoft SIEM-oplossing om zowel telemetrie als, in eerste instantie, securitylogmanagement en monitoring in de basis goed in te richten.

Hierbij geeft dit document:

- Inzicht te bieden in het ecosysteem van Microsoft Security-Producten;
- Een uiteenzetting vanuit een architectuur perspectief hoe de producten uit het ecosysteem het meest efficiënt kunnen worden ingezet voor detectie en respons afhankelijk van de potentiële dreiging;
- Een handreiking voor het design en de inrichting van de verschillende producten;
- Een handreiking voor het koppelen aan een SIEM-systeem, zowel de Microsoft native (Sentinel) als ook aan een SIEM van een derde partij; en,
- Handvatten voor het koppelen van de juiste logdata.

Naast de meer design-technische componenten wordt ook inzicht gegeven in het licentie-, kennis- en kostenaspect wat komt kijken bij het inrichten van een Microsoft gebaseerde SOC-omgeving. Dit geeft het nodige houvast om de juiste beslissingen te nemen in de architectuur- en designfasen bij het inrichten of verder uitwerken van een SOC.

Dit document zal, echter, niet ingaan op de detailinrichting van alle afzonderlijke Microsoft-producten en zal ook niet verder ingaan op het gebruik van Microsoft Sentinel als SIEM-oplossing omdat dit detailniveau te ver zou gaan voor één document. De handreiking omtrent kennis, die voornamelijk inzicht zal bieden in de verschillende opleidingsmodules die Microsoft aanbiedt, geeft de juiste aanknopingspunten voor de verdere detailinformatie betreft de afzonderlijke producten.

2.3 Doelgroep

De doelgroep voor dit document bestaat voornamelijk uit professionals die betrokken zijn bij het opzetten, beheren en verbeteren van een SOC. Specifiek kunnen de volgende rollen baat hebben bij dit document:

- **SOC-Leads en (Security) Architecten:** Krijgen inzicht in hoe Microsoft-oplossingen (zoals Sentinel en Microsoft XDR) geïntegreerd kunnen worden binnen de bestaande security-architectuur.
- **SOC-analisten (T1, T2, T3):** Begrijpen welke Microsoft security-oplossingen beschikbaar zijn en hoe deze dreigingen kunnen detecteren en mitigeren.
- **SIEM- en security engineers:**
  Begrijpen hoe Microsoft security-oplossingen ingezet en geïntegreerd kunnen worden met Microsoft Sentinel of een ander SIEM.

2.4 Leeswijzer

Binnen dit document wordt ingegaan op verschillende onderdelen die van belang zijn bij de deployment van een Logmanagement of SIEM-omgeving. In het eerste deel wordt ingegaan op architectuur overwegingen (3 Architectuur overwegingen) om tot de juiste keus te komen voor uw organisatie. Daarna (4 Design en Integratie) wordt gekeken naar verschillende designmogelijkheden voor het implementeren van beveiligingsmechanismen en sensoren in uw infrastructuur en de integratie met een SIEM- of Logmanagementomgeving.

3 Architectuur overwegingen

In dit hoofdstuk wordt aandacht gegeven aan het architectuurperspectief op het Microsoft security-productportfolio en hoe dit het best in te zetten voor security operations. Hierbij wordt eerst gekeken naar de beschikbare bouwblokken binnen het Microsoft-portfolio. Vervolgens worden deze bouwbokken gekoppeld aan een aanvalspatroon zodat helder uiteen wordt gezet welk bouwblok het beste voor welke doel kan worden ingezet. Daarna wordt verder gekeken naar additionele overwegingen voor implementatie als voorbereiding op het Implementatie Design in het volgende hoofdstuk. Hierbij wordt ingegaan op licentiemodellen en de benodigde kennis binnen een SOC om met de producten te kunnen werken. Dit helpt bij het inrichten van een SOC en het maken van een kosteninschatting.

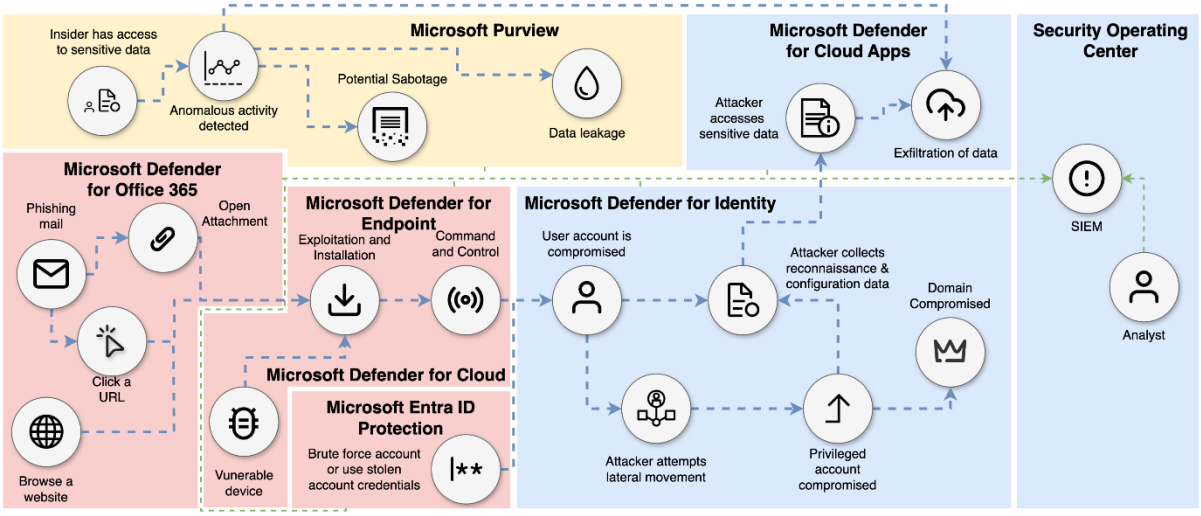
3.1 Microsoft Security Product Portfolio

Een SOC maakt gebruik van diverse security-oplossingen om dreigingen te detecteren, te analyseren en hierop te reageren. Microsoft biedt een breed scala aan security-producten die relevant zijn voor een SOC. De belangrijkste Microsoft-securityoplossingen en hoe deze bijdragen aan een robuuste beveiligingsstrategie worden hieronder uiteengezet. Hierbij worden drie gezichtspunten weergegeven:

1. Het eerste gezichtspunt is een generiek aanvalsscenario. Hiermee kan een architect de juiste keuzes maken uit het Microsoft-portfolio, afhankelijk van het onderdeel/de onderdelen uit het generieke scenario dat de organisatie wil ondervangen.
2. Het tweede gezichtspunt is meer compliance- en logmanagement gedreven maar is ook van toepassing op het Insider Threat-scenario. Op basis van dit gezichtspunt kan worden bepaald welke bijbehorende producten kunnen worden ingezet voor compliance-doeleinden.
3. Het derde gezichtspunt is een algeheel designoverzicht. Hiermee kan een architect bepalen wat de handigste keuzes zijn vanuit een infrastructuur gezichtspunt.

3.1.1 Aanvalsscenario externe dreigingen

Er zijn veel verschillende aanvalsscenario's die in verschillende situaties van toepassing zijn. Voor elke organisatie zal een scenario net anders uitpakken en het is dus ook goed om voor de eigen organisatie verschillende scenario's te analyseren en uiteen te zetten. Tegelijkertijd zijn er ook overeenkomsten in de aanvalstactieken binnen de verschillende scenario's. De belangrijkste tactieken zijn in een meer generiek overzicht weergegeven (Figuur 1) waarbij wordt aangegeven welke oplossingen uit het Microsoft-productportfolio hier het beste bij aansluit.



Figuur 1 Generiek aanvalsscenario

Om een beter begrip te kunnen vormen bij de beschikbare bouwblokken worden de producten in meer detail toegelicht. De meeste uitgebreide en recente informatie is direct beschikbaar op de Microsoft website.

Microsoft Defender for Office 365 (MDO)
Microsoft Defender for Office 365 beschermt e-mail en samenwerkingsplatformen tegen phishing, malware en geavanceerde cyberaanvallen. Het biedt real-time bescherming tegen dreigingen die via e-mail, links en samenwerkingstools worden verspreid.

Microsoft Entra ID Protection
Microsoft Entra ID Protection helpt organisaties bij het identificeren en beperken van identiteitsgerelateerde risico's. Het maakt gebruik van machine learning en real-time signalen om verdachte aanmeldingen, gecompromitteerde accounts en risicovolle gebruikersactiviteiten te detecteren. Door middel van risicogebaseerde beleidsregels kunnen organisaties automatisch passende maatregelen nemen, zoals Multi-Factor Authenticatie (MFA) of toegangsblokkades, om identiteiten te beschermen tegen bedreigingen.

Microsoft Defender for Endpoint (MDE)
Microsoft Defender for Endpoint biedt geavanceerde endpoint-bescherming en -detectie voor dreigingen met betrekking tot werkstations en servers. Het combineert preventieve bescherming, post-breach detectie en geautomatiseerde onderzoeks- en responsmogelijkheden.

Microsoft Defender for Identity (MDI)
Microsoft Defender for Identity richt zich op het detecteren van verdachte activiteiten binnen Active Directory (AD) en Entra ID. Het identificeert geavanceerde dreigingen, gecompromitteerde identiteiten en malafide insiders die zich in het netwerk bevinden.

Microsoft Defender for Cloud Apps (MDCA)
Microsoft Defender for Cloud Apps is een Cloud Access Security Broker (CASB) die uitgebreide zichtbaarheid, controle over gegevensreizen en geavanceerde bescherming biedt voor alle cloudapplicaties. Het detecteert gebruik van shadow-IT, beschermt gevoelige informatie en identificeert verdachte activiteiten binnen SaaS-applicaties zoals Microsoft 365, Salesforce, Google Workspace en meer.

Microsoft Defender for Cloud (MDC)
Microsoft Defender for Cloud biedt uitgebreide beveiligingsoplossingen voor het beschermen en beheren van cloudworkloads in multi-cloud omgevingen, waaronder Azure, AWS en Google Cloud. Het levert security posture-management en workload-specifieke bescherming voor verschillende clouddiensten. Hiervoor wordt gebruik gemaakt van ARC-agents.

Microsoft Sentinel
Microsoft Sentinel is een cloud-native SIEM (Security Information and Event Management) en SOAR (Security Orchestration, Automation, and Response) oplossing die is gebouwd bovenop Log Analytics. Het biedt SOC-teams uitgebreide mogelijkheden voor het verzamelen, analyseren en reageren op beveiligingsgebeurtenissen vanuit diverse bronnen.

Microsoft eXtended Detection and Response (XDR)
Als laatste nog een korte uitleg over Microsoft XDR omdat de term frequent wordt gebruikt. Microsoft Defender XDR is geen afzonderlijk product maar een geïntegreerde beveiligingssuite die bedoeld is voor detectie, preventie, onderzoek en reactie. Dit is samengebracht voor endpoints, identiteiten, e-mail en toepassingen en biedt bescherming tegen geavanceerde aanvallen. XDR helpt beveiligingsteams hun organisaties te beschermen met behulp van informatie uit andere Microsoft-beveiligingsproducten, waaronder:

- Microsoft Defender voor Endpoint
- Microsoft Defender voor Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management
- Microsoft Defender voor Cloud

3.1.2 Insider-Threat, compliance en log management

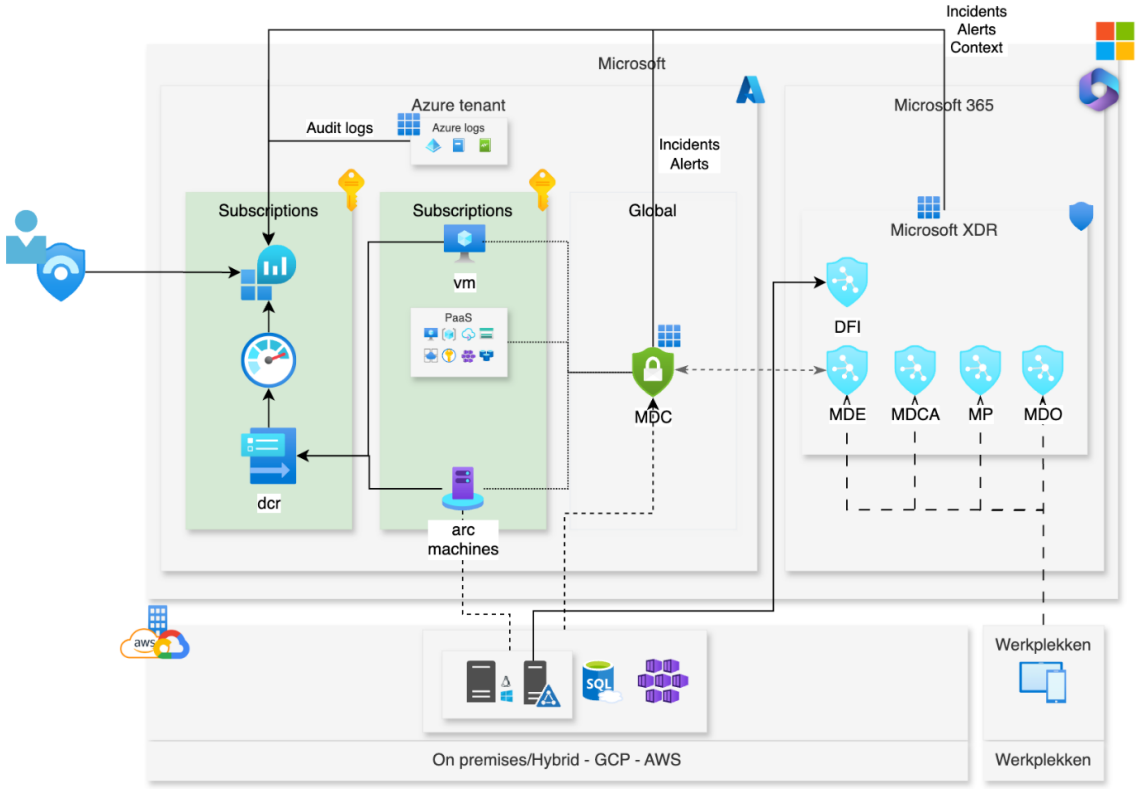
Naast het security-gerelateerde gezichtspunt is het veelal ook nodig om additionele logdata te verzamelen voor incidentonderzoek en compliance doeleinden (wettelijke bewaartermijnen). Daarnaast is het Insider-Threat scenario voor organisaties ook van belang Vanuit Azure is het mogelijk om security- en diagnostische logdata te verzamelen. De hiervoor benodigde producten zijn hieronder beschreven waarbij het Insider-Threat scenario in Figuur 1 is opgenomen.

Azure Audit Logs en Diagnostics
Azure biedt uitgebreide logging- en monitoringmogelijkheden voor specifieke cloudresources. Relevante functionaliteiten voor een SOC zijn onder meer activiteitenlogboeken, diagnostische instellingen en resource-specifieke beveiligingslogs.

Microsoft Purview
Microsoft Purview richt zich op compliance, data governance en auditing binnen Microsoft 365. Het helpt organisaties bij het beschermen van gevoelige gegevens, het naleven van regelgeving en het beheren van informatie over de gehele omgeving.

3.1.3 Design gezichtspunt

De verschillende hierboven genoemde producten kunnen vanuit een design gezichtspunt worden gegroepeerd en overzien zoals hieronder weergegeven in *Figuur 2*. De afzonderlijke componenten behoren bij verschillende Microsoft productgroepen op basis waarvan architectuur keuzes betreft volgorde van uitrol kunnen worden gemaakt.



Figuur 2: Algemeen Design Overzicht

Het overzicht laat zien dat voor werkplekken andere producten van toepassing zijn dan voor Azure Cloud-tenants of voor andere Cloud oplossingen, zowel public als private. Houd hier rekening mee bij het maken van keuzes en voor het plannen van een lange termijn verdedigingsstrategie. Bedenkt altijd wat de grootste kans heeft om aangevallen te worden, waarom en hoe. Daarna wordt het eenvoudiger om de juiste volgordelijkheid aan te brengen in strategie, planning en uitrol.

3.2 Licentiemodel

Een andere belangrijke keuze die komt kijken bij architectuur is het licentiemodel dat het beste past bij de doelstellingen van de organisatie en het SOC. De drie belangrijkste licentiecomponenten binnen het Microsoft-ecosysteem op het gebied van security zijn:

- Microsoft 365;
- Defender for Cloud; en,
- Microsoft Sentinel.

Deze oplossingen kunnen naadloos worden geïntegreerd, maar functioneren ook onafhankelijk van elkaar. In de volgende paragrafen wordt per component het licentiemodel en de securityfunctionaliteiten verder besproken zodat een architect tot de juiste keuze kan komen. Hierbij wordt voornamelijk ingegaan op de oplossingen die per licentiemodel beschikbaar zijn, maar niet op de bijbehorende prijsstelling. Voor prijsstelling is het verstandig om op de Microsoft-website te kijken omdat dit aan verandering onderhevig is.

3.2.1 Microsoft 365

Microsoft 365 omvat verschillende licenties. Voor Enterprise-omgevingen zijn de meest gangbare opties de Microsoft 365 E3 en de E5 oplossing.
De E3-licentie bevat niet alle Defender-producten, maar deze kunnen wel als aanvullende modules worden toegevoegd. De E5-licentie is de meest uitgebreide optie en bevat alle Defender-producten, inclusief het P2-plan (de meest geavanceerde versie).

Meer details zijn te vinden op de Microsoft-website. De informatie wordt hier niet in expliciet opgenomen omdat dit aan verandering onderhevig is waarmee de Microsoft-website de meest accurate informatiebron is:

- Microsoft 365 plannen en prijzen
- Vergelijking van Microsoft 365 plannen voor enterprise

Azure en Defender-producten in Microsoft 365 E3

- Microsoft Purview (deels)
- Defender for Endpoint plan 1
- Microsoft Entra ID Plan 1

Azure en Defender-producten in Microsoft 365 E5

- Defender for Office 365
- Defender for Cloud Apps
- Defender for Endpoint plan 2
- Defender for Identity
- Defender for Purview
- Microsoft Entra ID Plan 2

3.2.2 Defender for Cloud

Microsoft Defender for Cloud is een beveiligingsoplossing voor het beschermen van cloud-workloads en omvat verschillende producten met variërende prijzen:

- **Defender for Server plan 1 / plan 2**
- **Defender for containers**
- **Databases**
  - *Microsoft Defender for SQL on Azure-connected databases*
  - *Microsoft Defender for SQL outside Azure*
  - *Microsoft Defender for MySQL*
  - *Microsoft Defender for PostgreSQL*
  - *Microsoft Defender for MariaDB*
  - *Microsoft Defender for Azure Cosmos DB*
- **Storage**
  - *Microsoft Defender for Storage*
  - *Malware Scanning (add-on to Defender for Storage)*

- **Microsoft Defender for APIs Plan 1 t/m plan 5**
- **Service Layer**
  - *Microsoft Defender for App Service*
  - *Microsoft Defender for Key Vault*
  - *Microsoft Defender for Resource Manager*

De actuele prijzen zijn te vinden via de volgende link: Defender for Cloud – Prijzen

3.2.3 Microsoft Sentinel

Microsoft Sentinel is de SIEM (Security Information and Event Management) en SOAR (Security Orchestration, Automation, and Response) oplossing van Microsoft. Deze wordt aangeboden als een SaaS-oplossing in Azure.

Prijsstelling
De kosten van Microsoft Sentinel zijn gebaseerd op log-ingestie-volumes en retentie-opties[1]. De meest uitgebreide en functionele optie is het Analytics-plan, maar er zijn ook andere varianten beschikbaar:

- Analytics Logs
  De (duurste) standaardoptie met volledige SIEM-functionaliteit;
- Basic Logs
  Lagere kosten, geschikt voor minder kritische logs met beperkte query-mogelijkheden;
- Auxiliary Logs
  Hiermee kunnen specifieke logscenario's worden ingevuld.

Standaard (Analytics Logs):
De Analytics Logs optie biedt de meeste mogelijkheden en is daarmee ook de prijzigste. De standaardretentieperiode is 90 dagen, wat betekent dat logs binnen deze periode beschikbaar blijven voor interactieve zoekopdrachten en analyses.

Daarnaast biedt Sentinel extra opties voor logbewaring:

- Interactieve retentie: Indien logs langer bewaard dienen te worden dan de standaard 90 dagen. Dan worden er extra kosten in rekening gebracht, afhankelijk van de gekozen bewaartermijn.
  Let op: Dit is uitsluitend van toepassing op het Analytics-plan.
- Archivering: Voor langdurige opslag kunnen logs tegen een lager tarief worden gearchiveerd en later opnieuw worden opgehaald indien nodig.
  Let op: ophalen of doorzoeken van gearchiveerde logs zitten extra kosten aan verbonden.

Basic & Auxiliary Logs als alternatief
Sommige logs zijn noodzakelijk om te bewaren, maar de kosten van Analytics Logs kunnen te hoog zijn voor logbronnen die niet actief nodig zijn voor real-time detectie en analyse. Denk hierbij aan "verbose"-netwerk- en firewall-logs, die slechts sporadisch worden geraadpleegd.
Voor deze logbronnen kunnen Basic Logs of Auxiliary Logs een kostenefficiënt alternatief zijn. Hoewel deze opties minder mogelijkheden bieden dan Analytics Logs, zijn de kosten per GB aanzienlijk lager.

Volumekorting: Sentinel werkt met een pay-as-you-go model, waarbij logverwerking tot 100 GB per dag wordt afgerekend op basis van verbruik. Voor organisaties die meer dan 100 GB per dag verwerken, zijn er pakketten beschikbaar, die volumekorting bieden. Meer details over prijzen en opties zijn te vinden in de Microsoft Sentinel prijsinformatie.

Data connectors: Sommige data-connectoren, zoals Microsoft Defender en Microsoft 365, genereren geen extra kosten bij koppeling aan Sentinel wanneer deze vallen onder een Microsoft 365 E5-licentie. Een overzicht hiervan is te vinden op de officiële Microsoft-documentatie.

[1] Bijlage II – Overzicht Sentinel log-table plans

Wat kun je doen met Microsoft Sentinel?
Zodra de data zijn geïmporteerd en de kosten voor ingestie en retentie zijn verwerkt, biedt Microsoft Sentinel een breed scala aan functionaliteiten voor beveiligingsmonitoring en incidentrespons:

- Analytic Rules: Detectieregels voor het automatisch signaleren van bedreigingen.
- Workbooks: Dashboards en visualisaties voor inzicht in beveiligingsdata.
- Threat Hunting: Handmatige en geautomatiseerde analyses om dreigingen te identificeren.
- Incidentbeheer: Samenvoegen, analyseren en afhandelen van beveiligingsincidenten.
- Automatisering (Playbooks): SOAR-functionaliteit voor het automatisch uitvoeren van responsacties.
- Summary rules (Preview): Summary Rules is een functionaliteit in preview die helpt bij het samenvatten en groeperen van beveiligingsevents. Kan gebruikt worden als tussen oplossing voor tabellen met veel log data. Denk bijvoorbeeld aan firewall logs i.c.m. een tabel met de basic of auxiliary plan. Om zo toch enige vorm van detectie toe te passen.

Voor bovenstaande functies worden geen extra querykosten in rekening gebracht bij gebruik van Analytics Logs. Echter, voor queries die worden uitgevoerd op Basic Logs en Auxiliary Logs gelden wel kosten[2]. Voor een verdere vergelijking qua functionaliteiten wordt een overzicht geboden in Bijlage II – Overzicht Sentinel log-table plans. Voor de kosten van queries, zoekopdrachten en data-export, zie: Azure Monitor Pricing.

3.3 Kennis en certificering

Om op de juiste wijze gebruik te maken van de verschillende Microsoft-componenten heeft Microsoft verschillende trainingsmodules beschikbaar. De modules zijn hier genoemd inclusief hun toepassing op de verschillende rollen binnen een SOC.

3.3.1 Trainingen

Microsoft heeft de volgende trainingen beschikbaar:

- **SC-900:** Biedt basiskennis over Microsoft Security, Compliance en Identity.
- **SC-200:** Is gericht op threat detection, incident response en het gebruik van Microsoft XDR en Microsoft Sentinel.
- **SC-300:** Is gericht op identiteitsbeheer en toegangscontrole met Microsoft Entra ID.
- **AZ-500:** Is gericht op Azure security, netwerkbeveiliging en identiteitsbeheer.
- **SC-100:** Is gericht op het ontwerpen en evalueren van cybersecuritystrategieën met Microsoft-oplossingen, zoals Zero Trust, identiteitsbeheer en gegevensbeveiliging.

3.3.2 SOC-rollen vs. Trainingen

In *Tabel 1 – Microsoft security certificeringen* zijn de verschillende trainingsmodules uit de vorige paragraaf opgedeeld naar SOC-rol zodat een architect of SOC-manager eenvoudig kan zien welke rollen wat nodig hebben om tot een opleidingsplan en bijbehorende kosteninschatting te komen.

Rol	Certificering
SOC-Analist	• SC-900 • SC-200
Senior SOC-Analist / Security Engineer	• SC-900 • SC-200 • AZ-500
SOC-Architect	• SC-900 SC-100 • Een of meerdere van SC-200, SC-300, AZ-500

Tabel 1: Microsoft Security Certificering opgedeeld naar rol

[2] Controleer altijd op de Microsoft website wat de huidige inhoud van de licenties is want dit soort zaken kan veranderen.

4 Design en Integratie

Voor het inrichten van een volledige logmanagementoplossing voor security-doeleinden bestaan verschillende design- en implementatie-mogelijkheden. De mogelijkheden die hier worden geboden, zijn niet als uitputtend bedoeld en geven vooral richting bij het maken van de juiste keuzes voor uw organisatie. Bij het maken van het design dient rekening te worden gehouden met drie belangrijke componenten die betrekking hebben op de security log data, namelijk: 1) collectie, 2) transport, en 3) opslag.

Voor alle aandachtsgebieden zijn er verschillende implementatiemogelijkheden. Zoals aangegeven, richt dit document zich voornamelijk op de inrichting op basis van de Microsoft Product Suite. Voor de collectie wordt dan ook uitgegaan van actieve en passieve Microsoft-componenten die data verzamelen op endpoints. Voor de opslag wordt in eerste instantie uitgegaan van Microsoft Sentinel, maar daarnaast worden ook nog enkele alternatieven mogelijkheden beschreven op basis van andere SIEM- en Logmanagementoplossingen. Het transport is afhankelijk van het gekozen product en zal hier niet in detail worden besproken.

4.1 Design Opties

Bij de implementatie richten we ons op de kerncomponenten die essentieel zijn voor een solide beveiligingsfundament en het genereren van de benodigde logdata voor securitylogmanagement en security monitoring. In dit document nemen we gebruikers, werkplekken, servers en PaaS services binnen de context van Microsoft 365 en Azure als uitgangspunt. We bespreken hoe gebruikers optimaal beveiligd kunnen worden met een M365 E5-licentie en welke producten hiervoor beschikbaar zijn, evenals de beveiliging van werkplekken en servers. Meer specifieke beveiligingstoepassingen zoals File Integrity Monitoring (FIM), Just-in-Time (JIT) toegang en andere geavanceerde maatregelen zijn buiten de scope van dit document.

Een aanpak gebaseerd op de Microsoft Product Suite is geschikt voor ieder type organisatie maar heeft additionele voordelen voor kleine tot middelgrote organisaties die geen of een beperkt eigen standalone securityteam hebben en/of niet beschikken over de technische expertise om een complexe logmanagementinfrastructuur op te zetten waarbij de implementatie uitgebreide kennis en ervaring vereist. Met beperkte middelen en een overzichtelijke implementatie kan het grootste deel van de uitrol geschieden op basis van de management consoles die al bij beheerders in gebruik zijn voor het inrichten van de niet-security gerelateerde implementatieonderdelen. Hierbij is het wel verstandig om in kleine, overzichtelijke blokjes te werken zodat de omvang van de wijzigingen per keer beperkt is en de impact overzichtelijk. Ook de mogelijk alert-stroom naar Sentinel blijft beperkt en kan stap voor stap verder worde uitgebreid.

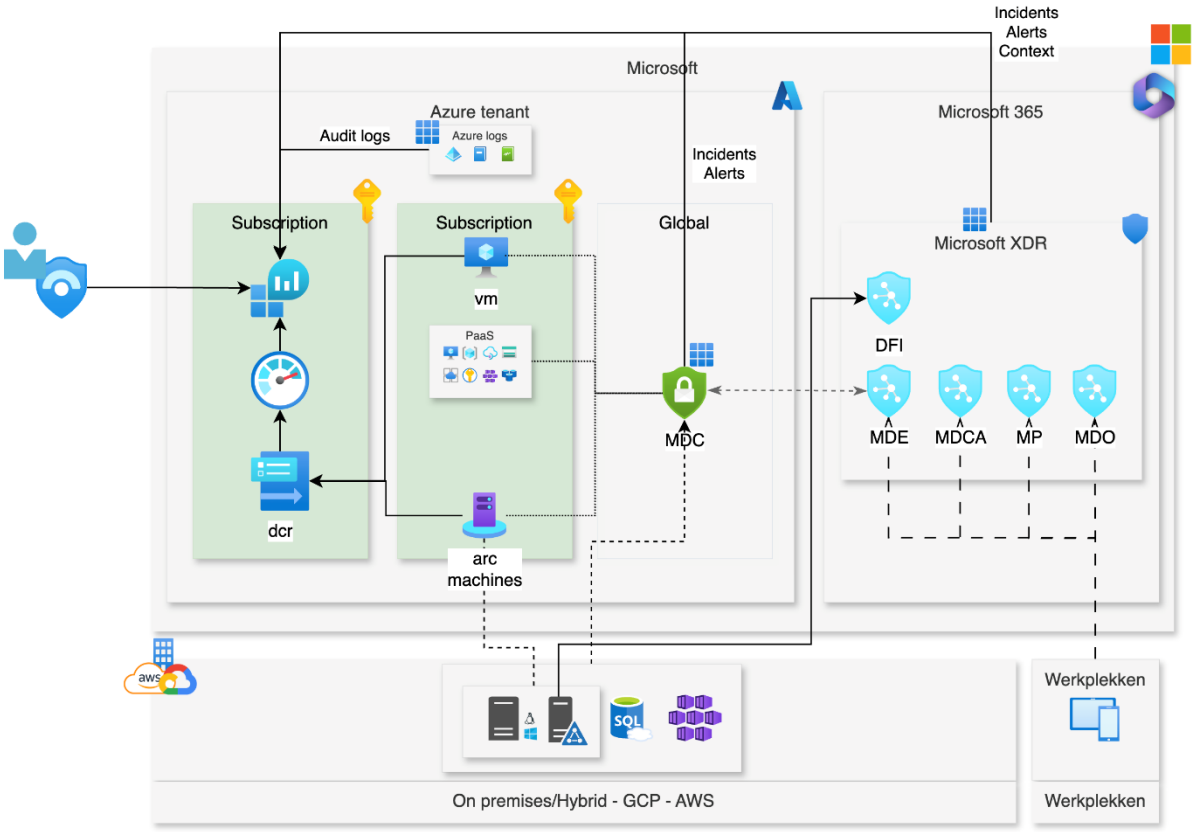
4.1.1 Logcomponenten

Bij het gebruik van de Cloud-producten van Microsoft krijg je vrijwel een out-of-the-box oplossing voor logmanagement. Deze aanpak biedt niet alleen een gecentraliseerde manier om logs te verzamelen en analyseren, maar voegt ook geavanceerde preventie- en detectiemogelijkheden toe.

De belangrijkste actieve en passieve verdedigings- en logcomponenten vallen uiteen in:

- **Microsoft Defender Suite**: Voor endpoint-, identity-, en emailbeveiliging met geïntegreerde detectie- en responsmogelijkheden (XDR).
- **Microsoft Defender for Cloud**: Voor continue beveiliging en bedreigingsbeheer binnen hybride en multi-cloudomgevingen.

De samenhang tussen de verschillende actieve en passieve componenten worden in Figuur 3 weergegeven waarbij de koppeling naar het SIEM-systeem tweeledig kan worden gezien. Het is mogelijk om gebruik te maken van Microsoft Sentinel als SIEM/SOAR, maar het is ook mogelijk om de data vanuit de Microsoft Cloud omgeving door te sturen naar een andere SIEM-oplossing.



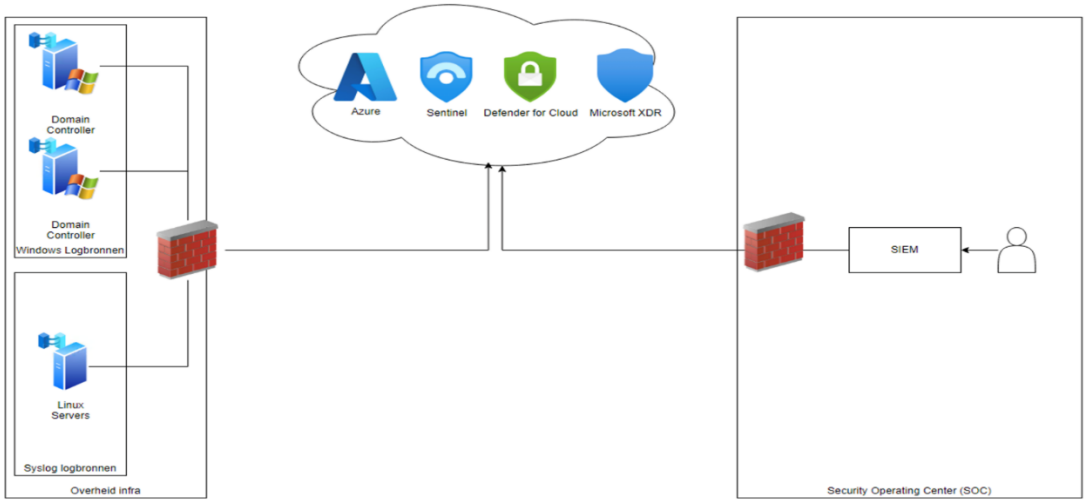
Figuur 3: Algemeen Design Overzicht

4.1.2 Microsoft Native SIEM (Sentinel)

Naast de verdedigings- en logcomponenten kan dus gebruik worden gemaakt van Microsoft Sentinel. Microsoft Sentinel is een cloud-native SIEM- en SOAR-oplossing die gebruik maakt van het Log Analytics Workspace (ook bekend als Analytics Workspace) platform die de onderliggende opslag- en beheerlaag vormt voor data, inclusief logs en metrics, binnen het Azure-ecosysteem. Sentinel gebruikt de data die is opgeslagen in Log Analytics Workspace voor beveiligingsanalyse, detectie van bedreigingen en incidentrespons.

In wezen bouwt Sentinel voort op de basis van Log Analytics Workspace om uitgebreide beveiligingsinformatie en automatiseringsmogelijkheden te bieden. Met deze oplossingen kun je logmanagement combineren met geavanceerde beveiligingsfunctionaliteiten via één enkele interface. Dit biedt niet alleen inzicht in loggegevens, maar helpt ook actief bedreigingen te detecteren en te voorkomen. Daardoor is het mogelijk om snel en eenvoudig inzicht te houden in alle oplossingen die een SOC nodig heeft voor de dagelijkse operatie. Ook worden configuratie en onboarding vereenvoudigd dankzij geïntegreerde tools en native ondersteuning voor Microsoft 365 en Azure-omgevingen.

Onderstaand diagram (Figuur 4) geeft de architectuur van deze oplossing weer. Als de organisatie resources in de Azure-cloud heeft, kan deze oplossing eenvoudig en native worden uitgerold. Voor on-premise apparaten is implementatie ook goed mogelijk.



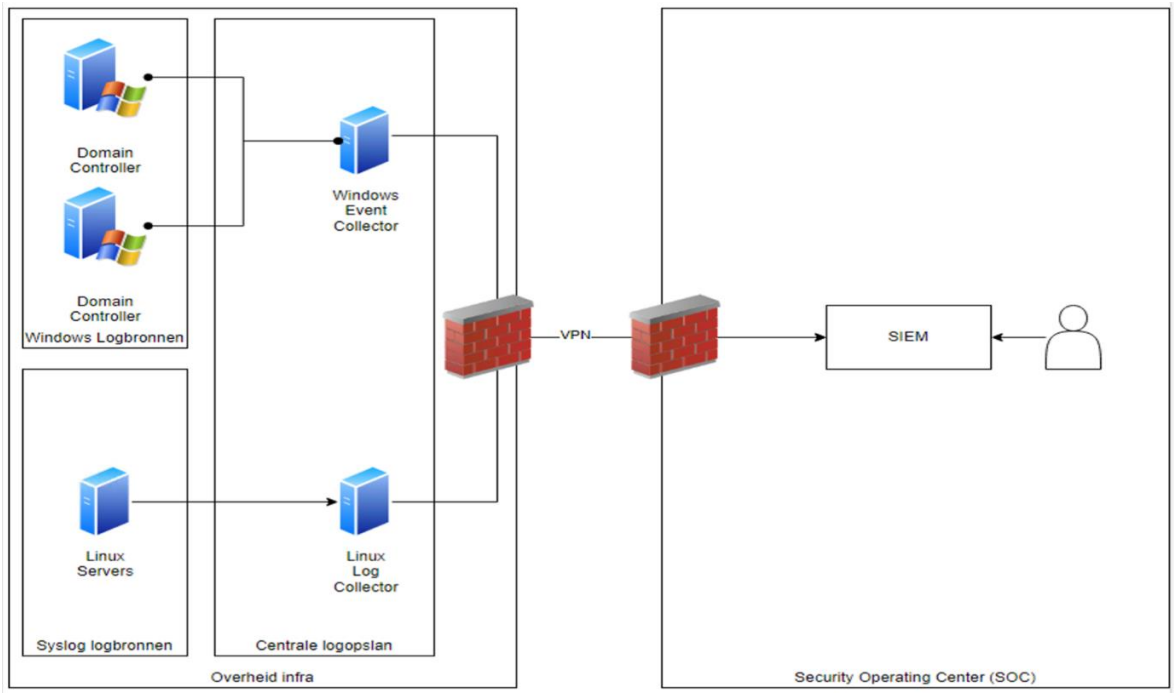
Figuur 4: Native Sentinel Integratie

Met behulp van een agent wordt een koppeling gelegd tussen de on-premise systemen en de Azure-tenant van de organisatie. Dit maakt centraal beheer van systemen mogelijk, evenals het uitrollen van de benodigde sensoren voor monitoring en beveiliging. Meer details over de implementatie van deze sensoren worden later in dit document besproken.

4.1.3 Alternatieve SIEM-oplossing

Dezelfde logcomponenten op endpoints kunnen ook loggen naar een alternatieve SIEM-oplossing. Deze optie is geschikt voor bestaande infrastructuren waarin gebruik wordt gemaakt van Windows en/of Linux. Op de endpoints wordt een logcollector geïmplementeerd die specifiek ontworpen is voor het verzamelen en centraliseren van audit events. Daarnaast wordt een afzonderlijke collector ingezet voor Windows-auditlogs en voor Linux-logs.

Onderstaand diagram (Figuur 5) illustreert hoe deze opzet functioneert. Een SOC kan hier vervolgens eenvoudig op aansluiten waarbij logdata vanaf de collectors kan worden opgestuurd of waarbij collectie-agents op de collectors worden geplaatst die de data doorsturen.



Figuur 5: 3-rd Party SIEM-Integratie

Voor de koppeling tussen de te monitoren infrastructuur en een SOC, loopt veelal via VPN-koppeling tussen de infrastructuur van de klant en die van het SOC. Daarnaast wordt er een agent geïnstalleerd op de logcollectoren om de verzamelde logs door te sturen naar het SIEM-systeem van het SOC.

Indien het SOC een Cloud-gebaseerde SIEM-oplossing gebruikt, kan de constructie er iets anders uitzien maar de principes zullen overeenkomstig zijn. Het uitgangspunt blijft echter dat de organisatie ervoor zorgt dat de logs centraal worden opgeslagen en georganiseerd. Dit maakt het mogelijk voor een SOC om direct in te haken en effectieve monitoring en incidentrespons te realiseren. Verschillende opties en designkeuzes worden verderop in dit hoofdstuk in meer detail toegelicht.

4.1.4 Vergelijking Microsoft native en alternatieve SIEM-oplossing

De voor- en nadelen van de twee oplossingsrichtingen worden in Tabel 2 weergegeven ter overweging bij de keuze voor uw organisatie.

Optie	Voordelen	Nadelen
Sentinel	• Schaalbaar en flexibel dankzij cloud-gebaseerde logverzameling. • Snelle implementatie met automatische updates en verbeteringen. • Inclusief EDR-functionaliteit, ideaal voor organisaties zonder bestaande EDR. • Extra beveiligingsfeatures van Defender for Server, zoals kwetsbaarhedenscans, aanvalsdetectie, Just-in-Time (JIT) toegang en Vulnerability Management.	• Vereist betrouwbare internetverbinding en cloud-infrastructuur. • Minder controle over data, beheerd in de cloud. • Mogelijke dubbele licentiekosten als er al een bestaande EDR-oplossing is.
Alternatieve SIEM	• Volledige controle over logs en infrastructuur. • Aanpasbare configuraties voor specifieke beveiligingsbehoeften. • Geen cloud-afhankelijkheid.	• Complexe installatie en onderhoud vereisen gespecialiseerde kennis. • Hogere initiële kosten voor hardware en licenties. • Minder schaalbaar bij grote hoeveelheden logdata.

Tabel 2: Sentinel vs. 3rd-party SIEM-Integratie

4.2 Sentinel Integratie

Deze paragraaf beschrijft in meer detail welke componenten voor verschillende doeleinden aan Sentinel kunnen worden gekoppeld.

4.2.1 Gebruikers

Gebruikersaccounts en identity management vormen het hart van elke organisatie en zijn een cruciaal onderdeel van de beveiligingsstrategie. Voor een SOC is het essentieel om zoveel mogelijk relevante securitylogs te verzamelen over deze identiteiten.

Voor het inrichten van Identity en Access Management binnen een organisatie met behulp van Microsoft Producten, bestaat de mogelijkheid dat zowel Entra ID (voor cloudgebaseerd identity management) als Active Directory (voor on-premises identiteitsbeheer) worden gebruikt. Voor beide oplossingen is de inrichting voor monitoring verschillend. Naast deze oplossingen bestaat ook nog de mogelijkheid om gebruik te maken van Defender for Identity. Deze oplossing is bedoeld voor aanvullende monitoring op lokale Acitve Directory implementaties. Voor Entra ID is het mogelijk om naast de standaard logging gebruikt te maken van Entra ID Protection voor extra bescherming en detectie.

4.2.1.1 Standaard monitoring (Entra-ID Active Directory, Entra-ID Protection)

Entra ID
Bij het monitoren van Entra ID zijn de volgende logbronnen van toegevoegde waarde:

- **Sign-in logs:** Geeft inzicht in alle aanmeldingspogingen en potentiële dreigingen.
  Beschikbaar via: Sign-In Events in Entra ID
- **Audit logs:** Logt alle wijzigingen en acties binnen Entra ID, zoals gebruikersbeheer en beleidsupdates.
  Beschikbaar via: Audit Log List in Entra ID

Voor gebruikers met een Entra ID P2-licentie (onderdeel van E5) is er aanvullende, risico gedreven informatie beschikbaar via Entra ID Protection (alleen beschikbaar met een P2-licentie), zoals:

- **Risky users:** Identificeert gebruikersaccounts die als mogelijk gecompromitteerd worden beschouwd.
- **Risky sign-ins:** Detecteert aanmeldingspogingen met een verhoogd risico, bijvoorbeeld vanaf ongebruikelijke locaties of anonieme netwerken.
- **Risky apps:** Herkent toepassingen die potentieel een beveiligingsrisico vormen.
- **Privileged Identity Management (PIM):** Beheert en monitort het gebruik van verhoogde rechten binnen de organisatie.

Door deze logs te integreren met een SIEM-oplossing zoals Microsoft Sentinel, kan een SOC proactief verdachte activiteiten detecteren en hier direct op reageren. Entra ID heeft een gestandaardiseerde set alarmen gerelateerd aan bovengenoemde onderwerpen. Meer informatie betreft de alarmenzijn te vinden op de Microsoft website[3].

Active Directory
Voor Active Directory is de inrichting anders dan voor Entra ID. Het monitoren van Active Directory is een veelbesproken onderwerp met uitgebreide online documentatie. Om relevante logs vast te leggen, is het noodzakelijk om via een GPO de Advanced Audit Policy wordt geconfigureerd[4][5]. Dit bepaalt welke acties worden geregistreerd. De gegenereerde logs worden opgeslagen in de Event Viewer van de betreffende domain controller(s).

Deze logs kunnen op twee manieren worden doorgestuurd naar een SIEM-systeem (zoals Sentinel):

1. Direct via een agent op de domain controller die de lokale logs uitleest en doorstuurt, of
2. Via een Windows Event Collector (WEC), die logs van een of meerdere systemen verzamelt en deze via een agent naar een SIEM stuurt.

4.2.1.2 Defender for Identity

Een aanvullende optie is Microsoft Defender for Identity (MDI). Dit is beschikbaar via een E5-licentie. MDI is een sensor gebruikt voor de monitoring van een of meerdere domain controllers. Hij detecteert verdachte activiteiten en stuurt meldingen naar een SIEM. Defender for Identity kan een waardevolle aanvulling zijn op de standaard correlatieregels binnen een SIEM.

Microsoft Defender for Identity richt zich op:

- **Identiteitsbeveiliging:** Detecteert verdachte activiteiten binnen Active Directory (AD).
- **Threat Detection:** Real-time waarschuwingen voor identiteitsaanvallen, zoals pass-the-hash en pass-the-ticket.
- **Gedragsanalyse:** Analyseert gebruikersgedrag om afwijkingen te detecteren.

De oplossing beschermt on-premises Active Directory implementaties tegen identiteit-gerelateerde aanvallen en geeft inzicht in beveiligingsrisico's binnen het netwerk. Dit helpt bij het identificeren van bedreigingen voordat ze schade kunnen aanrichten.

[3] What are risks in Microsoft Entra ID Protection - Microsoft Entra ID Protection | Microsoft Learn
[4] https://vssr.rijksapplicaties.nl/link?l=DOC-VSSR-MD-Log_Policies-Windows_Audit_Policies
[5] OR-10: https://vssr.rijksapplicaties.nl/link?l=DOC-VSSR-MD-SOC_Operational_Readiness_OR5-10

Een overzicht van alle mogelijke detecties is hier te vinden: Security alerts in Microsoft Defender for Identity.

Meer informatie over MDI is beschikbaar op de officiële Microsoft Defender for Identity-pagina.

4.2.2 Werkplekken

Voor de beveiliging en het beheer van werkplekken binnen een Microsoft 365 E5-omgeving zijn Microsoft Defender for Endpoint (MDE) en Defender for Cloud Apps (MDCA) de twee belangrijkste oplossingen. MDE biedt geavanceerde endpoint-detectie en -respons (EDR), terwijl MDCA inzicht geeft in en controle biedt over het gebruik van cloudapplicaties. In dit hoofdstuk worden beide oplossingen en hun functionaliteiten besproken. Ze vullen elkaar naadloos aan en integreren goed binnen Microsoft XDR.

4.2.2.1 Microsoft Defender for Endpoint (MDE)

Defender for Endpoint biedt geavanceerde bescherming tegen diverse aanvalstechnieken, waaronder Ransomware, Fileless malware attacks, Zero-day exploits en Credential theft. Dit doet Microsoft Defender for Endpoint met behulp van een aantal componenten:

- **Antivirus (AV):** Integreert met geavanceerde antivirusoplossingen om malware te detecteren en te verwijderen.
- **Endpoint Detection and Response (EDR):** Detecteert en reageert op endpointbedreigingen, en biedt uitgebreide forensische analyses.
- **Vulnerability Management (VM):** Identificeert en beheert kwetsbaarheden op endpoints door continue monitoring en risicobeoordeling.
- **Threat & Vulnerability Management (TVM):** Geeft een overzicht van prioritaire kwetsbaarheden en misconfiguraties en helpt deze proactief te beheersen.
- **Web Threat Protection (WTP):** Voorkomt toegang tot schadelijke URL's door het blokkeren van gevaarlijke websites en het beschermen tegen phishing-aanvallen.

Naast proactieve beveiliging biedt MDE met deze verschillende oplossingen uitgebreid inzichten in risicovolle apparaten, zoals systemen met kwetsbare besturingssystemen, applicaties en andere beveiligingsrisico's. Daarnaast bevat het een krachtige audit logging-functionaliteit.
Voor verschillende van deze oplossingen zijn diverse producten op de markt verkrijgbaar. Voornamelijk voor AV, VM en EDR-oplossingen is de keuze groot. Met een Microsoft 365 E5-licentie wordt standaard toegang geboden tot de Microsoft variant voor deze producten met ondersteuning voor Windows, Linux, macOS, Android en iOS waardoor een breed scala aan apparaten kan worden beschermd via één interface.

Logretentie

Standaard blijven de logs van Defender for Endpoint 30 dagen doorzoekbaar, terwijl alerts 180 dagen bewaard blijven. Voor langere retentie kan een koppeling met een logmanagementplatform zoals Azure Monitor met Log Analytics Workspace, waar logs tot 12 jaar kunnen worden opgeslagen. Microsoft Sentinel heeft een standaard integratie beschikbaar tussen beide oplossingen.

MDE-Implementatie

Microsoft Defender for Endpoint kan op Windows endpoints op verschillende manieren worden uitgerold.

- **Automatische uitrol via Endpoint Security policies in Intune**
  - Voorkeur voor organisaties die Intune gebruiken voor werkplekbeheer.
- **Group Policy (GPO) en Microsoft Endpoint Configuration Manager (MECM/SCCM)**
  - Voor on-premises beheerde Windows werkplekken zonder Intune.
  - Configuratie via een GPO met de Defender for Endpoint onboarding script.
  - MECM/SCCM kan de installatie en configuratie automatiseren.
- **Local Script Deployment**
  - Geschikt voor kleinere omgevingen (<10 werkplekken).
  - Uitrol via PowerShell-scripts met het MDE onboarding package.

Meer informatie over implementatiemethoden is hier te vinden: Microsoft Defender for Endpoint Deployment Strategy

4.2.2.2 Microsoft Defender for Cloud Apps

Microsoft Defender for Cloud Apps (MDCA) is de Cloud Access Security Broker (CASB) binnen het Microsoft security-ecosysteem. Het biedt beveiligingsmaatregelen voor cloudapplicaties en SaaS-oplossingen.

Functionaliteit binnen Defender for Cloud Apps

MDCA monitort en beveiligt toegang tot cloudapplicaties en ondersteunt onder andere:

- **Schaduw-IT detectie:** Identificeer ongeautoriseerde cloudapplicaties binnen de organisatie.
- **Realtime bedreigingsdetectie:** Herken en blokkeer verdachte activiteiten in cloud apps zoals Microsoft 365, Salesforce, Dropbox, AWS, en Google Workspace.
- **Geautomatiseerde beleidsregels:** Handhaaf beveiligingsregels voor compliance en databeheer.
- **Beveiliging van gevoelige data:** Integreert met Microsoft Purview om datalekken en misbruik te detecteren.
- **Identiteits- en toegangsbeheer:** Integreert met Conditional Access en Microsoft Entra ID voor risicogebaseerde toegangscontrole.

Detectie en Incidentrespons

Defender for Cloud Apps detecteert bedreigingen door gebruik te maken van:

- **Anomalie detectie**: Identificeert afwijkend gebruikersgedrag, zoals inlogpogingen vanuit verdachte locaties.
- **Threat intelligence**: Gebruikt AI en Microsoft Threat Intelligence om aanvallen vroegtijdig te herkennen.
- **API-integratie met SaaS-applicaties**: Beveiligt en monitort populaire clouddiensten.

Voor configuratie best-practices met betrekking tot MDCA zie: Best practices for protecting your organization with Defender for Cloud Apps

MDE- en MDCA-integratie

Nadat MDE is uitgerold, kan het worden gekoppeld aan MDCA voor extra beveiliging op Windows endpoints die toegang zoeken tot cloud-apps. Hiermee geniet uw organisatie een bredere beveiliging betreft:

- **MDE Cloud Discovery:** Detecteert en logt het gebruik van shadow IT door netwerkverkeer te monitoren.
- **Conditional Access App Control:** Kan risicovol gedrag in cloudapplicaties blokkeren (vereist Entra ID en MDCA).
- **Realtime dreigingsdetectie:** Analyseert endpoint- en cloudactiviteiten om verdachte acties te signaleren.

Meer informatie over de integratie van MDE en MDCA:
Integrate Microsoft Defender for Endpoint with Microsoft Defender for Cloud Apps

4.2.3 Defender for Cloud

Defender for Cloud is ontwikkeld voor het beveiligen van toepassingen op cloud-platformen. Hierin worden twee smaken onderkend:

1) Azure (de Microsoft Cloud); en,
2) Alternatieve Cloud-oplossingen zoals van Google Cloud Platform en AWS.

In eerste instantie worden enkele mogelijkheden binnen Azure aangestipt. Daarna wordt Infrastructure-as-a-Service behandeld voor zowel Azure als alternatieve platformen omdat de implementatie hiervoor afwijkt. Als laatste worden Azure specifieke Platform-as-a-Service oplossingen aangeraakt.

4.2.3.1 Azure

Het effectief monitoren van een Azure-omgeving is complex en vereist diepgaande kennis van de verschillende componenten binnen het platform. Azure bestaat uit meerdere lagen die elk hun eigen logging en monitoring vereisen. De drie belangrijkste onderdelen voor monitoring zijn Entra ID, Azure Activity Logs en Diagnostic Logs van resources.

Entra ID
Entra ID (voorheen Azure Active Directory) vormt de kern van identiteits- en toegangsbeheer binnen Azure. Het biedt authenticatie, autorisatie en toegangscontrole voor gebruikers en applicaties. Sign-in logs en audit logs worden standaard vastgelegd en bieden inzicht in aanmeldpogingen, wijzigingen in gebruikersrechten en verdachte activiteiten. Met een Entra ID P2-licentie zijn aanvullende beveiligingsmaatregelen beschikbaar, zoals Identity Protection en risicodetectie. Microsoft Sentinel integreert naadloos met Entra ID en biedt vooraf ontwikkelde detectieregels en dashboards om identiteitgerelateerde dreigingen snel te signaleren.

Azure Activity Logs
Azure Activity Logs registreren wijzigingen en beheerdersacties binnen de Azure-omgeving. Dit omvat het aanmaken, wijzigen en verwijderen van resources, evenals beleidswijzigingen en toegangsaanpassingen. Deze logs zijn essentieel voor inzicht in wie welke wijzigingen heeft doorgevoerd en wanneer deze hebben plaatsgevonden. Sentinel beschikt over een standaardconnector voor Azure Activity Logs, waardoor organisaties snel verdachte activiteiten kunnen detecteren en analyseren.

Diagnostic Logs van resources
Naast beheerdersacties registreren individuele Azure-resources ook gedetailleerde operationele en prestatiegegevens via Diagnostic Logs. Dit omvat bijvoorbeeld sign-in pogingen, foutmeldingen en specifieke servicegebeurtenissen. Voorbeelden van resources die uitgebreide logging bieden zijn Azure Firewall, Key Vault en SQL-databases. De integratie met Sentinel varieert per service; sommige hebben een standaard data connector, terwijl andere handmatige configuratie vereisen. Door deze logs centraal te verzamelen in Sentinel kunnen organisaties afwijkingen detecteren en geavanceerde dreigingsanalyses uitvoeren.

Integratie met Microsoft Sentinel
Microsoft Sentinel biedt native integraties met deze drie componenten en beschikt over out-of-the-box detectieregels voor het identificeren van beveiligingsdreigingen. Door Entra ID, Azure Activity Logs en Diagnostic Logs te combineren, ontstaat een compleet beeld van de beveiligingsstatus van een Azure-omgeving.

4.2.3.2 IAAS

Voor servers binnen Infrastructure-as-a-Service omgevingen zijn er twee beveiligingsopties beschikbaar:

1. **Defender for Endpoint**
   Dit kan op dezelfde manier worden uitgerold als op werkplekken en biedt dezelfde geavanceerde detectie- en responsmogelijkheden.
2. **Defender for Servers**
   Dit is een uitgebreide beveiligingsbundel die niet alleen Defender for Endpoint omvat, maar ook aanvullende beveiligingsfunctionaliteiten, zoals bedreigingsdetectie op besturingssysteemniveau en integratie met andere Microsoft-beveiligingsproducten.

Aangezien servers niet zijn inbegrepen in de E5-licentie, zijn aanvullende licenties vereist voor zowel Defender for Endpoint als Defender for Servers.

Onderstaande tabel geeft een overzicht van de verschillen tussen Defender for Servers Plan 1 en Plan 2.

Functionaliteit	Plan 1	Plan 2
Microsoft Defender for Endpoint	✅	✅
Microsoft Defender vulnerability management	✅	✅
Automatic agent onboarding, alert en data integratie	✅	✅
Gedetailleerde, context-gebaseerde security alerts	✅	✅
Alerts met richtlijnen voor mitigatie	✅	✅
Agentless VM vulnerability scanning	❌	✅
Agentless VM secrets scanning	❌	✅
Agentless malware detection	❌	✅
Control plane security alerts	❌	✅
Regulatory compliance en best practices	❌	✅
Just-in-time VM access voor management ports	❌	✅
Network layer threat detection	❌	✅
File integrity monitoring	❌	✅
Baselines assessment	❌	✅
Log Analytics 500MB free data ingestion	❌	✅

Tabel 3: Defender for Server plans

In deze sub-sectie wordt niet verder ingegaan op de hierboven genoemde functionaliteiten maar gaat de aandacht vooral uit naar de beveiliging met Defender for Endpoint en de onboarding van servers in Defender for Cloud om Defender for Servers uit te kunnen rollen.

Defender for Servers kan op twee manieren worden uitgerold, afhankelijk van de herkomst van de server:

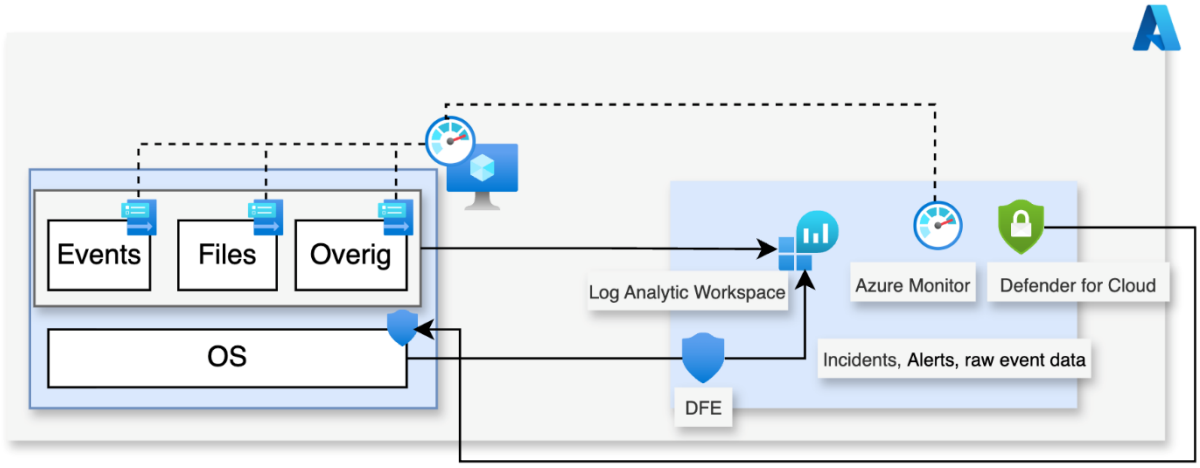
- Azure VM's: Voor virtuele machines binnen Azure kan Defender for Servers met een eenvoudige configuratie in Defender for Cloud worden geactiveerd.
- Niet-Azure VM's: Voor servers buiten Azure, zoals on-premises of in andere cloudomgevingen (AWS, GCP), is eerst onboarding via Azure Arc vereist voordat Defender for Servers kan worden ingeschakeld. Dit wordt verderop uitgebreider beschreven.

Wanneer gekozen wordt voor Defender for Endpoint, zijn er meerdere uitrolstrategieën beschikbaar, afhankelijk van de infrastructuur en het beheermodel. Hieronder worden deze implementatieopties en bijbehorende stappen besproken.

Defender for Servers in Azure Virtual Machines

Voor Azure Virtual Machines (VMs) biedt Defender for Servers een geautomatiseerde onboarding:

- Azure VMs worden automatisch zichtbaar in Defender for Cloud zodra ze aan een Azure Subscription zijn gekoppeld.
- Er is geen extra onboarding vereist. Activeren van Defender for Servers gebeurt simpelweg door het inschakelen van de service in de juiste subscription.



Figuur 6: DFS on Azure

Op het gebied van aanvalsdetectie en logbeheer speelt Defender for Endpoint een centrale rol. Wanneer Defender for Servers is ingeschakeld, wordt Defender for Endpoint automatisch uitgerold waardoor diepgaande detectie en responsmogelijkheden beschikbaar komen.

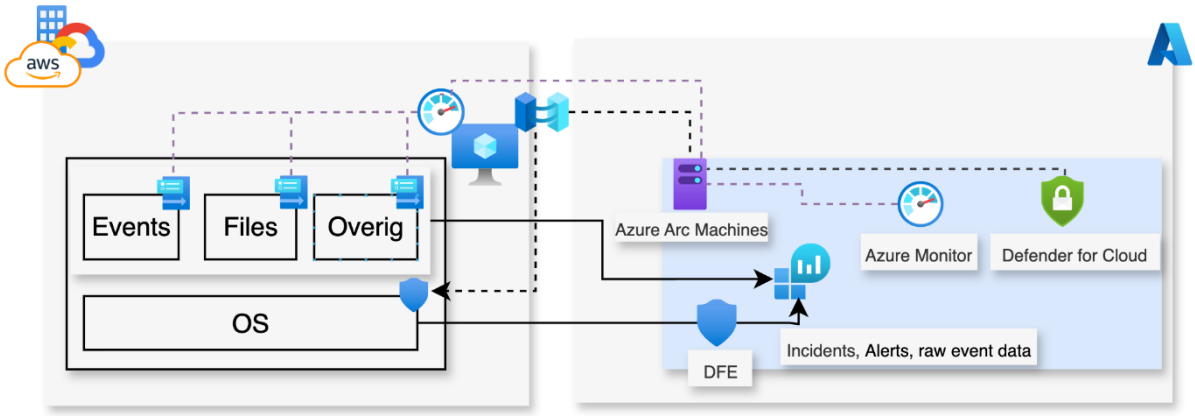
Belangrijke aandachtspunten voor logging:

- Defender for Endpoint logs bevatten uitgebreide (verbose) gegevens over bedreigingen en beveiligingsgebeurtenissen, maar nemen niet alle traditionele Windows Event Logs mee.
- Om extra Event IDs te verzamelen, kunnen deze worden geconfigureerd via Advanced Audit Policy in Group Policy (GPO).
- Voor een volledige integratie met Sentinel kunnen specifieke event logs uit Event Viewer worden opgehaald en doorgestuurd naar een Log Analytics Workspace via een Data Collection Rule (DCR) in Azure Monitoring.
- Naast events kunnen ook andere data/logs opgehaald worden, denk hierbij aan bestanden, performance data etc.
- Bij Linux werkt dit anders. Hier kan gebruik worden gemaakt van logoplossingen zoals Syslog, Sysmon for Linux, Auditd en andere methoden. Deze logs kunnen lokaal naar een bestand worden geschreven en vervolgens via een Data Collection Rule (DCR) worden uitgelezen, of direct worden doorgestuurd naar een centrale Syslog-logcollector. In dat laatste geval kan een Azure Monitor Agent (AMA) in combinatie met een DCR de loggegevens doorsturen naar een Log Analytics Workspace voor verdere analyse en correlatie.

Met deze aanpak kun je een volledige dekking realiseren, waarbij Defender for Endpoint geavanceerde dreigingsinformatie levert, terwijl aanvullende Windows-logboeken inzicht geven in bredere systeemactiviteiten.

Defender for Servers voor niet-Azure Virtual Machines
Voor virtuele machines buiten Azure, zoals in AWS, GCP of on-premises omgevingen, vereist Defender for Servers een extra onboardingsproces. In tegenstelling tot native Azure-VM's, die automatisch worden opgenomen in Defender for Cloud, moeten externe systemen eerst worden gekoppeld aan Azure voordat ze beveiligd kunnen worden. Dit gebeurt via Azure Arc. Dit is een hybride beheerplatform dat niet-Azure resources integreert binnen het Azure-ecosysteem. Azure Arc fungeert als een brug tussen on-premises en cloudomgevingen waardoor Defender for Cloud deze systemen kan herkennen en beheren alsof ze native Azure-resources zijn.

Zodra de onboarding via Azure Arc is voltooid, kunnen deze systemen worden opgenomen in Defender for Servers. Via de instellingen in Defender for Cloud wordt bepaald onder welke Azure-subscriptie de beveiliging wordt geactiveerd en welk licentieplan wordt toegepast (Plan 1 of Plan 2). Meer informatie hierover is te vinden in de documentatie: Azure Arc Overview



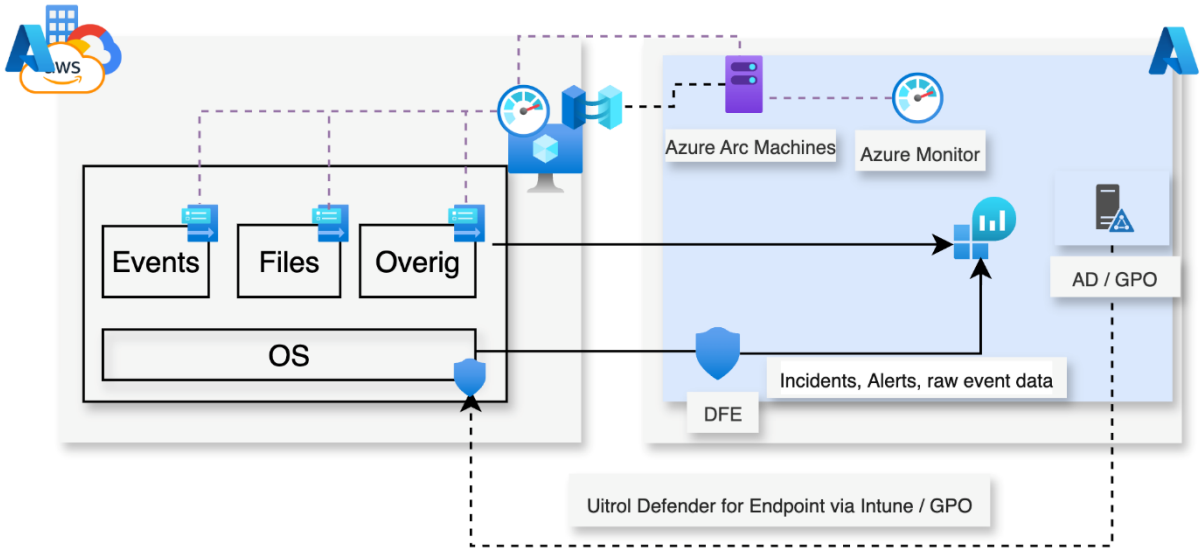
Figuur 7: DFS on Alternative Cloud Platform

Defender for Endpoint-only
In sommige scenario's kan het wenselijk zijn om uitsluitend gebruik te maken van MDE zonder Defender for Servers (zie Figuur 8: DFE on Azure). Dit kan bijvoorbeeld het geval zijn wanneer organisaties een lichtere beveiligingsoplossing verkiezen of geen behoefte hebben aan de extra functionaliteiten die Defender for Servers biedt. In dergelijke gevallen is het mogelijk om Defender for Endpoint als stand-alone oplossing uit te rollen zonder gebruik te maken van Defender for Server.

De implementatie van Defender for Endpoint op servers kan op verschillende manieren worden uitgevoerd, afhankelijk van de omvang van de omgeving:

- Kleine omgevingen (tot 10 machines): Uitrol kan eenvoudig worden gedaan via een lokaal script dat handmatig op de betreffende servers wordt uitgevoerd.
- Grotere omgevingen: Voor een geautomatiseerde en schaalbare uitrol is Group Policy (GPO) een effectieve methode om Defender for Endpoint centraal te implementeren.

Meer informatie over de verschillende implementatiemethoden is te vinden in de officiële documentatie: Microsoft Defender for Endpoint – Configure Server Endpoints



Figuur 8: DFE on Azure

4.2.3.3 PAAS

Azure biedt een breed scala aan Platform-as-a-Service (PaaS) oplossingen, zoals databases, containers, key vaults, etc. Deze resources kunnen worden beveiligd en gemonitord via Microsoft Defender for Cloud dat geïntegreerde beveiliging biedt voor verschillende PaaS-services.

Microsoft Defender for Cloud werkt met een modulaire aanpak, waarbij specifieke beveiligingsmodules (blades) beschikbaar zijn voor verschillende typen PaaS-resources. Deze kunnen per Azure Subscription worden geactiveerd en bieden automatische monitoring en bescherming. Enkele belangrijke Defender-modules voor PaaS zijn:

- Defender for Containers: Beschermt containers, Kubernetes-omgevingen en container image registries.
- Defender for Databases: Biedt beveiliging voor Azure SQL, Cosmos DB en andere databases.
- Defender for Storage: Detecteert verdachte activiteiten in Azure Storage-accounts.
- Defender for App Service: Beveiligt webapplicaties gehost in Azure App Service.
- Defender for Key Vault: Beschermt gevoelige secrets en API-sleutels in Azure Key Vault.

Zodra een Defender module is ingeschakeld, worden de gekoppelde PaaS services automatisch gemonitord en beveiligd, zonder dat handmatige configuratie per resource nodig is.

Detectie en alarmen

Defender for Cloud genereert beveiligingswaarschuwingen voor gedetecteerde bedreigingen en kwetsbaarheden binnen PaaS-resources. Een volledig overzicht van de mogelijke detecties en waarschuwingen is te vinden in de officiële **Microsoft Defender for Cloud Alerts Reference**.

Microsoft Sentinel integreert naadloos met Defender for Cloud, waardoor alle beveiligingsalerts automatisch worden doorgestuurd naar Sentinel. Dit een bi-directionele koppeling. Dit houdt in dat incidenten die bijgewerkt of gesloten worden in Sentinel bijgewerkt worden in Defender for Cloud.

4.3 Alternatieve SIEM Integratie Opties

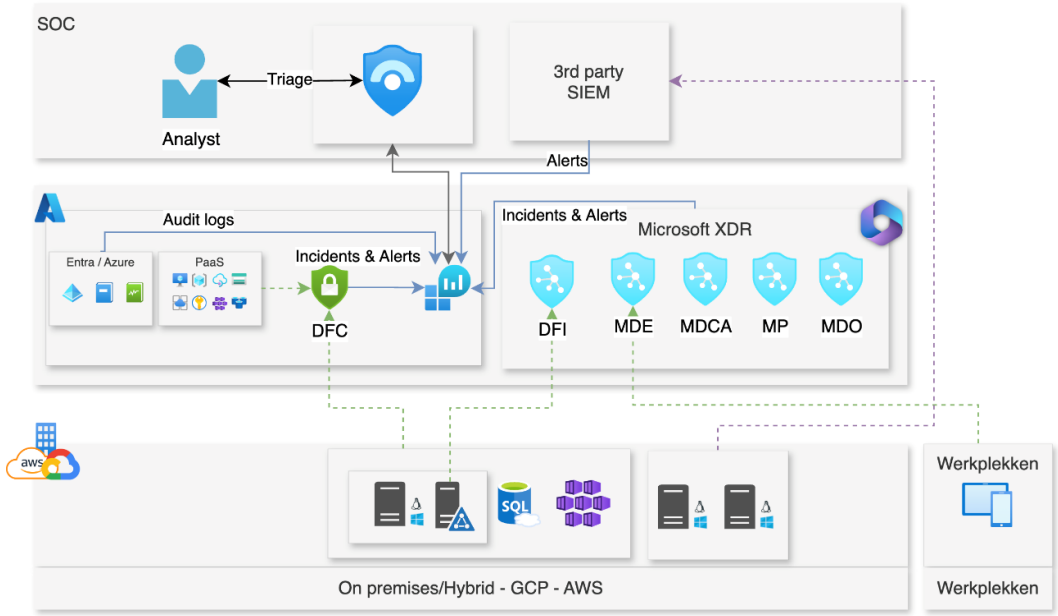
Veel organisaties maken gebruik van Microsoft-producten die naadloos integreren met Microsoft Sentinel. Microsoft biedt echter ook ondersteuning voor SOC's die een ander SIEM-platform gebruiken. Alle Microsoft-producten beschikken over API's om integratie met externe systemen mogelijk te maken. Bedenk wel dat de API's beschikbaar zijn op het Cloud-platform en dat de data die vanuit de verschillende Microsoft-producten wordt opgehaald dus uit de Cloud worden opgehaald naar een on-premis of eigen Cloud-SIEM. Dit is vooral belangrijk om te realiseren als Cloud voor de organisatie geen optie is. Bij gebruikmaking van de API's gaat de data dus eerst vanuit de endpoints (bijvoorbeeld MDE) **naar de Cloud**, waarna deze via een API overgehaald kan worden naar een SIEM-systeem.

In dit hoofdstuk worden de belangrijkste SIEM- en XDR-oplossingen besproken waarvoor Microsoft officiële documentatie biedt. Dit betekent niet dat andere oplossingen niet kunnen worden gekoppeld maar Microsoft biedt hier dus geen standaard ondersteuning op. Dankzij de beschikbare integratiemogelijkheden zijn er diverse opties om data uit Microsoft-producten te benutten binnen andere SIEM-omgevingen.

Microsoft heeft twee veelgebruikte opties voor een hybride SIEM-oplossing uitgebreid beschreven in het volgende artikel: Deploying Microsoft Sentinel side-by-side to an existing SIEM. Daarnaast is er een derde optie waarbij Microsoft Sentinel volledig wordt overgeslagen en Microsoft-producten direct worden gekoppeld aan een externe SIEM-oplossing. Deze drie opties worden hieronder verder uiteengezet.

4.3.1 Optie 1: Alerts uit een bestaande SIEM naar Microsoft Sentinel sturen

In deze aanpak wordt Microsoft Sentinel de centrale SIEM-oplossing (Single Point of Truth), terwijl de bestaande SIEM als dataleverancier fungeert en alerts naar Sentinel doorstuurt. Dit kan in een scenario fungeren waarbij bijvoorbeeld specifieke brondata niet naar de Cloud mag, maar alerts wel, of wanneer een migratie van een bestaand SIEM-systeem naar Sentinel plaats vindt. Voor meer informatie, zie: https://learn.microsoft.com/en-us/azure/sentinel/deploy-side-by-side



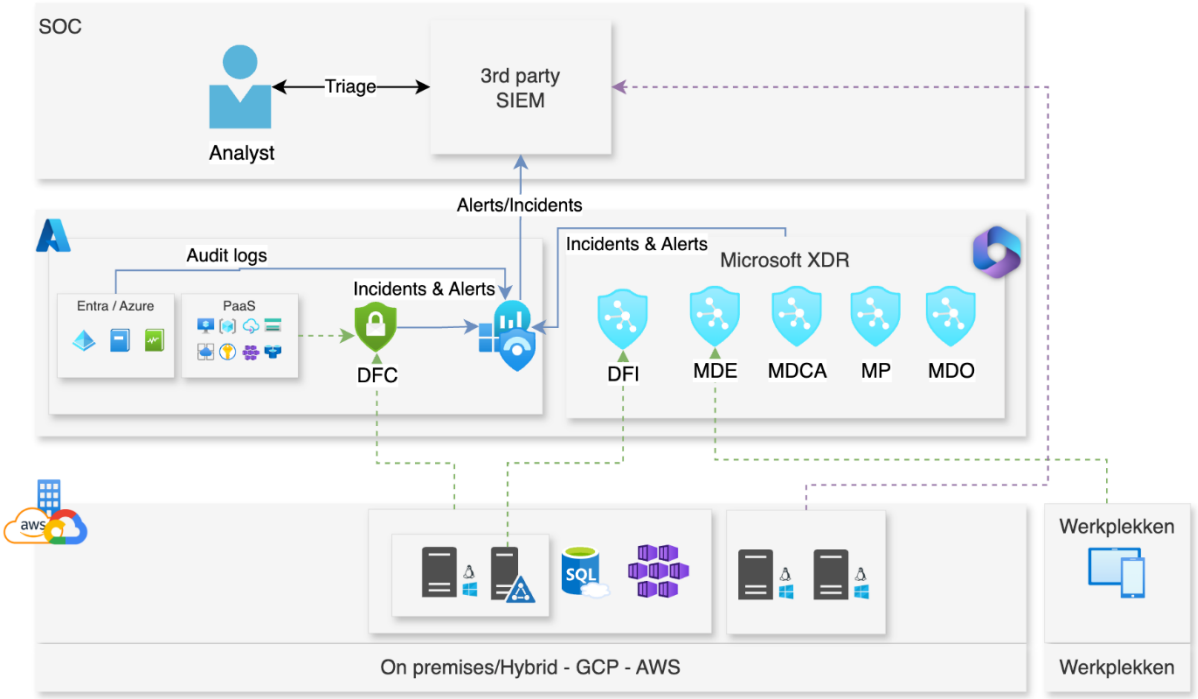
Figuur 9: Alert-stream from 3rd-party SIEM to Sentinel

4.3.2 Optie 2: Microsoft-logbronnen koppelen aan Sentinel en Sentinel integreren met een externe SIEM

Bij deze aanpak worden alle Microsoft-logbronnen eerst verzameld in Microsoft Sentinel, waarna Sentinel de relevante gegevens doorstuurt naar de externe SIEM. Dit is geschikt voor organisaties die Sentinel niet als primaire SIEM willen gebruiken maar wel de voordelen ervan willen benutten.

Redenen om deze aanpak te kiezen:

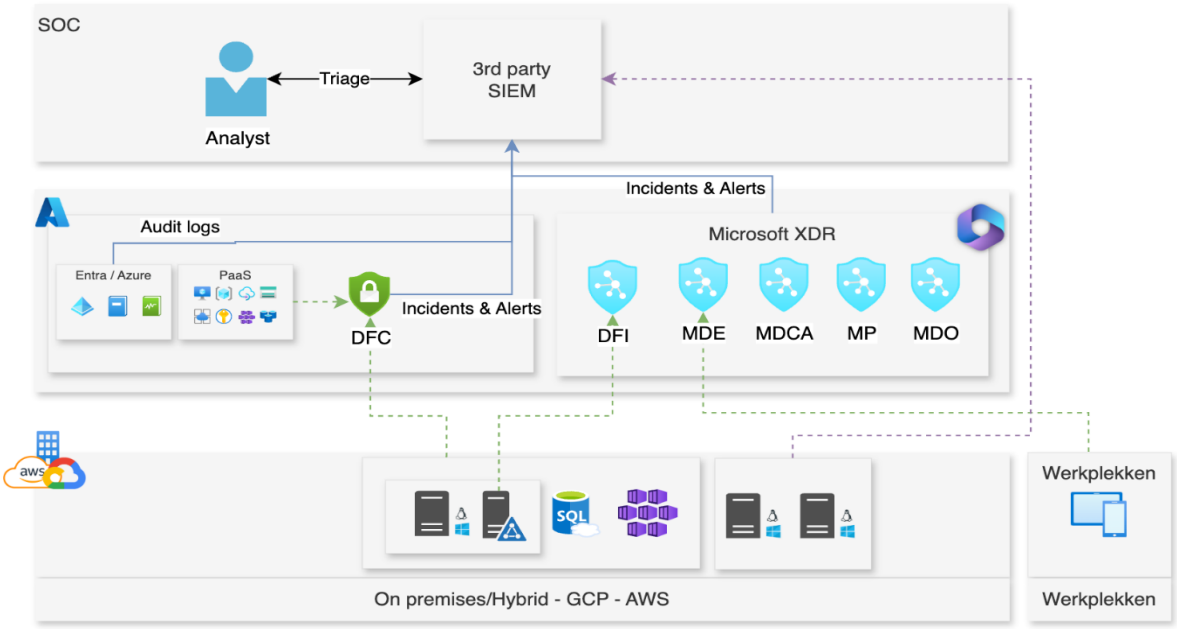
1. Sentinel biedt krachtige detectieregels en inzichten specifiek voor Microsoft-producten zoals Azure-resources, Entra ID en Azure Activity Logs. Door deze logbronnen aan Sentinel te koppelen, kan de detectie aanzienlijk worden verbeterd op een efficiënte manier, zonder dat er veel tijd en moeite nodig is voor het zelf ontwikkelen van detectieregels binnen de bestaande SIEM.
2. Een directe koppeling tussen Microsoft-producten en een externe SIEM is vaak complex of ontbreekt volledig. Door Sentinel als tussenlaag te gebruiken, wordt integratie eenvoudiger.
3. Organisaties die volledige controle willen behouden over hun data kunnen logbestanden lokaal houden. In dit model blijven ruwe logs binnen Sentinel, terwijl alleen alerts en incidentcontext worden doorgestuurd naar de externe SIEM. Analisten kunnen indien nodig direct inloggen op Sentinel voor verdere analyse.



Figuur 10: Alert-stream van Sentinel naar 3rd-party SIEM

4.3.3 Optie 3: Integreren van Microsoft (security) producten met 3rd party SIEM

In deze aanpak wordt Microsoft Sentinel volledig buiten beschouwing gelaten, en worden Microsoft-producten rechtstreeks gekoppeld aan een 3rd-party SIEM. Dit vereist integratie met de API's of logmogelijkheden van elk afzonderlijk Microsoft-product, wat betekent dat organisaties de verschillende productlogs en signalen handmatig moeten integreren in de bestaande SIEM-oplossing.



Figuur 11: Directe integratie van sensoren met 3rd-party SIEM

De belangrijkste producten in aanmerking komen voor integratie, zijn onder andere:

- **Microsoft Defender XDR-suite**: Integratie met 3rd-party SIEM
- **Entra ID audit logs:** Log Streaming opties
- **Azure Activity Logs:** Azure Activity Log Integratie
- **Azure Diagnostics:** Azure Diagnostics Logging Instellingen
- **Defender for Cloud:** Exporteren naar 3rd-party SIEM

Deze aanpak kan interessant zijn voor organisaties die al beschikken over een goed geïntegreerde SIEM-oplossing en geen extra laag, zoals Sentinel, willen toevoegen. Het kan ook voordelen bieden voor organisaties die volledig de controle willen behouden over hun bestaande SIEM-configuraties. Het nadeel is dat er meer handmatige configuratie is en onderhoud van de integratie zal vereisen. Met deze oplossing kunnen alle relevante beveiligingslogs van Microsoft-producten direct worden doorgestuurd naar de bestaande SIEM, wat de mogelijkheid biedt om analyses en meldingen te genereren zonder dat een tweede SIEM-oplossing noodzakelijk is.

Bijlage I – Intake voor SOC-onboarding

Ondanks dat public Cloud veel operationele overhead wegnemen bij ICT-afdelingen, verschuift een aanzienlijk deel van de benodigde securitykennis naar securityteams en het SOC. De onderstaande vragenlijst vormt een vertrekpunt voor een SOC-dienstverlener die derde-partijen bedient. Dit benadrukt hoe complex en veelzijdig het eigenaarschap over security wordt binnen een organisatie die Microsoft 365 en Azure gebruikt. Een diepgaande kennis van deze platformen is essentieel om de beveiliging effectief te waarborgen en risico's proactief te beheersen.

Of het nu gaat om een interne organisatie of een nieuwe externe organisatie die wordt aangesloten op het SOC voor proactieve security monitoring, het is belangrijk om een goed overzicht van de omgeving te krijgen. Deze lijst is niet volledig, maar richt zich specifiek op vragen die relevant zijn voor de Microsoft (security) producten. Als dienstverlener kan dit worden gebruikt bij een klant-intake terwijl een opdrachtgever of intern SOC dezelfde lijst kan gebruiken om te zien of aan alle belangrijke randvoorwaarden is voldaan om goed gebruik te kunnen maken van de Microsoft-securityproducten.

Algemene informatie

- Welke licenties worden gebruikt? (Bijv. Microsoft E3, E5, standalone licenties, of andere bundels?)
- Hoeveel Azure-tenants zijn er?
- Wordt er gebruikgemaakt van meerdere subscriptions binnen een tenant?
- Staan alle resources in één regio, of worden er meerdere Azure-regio's gebruikt?
- Wordt er gebruikgemaakt van hybride infrastructuur (Azure Arc, On-Prem, Multi-Cloud)?

Endpoints & Werkstations

- Zijn er werkstations in gebruik?
- Hoe worden deze beheerd? (Bijv. Microsoft Intune, Jamf, SCCM, third-party MDM-oplossingen?)
- Worden werkstations automatisch toegevoegd aan Defender for Endpoint?
- Wat is de huidige configuratie in Defender for Endpoint en hoe verhoudt deze zich tot de best practices?
- Is Defender for Endpoint geïntegreerd met Defender for Cloud Apps?
- Wordt attack surface reduction (ASR) toegepast op endpoints?
- Wordt endpoint detection & response (EDR) in block mode gebruikt?
- Zijn er specifieke compliance-eisen of security-frameworks waaraan voldaan moet worden?

Servers & Backend Infrastructuur

- Zijn er servers in gebruik?
- Waar worden deze gehost? (On-premises, Azure, AWS, Google Cloud, hybride?)
- Welke besturingssystemen worden gebruikt? (Windows Server, Linux-distributies, versies?)
- Zijn er kritieke systemen en kroonjuwelen geïdentificeerd?
- Wordt Defender for Servers gebruikt, en zo ja, welk plan (Plan 1, Plan 2)?
- Zijn de Defender for Servers-onderdelen geconfigureerd (bijv. File Integrity Monitoring, Just-In-Time VM Access)?

Active Directory & Identity Management

- Wordt gebruikgemaakt van on-premises Active Directory, Azure AD of een hybride setup?
- Zijn er Domain Controllers aanwezig?
- Is de Defender for Identity-sensor geïnstalleerd op de Domain Controllers?
- Is de Defender for Identity-sensor in een gezonde status (Health monitoring)?
- Worden er Identity Protection policies gebruikt (Bijv. risk-based Conditional Access, MFA-beleid)?

Is Privileged Identity Management (PIM) ingeschakeld voor beheerdersrollen?

- Worden Global Admins en andere gevoelige rollen beschermd met PIM?
- Zijn er tijdsgebonden en just-in-time (JIT) activatievereisten ingesteld?
- Wordt multi-factor authenticatie (MFA) afgedwongen bij rolactivering?
- Is er auditing en alerting ingeschakeld op PIM-gebruik?

Cloud & PaaS Oplossingen

- Wordt er gebruikgemaakt van Platform-as-a-Service (PaaS)-oplossingen?
  - **Databases** (Bijv. Azure SQL, Cosmos DB, AWS RDS, Google Cloud SQL)
  - **Azure App Services** (Bijv. Web Apps, Function Apps, Logic Apps)
  - **Containers / Kubernetes** (Bijv. AKS, EKS, GKE, On-Prem Kubernetes clusters)
  - **Azure Storage** (Welke storage accounts, toegangsbeveiliging, logging geconfigureerd?)
- Is Defender for Cloud correct geconfigureerd voor deze PaaS-oplossingen?
- Zijn er security alerts of misconfiguraties binnen Defender for Cloud?

DevOps & Source Control

- Wordt gebruikgemaakt van Azure DevOps of GitHub?
- Zijn security controls zoals code scanning, secret scanning en CI/CD-pipeline beveiliging ingeschakeld?
- Is Defender for DevOps geconfigureerd en geïntegreerd met de pipeline?
- Wordt er gebruikgemaakt van Infrastructure-as-Code (IaC) en zo ja, hoe wordt security geborgd?

E-mail & Samenwerkingstools

- Wordt Microsoft 365 gebruikt voor e-mail?
- Wordt Defender for Office 365 ingezet?
  - Zijn anti-phishing, anti-malware en Safe Links correct geconfigureerd?
  - Worden geavanceerde hunting queries en attack simulations ingezet?
- Zijn er specifieke security-zorgen met betrekking tot e-mailbeveiliging (bijv. BEC, phishing-campagnes)?

Netwerk & Toegangsbeheer

- Worden er firewall- en netwerkbeveiligingsoplossingen gebruikt? (Bijv. Azure Firewall, NSG's, WAF?)
- Is er een VPN of Zero Trust Network Access (ZTNA) oplossing in gebruik?
- Wordt Conditional Access correct toegepast voor verschillende gebruikersgroepen?
- Wordt Privileged Access Management (PAM) gebruikt voor kritieke accounts en beheerders?
- Wordt gebruikgemaakt van Privileged Access Workstations (PAW) of Just-In-Time (JIT) toegang?
- Wordt er al gebruik gemaakt van een CASB-oplossing?

Bijlage II – Overzicht Sentinel log-table plans

Features	Analytics	Basic	Auxiliary
Best for	High-value data used for continuous monitoring, real-time detection, and performance analytics.	Medium-touch data needed for troubleshooting and incident response.	Low-touch data, such as verbose logs, and data required for auditing and compliance.
Supported table types	All table types	Azure tables that support Basic logs and DCR-based custom tables	DCR-based custom tables
Ingestion cost	Standard	Reduced	Minimal
Query price included	✓	✗	✗
Optimized query performance	✓	✓	✗ Slower queries. Good for auditing. Not optimized for real-time analysis.
Query capabilities	Full query capabilities.	Full Kusto Query Language (KQL) on a single table, which you can extend with data from an Analytics table using lookup.	Full KQL on a single table, which you can extend with data from an Analytics table using lookup.
Alerts	✓	✗	✗
Insights	✓	✗	✗
Dashboards	✓	✓ Cost per query for dashboard refreshes not included.1	Possible, but slow to refresh, cost per query for dashboard refreshes not included.1
Data export	✓	✓	✗
Microsoft Sentinel	✓	✓	✓
Search jobs	✓	✓	✓
Summary rules	✓	✓ KQL limited to a single table	✓ KQL limited to a single table
Restore	✓	✓	✗
Interactive retention	30 days (90 days for Microsoft Sentinel and Application Insights). Can be extended to up to two years.	30 days	30 days
Total retention	Up to 12 years	Up to 12 years	Up to 12 years

Uitgave

Versterken SOC Stelsel Rijk (VSSR)

Postbus 117, 2501 CC Den Haag

Turfmarkt 147, 2511 DP Den Haag

070 751 5555

Meer informatie

https://vssr.rijksapplicaties.nl/

vssr.info@minjenv.nl

Juli 2025