Dienstbeschrijving

Managed Security

Classificatie: Extern

avit

part of springboardnetwork

Building the foundation to empower your business

Dienstbeschrijving

Documentinformatie

Datum:	20-05-2025
Classificatie:	Extern
Auteur:	Service Owner
Eigenaar:	Service Owner
Eindverantwoordelijke:	Managing Director Services
Versie:	1.8

Status

☐ Concept

☒ Geaccepteerd

Inhoudsopgave

1. Introductie

1.1 Algemeen

Binnen onze dienstverlening zien we een toenemende trend richting ontzorging: van Support en Managed Support op basis van uw eigen infrastructuur naar Managed Services, volledig geleverd vanuit onze eigen faciliteiten en medewerkers. Wij kunnen ook optreden als service-integrator en fungeren als centraal aanspreekpunt voor andere leveranciers van producten en diensten die samen uw totale IT-landschap vormen. Hierdoor kunt u zich volledig richten op uw primaire bedrijfsactiviteiten.

Wij bieden ondersteuning van 'Enterprise-kwaliteit' en ondersteunen honderden klanten in Nederland en ver daarbuiten. U kunt rekenen op onze supportorganisatie met deskundige, gecertificeerde medewerkers die producten en diensten van een breed scala aan leveranciers ondersteunen. Wij realiseren projecten op basis van Cisco en Microsoft en leveren daarbij passende ondersteuning.

Onze diensten zijn onderverdeeld in de volgende categorieën:

- Enterprise Networking
- Collaboration
- Cyber Security
- Hybrid Cloud

Dit document beschrijft de dienst Avit Managed Security, onderdeel van "Cyber Security".

1.2 Kenmerken en Bouwstenen van de Managed Security-dienst

Het implementeren van oplossingen om de IT-omgeving veilig te maken, gebeurt bij vrijwel alle organisaties. Maar wat gebeurt er met de meldingen die voortkomen uit deze beveiligingsoplossingen? Hoe richt je deze oplossingen zo efficiënt mogelijk in? Wat zijn de best practices?

Bij de ontwikkeling van de Managed Security-dienst zijn we uitgegaan van de vraag hoe we u kunnen ondersteunen bij het beheren van beveiligingsoplossingen en het opvolgen van meldingen die daaruit voortkomen. Standaard bieden wij binnen Managed Security proactief beheer tijdens kantooruren en reactief beheer buiten kantooruren. Deze diensten kunnen worden uitgebreid met 24/7 SOC-monitoring, waarbij continu wordt gekeken naar beveiligingsmeldingen uit uw omgeving (inclusief correlatie tussen meldingen uit verschillende systemen), met een beoordeling van de ernst van de melding.

De Managed Security-dienst is opgebouwd uit specifieke producten en diensten die als bouwstenen naar wens en behoefte kunnen worden afgenomen. Momenteel zijn de volgende bouwstenen beschikbaar:

- Managed Umbrella
- SOC Monitoring
- Managed Secure Endpoint
- Managed Secure Email
- Managed XDR

Dit document beschrijft de algemene kenmerken van de dienst, inclusief de specifieke aanvullingen per bouwsteen. Voor elke bouwsteen is een paragraaf opgenomen in hoofdstuk 3 met de naam van de betreffende bouwsteen.

1.3 Verdere informatie over deze dienst

Voor meer informatie over deze dienst kunt u contact opnemen met een van onze Accountmanagers via telefoon of e-mail. Raadpleeg onze website voor de meest actuele contactgegevens.

2. Beschrijving Managed Security dienstverlening

2.1 Algemeen

Binnen Managed Security bestaan de diensten per bouwsteen uit de volgende standaardfunctionaliteiten:

- Monitoring en afhandeling van beveiligingsincidenten, inclusief advies;
- Volledig beheerde componenten, inclusief benodigde licenties. Als uw organisatie al over de benodigde licenties beschikt (bijvoorbeeld via een Enterprise Agreement), maakt deze dienst gebruik van de reeds beschikbare licenties (voor zover technisch mogelijk);
- Implementatie volgens het overeengekomen ontwerp;
- Ondersteuning in overeenstemming met de serviceniveaus zoals beschreven in de Avit Managed Services SLA, inclusief monitoring, beheer en onderhoud.

De specifieke functionaliteiten worden nader toegelicht in de paragrafen per bouwsteen in hoofdstuk 3 van dit document. Algemene aspecten van de standaardfunctionaliteiten worden beschreven in dit hoofdstuk (monitoring en beheer) en in hoofdstuk 4 (implementatie en ondersteuning).

Naast deze dienstbeschrijving is er een Service Level Agreement (SLA) voor Avit Managed Services en (optioneel) een Dossier van Afspraken en Procedures (DAP), waarin aanvullende afspraken over deze dienstbeschrijving en de genoemde SLA kunnen worden vastgelegd.

2.2 Standaard functionaliteiten

2.2.1 Monitoring en afhandeling van beveiligingsincidenten

Wij voeren tijdens kantooruren de volgende monitoringactiviteiten uit:

- We monitoren de gebeurtenissen (meldingen/waarschuwingen) van de producten, zowel op beveiligings- als systeemtechnisch niveau, en handelen deze af (zie event management). De te monitoren meldingen zijn product specifiek en worden daarom opgenomen in de product specifieke paragrafen in hoofdstuk 3;
- We monitoren de beschikbaarheid en prestaties van het product.

24x7 monitoring (ook wel ‘Security Operations Center Monitoring’ genoemd) is een geavanceerdere vorm van monitoring. Binnen de Managed Security-dienstverlening is dit een aparte bouwsteen die aanvullend wordt afgenomen op de andere beveiligingsdiensten.

Wanneer monitoring aangeeft dat actie vereist is, worden er ‘alerts’ gegenereerd op basis van ‘events’. Wij behandelen deze alerts als volgt:

- We beoordelen de alerts op prioriteit (gebaseerd op impact en urgentie);

- We volgen de alerts op door de directe oorzaak van het event te verhelpen;
- Als verdere opvolging buiten het product nodig is, sturen we een signaal (instructie) naar de verantwoordelijke contactpersoon voor het betreffende component of systeem. Dit kan een contactpersoon bij Avit zijn (als wij het component beheren), maar ook iemand binnen uw organisatie of een externe leverancier;
- Als tijdens de afhandeling blijkt hoe toekomstige meldingen voorkomen kunnen worden, adviseren wij de verantwoordelijke persoon over te nemen stappen.

2.2.2 Volledig beheerde componenten

Avit voert de volgende beheeractiviteiten uit (met uitzondering van SOC-monitoring, waarbij dagelijks beheer van de aangesloten componenten niet standaard inbegrepen is – dit kan via een aparte overeenkomst worden toegevoegd):

- We houden de betrokken componenten beschikbaar en veilig via proactieve acties (zoals periodieke health checks, optimalisaties, herstel bij dreigende uitval) en reactieve acties (zoals herstel bij storingen en andere geïdentificeerde problemen);
- We zorgen ervoor dat de componenten up-to-date blijven (patches en updates van de leverancier) zodat de beveiliging en stabiliteit van de dienst gewaarborgd blijven. De exacte invulling hiervan ligt bij Avit binnen de kaders van de SLA;
- Op verzoek voeren we standaardwijzigingen uit zoals gedefinieerd per bouwsteen;
- We beantwoorden vragen en behandelen incidenten als onderdeel van reguliere ondersteuning.

Wanneer we gebruikmaken van componenten van derden, worden de beheeractiviteiten uitgevoerd door deze partijen en fungeert Avit als Single Point of Contact (SPoC) voor uw organisatie. Als u zelf het beheer uitvoert, kunnen wij u hierin ondersteunen.

2.2.3 Release management

Nieuwe versies kunnen voortkomen uit wijzigingen van leveranciers of uit aanpassingen aan de dienst door Avit. In deze sectie beschrijven we de wijzigingen vanuit leveranciers. Voor wijzigingen aan de dienst zelf, zie paragraaf 3.3.2.
Wij behandelen alle vormen van nieuwe versies (patches, updates, upgrades) van producten die onderdeel zijn van de dienst als volgt:

- We passen product- en levenscyclusbeheer toe op alle producten en diensten, tenzij dit automatisch gebeurt door de leverancier of door uw organisatie zelf (in dat geval informeren wij u over noodzakelijke updates). Daarbij hanteren we de volgende richtlijnen:
- Functionele updates elk kwartaal;
    - Beveiligingsupdates op basis van CVSS-score:
    - Kritiek: binnen 24 uur;
    - Hoog: binnen één week;
    - Gemiddeld: binnen één maand;
    - Laag: opgenomen in de kwartaalupdate;

- Aanpassingen aan de dienst worden uitgevoerd na overleg met u binnen het afgesproken onderhoudsvenster. Uitzonderingen hierop zijn wijzigingen die geen onderbreking van de dienst veroorzaken – deze worden naar eigen inzicht van Avit of betrokken leveranciers uitgevoerd;
- Wijzigingen die invloed hebben op de (vaste of initiële) kosten worden altijd in overleg met u doorgevoerd.

2.3 Voorwaarden en beperkingen

2.3.1 Reikwijdte van de dienst

De dienst is beperkt tot de bouwstenen die zijn afgenomen, zoals beschreven in paragraaf 1.2 en de specifieke paragrafen per bouwsteen in hoofdstuk 3. Dit betekent dat de beschreven functionaliteiten niet automatisch beschikbaar zijn voor producten waarvoor de bijbehorende Managed Security-bouwsteen niet is afgenomen.

2.3.2 Toegang tot uw IT-omgeving

Avit beschikt over de benodigde toegang tot de componenten van de afgenomen bouwstenen op beheerniveau.

Onze engineers moeten te allen tijde toegang hebben tot de beheerde componenten. Dit geldt zowel voor fysieke toegang tot apparatuur op locatie als voor toegang tot de configuratie van apparatuur via een netwerkverbinding (zowel op locatie als op afstand) of via een beheer console.

In uitzonderlijke gevallen kan het nodig zijn om externe of lokale toegang te verlenen aan medewerkers van de leverancier (bijvoorbeeld Cisco Technical Assistance Center). Door het aangaan van een Managed Services-overeenkomst stemt u in met dergelijke toegang op afstand.

In sommige gevallen kunnen wij u vragen om assistentie op locatie te verlenen om problemen sneller op te lossen, bijvoorbeeld door een apparaat uit en weer aan te zetten.

3. Managed Security building blocks

Onze Managed Security-dienst is gericht op het ondersteunen van (vertegenwoordigers van) uw IT- en beveiligingsorganisatie (zoals uw Servicedesk), maar niet op het ondersteunen van eindgebruikers. De dienst wordt 24/7 geleverd in overeenstemming met de Managed Services SLA. Zie de paragraaf Ondersteuning verderop voor een korte toelichting.

Een belangrijk kenmerk van deze dienst is dat het gaat om Avit-diensten op uw eigen componenten en dat deze proactief van aard zijn. Dit betekent dat wij de afgesproken acties uitvoeren zonder dat u daar expliciet om hoeft te vragen (met uitzondering van acties die op verzoek plaatsvinden).

3.1 Managed Umbrella

Cisco Umbrella DNS Security beschermt uw organisatie door DNS-verzoeken binnen een Cisco-omgeving af te handelen. Hierbij wordt de geschiktheid van het DNS-verzoek beoordeeld (tegen klant gespecificeerde beleidsregels) voordat er een antwoord wordt gegeven. Avit controleert de logging van DNS-verzoeken (geweigerd en toegestaan) in Umbrella om problemen te identificeren die actie vereisen. Bijvoorbeeld: terugkerende communicatie met kwaadaardige servers, wat kan wijzen op een malware-infectie binnen uw netwerk.

Managed Umbrella SIG omvat alle diensten van Managed Umbrella DNS Security, met aanvullende functionaliteiten die horen bij SIG (Secure Internet Gateway). Deze omvatten onder andere een veilige webgateway, cloudgebaseerde firewall en cloud access security broker (zie onderstaande tabel).

	DNS Security Advantage	SIG Essentials
Security & control		
Secure web gateway		
Proxy and inspect web traffic (incl. decryption of SSL (HTTPS) traffic)	Partial	✓
Enable web filtering by domain or category (SIG filtering by URL)	✓	✓
Create custom block/allow lists of domains	✓	✓
Create custom block/allow lists of URLs		✓
Block files based on AV Engine and malware defense	Partial	✓
Use malware analytics (sandbox) on suspicious files		500/day
Cloud access security broker		
Cloud app discovery, risk scoring, blocking or activity controls	Partial	✓
Scan and remove malware from cloud-based file storage apps		Two apps
DNS-layer security		
Block domains with malware, phishing, botnet, or other high risk items	✓	✓
Cloud delivered firewall		
Create layer 3/layer 4 policies to block specific IPs, ports, and protocols		✓
Leverage layer 7 protection including an Intrusion Prevention System		Add-on
Multimode cloud data loss prevention		
Enable inline and out-of-band data inspection and blocking capabilities to protect sensitive data		Add-on
Remote browser isolation		
Provide safe access to risky sites, web apps and all web destinations		Add-on
XDR and threat intelligence		
Utilize XDR cross product security data and automated response actions	✓	✓
Access Umbrella's deep domain, IP, and ASN data for rapid investigations	✓	✓
Deployment & management		
Traffic forwarding		
Forward external DNS for on-network coverage and off-network devices	✓	✓
Cisco Secure Client to deploy Umbrella module to forward traffic	✓	✓
User attribution		
Create policies and view reports by network, device, and user	✓	✓
Create policies and view reports using SAML		✓
Management		
Customize block pages and bypass options	✓	✓
Use our multi-org console to centrally manage decentralized orgs	✓	✓
Umbrella API to create, read, update, and delete IDs child orgs	✓	✓
Reporting & logs		
Real-time activity search, plus Umbrella API to easily extract key events	✓	✓
Choose North America or Europe log storage	✓	✓
Use Cisco-managed S3 buckets or customer AWS S3 bucket	✓	✓

Wanneer we het hebben over zaken die gemeenschappelijk zijn voor zowel Umbrella DNS Security als Umbrella SIG, schrijven we 'Umbrella (SIG)'. Umbrella SIG specifieke toevoegingen worden in de tekst in deze paragraaf aangegeven als functionaliteit specifiek voor Umbrella SIG.

3.1.1 Wat doet Avit bij implementatie

We implementeren Umbrella (SIG) bij de klant volgens ons eigen High Level Design en documenteren dit in een klant specifiek Low Level Design.
Voor klanten met 'Managed Umbrella DNS Security' diensten implementeert Avit de 'Umbrella DNS Security Advantage' licentie. Voor klanten met 'Managed Umbrella SIG' diensten implementeert Avit de licentie 'Umbrella SIG Essentials'. Standaard wordt de MSLA licentievorm gebruikt voor de diensten.

Avit past deze licentie aan (binnen de bandbreedtes gegeven door de HLD en LLD):

- Voor Umbrella SIG de verbinding van het klantennetwerk naar de Umbrella SIG cloud omgeving;
- Het Cisco Secure Client installatiepakket voor gebruik op roaming apparaten;-De policies en block pages die de klant nodig heeft;
- Alle instellingen die binnen Umbrella nodig zijn om Umbrella (SIG) operationeel te krijgen voor de omgeving van de klant;
- De configuratiedocumentatie.

3.1.2 Wat doet Avit vanuit de dienst

- Avit controleert de logging dagelijks op het bestaan van elementen die zijn geclassificeerd als (mogelijk) kwaadaardig (malware, botnet en cryptomining weergegeven in de 'berichten' op het overzichtsscherm);
- Avit bepaalt de prioriteit van beveiligingswaarschuwingen en handelt deze af. Indien nodig onderneemt Avit (verdere) acties om de IT-beheerders van de omgeving op te volgen. Dit kan inhouden: beoordelen van de onwenselijkheid (vanuit klantperspectief, op basis van eigen risico's en beleidskeuzes), afstemmen met eindgebruikers over de oorzaak van bepaald DNS-verkeer (bewust gebruik/onbewust gebruik, begrijpen bedrijfsbehoefte, etc.) Avit kan desgewenst situationele ondersteuning bieden bij deze opvolging;
- Avit rapporteert maandelijks over de afgelopen maand (aantal geblokkeerde verzoeken, aantal security gerelateerde verzoeken, ontdekte apps, aantal actieve clients en netwerken) en geeft advies over mogelijke maatregelen/verbeterpunten (wanneer de rapportages daar volgens Avit aanleiding toe geven). Dit advies kan per e-mail worden gegeven, maar ook mondeling tijdens een gesprek met de klant om het rapport te bespreken en direct te vertalen naar keuzes (andere toe te voegen bouwstenen, eenmalige acties, etc.) of aanpassingen (in de vorm van standaard wijzigingen of niet-standaard wijzigingen);
- Avit levert reactieve ondersteuning (op vraag van de klant) bij het gebruik van Umbrella (SIG) aan de Service Desk en/of IT-beheerders van de klant (niet aan

eindgebruikers). Dit betreft bijvoorbeeld de functionele werking van de applicatie, het inzetten van Umbrella clients, vragen over policies (waarom iets wel of niet gebeurt op het gebied van DNS), het blokkeren van verzoeken, etc.;
- Avit werkt de productinstellingen bij om nieuwe functies op te nemen in nieuwe versies in lijn met de steeds evoluerende dienstverlening.

3.1.3 Welke standaardwijzigingen voert Avit uit op verzoek van de klant

Bij wijzigingen past Avit waar nodig de documentatie aan.

- Aanpassing van beleid met betrekking tot:
  - inhoud van applicatie (toestaan of blokkeren categorieën);
  - bestemmingslijsten (blokkeren/toestaan: specifieke sites blokkeren of toestaan);
  - pagina's blokkeren;
- Aanpassen van bestaande deployment-eigenschappen (d.w.z. niets maken dat betrekking heeft op deployment).

3.1.4 Wat doet de klant zelf

- Klanten kunnen zelf inloggen op het Umbrella Dashboard met leesrechten om een beeld te krijgen van actuele problemen binnen Umbrella;
- Klanten implementeren zelf de Cisco Secure Client applicatie op apparaten die Umbrella buiten het netwerk moeten gebruiken (zoals mobiele telefoons, laptops, etc.). Avit biedt reactieve ondersteuning (op vraag van de klant) wanneer dit buiten een Avit implementatieproject valt, maar neemt geen verantwoordelijkheid voor de implementatie zelf;
- Klanten beheren zelf de server van eventuele on-prem componenten. Standaard heeft Avit geen toegang tot on-prem servers, tenzij dit wordt geregeld vanuit andere beheeractiviteiten. Dit betekent ook dat klanten on-prem componenten zelf updaten. Avit biedt hierbij reactieve ondersteuning (op verzoek van de klant).

3.1.5 Belangrijk om te weten voor de klant

- Zonder de Cisco Secure client bepaalt het huidige netwerk van een systeem hoe het naar DNS routeert;
- Bij gebruik van Umbrella SIG is het uitgaande IP-adres afkomstig van de Umbrella-cloud;
- De Umbrella-service van Cisco wordt beschreven op https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_umbrella_offer_description.pdf;
- Cisco's gegevensverwerking van de Umbrella-service wordt beschreven op https://trustportal.cisco.com (zoek op 'Umbrella').
- Naast Managed Umbrella zijn er meer maatregelen nodig om uw IT-omgeving op een verstandige manier te beveiligen, zowel technisch als organisatorisch. Avit kan klanten ondersteunen met advies, maar de klanten blijven zelf

verantwoordelijk voor het nemen van de benodigde maatregelen in hun eigen IT-omgeving.

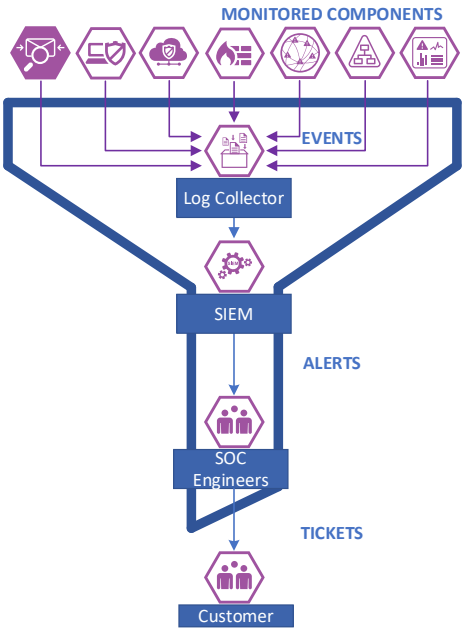
3.2 SOC Monitoring

SOC Monitoring is een dienst waarbij ons Security Operations Center (SOC) uw IT-omgeving 24/7 bewaakt op beveiligingsincidenten. Dit omvat het analyseren van meldingen, het bepalen van de ernst en prioriteit, en het doorgeven van waarschuwingen inclusief advies aan de verantwoordelijke beheerder. Als Avit verantwoordelijk is voor het beheer van de betreffende component, handelen wij het incident direct af in overeenstemming met de beheerovereenkomst. Buiten kantooruren kunnen afwijkende procedures gelden.

3.2.1 Wat doet Avit bij implementatie?

- Adviseren en ondersteunen bij het bepalen van de te monitoren apparaten.
- Verzamelen van informatie over rollen, medewerkers en afdelingen binnen uw organisatie die relevant zijn voor monitoring.
- Implementatie van logcollectoren die beveiligingslogboeken doorsturen naar de centrale SOC-dienst.
- Configuratie van te monitoren componenten zodat deze correct zijn aangesloten op de logcollectoren.
- Samen met de klant vaststellen van de “baseline” van de omgeving: wat is normaal gedrag en wat zijn de bijbehorende risico’s?
- Indien toegang niet mogelijk is, ondersteunen wij u bij de benodigde handelingen.

3.2.2 Wat doet Avit als doorlopende dienst?



- Verwerken van loggegevens in een SIEM (Security Information and Event Management) systeem.
- Real-time correlatie van gebeurtenissen op basis van meer dan 200 use cases, ondersteund door Cyber Threat Intelligence (CTI)-feeds.
- Beoordeling van meldingen op impact en urgentie, 24/7.
- Indien een melding leidt tot een incident (ticket), wordt een contextuele analyse uitgevoerd door een SOC-engineer, inclusief advies voor opvolging.
- Actieve “threat hunting” om dreigingen op te sporen die niet automatisch worden gedetecteerd.
- 24/7 informeren van de verantwoordelijke beheerder of afdeling over incidenten, inclusief advies voor mitigatie en preventie.

- Directe opvolging van incidenten als Avit ook de betreffende component beheert.
- Regelmatige evaluatie van de dienst en advies over optimalisatie van beveiligingsmaatregelen.
- Beheer van logcollectoren (zonder toegang tot de hypervisor), inclusief updates en prestatiecontroles.
- Doorlopende optimalisatie van de dienst via 'baselining' en 'tuning' van use cases.

3.2.3 Standaardwijzigingen door Avit op verzoek van de klant.

- Aanpassen van documentatie indien nodig.
- Toevoegen van extra componenten aan de monitoring (let op: dit kan extra kosten met zich meebrengen als het buiten het afgesproken aantal Events Per Second valt).

3.2.4 Wat doet de klant zelf?

Tijdens implementatie:

- Aanleveren van benodigde informatie.
- Installeren van componenten of Avit toegang geven om dit te doen.

Tijdens dienstverlening:

- Up-to-date houden van contactgegevens en relevante informatie.
- Zorgen dat apparaten blijven loggegevens aanleveren aan de SOC (voor componenten die niet door Avit worden beheerd).
- Indien van toepassing: beheer van logcollectoren op VM-niveau.
- Avit kan ondersteuning bieden bij bovenstaande verantwoordelijkheden, mits overeengekomen in een apart projectvoorstel.

3.2.5 Belangrijke aandachtspunten voor de klant

- Avit werkt samen met de gespecialiseerde SOC-partner SecurView. Alle data worden opgeslagen in Nederland. Medewerkers van SecurView hebben alleen op afstand (buiten Europa) toegang tot de gegevens.
- De dienst is gebaseerd op het aantal geanalyseerde logs (Events Per Second). Dit aantal wordt elke zes maanden geëvalueerd en kan leiden tot aanpassing van de tarieven.
- Avit voert geen mitigaties of responsacties uit op componenten die niet onder ons beheer vallen. Hiervoor is een beheerpartij of interne beheerder noodzakelijk.
- De effectiviteit van SOC Monitoring is sterk afhankelijk van de volledigheid en actualiteit van de aangeleverde informatie.
- Klanten krijgen leesrechten in het SOC-portaal om incidenten en rapportages zelf in te zien.
- Dagelijks beheer van de aangesloten componenten valt niet standaard onder deze dienst, maar kan apart worden overeengekomen.

3.3 Managed Secure Endpoint

Cisco Secure Endpoint beschermt uw organisatie door eindpunten (zoals laptops, desktops en mobiele apparaten) te beveiligen. Deze oplossing combineert preventie, detectie, threat hunting en respons in één platform, ondersteund door cloudgebaseerde analyses. Secure Endpoint is beschikbaar voor Windows, macOS, Linux, Android en iOS.

Avit levert deze dienst als een beheerde cloudoplossing, waarbij meldingen uit Secure Endpoint worden beoordeeld op ernst en prioriteit. Vervolgens worden deze meldingen afgehandeld of doorgestuurd naar de juiste personen of afdelingen. Indien nodig biedt Avit ondersteuning bij verdere opvolging, ook wanneer het gaat om componenten die niet door Avit worden beheerd.

3.3.1 Wat doet Avit bij implementatie?

- Implementatie van Secure Endpoint volgens onze best practices.
- Documentatie van de implementatie in een klant-specifiek Low-Level Design (LLD), inclusief alle afwijkingen en aanvullingen.
- Levering en/of gebruik van Cisco Secure Endpoint-licenties. Indien u al over een geldige licentie beschikt, wordt deze gebruikt.

3.3.2 Wat doet Avit als doorlopende dienst?

- Realtime monitoring van meldingen die als (mogelijk) kwaadaardig zijn geclassificeerd, met gebruik van de ingebouwde prioriteringsfunctionaliteit van Secure Endpoint.
- Prioritering en opvolging van beveiligingsmeldingen. Indien nodig:
- Verdere analyse van gebeurtenissen of software op specifieke eindpunten.
- Advies over herstelmaatregelen (zoals terugzetten van back-ups of herontwerp).
- Implementatie van mitigerende maatregelen in andere componenten.
- Maandelijkse rapportage met onder andere:
    - Status van connectoren op eindpunten
    - Gedetecteerde malware en verdachte activiteiten
    - Kwaadaardige netwerkverbindingen
    - Oorzaken van infecties
    - Resultaten van automatische bestandsanalyses
    - Geconstateerde kwetsbaarheden in software
- Bespreking van het rapport met de klant, inclusief advies over mogelijke acties of aanpassingen.
- Proactieve en reactieve ondersteuning aan de servicedesk of IT-beheerders van de klant (niet aan eindgebruikers).
- Periodieke updates van productinstellingen om nieuwe functionaliteiten te activeren.
- Elk kwartaal wordt de nieuwste geteste versie van de Secure Endpoint-client uitgerold naar alle actieve eindpunten.

3.3.3 Standaardwijzigingen door Avit op verzoek van de klant

- Aanpassingen in beleidsregels
- Beheer van groepen
- Wijzigingen in blokkeer-/toestaan-lijsten
- Updates van uitzonderingslijsten

3.3.4 Wat doet de klant zelf?

- Inloggen met leesrechten op het Secure Endpoint-dashboard om inzicht te krijgen in de actuele situatie.
- Zelf verantwoordelijk voor de distributie van de clientsoftware naar eindpunten.
- Avit biedt reactieve ondersteuning op verzoek.
- Tijdens het initiële implementatieproject kan Avit de uitrol uitvoeren, maar dit valt niet onder de standaard doorlopende dienstverlening.

3.3.5 Belangrijke aandachtspunten voor de klant

- In geval van een aanval of besmetting kan een incident response-traject nodig zijn (zoals schoonmaak en herstel van getroffen systemen). Dit valt niet onder de standaarddienst, maar kan op basis van het overeengekomen uurtarief worden geleverd.
- De Cisco Secure Endpoint-dienst (ook wel "AMP for Endpoints" genoemd) is gedocumenteerd op: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/amp-threatgrid-clarity-offer-description.pdf.
- Informatie over gegevensverwerking door Cisco is beschikbaar via: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet (zoek naar 'AMP')
- Er wordt een verwerkersovereenkomst gesloten tussen Avit en de klant voor de opslag en verwerking van gebruikersgegevens in het kader van deze dienst.

3.4 Managed Secure Email

Cisco Secure Email beschermt uw organisatie door e-mailverkeer te beveiligen tegen spam, malware, virussen en impersonatiepogingen. De oplossing combineert meerdere beveiligingslagen voor zowel inkomende als uitgaande e-mail. Secure Email is beschikbaar als volledige cloudoplossing, hardware appliance, virtuele appliance of hybride model. Avit levert deze dienst uitsluitend op basis van de cloudversie van Cisco Secure Email Essentials, eventueel aangevuld met Cisco Secure Email Threat Defense bij gebruik van Exchange Online.

Avit voegt aan deze dienst een veilige basisconfiguratie toe, evenals periodieke beoordeling van loggegevens en advisering op basis van trends en risico's.

3.4.1 Wat doet Avit bij implementatie?

- Implementatie van Secure Email volgens onze best practices.
- Advies over DNS-configuratie.
- Documentatie van de implementatie in een klant-specifiek Low-Level Design.
- Gebruik van geavanceerde configuratieopties afgestemd op uw behoeften.
- Gebruik van klantlicenties indien beschikbaar. Indien niet, levert onze organisatie de benodigde Cisco Secure Email XaaS Subscription-licentie.

3.4.2 Wat doet Avit als doorlopende dienst?

- Waarschuwing bij detectie van uitgaande malware (indicatie van besmetting binnen uw netwerk).
- Maandelijkse beoordeling van loggegevens en advisering over:
    - Veranderingen in e-mailverkeer (volume, TLS-status, geografische spreiding)
    - Status van SPF, DKIM en DMARC op ontvangen e-mails
    - Pogingen tot impersonatie
    - Malware-incidenten
    - Preventie van CEO-fraude
- Advies wordt bij voorkeur mondeling besproken, zodat dit direct kan worden vertaald naar acties of wijzigingen.
- Monitoring van beschikbaarheid van de Cloud service, inclusief meldingen bij onderhoud of storingen.
- Proactieve en reactieve ondersteuning aan de servicedesk of IT-beheerders van de klant (niet aan eindgebruikers).
- Doorvoeren van updates om nieuwe functionaliteiten beschikbaar te maken voor bestaande klanten.

3.4.3 Standaardwijzigingen door Avit op verzoek van de klant

- Aanpassen van documentatie indien nodig.

- Beheer van blokkeer-/toestaanlijsten (e-mailadressen of servers die altijd moeten worden toegelaten).
- Kleinschalige configuratiewijzigingen op basis van fair use, zoals:
    - Toevoegen of verwijderen van domeinen
    - Monitoring van specifieke kenmerken of inhoud (bijvoorbeeld via reguliere expressies)

3.4.4 Wat doet de klant zelf?

- Beheer van vereiste DNS-records.
- Configuratie van eigen mailservers (zoals Microsoft Exchange of Exchange Online).
- Aanleveren van organisatie-specifieke informatie (zoals namen van directieleden voor detectie van CEO-fraude).

3.4.5 Belangrijke aandachtspunten voor de klant

Deze dienst richt zich uitsluitend op de beveiliging van e-mailverkeer van en naar uw organisatie. Het beheer van de e-mailomgeving zelf valt buiten de scope.

Voor deze dienst kan toestemming van de ondernemingsraad vereist zijn, aangezien monitoring van e-mailverkeer als personeelsvolgsysteem kan worden gezien. Wij adviseren om hier transparant en proactief over te communiceren.

Meer informatie over Cisco Secure Email:

- Secure Email service: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/ces-cres-dmp-app-od.pdf
- Data processing van Secure Email service https://trustportal.cisco.com/c/r/ctp/trust-portal.html (zoek naar ‘Secure Email’).

3.5 Managed XDR

Cisco XDR (Extended Detection and Response) verandert de manier waarop beveiligingsteams dreigingen detecteren en erop reageren. Deze cloudgebaseerde oplossing is ontworpen om beveiligingsoperaties te vereenvoudigen en teams in staat te stellen om snel en effectief te reageren op geavanceerde dreigingen. Cisco XDR integreert met het bredere Cisco-beveiligingsportfolio en met geselecteerde oplossingen van derden, en biedt daarmee een van de meest complete en flexibele detectie- en responsplatforms op de markt. Avit maakt gebruik van het Cisco XDR-platform en voegt daar 24/7 detectie- en responsdiensten aan toe. Beveiligingsgebeurtenissen worden beoordeeld op ernst en prioriteit en vervolgens afgehandeld of doorgestuurd naar de juiste personen of afdelingen. Waar nodig biedt Avit ondersteuning bij verdere opvolging, mits toegang tot de betreffende componenten beschikbaar is.

3.5.1 Wat doet Avit bij implementatie?

- Implementatie van Cisco XDR volgens onze best practices.
- Documentatie van de implementatie in een klant-specifiek Low-Level Design (LLD), inclusief afwijkingen en aanvullingen.
- Bepalen van de databronnen die geïntegreerd worden in XDR.
- Ondersteuning bij de configuratie van deze bronnen.
- Levering van Cisco XDR-licenties, of gebruik van bestaande geldige klantlicenties.

3.5.2 Wat doet Avit als doorlopende dienst?

- Realtime monitoring van (mogelijk) kwaadaardige gebeurtenissen met behulp van de ingebouwde prioriteringsfunctionaliteit van XDR.
- Afhandeling van beveiligingsmeldingen, inclusief containmentmaatregelen.
- Indien nodig: verdere analyse van gebeurtenissen, software of instellingen op specifieke componenten, en advies over herstelmaatregelen.
- Actieve threat hunting bij opkomende dreigingen.
- Maandelijkse rapportage met onder andere:
    - Gezondheidsstatus van de omgeving
    - Incidenten per MITRE ATT&CK-tactieken en -technieken
    - Detectiebronnen
    - Rapportages over assets en gebruikers
    - Status van de uitrol
- Bespreking van het rapport met de klant, inclusief vertaling naar mogelijke acties of wijzigingen.
- Proactieve en reactieve ondersteuning aan de servicedesk of IT-beheerders van de klant (niet aan eindgebruikers).
- Updates van productinstellingen om nieuwe functionaliteiten beschikbaar te maken.
- Elk kwartaal wordt de nieuwste geteste versie van de XDR-client uitgerold naar alle actieve eindpunten.

3.5.3 Standaardwijzigingen door Avit op verzoek van de klant

- Aanpassen van documentatie indien nodig.
- Ondersteuning bij het toevoegen of verwijderen van databronnen.
- Wijzigen van assetwaarderingen.
- Bijwerken van clientinstellingen.

3.5.4 Wat doet de klant zelf?

- Inloggen met leesrechten op het XDR-dashboard voor inzicht in de actuele situatie.
- Verantwoordelijk voor distributie van de clientsoftware.
- Avit biedt reactieve ondersteuning op verzoek.
- Tijdens het initiële project kan Avit de uitrol uitvoeren, maar dit valt niet onder de standaard doorlopende dienst.
- Verantwoordelijk voor de uitrol van on-premise sensoren voor het verzamelen van flowdata.
- Verantwoordelijk voor correcte configuratie van databronnen die XDR van input voorzien.

3.5.5 Belangrijke aandachtspunten voor de klant

- In geval van een aanval of besmetting kan incident response nodig zijn (zoals schoonmaak en herstel van systemen). Dit valt niet onder de standaarddienst, maar kan op basis van het overeengekomen uurtarief worden geleverd.
- Meer informatie over Cisco XDR: https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/XDR-Product_Description.pdf.
- Informatie over gegevensverwerking door Cisco: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?search_keyword=xdr (zoek naar "XDR")
- Er wordt een verwerkersovereenkomst gesloten tussen Avit en de klant voor de verwerking van gebruikersgegevens in het kader van deze dienst.
- De volgende tabel wordt gebruikt om de vertaalslag te maken tussen de Cisco XDR Priority score en de Avit Incident Priority zoals gebruikt in onze SLA.

Kleur	Prioriteit Score	Gevoeligheid	SLA Prioriteit
(rood)	800 en hoger	Kritiek	1
(oranje)	600 - 799	Hoog	2
(geel)	400 - 599	Medium	3
(blauw)	399 en lager	Laag	4
(grijs)	—	Onbekend	--

4. Aanvullende Managed Services informatie

4.1 Aanvragen van de dienst

De Managed Security-dienst kan worden aangevraagd via een van onze Accountmanagers. Neem contact met ons op via telefoon of e-mail. De actuele contactgegevens vindt u op onze website.

4.2 Implementatie

De implementatie van de dienst verloopt in vier fasen:

1. Planning en coördinatie
   Een Projectmanager van Avit begeleidt de implementatie. Deze stelt de planning op, coördineert de uitvoering en bewaakt de voortgang en communicatie. Ook stemt de Projectmanager de activiteiten af tussen u en eventuele leveranciers. Uw betrokkenheid is hierbij essentieel.

2. Implementatie
   - Inventarisatie van de scope van de dienstverlening.
   - Opstellen van een functioneel ontwerp als basis voor de implementatie.
   - Uitwerken van ontwerpdocumenten per bouwsteen.

   Activiteiten omvatten o.a.:
   - Vaststellen van de bestaande infrastructuur
   - Registreren van contactgegevens
   - Inrichten van remote toegang
   - Configureren van benodigde servers en klantportaal

   Uw verantwoordelijkheden tijdens deze fase:
   - Ondersteuning bieden bij het opstellen en uitvoeren van het projectplan.
   - Configureren van eigen componenten (zoals routers, switches, firewalls) volgens het afgesproken IP-plan.
   - Beschikbaar stellen van medewerkers en middelen voor testen en acceptatie.
3. Transitie
   Bij bestaande implementaties voert Avit een technische controle uit op de randvoorwaarden en past deze aan naar het standaardontwerp van de dienst.

4. Instructie
   Na oplevering ontvangt u:
   - Toegang tot documentatie en portalen
   - Uitleg over supportprocessen

- Contactgegevens

Eventuele afwijkende afspraken worden vastgelegd in het Dossier van Afspraken en Procedures (DAP)

4.3 Ondersteuning

4.3.1 Algemeen

De Managed Security-diensten zijn proactief en gericht op het monitoren van uw omgeving. De “Managed Security SLA” is van toepassing.

Voor sommige bouwstenen is aanvullende NOC-dienstverlening vereist, zoals bij Managed Secure Firewall. Deze wordt alleen geleverd in combinatie met onze Service Continuity-dienst.

Voor een volledige beschrijving van onze dienstverlening verwijzen wij naar het document Avit Managed Services SLA.

4.3.2 Change Management

Elke bouwsteen kent een set standaardwijzigingen die binnen de dienst vallen.
Wijzigingen met contractuele impact verlopen via uw Accountmanager.
Andere wijzigingen worden beoordeeld door onze Change Advisory Board (CAB).
De CAB bepaalt of een wijziging standaard wordt of wordt afgewezen op basis van beheersbaarheid en risico’s.

4.3.3 Rapportage

Naast standaardrapportages over Service Desk KPI’s ontvangt u maandelijks een inhoudelijk rapport met aanbevelingen.
Afhankelijk van de bouwstenen is er ruimte voor maandelijkse inhoudelijke overleggen.

4.3.4 Privacy en logging

Beveiligingsdiensten gaan gepaard met logging, wat gevolgen kan hebben voor de privacy van medewerkers, klanten of andere betrokkenen. Daarom sluit Avit een verwerkersovereenkomst met u af waarin dit goed wordt geregeld.

In sommige gevallen is ook een verwerkersovereenkomst tussen u en de leverancier nodig, afhankelijk van de gebruikte bouwstenen.

Aanbeveling: Informeer uw medewerkers en andere betrokkenen proactief over de logging, zodat u transparant bent en vragen kunt beantwoorden.

Avit gebruikt klantgegevens uitsluitend voor het leveren en verbeteren van de dienst. Derden krijgen alleen toegang als zij betrokken zijn bij de dienstverlening, en u wordt hierover vooraf geïnformeerd.

Informatie over gegevensverwerking door fabrikanten:

- Cisco: https://trustportal.cisco.com/c/r/ctp/trust-portal.html?doctype=Privacy%20Data%20Sheet
- Microsoft: https://www.microsoft.com/en-us/trust-center/product-overview

4.4 Kostenverrekening

De kosten van de dienst worden per bouwsteen bepaald en bestaan uit:

- Eenmalige kosten: voor implementatie, hardware, licenties, etc.
- Maandelijkse kosten: voor licenties, operationele kosten van Avit en leveranciers.
- Overige kosten: zoals niet-standaard wijzigingen, op basis van nacalculatie tegen het afgesproken tarief.

4.5 Contractuele aspecten

De startdatum, looptijd en verlengingsperiode worden in overleg vastgesteld en opgenomen in uw Managed Security Service Agreement.

Wijzigingen in het contract worden altijd afgestemd met uw Accountmanager.

4.6 Certificeringen van Avit

Avit beschikt over de volgende internationaal erkende certificeringen:

- ISO 9001 (kwaliteit)
- ISO 14001 (milieu)
- ISO 27001 (informatiebeveiliging)
- ISAE 3402 Type II

Meer informatie: www.avitgroup.com/we-are-avit/#certificates