avensus

Whitepaper

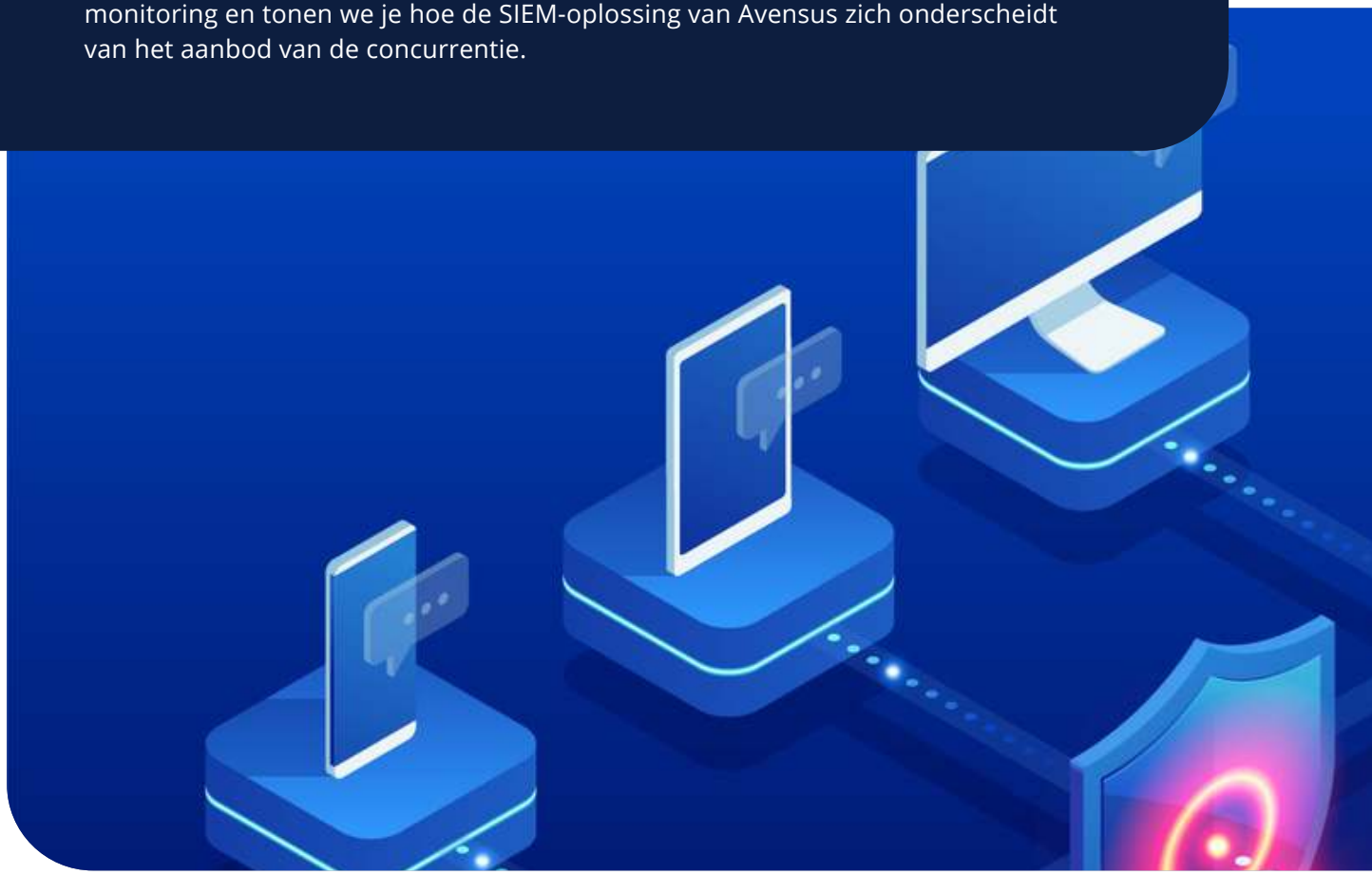
Cyberaanvallen, datadiefstal en datalekken voorkomen? Gebruik security monitoring

Inleiding

Cyberaanvallen die je hele IT-netwerk platleggen? Ransomware die alle apparaten en bestanden gijzelt? Of datalekken die ervoor zorgen dat persoonsgegevens en andere privacygevoelige informatie op straat komen te liggen? Dergelijke incidenten zijn een nachtmerrie voor elke organisatie en zadelen je op met technische problemen, torenhoge AP-boetes of een berg reputatieschade. Bedreigingen en risico's blijven bovendien evolueren en worden ook steeds geavanceerder.

Individuele beveiligingsoplossingen zijn vaak gericht op 1 aspect van beveiliging, werken dus in silo's en schieten daarom vaak tekort bij het detecteren en verhelpen van de bovengenoemde problemen. Kwalitatief hoogwaardige security monitoring, ook vaak Security Information Event Management (SIEM) genoemd is dan de oplossing. Deze oplossing gaat uit van een optimale samenwerking tussen techniek, mensen en processen.

In deze whitepaper gaan we in op de belangrijkste voordelen van security monitoring en tonen we je hoe de SIEM-oplossing van Avensus zich onderscheidt van het aanbod van de concurrentie.



Waarom security zo'n hot topic is

Het is niet zo vreemd dat IT-veiligheid en security monitoring hot topics zijn. Naarmate de samenleving meer en meer digitaliseert, wijken ook criminelen, oplichters en cyberterroristen steeds vaker uit naar de digitale snelweg. IT wordt dankzij technologieën als AI, Internet of Things (IoT) en cloud computing steeds complexer, terwijl cybercriminelen tegelijkertijd ook diezelfde technieken gebruiken en dus ook steeds slimmer en creatiever worden. Bovendien werken zij vaak heel goed samen (Darknet); iets wat de beveiligingsindustrie nog niet genoeg doet.

De gevolgen hiervan lezen we met enige regelmaat terug in de krant: gebruikersnamen en wachtwoorden die uitlekken en gijzelsoftware of (D) DoS-aanvallen die complete IT-netwerken platleggen.

Daarnaast zijn er nog andere veiligheidsissues die in de praktijk vaak terugkomen, een aantal voorbeelden

- Je ziet dat een vertrokken medewerker nog steeds actief is op het netwerk, terwijl je toch zeker denkt te weten dat zijn gebruikersaccount is opgeheven.
- Je ziet dat een medewerker met bepaalde rechten een database benadert die hij normaal niet gebruikt. Dit kan duiden op kwade bedoelingen, maar ook een geval zijn van aangepaste verantwoordelijkheden.
- Je ziet een medewerker die actief is in een bepaald land plots activiteiten ontplooien vanuit een ander land. Dit kan erop duiden dat zijn account wordt misbruikt.
- Een gebruiker klikt op een link die hem omleidt naar een kwaadaardige website. In deze website is een nieuwe, malicieuze code ingebouwd die een backdoor installeert op de pc van deze gebruiker. De computer realiseert vervolgens een IRC-verbinding en verbergt zo de verbinding voor de bestaande beveiligingsoplossingen. Zodra er verbinding is gemaakt met de IRC-server, wacht deze op een opdracht om bepaalde subnetten te scannen op open mailservers en de resultaten te uploaden naar een chatroom. Zodra de resultaten zijn geretourneerd, stuurt de aanvaller een commando naar de besmette pc om mail te sturen naar hosts met open poorten.

"criminelen, oplichters en cyberterroristen wijken steeds vaker af naar de digitale snelweg"

De waarde en voordelen van security monitoring

Goede security monitoring is een beproefd medicijn tegen de bovengenoemde kwalen en geeft je inzicht in jouw systemen, applicaties en programma's. **Het resultaat: meer informatie over de status van je digitale veiligheid en meer mogelijkheden om jouw ICT-beveiliging op tijd te optimaliseren.**

Security monitoring levert de organisatie veel voordelen op:

- Veel aanbieders van security monitoring werken met een toegewijd Security Operation Center (SOC). Dit is een speciale afdeling of gespecialiseerd team dat veiligheidsdiensten als pentests, phishing campaigns en SIEM-diensten aanbiedt. De SOC-specialisten staan doorlopend in verbinding met de netwerken, systemen, applicaties en data van opdrachtgevers. Vitale onderdelen worden zo 24/7 bewaakt door erkende experts.
- Security monitoring analyseert al jouw intern en extern dataverkeer. Hierdoor signaleer je snel bedreigingen en verdachte activiteiten binnen het netwerk.
- Logboekregistraties van ongewenste gebeurtenissen staan garant voor digitaal sporenonderzoek en geven je de mogelijkheid om bedreigingen en verdachte gebeurtenissen op een tijdlijn te plaatsen.
- Je kunt security monitoring in de vorm gieten van op maat gebouwde oplossingen die helemaal zijn toegespitst op jouw IT-omgeving.

Security monitoring van Avensus

Avensus Managed SIEM omvat veel informatiebronnen en gaat daardoor net wat verder dan andere security-oplossingen. Maar wat maakt de security monitoring van Avensus zo anders dan de overige opties die beschikbaar zijn?

Verdachte netwerkactiviteit rapporteren in realtime

Het monitoren van gebruikersactiviteiten binnen je netwerk is een belangrijk aandachtspunt voor elke business- en IT-manager. Om verdachte gebruikersactiviteiten tijdig op te merken, heb je in het huidige IT-landschap een SIEM-oplossing nodig die mogelijk risicovolle gebruikersactiviteiten snel detecteert. Met Avensus Managed SIEM maak je security-incidenten inzichtelijk, in realtime of via periodieke rapporten.

'Zero-day threats' opsporen die anderen missen

Avensus Managed SIEM gebruikt flowgegevens van het netwerk om nieuwe bedreigingen te detecteren zonder daarbij gebruik te maken van 'vulnerability signatures'. Zo spoor je ook bedreigingen op die gemist zijn door antivirussoftware en andere traditionele beveiligingssystemen. Denk bijvoorbeeld aan het ontdekken van een nieuwe service zoals een mailserver in de DMZ of een FTP-service die ineens actief wordt op een bestaande server.

Interne botnet activiteiten detecteren

Nieuwe regels op het gebied van compliancy stellen steeds hogere eisen aan het interne security beleid van organisaties. Avensus zet hier net een stapje extra in. Onze Managed SIEM oplossing maakt het mogelijk om applicaties te detecteren en gebruikers te identificeren die inloggen op kritische servers met clear text-wachtwoorden. Daarnaast zorgen we ervoor dat versleutelde protocollen goed worden ingezet in specifieke segmenten van het netwerk.

Een veelvoorkomend probleem in klantomgevingen is bijvoorbeeld de aanwezigheid van botnet-communicatiekanalen (IRC-verkeer). Door de inspectie van de inhoud op (meta)applicatieniveau, kunnen IRC-kanalen en IRC-communicatie niet alleen worden gedetecteerd en gesignaleerd, maar ook worden vastgelegd voor forensisch bewijs.

Kwaadaardige websites registreren

Het is een veelvoorkomend probleem: medewerkers die nietsvermoedend op een link klikken die hen doorstuurt naar een kwaadaardige website. Reguliere firewalls en antivirus programma's zijn niet altijd goed in het effectief detecteren van dit soort bedreigingen. Avensus Managed SIEM biedt de totale zichtbaarheid die nodig is om dit te ontdekken en samen te voegen tot een duidelijk zicht- en analyseerbaar veiligheidsincident.

Veiligheidsrisico's beter beoordelen met asset profiles

Veel netwerktoepassingen (denk aan applicaties en host-tabellen) hebben een dynamisch karakter. Dit maakt het adequaat beheren van veiligheidsrisico's tot een uitdagende klus die de mogelijkheden van veel beveiligingsoplossingen te boven gaat. Security Management van Avensus maakt het gemakkelijker om gebeurtenissen op het gebied van veiligheid te beoordelen en prioriteren.

Betere bescherming tegen DoS-aanvallen

(D)DoS-aanvallen komen steeds vaker voor en zijn een ware plaag voor menig bedrijf. Hoewel (D)DoS aanvallen doorgaans wel worden geregistreerd, rapporteren veel beveiligingsinstallaties over een stroom van gebeurtenissen verspreid over meerdere doelen en diverse netwerkapparaten.

Avensus Managed SIEM geeft meer inzicht in de (D)DoS-aanval en komt daarom sneller tot een herstel van dergelijke aanvallen.

Detecteer illegale diensten, servers of verkeer

Nieuwe netwerkservices kunnen wijzen op onlangs geïnstalleerde backdoors of per ongeluk geïnstalleerde services die hackers kunnen gebruiken voor het uitvoeren van aanvallen. Hoewel deze gebeurtenissen niet per definitie een bewijs vormen voor illegale activiteiten, kan het detecteren en verwijderen van apparaten als draadloze toegangspunten of niet-standaard werkplekken helpen bij het voorkomen van toekomstige aanvallen.

Met Avensus Managed SIEM kun je de aanwezigheid van een nieuwe service opsporen in bijvoorbeeld een DMZ. Deze functie is gemakkelijk aan te passen, waarna je kunt kijken naar veranderingen in andere netwerksegmenten of specifieke hosts.

Over Avensus

Omgaan met moderne informatietechnologie draait om het bewaren van een delicate balans. Aan de ene kant wil je slimmer en efficiënter worden door gebruik te maken van de vele extra mogelijkheden die gesofisticeerde IT-oplossingen je brengen. Anderzijds nemen de complexiteit, risico's en reguleringen in IT-land continu toe.

Avensus beschikt over de kennis op het gebied van cloud computing en security die nodig is om de ideale balans tussen functionaliteit en veiligheid te vinden. Wij zijn volledig gecertificeerd en actief in een divers spectrum aan verschillende branches, waardoor we maatwerk voor jouw organisatie kunnen leveren.

Benieuwd naar wat wij voor jouw organisatie kunnen betekenen? Neem gerust vrijblijvend contact met ons op voor een goed gesprek of gedegen advies. Bel ons direct op 036-5393100 of stuur een e-mail naar info@avensus.nl.