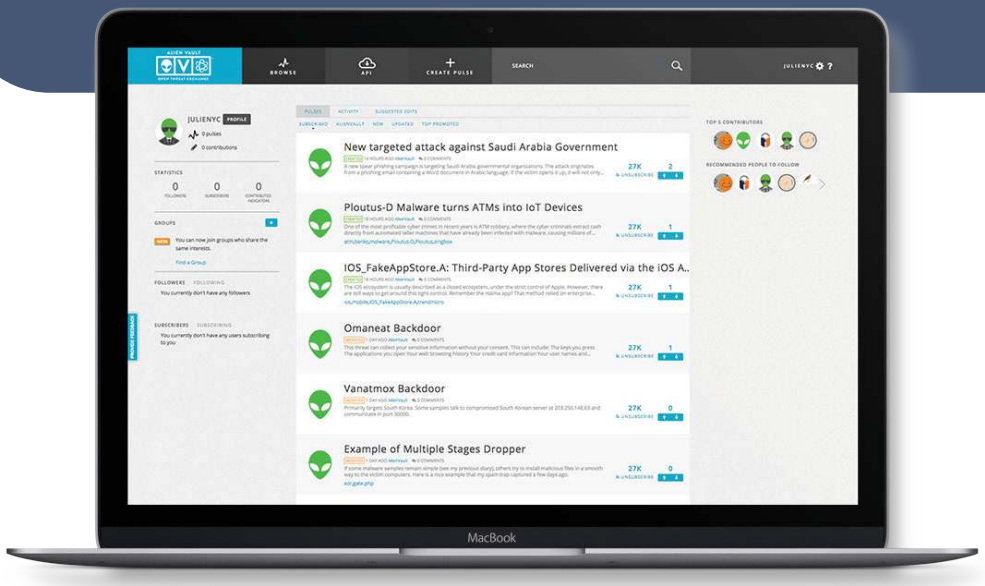
avensus

Managed SIEM
Use Cases

Inhoud



INLEIDING

Een belangrijke uitdaging voor veel organisaties, van welke omvang ook, is hoe nuttige informatie te halen uit de vloed van netwerk en security events die dagelijks worden gegenereerd. Bedreigingen en risico's blijven evolueren en worden meer en meer geavanceerd. Nieuwe bedreigingen van vandaag proberen vertrouwelijke gegevens te verkrijgen voor illegale financiële doeleinden en om bedrijfs-IT-middelen te misbruiken voor illegale doeleinden.

Zelfs wanneer bedreigingen worden gedetecteerd door bestaande beveiligingsoplossingen kunnen deze vaak niet worden gedetecteerd door de bestaande event monitoring oplossingen, omdat deze events (de indicatoren voor een bedreiging) niet goed zijn gecorreleerd of geprioriteerd. Organisaties beginnen zich te realiseren dat ze gecentraliseerde "command & control" nodig hebben die effectiever de bestaande en nieuwe bedreigingen op hun netwerk kan managen. Dit kan worden geleverd door een geïntegreerde Security Intelligence oplossing van **Avensus Managed SIEM** gebaseerd op de **AlienVault SIEM oplossing van AT&T Cybersecurity**.

Avensus is MSSP partner van AT&T Cybersecurity en gebruikt de AlienVault SIEM oplossingen als basis van haar SOC diensten. AlienVault USM is onderscheidend in de mate van integratie van Network Intrusion Detection, Vulnerability Management, Endpoint Detection, Asset discovery en Security Information Event Management (SIEM).

Dit document beschrijft een aantal real-life situaties van bedreigingen die kunnen worden opgespoord en gerapporteerd door een SIEM oplossing dat veel informatiebronnen omvat en daarom kan worden beschouwd als een echte Security Intelligence oplossing.

RAPPORTEER OP GEBRUIK VAN PRIVILEGED USER ACCOUNTS

User Activity Monitoring is een zeer belangrijk onderwerp voor de hedendaagse Business- en Security Manager. Wat kan user activity monitoring betekenen? Je kunt denken aan enkele use cases:

- Een vertrokken medewerker die nog steeds actief lijkt op het netwerk (hoe kan dit? De user account is toch disabled?)
- Een medewerker met speciale rechten benadert databases die zij normaliter niet benaderd. (duidt dit soms op kwade bedoelingen of is haar account door iemand gehackt? Of zijn alleen haar verantwoordelijkheden aangepast?)
- Zien we een medewerker uit een bepaald land, ineens activiteiten ontplooien vanuit een ander land? (wordt zijn account soms misbruikt?)

Zonder een SIEM oplossing dat real-time Identity & Access Management (IAM) informatie kan correleren met netwerk activiteit en security events, zouden de meeste organisaties deze voorvallen niet opmerken en dus niet hierop kunnen acteren. Avensus Managed SIEM voorziet in de noodzakelijke zichtbaarheid op verdachte en mogelijk risicovolle gebruikers activiteit.

Of u nu real-time wilt worden gewaarschuwd voor security incidenten of periodiek geautomatiseerde rapporten wilt bekijken, Avensus Managed SIEM maakt het u gemakkelijk om een proactieve houding aan te nemen ten opzichte van de gebruiker risico's en zo uw beveiligingsstatus te verbeteren.

DETECTIE VAN 'ZERO-DAY THREATS' DIE ANDEREN MISSEN

Avensus Managed SIEM gebruikt netwerk flow gegevens van het netwerk om nieuwe bedreigingen te detecteren zonder gebruik te maken van 'vulnerability signatures'. Hierdoor is threat detectie mogelijk van zaken die gemist zijn door antivirus- en andere beveiligingssystemen. Netwerk flow gegevens kunnen worden gebruikt om veranderingen in het netwerkverkeer te detecteren die kunnen wijzen op een bedreiging. Bijvoorbeeld het ontdekken van een nieuwe service of protocol zoals een-mailserver in de DMZ of een FTP-service die ineens actief wordt op een bestaande server. Ook kunnen veranderingen van activiteit van bepaalde services worden gedetecteerd. Zo kan SSH geïnstalleerd worden op de mailserver om slechts incidenteel legaal gebruikt te worden.

Als een kwaadwillende gebruiker de server heeft gehackt en vervolgens de SSH service benut als een springplank om andere servers te hacken, zou dit meteen worden gedetecteerd en gesignaleerd. Avensus Managed SIEM biedt de zichtbaarheid en de context die nodig zijn om dit soort risico's te identificeren.

DETECTIE VAN INTERNE BOTNET ACTIVITEIT

De eerste generatie log management en SIEM producten ondersteunden organisaties met name op gebied van compliancy hetgeen niet langer voldoende is. Nieuwe compliancy normen, zoals PCI DSS, evenals een grotere focus op de interne naleving van het security beleid, vereisen application-aware monitoring en zichtbaarheid, en dat is niet goed haalbaar door middel van alleen log analyse. Avensus Managed SIEM biedt de mogelijkheid om applicaties te detecteren, gebruikers te identificeren die inloggen op kritische servers met clear text wachtwoorden, en om ervoor te zorgen dat de versleutelde protocollen goed worden ingezet in bepaalde segmenten van het netwerk. Een veelvoorkomend voorbeeld in klantomgevingen is de aanwezigheid van botnet communicatiekanalen (IRC verkeer). Door de inspectie van de inhoud op (meta)applicatieniveau, kunnen IRC kanalen en IRC communicatie worden gedetecteerd, gesignaleerd en vastgelegd voor forensisch bewijs.

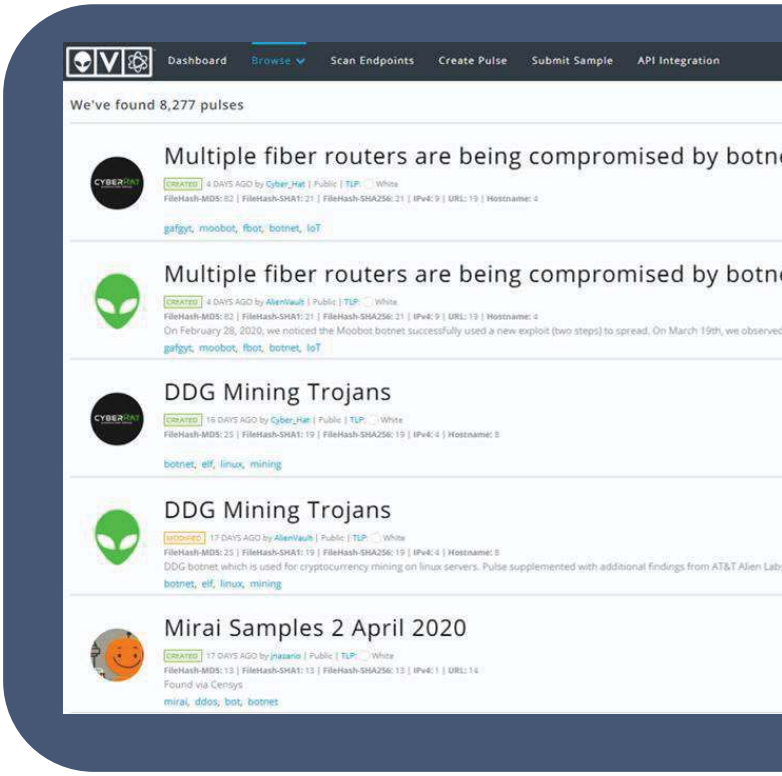
Het ontwikkelen van verschillende rapporten voor intrusion detection is vaak een enorme uitdaging, ook vanwege het probleem van false positives. Toch zou men kunnen stellen dat het detecteren van 'verboden' verkeer (verboden door security policies) meer indicatief is voor kwaadaardige activiteiten.

Een goed advies is daarom: wees alert op grote hoeveelheden outbound SMTP verkeer. Dergelijke patronen, met name afkomstig van niet-SMTP Servers, zullen waarschijnlijk duiden op een malware spam bot uitbraak in uw organisatie. Ook kunnen rapporten over DNS-verkeer zeker helpen bij het opsporen van botnet infecties.

ONWETENDE GEBRUIKERS BENADEREN KWAADAARDIGE WEBSITES

Een gebruiker klikt op een link die hem omleid naar een nog onbekende kwaadaardige website. In deze website is nieuwe kwaadaardige code ingebed die een backdoor installeert op de PC van deze gebruiker. Deze computer maakt vervolgens een IRC-verbinding via een niet-standaard poort, om zodoende de verbinding te verbergen van de bestaande beveiligingsoplossingen. Zodra er verbinding is gemaakt met de IRC server wacht deze op een opdracht om bepaalde subnetten te scannen op open mail servers (poort 25) en de resultaten te uploaden naar een bepaalde chatroom. Zodra de resultaten zijn geretourneerd, stuurt de aanvaller een commando naar de besmette PC om mail te sturen naar hosts met open mail poorten.

Firewall en Intrusion Detection Systems zijn niet altijd even effectief in het detecteren van dergelijke aanvallen en daarbij ontbreekt de zichtbaarheid van dergelijke security incidenten. Avensus Managed SIEM biedt de overall zichtbaarheid dat nodig is om de beschreven gebeurtenissen te ontdekken en samen te voegen tot een Security Incident; zonder dat zou een dergelijke exploit wellicht onopgemerkt zijn gebleven.



BETERE BEOORDELING VAN SECURITY INCIDENTEN VIA ASSET PROFILES

Het beheren van veiligheidsrisico's kan een redelijke uitdaging zijn voor organisaties vanwege het dynamische karakter van de verschillende netwerk toepassingen. Gebieden van de IT-infrastructuur die constant veranderen zijn onder meer:

- Netwerk adres – host tabellen
- Applicaties op een bepaalde server
- Netwerk poorten gebruikt voor een specifieke applicatie
- Kwetsbaarheid van servers voor een bekende exploit
- Business kritikaliteit van specifieke servers en applicaties
- Mogelijkheid van netwerk en security systemen om accuraat security incidenten te rapporteren

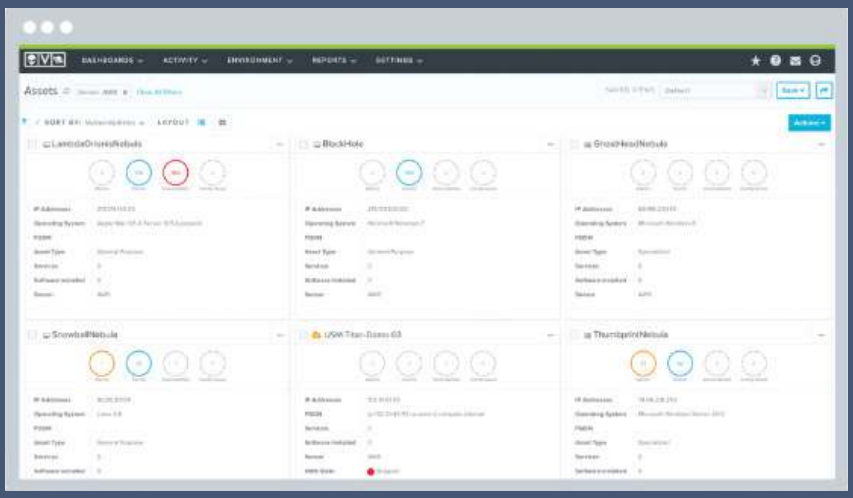
Het is belangrijk voor een netwerk security management oplossing om veranderingen in deze gebieden mee te nemen in de afweging en beoordeling van prioriteit en relevantie van de verschillende waargenomen gebeurtenissen. Avensus Managed SIEM biedt deze mogelijkheid.

BESCHERMING TEGEN AANVALLEN VAN BINNENUIT

Een aanvaller lanceert een Denial of Service (DoS) aanval van binnen een netwerk en voert met succes een buffer overflow aanval uit op een van de servers. Vanuit de aldus aangevallen server wordt vervolgens een verkenning op meer resources binnen het netwerk uitgevoerd. Vervolgens worden pogingen gedaan om met extra rechten in te loggen op de mailserver, hetgeen uiteindelijk mislukt.

Terwijl verschillende beveiligingsinstallaties (bv firewall en IDP) correct rapporteren over een stroom van gebeurtenissen verspreid over meerdere doelen en diverse netwerkapparaten een vloed van gebeurtenissen ook verspreid over meerdere categorieën rapporteren, is het van groot belang om al deze activiteiten te bundelen in één rapport van een DoS aanval die informatie over alle systemen die werden getroffen omvat.

Verborgen in de stortvloed van gebeurtenissen die afkomstig kunnen zijn van zelfs de meest modale firewall/ IDP implementaties op een high-traffic netwerk, bevinden zich de puzzel stukjes van wat een inleiding is op iets veel schadelijker. Inderdaad, aanvallen als deze kunnen zich over vele dagen ontwikkelen. Terwijl individuele beveiligingsoplossingen normaliter hun bijdrage leveren bij het signaleren van activiteiten die specivfiek zijn voor het segment of het verkeer waarnaar zij kijken, is een grotere zichtbaarheid noodzakelijk over alle devices die de betreffende netwerk- en security-activiteit vertonen.



MISLUKTE LOGIN POGINGEN: HET KAF VAN HET KOREN SCHEIDEN

Veel **security monitoring oplossingen** bieden correlatie regels die op zoek gaan naar overmatige mislukte inlog pogingen op servers met gevoelige informatie. Stel dat de gedefinieerde regel is geconfigureerd om een 'failed login' melding genereren als een systeem meer dan 5 inlogpogingen in een minuut tijd te verwerken krijgt. Elke keer dat een legitieme gebruiker van het systeem per ongeluk 6 keer of meer zijn wachtwoord verkeerd invoert, zal dit ook resulteren in een waarschuwing die moet worden uitgezocht door een security administrator. Een goede correlatie functie herkent echter een succesvolle inlog poging van dezelfde host nadat hier eerst mislukte logins voor zijn gerapporteerd en dat de gebruiker die met succes is ingelogd een legitieme gebruiker is; deze verbeterde intelligentie voorkomt een vals alarm. Avensus Managed SIEM biedt de mogelijkheid die voorziet in krachtige correlatie die de nauwkeurigheid van de gedetecteerde security incidenten sterk verbetert. Het resultaat is een vermindering van de 'False Positives' en een sterk verbeterde efficiëntie van de security managers door alleen met de meest relevante informatie aan de slag te gaan.

DETECTEER & REPORTEER ILLEGALE SERVERS, SERVICES OF VERKEER

Nieuwe netwerk services kunnen een indicatie zijn van onlangs geïnstalleerde backdoors of per ongeluk geïnstalleerde services die zouden kunnen worden gebruikt voor het uitvoeren van nieuwe aanvallen. Nieuwe hosts op het netwerk kunnen bijvoorbeeld een wireless accesspoint of een niet-standaard werkplek zijn. Hoewel deze gebeurtenissen geen garantie zijn voor illegale activiteiten, kan het detecteren en verwijderen van dergelijke apparaten helpen bij het voorkomen van toekomstige aanvallen.

Avensus Managed SIEM heeft de mogelijkheid om de aanwezigheid van een nieuwe service op te sporen in bijvoorbeeld een DMZ. Deze functie kan gemakkelijk worden aangepast om vervolgens te kijken naar veranderingen in andere netwerksegmenten of specifieke hosts.

Zogenaamde "darknets" zijn een klassieke methode voor het detecteren van verdacht verkeer. Het concept is heel simpel: maak netwerksegmenten in uw infrastructuur die routeerbaar zijn maar geen enkel systeem of device bevat. Daarom mag geen enkel systeem binnen de infrastructuur proberen om iets binnen het darknet te openen. Elk pakket dat een darknet binnen komt is door zijn aanwezigheid afwijkend en per definitie verdacht. Dergelijke pakketten kunnen zijn aangekomen per vergissing of door een fout in de configuratie maar de meerderheid van dergelijke pakketten zullen zijn verzonden door malware. Deze malware scant actief voor kwetsbare apparaten en stuurt derhalve pakketten naar het Darknet. Avensus Managed SIEM kan deze netwerksegmenten monitoren dienovereenkomstig een alarm genereren.

Meer informatie

Wilt u meer weten over de Managed SIEM en onze dienstverlening?
Neem contact met ons op via **036-5393100** of **info@avensus.nl**