RSA NetWitness

Factsheet

DIT MOETEN MSSP'S WETEN OVER EVOLVED SIEM

De IT-omgeving van uw klant is er – met de opkomst van cloud, het Internet of Things en de digitale transformatie – niet eenvoudiger op geworden. Hoe weet u dan zeker dat uw SOC-analisten alle dreigingen in het vizier hebben, en hier ook op kunnen reageren? Daar hebben ze geavanceerde SIEM-tooling voor nodig. Een 'evolved SIEM', zoals RSA NetWitness. Wat moet u weten over dit platform?

WAT IS SIEM?

De meeste MSSP's weten het antwoord op deze vraag wel, maar het kan nooit kwaad om weer even het geheugen op te frissen. SIEM staat voor Security Information and Event Management en is onmisbaar in een Security Operations Center. SIEM-tools verzamelen de logfiles die afkomstig zijn van applicaties, databases, besturingssystemen, netwerken en hardwarecomponenten. Door de beveiligingsdata uit deze logfiles te filteren en ze vervolgens te combineren en analyseren, komen securityteams verdachte netwerkactiviteiten op het spoor.

Het handmatig doorlopen van alle logdata is voor de meeste teams niet te doen. Ook het aantal alerts kan overweldigend zijn. Sommige SIEM-tools helpen daarom een handje door potentiële dreigingen niet alleen te markeren, maar ook te prioriteren. Naast detectie van dreigingen worden SIEM-tools ook gebruikt voor het aantonen van compliance.

WAT IS HET VERSCHIL TUSSEN EEN TRADITIONEEL EN EEN 'GEËVOLUEERD' SIEM?

De focus van traditionele SIEM-tools lag oorspronkelijk op het verzamelen en opslaan van de logfiles, die afkomstig zijn van de preventieve securitycomponenten zoals de antivirus, firewalls, VPN's en de systemen voor inbraakdetectie en -preventie. Bijvoorbeeld ongebruikelijke activiteiten op een pc, afwijkingen in het netwerkverkeer of ongeautoriseerde verbindingen met apparaten en applicaties bleven hiermee echter buiten beeld.

Security-analisten hebben behoefte aan een vollediger beeld van wat er zich allemaal afspeelt op de IT-infrastructuur van de klant. En dan niet alleen

on-premises. Cybercriminelen hebben met de opkomst van onder andere de cloud en het Internet of Things immers meer kanalen tot hun beschikking om organisaties aan te vallen. Evolved SIEM maakt de gehele infrastructuur inzichtelijk door logdata uit alle mogelijke bronnen op te halen, ongeacht waar die bronnen zich bevinden.

Daar blijft het echter niet bij. Een evolved SIEM-oplossing zoals RSA NetWitness biedt bijvoorbeeld ook User and Entity Behavior Analytics (UEBA) voor detectie van afwijkend gedrag van een gebruiker of device. Daarnaast maakt RSA NetWitness gebruik van threat intelligence uit externe bronnen. Het biedt daarmee analisten de mogelijkheid om potentiële dreigingen al in een vroeg stadium te detecteren en erop te reageren.

HEEFT EVOLVED SIEM DAN NIET VEEL OVEREENKOMSTEN MET XDR?

Die overeenkomsten zijn er zeker, maar er zijn ook belangrijke verschillen. Net als evolved SIEM is Extended Detection and Response (XDR) gericht op het zo snel mogelijk detecteren van en reageren op dreigingen, met als doel om incidenten snel en efficiënt op te lossen. XDR biedt echter geen registratiesysteem voor compliance-, archiverings- en rapportagedoeleinden.

XDR kan volstaan voor organisaties die al beschikken over compliancetooling en alleen behoefte hebben aan een oplossing voor detectie en response. Met het RSA NetWitness-platform, dat het beste is te omschrijven als een combinatie van evolved SIEM en XDR, weet u zeker dat u alle benodigde componenten in huis heeft. Met een geïntegreerd platform voorkomt u bovendien dat onderbemande securityteams securitydata uit verschillende systemen moeten ophalen en bedolven raken onder alerts.

UIT WELKE COMPONENTEN BESTAAT HET RSA NETWITNESS-PLATFORM?

RSA NetWitness is een omvangrijk platform dat onder andere bestaat uit de volgende componenten:

- NetWitness Logs, voor het centraal beheren en bewaken van loggegevens van zowel de on-premises als cloudinfrastructuur;
- NetWitness Network, voor realtime inzicht in de volledige infrastructuur zodat zowel bekende als onbekende dreigingen snel aan het licht komen en worden geprioriteerd;
- NetWitness Endpoint, voor bewaking van de activiteiten op alle endpoints, zowel binnen als buiten het netwerk.
- NetWitness Orchestrator, een Security Orchestration, Automation and Response (SOAR)-oplossing die SOC's en incident-reponse-processen een stuk efficiënter en effectiever maakt;
- NetWitness Detect AI, een SaaS-oplossing die onbekende bedreigingen snel detecteert door geavanceerde gedragsanalyses (UEBA) en machine learning toe te passen op gegevens die zijn vastgelegd door het NetWitness-platform.

WAT ZIJN VOOR MIJN ORGANISATIE DE VOORDELEN VAN HET RSA NETWITNESS-PLATFORM?

Het RSA NetWitness-platform biedt MSSP's meerdere voordelen:

- Ze beschikken hiermee over een schaalbaar en modulair opgebouwd platform zodat ze de componenten kunnen afnemen die op dat moment nodig zijn.
- Beveiligingsteams kunnen dreigingen sneller detecteren en erop reageren, nog voordat de dreiging impact heeft op de business van de klant.
- Door het gebruik van een geïntegreerd platform in plaats van losse tools gaat het aantal waarschuwingen omlaag.
- De kwaliteit van de alerts waarop de SOC-analisten moeten reageren, gaat omhoog.
- Door een verbeterde workflow en automatisering gaat de efficiëntie van het SOC eveneens omhoog.
- Uit een onafhankelijk onderzoek blijkt dat RSA NetWitness een hoge Return on Investment (ROI) heeft, onder andere door de besparing die kan worden gerealiseerd op het mitigeren van risico's.

Meer weten over hoe u uw SOC slimmer en efficiënter maakt met RSA NetWitness? Neem dan vrijblijvend contact met ons op.

RSA

WWW.TECHDATA.NL

Tech Data Nederland B.V.
Tolnasingel 2 · 2411 PV Bodegraven
+31 (0) 88 133 40 00 · tdsecurity@techdata.nl