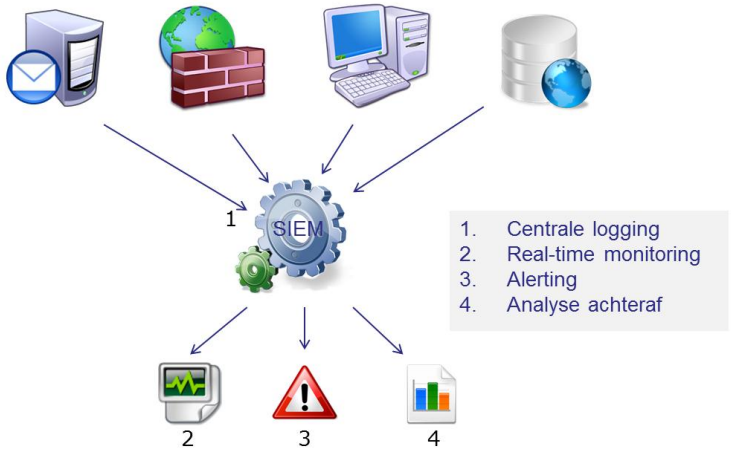
SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

KRISTOF VERSLYPE

1. Inleiding

IT-infrastructuren worden complexer en dynamischer, de cyberaanvallen gesofisticeerder en de aanvallers professioneler. Zowel interne als externe aanvallen vormen een bedreiging.

In een moderne IT-infrastructuur van een bedrijf worden vandaag de dag al snel miljoenen security gerelateerde logs door honderden of meer devices gegenereerd, potentieel vanaf verschillende geografisch verspreide locaties. Typisch zijn er op een dag hoogstens enkele incidenten. De uitdaging is om aan de hand van die miljoenen logs die paar incidenten in real-time te extraheren. Indien nodig kan dan ingegrepen worden om de schade te minimaliseren of kunnen achteraf maatregelen genomen worden om dergelijke incidenten in de toekomst te voorkomen. Dergelijke reactieve maatregelen vallen echter buiten de basisfunctionaliteit van SIEM. Het extraheren van incidenten uit logs is wat SIEM-systemen op een geautomatiseerde manier beloven te doen. Daarnaast bieden ze de mogelijkheid achteraf uitgebreide analyses op de verzamelde logs te doen.



Figuur 1: Werking SIEM

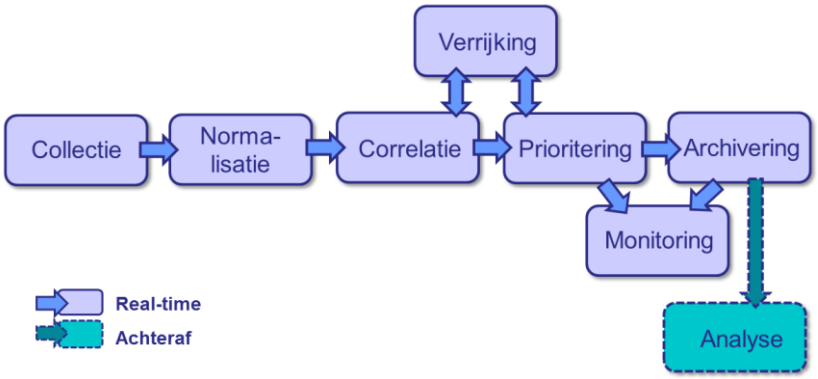
Figuur 1 toont op hoog niveau de werking van SIEM. Het centrale SIEM-systeem ontvangt de security gerelateerde logs vanuit de hele IT-infrastructuur. Dit gaat van firewalls, IDS (Intrusion Detection Systems)

machines, applicatieservers tot end-user devices, etc. Zowel het besturingssysteem als de bovenliggende applicaties kunnen in principe logs naar het SIEM-systeem sturen, alsook firmware en middleware.

De SIEM-functionaliteit kunnen we opdelen in: 1) centrale logging, 2) het aanbieden van real-time monitoring, 3) alarmgeneratie bij een incident en 4) het aanbieden van analyse achteraf.

2. Verwerking logs

Figuur 2 onderscheidt acht stappen bij de verwerking van logs die het SIEM-systeem binnenkomen. Deze stappen worden nu kort toegelicht.



Figuur 2 Verwerking logs door SIEM-systeem

Bij de *collectie* worden de logs door het SIEM-systeem verzameld. Hierbij onderscheiden we het push- en het pull-principe. In de praktijk zien we vaak push over UDP. Bij pull worden de logs op de device op regelmatige tijdstippen opgehaald waardoor het real-time gehalte daalt.

Na de collectie volgt de *normalisatie* waarbij de binnengekomen logs, die verschillende formaten kunnen hebben (Windows Event logs, syslog, Cisco logs, etc.), omgezet worden naar een uniform formaat zodat de volgende stap, de correlatie, vergemakkelijkt wordt.

Deze *correlatie* komt erop neer dat er verbanden tussen logs gezocht worden, ook al zijn deze op verschillende momenten door verschillende devices gegenereerd. We illustreren dit aan de hand van een klein voorbeeldje. Te midden van talloze andere log entries detecteert een firewall een port scan. Kort daarna detecteert een applicatieserver een hele reeks gefaalde SSH-authenticaties, een succesvolle SSH-authenticatie en ten slotte de installatie van een stukje software op de applicatieserver zelf. Daaropvolgend detecteert de IDS een reconnaissance scan[1]. Een SIEM-systeem zou als resultaat van een eerste correlatie kunnen detecteren dat er een geslaagde brute-force SSH-authenticatie gebeurd is. Bij een tweede correlatie zou deze brute-force aanval geplaatst kunnen worden in een bredere aanval.

[1] Een reconnaissance scan is een verkenning van het netwerk; welke zijn de actieve systemen, welke besturingssystemen gebruiken ze, welke services draaien ze, etc.

Bij *verrijking* wordt externe informatie aan de logs gekoppeld. Enkele voorbeelden zijn 1) gekende kwetsbaarheden van een betrokken server, 2) de functie van deze server, 3) de volledige naam en functie van de persoon horend bij het betrokken account en 4) de geografische locatie van het externe IP-adres. Deze informatie haalt het SIEM-systeem uit bronnen zoals een CMDB en active directory.

Bij *prioritering* wordt aan de hand van een aantal parameters berekend hoe risicovol een event (dat uit één of meerdere log entries bestaat) is. Hierbij wordt typisch gekeken naar o.a. de waarde van de asset (vb. kritische server of client machine), de impact bij succes (vb. root access of slechts heel beperkte privileges) en de waarschijnlijkheid dat het event tot een effectief incident leidt (vb. 5 gefaalde SSH-authenticaties of 10 000 gefaalde SSH-authenticaties).

Bij de *archivering* zijn er traditionele vereisten zoals confidentialiteit, integriteit en beschikbaarheid. Daarnaast is ook de efficiëntie cruciaal. Enerzijds worden er dagelijk miljoenen logs toegevoegd, en anderzijds is er een stevig indexeringsmechanisme nodig voor de analyse achteraf. Genormaliseerde logs hebben typisch geen juridische bewijswaarde, wat ook de opslag van de originele logs noodzaakt. SIEM-systemen zijn dus doorgaans ook geschikt om logs op een veilige manier te bewaren.

Monitoren houdt in dat via dashboards de kwetsbaarheden, de verdachte activiteit en de effectieve incidenten in het oog gehouden worden. Het SIEM-systeem kan alarmen genereren wanneer events met een voldoende hoog risico gedetecteerd worden. Alarmen kunnen via o.a. dashboards, e-mail en sms kenbaar gemaakt worden.

De *analyse* achteraf resulteert in een dieper inzicht in de security van de eigen IT-infrastructuur en is waardevol bij forensisch onderzoek alsook bij het nagaan van compliancy met reguleringen zoals HIPAA[2] en PCI DSS[3]. De analyse gebeurt d.m.v. rapporten en query's. Rapporten geven eerder algemene informatie, terwijl query's specifieke informatie zoeken.

3. SIEM-producten

State-of-the-art producten zijn ArcSight (HP), QRadar (IBM), NitroView (McAfee) en EnVison (EMC²/RSA)[4]. Een gedeeltelijk gratis open source SIEM-product is AlienVault.

AlienVault is getest door Smals Onderzoek in een beperkte virtuele omgeving. AlienVault is erin geslaagd heel wat open source producten in één SIEM-tool te integreren. Voor analyse achteraf is de betalende Logger component vereist. Voor de correlatieregels heeft AlienVault een 90-tal richtlijnen, die elk een set gerelateerde regels groeperen. Richtlijnen

[2] De Health Insurance Portability and Accountability Act (kortweg HIPAA) is de Amerikaanse wetgeving uit 1996 voor de gezondheidssector.

[3] De Payment Card Industry Data Security Standard (PCI DSS) is een information security standaard voor organisaties die elektronische financiële transacties verwerken.

[4] Bron : Magic Quadrant for Security Information and Event Management, Gartner, May 12 2011.

kunnen gecreëerd en aangepast worden. Toch blijven de correlatieregels eerder op een laag niveau (SSH brute-force aanval, reconnaissance, malware activiteit, etc.).

ArcSight is een krachtigere en duurdere oplossing. Naast de standaardfunctionaliteit zijn er uitbreidingen voor o.a. de detectie van low-and-slow aanvallen, optimalisatie voor analyse, monitoring van gebruikers waaronder ook gedeelde en geprivilegeerde accounts. Standaard biedt ArcSight een uitgebreid gebruikersbeheer aan waarbij gebruikers gepersonaliseerde dashboards en rapporten te zien krijgen.

4. Managed SIEM

De klassieke SIEM-aanpak waarbij elk bedrijf via een eigen SIEM-systeem zijn eigen IT-infrastructuur monitort en zelf de escalatie doet bij een incident, resulteert potentieel in een aantal nadelen zoals investeringskosten, onderhoud, beperkte expertise en beperkte monitoring.

Managed SIEM is een alternatief waarbij bedrijven hun logs naar een externe partij, de MSSP (Managed Security Services Provider), sturen die ook het monitoren en de escalatie op zich neemt. Een MSSP heeft meer SIEM-expertise en een grotere security intelligence. Afhankelijk van de bedrijfsfilosofie kan het outsourcen van de verwerking van potentieel gevoelige logs wenselijk of minder wenselijk zijn.

MSSP's kunnen ook op andere manieren ondersteuning bieden in het SIEM-verhaal, door bijvoorbeeld een SIEM in het bedrijf zelf te monitoren of door staffing te leveren bij bijvoorbeeld de uitrol van het SIEM-systeem.

IBM, Symantec, BT, HP, Verizon Business en Fujitsu zijn de grotere MSSP's. Een Belgische speler is Belgacom.

5. Aandachtspunten

De aandachtspunten bij de uitrol van een SIEM-systeem verdelen we onder in "business", "infrastructuur" en "uitrol en gebruik".

Wat betreft het *business* aspect moeten een incident response plan, skills, mankracht en duidelijke formulering van de security requirements aanwezig zijn en is een betrokkenheid nodig door de verschillende bedrijfsafdelingen die met het SIEM-systeem zullen te maken krijgen.

Op *infrastructureel* vlak is een duidelijk beeld van de IT-infrastructuur nodig, mogen er geen zwarte gaten zijn bij het (nu nog gedecentraliseerd) monitoren, moeten de klokken van de verschillende devices gesynchroniseerd zijn en is een goed beeld nodig van de opslagvereisten van de logs (6 maanden opslag is een goed begin).

Wat betreft de *uitrol en het gebruik* van het SIEM-systeem mag men geen plug-and-play verwachten en finetuning zal nodig zijn. Documentatie van de SIEM-uitrol kan tijdverlies later voorkomen. Zorg voor een gefaseerde

uitrol; pas wanneer een (eventueel vereenvoudigde) use case een aanvaardbaar aantal hoge prioriteitsevents genereert, kan een stap verder gegaan worden. Ten slotte verandert het threat landscape alsook de IT-infrastructuur constant, wat onderhoud van het SIEM-systeem noodzaakt.

6. Te onthouden

Een *goede security* op voorhand is onontbeerlijk. SIEM is een *project*. Zonder de nodige technische voorbereiding en de nodige mensen heeft het project geen kans op slagen. Een SIEM-uitrol vergt tijd. 12 tot 18 maanden is een vuistregel, maar dit varieert uiteraard naargelang de concrete condities. Ten slotte moet een SIEM-systeem in productie onderhouden worden.

Het heikele punt van een SIEM-systeem vandaag de dag zijn de *correlatieregels*. De afstemming ervan zal het verschil maken tussen enkele hoge prioriteitsevents of enkele honderdduizenden en bepaalt dus de mogelijke toegevoegde waarde van het SIEM-systeem.

SIEM blijft zowel in aankoop als in onderhoud een *aanzienlijke kost*. De aanschaf beloopt al snel enkele honderdduizenden euro's en de nodige mankracht en expertise in huis halen en houden is vaak geen evidentie. Managed SIEM kan een alternatief bieden, maar ook hier spreken we over 10 000 à 20 000 euro per managed device.

AlienVault is geschikt als eerste kennismaking met SIEM. Verschillende vendors zijn bereid om een appliance uit te lenen voor testdoeleinden en vaak hebben ze in hun gebouwen een testomgeving waar demo's gegeven kunnen worden.

Er zijn omwille van de bovengenoemde redenen *vele SIEM-uitrollen mislukt*, wat niet wegneemt dat een succesvolle uitrol, die een effectieve meerwaarde biedt, mogelijk is. We zien dit bevestigd in onder meer de financiële sector, de energie- en de farmasector en in defensie.

In de VS is 80 % van de SIEM-uitrollen gedreven vanuit de vereiste voor *compliancy* met reguleringen. We kunnen verwachten dat dergelijke reguleringen ook Europa zullen bereiken. Dit zal de interesse voor SIEM doen toenemen.

De slides van de infosessie (maart 2012) kunnen bekeken worden op http://documentatie.smals.be.