

Kort og godt om Log Management (SIEM)



Christian Schmidt

Læs hvordan du kommer i gang med Log Management / SIEM og hvilke forholdregler, du skal tage for at få valgt den rigtige løsning.

Få mere information på [Drawares hjemmeside](#) eller se vores YouTube video ([YouTube](#)).

Draware™ A/S

Teglgården 46, DK-3460
Birkerød

Tel: +45 45 76 20 21

www.draware.dk

2/7/2012

Indholdsfortegnelse

Hvad er logs?	2
Hvordan indsamles logs?	2
Hvad sker der efter indsamlingen?	2
Indexering.....	2
Arkivering.....	2
Metadata	2
Filtrering	2
Korrelering.....	3
Hvordan præsenteres resultatet?	3
Grafisk interface	3
Compliance	3
Alarmering	3
Rapportering.....	3
Overvejelser ved anskaffelse af et logmanagement / SIEM system	3
Mål.....	3
Systemkrav	4
Vokseværk	4
Forstå og forankre	4
Eksperimentér	4
Eksempler på Log Management løsninger	5
Entry level – Software.....	5
Midrange – Hardware/Software	5
Highend – Hardware.....	5
Nyttige links	5

Hvad er logs?

Logs er DNA eller fingeraftryk fra applikationer (SQL/Mail/Web), OS (Windows / Unix / Linux), hardware (servere, switches, FW, AP, IDS/IPS/UPS m.fl) men findes også i specielle formater fra andre systemer. En log er en fællesbetegnelse for en fil med individuelle linjer, der hver især betegnes et event. Disse events indeholder forskellige informationer afhængigt af, hvilket system de kommer fra, men typisk drejer det sig om IP-adresse, tids/dato stempel og nogle metada om eventtypen, koder, beskrivelser mm. Den aktive håndtering af logs kaldes normalt for Log Management og i lidt større og mere avancerede systemer, hvor logs også korreleres (herom senere) bruges udtrykket Security Information and Event Management (SIEM).

Et log management system indsamler logs automatisk til et centralt punkt (typisk en database) hvorfra al behandlingen sker. Du kan således søge, rapportere, alarmere og korrelere på tværs af alle logs på én gang fra ét centralt punkt, uanset om de individuelle logs på opsamlingspunktet er blevet slettet eller overskrevet. Et log management system samler og forædler den samlede informationsmængde og giver dig brugbar indsigt i hvem, der gjorde hvad og hvornår på din IT infrastruktur.

Hvordan indsamles logs?

Logs kan enten aktivt videresendes til det opsamlende device eller en mellemstation – typisk i form af syslogs (hardware enheder) eller traps (servere). Logs kan også aktivt indsamles fra text logs og eventlogs via en lokal agent installeret på en desktop eller en server. Der indsamles logs i realtid eller nær realtid.

Hvad sker der efter indsamlingen?

Indexering

Alle de individuelle ord i de enkelte logs registreres og danner således et index over hvor mange ord, der optræder med hvilken frekvens.

Arkivering

De enkelte logs/events gemmes i et format (fx en database eller en zippet fil), således at de kan genfindes på et senere tidspunkt. Typisk opbevares den nyeste del af alle logs i et format, hvor de meget hurtigt kan behandles, mens alle logs, der er ældre end en hvis dato, arkiveres i en form og/eller på et medie, der egner til opbevaring af meget store datamængder.

Metadata

Baseret på grundlæggende informationer i den enkelte event såsom IP adressen, tidsstempelt, enheden eventet er sendt fra mm, udledes og tilhæftes en række metadata, som ikke direkte står i det enkelte event, men som giver mening ved den efterfølgende analyse og korrelering af logs.

Filtrering

Nogle events når ikke korreleringssystemet baseret på en smart filtrering for at forhindre at korreleringssystemet overbebyrdes og at mængden af logs vokser ukontrollabelt.

Korrelering

Ud fra et sæt af regler sammenholdes (korreleres) de enkelte logs typisk baseret på frekvens (hvor ofte logs forekommer eller antallet af logs) og sammenhænge mellem forskellige typer af logs eller enkelte logs. Denne type af "intelligens" er den egentlige kerne i et log management / SIEM system og gør det muligt for systemet at opdage ting og sammenhænge, som det ville være helt umuligt at opdage ved en manuel gennemgang af logs.

Hvordan præsenteres resultatet?

Grafisk interface

Du ser en grafisk præsentation af de korreleringsdata, som passer til det formål, du ønsker og har indikeret ved dit personlige login. I form af søjle- og lagkagediagrammer får du serveret "toppen af isbjerget".

Compliance

En række regler og filtre ligger til grund for rapporter, der modsvarer krav fra officielle standarder som fx, PCI, FISMA, SOX, ITIL, HIPPA m.fl.

Alarmering

Baseret på tærskelværdier eller triggers kan du bruge logs / korreleringer i realtid til at få alarmer om events, du gerne vil have mulighed for at få umiddelbar indsigt i. En del systemer understøtter også muligheden for udbedring, hvilket svarer til en aktion baseret på en alarm, som skal modvirke alarmens årsag.

Rapportering

Fra faste skabeloner kan du trække rapporter - som oftest i PDF format. Så spørger revisoren eller sikkerhedsmedarbejderen efter en bestemt dokument, kan du trække det frem med det samme.

Overvejelser ved anskaffelse af et logmanagement / SIEM system

Mål

Hvad vil vi opnå med at kigge på vores logs og hvilket fokus har vi med logs?

- Er det af sikkerhedsmæssige hensyn?
- Er det for at blive standard compliant eller
- Er det bestemte rapporter (ofte en del af compliance) som vi gerne vil se som fx failed logins?

Disse mål lægger grunden til systemkravene og valgene af den rigtige løsning, hvilket ofte er med til at definere om du:

- Kun ønsker log opbevaring
- Ønsker log management
- Ønsker SIEM (inklusive korrelering)

Kort og godt om Log Management (SIEM)

Systemkrav

Når målene med din Eventlog Management løsning er defineret, skal du opsætte nogle systemkrav og her er det vigtigt at tage følgende op til overvejelse:

- Hvilke og hvor mange typer af endpoints vil du indsamle logs fra?
- Hvilke indsamlingsmetoder vil du baseret på ovenstående bruge: lokale agenter, WMI, syslog, SNMP-traps m.fl.?
- Kan du herfra vurdere Events Per Second (EPS) og deraf vurdere mængden af indsamlede data over tid?
- Hvilke data ønsker du bare skal være søgbare og hvilke data skal korreleres (filtrering)?
- Hvilke hardware krav skal du stille til databasen bag logmanagement systemet?

Vokseværk

Hvor meget vil systemet vokse pr. år baseret på vækst i endpoints eller vækst i log mængder. Der skal afsættes plads i løsning og systemkrav således, at systemet også kan håndtere en pludselig voldsom (x2) vækst i logmængden som fx under et attack/orm/virus mm.

Regn således med at du mindst har 40% uudnyttet kapacitet i dit logmanagement system, og at systemet kan udbygges efter det beregnede behov.

Forstå og forankre

Hvem skal administrere logmanagement systemet og hvem skal bruge data/rapporter fra logmanagement systemet?

- De brugere som skal administrere systemet skal lægge vedligeholdelse af systemet ind i den daglige drift, således at nye noder bliver lagt ind og slettede noder fjernes (efter noget tid) fra systemet. Desuden skal de tilrettelægge tiden omkring logmanagement systemet således, at der laves rapporter og skærmbilleder (dashboards), som passer til brugernes behov.

Kommer der nye lovmæssige krav i forbindelse med revisionsrapporter eller compliance rapporter skal disse naturligvis tilgodeses. Det gælder også hvis der tilføjes nye typer af endpoints (fx nye switches), hvis traps skal kunne fortolkes af systemet.

Der skal også afsættes til database og systemadministration.

- Hvad angår brugerne skal de specificere de krav, de stiller til output fra systemet i form af rapporter og dashboards. Eventuelle alarmer af sikkerhedsmæssig karakter skal også defineres.

Eksperimentér

Betyder det så, at du skal glemme alt om at få glæde af et log management system, hvis du ikke gør log management til et større IT projekt?

Kort og godt om Log Management (SIEM)

Naturligvis ikke. Her er det en god idé at vælge et system, som du kan vokse med og som leverer så meget "out-of-the-box" som muligt. Selve den grundlæggende installation og opsætning er ikke særlig ressourcekrævende, og så kan du bruge tiden (når den er til rådighed) til at kigge på resultatet og få inspiration til i hvilke detaljer, du vil bruge systemet i den daglige drift.

Eksempler på Log Management løsninger

Baseret på den foregående information står du så med opgaven at vælge et log management system, som passer til dit behov og rammer plet inden for budgettet. Typisk er der 3 kategorier at vælge imellem og herunder finder du eksempler på alle 3:

Entry level – Software

[Correlog®](#)

[ManageEngine Eventlog Analyzer®](#)

[SolarWinds Log & Event Management®](#)

Midrange – Hardware/Software

[LogRhythm®](#)

[LogLogic®](#)

Highend – Hardware

Q1Labs® (IBM)

ArcSight® (HP)

Nyttige links

1. [Drawares emneside om log management](#)
2. Dette document på Internettet
(http://www.draware.dk/fileadmin/Tema/Logs/Kort_og_godt_om_log_management.pdf)
3. [Dokumentet om "Strudsemetoden"](#)
4. [Videoen "Kort og godt om Log Management"](#)
5. [Video om "Strudsemetoden"](#)