# SIEM – for små og mellemstore virksomheder

Indholdsfortegnelse

[SIEM – for små og mellemstore virksomheder 1](#_Toc41491364)

[Indledning 3](#_Toc41491365)

[Empiri 3](#_Toc41491366)

[Præsentation af problemstilling 4](#_Toc41491367)

[Hvad er SIEM? 4](#_Toc41491368)

[Hvorfor er SIEM en god løsning? 4](#_Toc41491369)

[Problemformulering 5](#_Toc41491370)

[Afgrænsning 6](#_Toc41491371)

[Tilgangsvinkeler 6](#_Toc41491372)

[Teori 6](#_Toc41491373)

[Projektbeskrivelsen 7](#_Toc41491374)

[Analyse 8](#_Toc41491375)

[Tænkt Case 8](#_Toc41491376)

[Planlægningsfasen 9](#_Toc41491377)

[Security Polices 9](#_Toc41491378)

[Sysmon 10](#_Toc41491379)

[Eksempel på vigtige event ID ‘er 10](#_Toc41491380)

[Hardware vs Skyen 11](#_Toc41491381)

[Netværk 12](#_Toc41491382)

[Hvor meget kan logges? 13](#_Toc41491383)

[Log og tidssynkronisering 13](#_Toc41491384)

[Sikkerheden på Log server / under overførsel af log data 13](#_Toc41491385)

[Hvor langtid skal log gemmes? 14](#_Toc41491386)

[Opsummering 14](#_Toc41491387)

[Konklusion 15](#_Toc41491388)

[Perspektivering 17](#_Toc41491389)

[Litteraturliste 18](#_Toc41491390)

[Ordliste 19](#_Toc41491391)

[Bilag 20](#_Toc41491392)

# Indledning

Hvorfor dette område?

Dette bachelorprojekt handler om de udfordringer der kan være når en virksomhed vil have SIEM bygget ind som en del af deres it-sikkerhed. har til formål at komme med nogle ideer til hvordan små og mellemstore virksomheder kan komme i gang med at lave analyse af deres logfiler, logfiler som der automatisk generes på største delen af de it-systemer som virksomhederne typisk bruger, men hos rigtig mange virksomheder ligger disse logfiler bare på serverne og bliver sjælden brugt.

SIEM er et overset område i mange virksomheder, men der begynder at komme mere fokus på det pga. Den øgede cybertrussel som der findes i dag.

En anden grund til at der kommer mere fokus på SIEM, er GDPR som til virksomheder kan give store bøder hvis ikke de passer godt på kundernes data, bøderne kan gå op til 4% af virksomhedens globale omsætning, så det er ikke små beløb vi snakker om.

Hvis man som virksomhed håndter kortsystemer til dankort og onlinebetalinger er der PCI-krav der pålægger at man har en SIEM løsning.

## Empiri

I rapporten vil der blive taget udgangspunkt i en tænkt case, og der vil blive gennemgået forskellige typer af problemstillinger med udgangspunkt i case’en.

Der tages udgangspunkt i Best Practice som er beskrevet af NIST

Samt i den undervisning vi har fået i faget SIEM på skolen.

# Præsentation af problemstilling

Skrive en halv til hel side om SIEM

Inden for it-sikkerhed, er der et område som er meget undervurderet, og som ikke har haft megen opmærksomhed når virksomheder skulle til at forbedre det. Mange tror at sikkerhed handler om firewall og antivirus, men hvis nogen kommer ind i ens netværk, så vil man måske slet ikke opdage det før det er for sent.

## Hvad er SIEM?

SIEM står for Security Event Information Management, og blev beskrevet første gang i 2005 af analysevirksomheden Gartner, SIEM er som løsning til opsamling af logfiler fra forskellige kilder, det kan være netværksudstyr, Windows og Linux server mv.

Det gælder både operativsystemet og for de services man har installeret oven på sin OS.

## Hvorfor er SIEM en god løsning?

Næsten alle it og netværkssystemer generer en masse logfiler, logfiler som mange steder bare ligger på de enkle enheder, og som kun kigges på meget lidt. Hvis man ikke har en SIEM løsning kan det være meget svært at

Der findes en del forskellige SIEM løsninger som man kan bruge, men i denne rapport tages der til dels udgangspunkt i de generelle ting man skal inddrage uanset hvilken SIEM løsning man vælger, og derudover så tager jeg udgangspunkt i ELK stack’en som består af Elastic Search, Logstash og Kibana.

Elasticsearch: Indeksere og gemmer

Logstash: Indsamler og parser logdata

Kibana: Visualiserer log data, gør brug af dashboards

Elastic har også lavet mulighed for machine learning men dog kun i betalingsudgaven af deres produkt.

## Problemformulering

De seneste år er It-sikkerhed blevet et fokusområde som flere og flere virksomheder tager alvorligt, især set i lyset af de virksomheder der rammes af Ransomware som Mærsk blev det i 2017 som endte med at koste Mærsk i omegnen af 2 milliarder kroner, en af de områder inden for it-sikkerhed som kommer til at skal være mere i fokus er SIEM. For hvordan kan man som mindre eller mellemstor virksomhed komme i gang med SIEM?

Jeg har arbejdet flere steder hvor man slet ikke har brugt nogen former for SIEM løsning, og med den viden jeg har tilegnet mig på studiet, har jeg fundet at dette område kunne være interessant at dykke nærmere ned i og belyse de problemstillinger som man vil komme ud for i planlægnings og implementationsfasen.

Der tages udgangspunkt i en case baseret tilgang til projektet.

1. **Hvordan kommer man i gang med SIEM (Elk Stack)**

Hvordan kommer man som lille eller en mellem stor virksomhed i gang med Elk stack’en? Hvor meget udstyr (servere mv.) skal der bruges? Hvilken software skal man bruge?

1. **Hvilke logs skal man gemme i sin SIEM løsning?**

Server og klienter generer mange logs, så hvilke logs skal man gemme? Hvilke server / klienter skal man gemme logs fra?

1. **Hvilke udfordringer kan man have i forhold til sikkerhed?**

Hvordan skal man forholde sig i forhold til sikkerhed, når man skal opsætte en log management system som Elastic Search?  
Hvordan sikres Log management systemet imod uvedkommende kan se logs og hvordan sikrer man imod at udefrakommende kan skrive eller slette logs inde fra ens netværk?

1. **Hvor langtid skal man gemme logs?**

Hor meget diskplads skal man påregne til opbevaring af logs eller hvor længe skal man gemme sine logs i?

1. **Hvor skal SIEM løsningen stå?**

Skal man have det til at stå̊ i egen serverrum, eller skal man bruge skyen? Hvilken sikkerhedsmæssige udfordringer kan der være med egen serverrum kontra Skyen?

## Afgrænsning

I henhold til overstående problemformulering, er det hensigten at afgrænse hvilke SIEM løsning man kunne vælge, jeg har valgt at tage udgangspunkt i Elastic Search da det er et meget brugt system, og der findes en open source-udgave, jeg er helt med på at der findes mange produkter så som Splunk, IBM Qradar. Men for at projektet ikke skulle blive for stort og uoverskueligt har jeg taget dette beviste valg at se på Elk stack’en sammen med den planlægningsfase som vil være forud.

SIEM er et stort område i sig selv, men det er de her ting jeg har fundet som kunne være rigtig interessant at få belyst i forhold til hvis man skal i gang med SIEM i sin virksomhed, der findes sikkert andre spørgsmål man kunne stille.

## Tilgangsvinkeler

Jeg har valgt at starte med at kigge på overblikket, når man som virksomhed skal i gang med SIEM, der tages i projektet også udgangspunkt i en tænkt case, hvor der beskrevet nogle af de problemstillinger som man som virksomhed vil kunne komme ud for når man skal i gang med SIEM.

så er man nødt til at få lavet en behovsanalyse først, hvilke systemer har man, hvilke logs kan man få adgang til der?

Nogen har i forvejen værktøjer som laver registrering af alle virksomhedens enheder, software og services som der drives, hvis man har dette, så vil det gøre arbejdet meget nemmere.

Ellers må man starte fra en ende.

## Teori

Der findes ikke megen teori på SIEM området.

Vil tage udgangspunkt i tre publikationer som er *Successful SIEM and Log*

*Management Strategies for Audit and Compliance* af *David Swift* fra SANS

Derudover vil jeg også tage uddrag og viden fra *Logning – en del af et*

*godt cyberforsvar* fra *Center for Cybersikkerhed* fra *2016*

Den sidste opslag er *Guide to Computer Security Log Management* af *Karen Kent*

*Murugiah Souppaya* fra *National Institute of Standards and Technology*

Jeg tager udover disse online publikationer udgangspunkt i den læring vi har fået af Kenneth i hans undervisning om SIEM.

# Projektbeskrivelsen

**Projektets titel:**

SIEM – for små og mellemstore virksomheder

Virksomhed: Deloitte

8000 Aarhus C

**Kontakt hos Deloitte**

Mikkel Rømer

**Navn og holdnummer**

Michael Mørch Madsen

Hold nummer

**Baggrund for projektet**

Projektet tager udgangspunkt i SIEM løsning baseret på ELK stack’en

**Forventet resultater**

Beskrive processen som man typisk skal igennem i forbindelse med opsætning af et SIEM miljø, herunder tanker omkring hvilke problemstillinger man kan komme ud for, og som man skal have løst før, og under processen med opbygning af SIEM miljø. Derunder er planen at bygge en vejledning som belyser de ting man skal tage højde for før og under opsætning af Elk stack (Elasticsearch Logstash Kibana)

Prototype af et Elk stack miljø som man kunne se i et lille format hos virksomheder

Vejledning til opsætning af et SIEM miljø.

# Analyse

I dette afsnit vil der blive kigget på hvordan man håndter disse udfordringer som virksomhed.

## Tænkt Case

En mindre virksomhed der arbejder inden for industriproduktion, har inden for det sidste år været ramt af Ransomware angreb, og har i den forbindelse besluttet at vil højne it sikkerheden, og har taget fat i en it sikkerhedskonsulent firma, virksomheden har valgt at højne sikkerheden på flere områder og herunder at få samlet logfiler fra alle virksomhedens it-systemer.

Virksomheden har et mindre netværk, og en Router / Firewall samt Windows 2008 server som kører som lokal domæne controller, virksomheden har desuden en lokal filserver og print server som bruges i det daglige bogholderi, derudover har virksomheden en server som kører økonomi system.

Virksomheden har backup løsning ude i byen hos en leverandør, og mail kører i Office365.

Der bruges også VPN forbindelse til arbejde hjemmefra for medarbejdere.

Hvordan kommer virksomheden i gang med at få implementeret SIEM i deres infrastruktur?

!Indsætning af Diagram her!

## Planlægningsfasen

Når man skal i gang med at kigge på SIEM som en sikkerhedsløsning, så kan det være meget godt at sætte sig ned og tænke lidt over hvad man gerne vil have ud af det?

Hvad vil man som virksomhed gerne have ud af SIEM?

Hvilke informationer kunne man godt tænke sig at få ud af ens virksomhed?

Hvilken logs og fra hvilken enheder kan og bør man få hivet logs ud?

Skal det bruges som led i en SOC hvor nogen sidder døgnet rundt og holder løbende øje?

Eller skal man blot gemme logs også tjekke det op en gang i mellem?

Start ud i det små, og her vil ens AD være et godt sted at starte.

Hvorfor er AD’et et godt sted at starte?

AD’et er i rigtig mange virksomheder grundstammen i deres brugerhåndtering, typisk så opretter man medarbejderen i AD’et og tildeler dem adgang til f.eks. mail system, grupper for de afdelinger / systemer som de skal have adgang til.

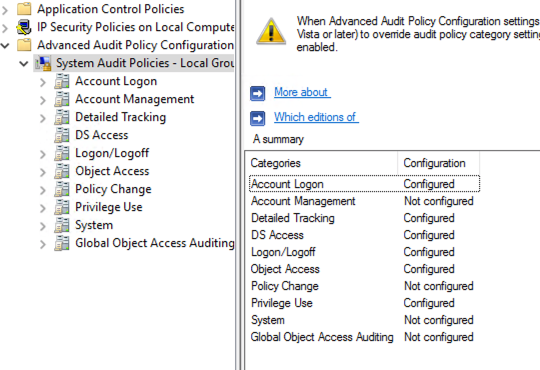
Hvordan ville et SIEM løsning kunne se ud?

AD’et har tilføjet x antal computer, en GPO (Group Policy Object) har fortalt hver enkel computer at de skal sende alle deres event logs til en WEF (Windows Event Forwarder) som har Winlogbeat kørende, og herfra kommer alle logs videre til Logstash som bruges til at kunne ensarte de log data som der kommer, man kan også via Logstash udtage de informationer som ikke er nødvendig så man får sparet på pladsen, fra Logstash bliver al logdata nu gemt videre i Elasticsearch, hvor der kan laves analyser mv.

## Security Polices

Der laves på AD’et en GPO som fortæller computere som er tilmeldt AD’et at de skal videresende alle logfilerne en lokal maskine som står som WEF (Windows Event Forwarder)

Der laves også en regel der fortæller computerne om hvilke typer event logs der skal gemmes, det ses der et eksempel af neden for på billedet.



Hvad vil man kunne se ud fra de logs i ens Dashboard baseret ud fra de regler som der er sat op?

Når en bruger f.eks. logger af, vil det i Event log dette ses som event id 4634

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

## Sysmon

Når man skal tage logs fra Windows maskiner er det en god ide at sætte sysmon op sammen med Winlogbeat. Her er et eksempel på hvad man kan se af informationer i eventloggen ud fra Sysmon.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

### Eksempel på vigtige event ID ‘er

Jeg har valgt i selve rapporten at komme med nogle eksempler på hvad jeg mener er vigtige Event id’er baseret ud fra Microsofts egen Best Practies.

|  |  |
| --- | --- |
| Event ID | Beskrivelse |
| 1102 | Audit log er blevet ryddet |
| 4624 | En konto er blevet logget på |
| 4625 | En konto kunne ikke logge på |
| 4672 | Særlige privilegier tildelt ny logon. |
| 4720 | En bruger er blevet oprettet |
|  |  |
|  |  |
|  |  |

I Windows operativsystemerne er eventloggen opdelt i forskellige event kategorier som man bør kigge på. Hvilke

## Hardware vs Skyen

Hvilke krav skal der stilles til de servere som et SIEM platform vil bestå af?

Skal man bruge egne serverer eller stille det i skyen og derved uploade logs løbende?

Hvilke risikoer er der ved det?

Rackserver eller i Skyen hos Amazon/Google Cloud eller hos Azure bare for at nævne nogen, men hvad er fordelene ved at have det i egen serverrum kontra at lægge SIEM løsningen op i skyen?

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

Hvilken krav stilles der til Hardware og operativsystem for at køre et ELK stack miljø?

Elastic anbefaler at man inden man starter sørger for

<https://www.elastic.co/support/matrix>

## Netværk

Med udgangspunkt i case’en, så er AD’et en af de centrale elementer som ville være oplagt at starte ud med at sætte en Windows Event Forwarding op som vil være den maskine som modtager logs fra alle windows maskinerne og sender det videre til Logstash hvor man kan lave aggration, og filtering af de logdata som kommer ind inden de sendes til elastic search.

Isolering af SIEM miljøet i sit eget lukket netværk for at sikre at nogen fremmede ude fra kan komme ind og slette eller manipulerer med logdata,

## Hvor meget kan logges?

Netværksprodukter – Router, Firewall, og switche, IP-camera, SAN og andre storage typer.

Det er normalt at operativsystemer som Windows, Linux og macOS har support for event logging eller kører via syslog, rigtig mange softwareprogrammer har også support for en eller anden form for audit logning som man kan gøre brug af.

Office365 har audit logs ved hjælp af Office 365 Advanced Threat Protection

Servere og klienter / Operativsystemer

Diverse Services / Skyen Office365

## Log og tidssynkronisering

En korrekt tid er en vigtig del af SIEM, hvis en forbrydelse sker i ens virksomhed, så er det afgørende at man kan se den korrekte tid for hvornår det er sket, hvis det skal kunne bruges som bevismateriale ved en domstol, det er også nødvendigt at al ens udstyr har den samme tid da det ellers kan være besværligt for ikke at sige umuligt at skulle finde spor på tværs af ens systemer.

## Sikkerheden på Log server / under overførsel af log data

CIA-triaden

fortrolighed, dataintegritet og tilgængelighed.

Login audit på SIEM systemet

Begrænsning af hvem og hvor mange som kan tilgå logdata.

Kryptering af filsystemet

## Hvor langtid skal log gemmes?

Man kan enten vælge at kigge på hvor stor mænge data man har plads til at gemme eller vælge at gemme ud fra tidsperiode, rigtig mange vil vælge at gemme det i en given tidsperiode

Hvor meget fylder en event Log?

Hvor meget fylder en syslog fil?

Er der en best practices for det?

Hvis man får en stor mængde data, kan det være en god ide at gøre brug af Grok og parseing som man gør i Logstash inden det bliver gemt i Elasticsearch

Udregning af Events pr sekund (EPS) udregnes ved at finde antallet af peaks pr dag samt den normale antal events pr sekund.

## Opsummering

Lad os opsummere hvad der er gennemgået i analysen af projektet.

I Rapporten har jeg kommet ind på de udfordringer som virksomhederne står med når de skal i gang med SIEM løsninger, det inddrager en del beslutninger, og overvejelser men jeg vil mene at fordelen overskyder langt ulemperne og udfordringer ved det, man får en masse nyttige data som man kan arbejde videre ud fra.

# Konklusion

Hvis jeg skal tage det fra starten til enden af de ting jeg mener man skal gøre som virksomhed / it administrator / systemadministrator i forbindelse med opsætning af et SIEM miljø bør man starte ud i det små, start med de at høste de nemme og lavest hængende frugter.

Det skal forståes på den måde at man hvis virksomheden har et miljø bestående af Microsoft produkter som nok hovedparten af virksomheder herhjemme har så skal man starte med sit Domain Controller.

Lav en plan og prioritere hvilke servere og klienter som er vigtigst og kritisk i din virksomhed, det er umuligt hvis man har et større setup af it-systemer at få en god og effektiv SIEM løsning.

Min anbefaling vil være at man vælger at sætte en GPO op som fortæller alle maskiner der er tilmeldt ens AD hvilken security policy der skal slåes til og fra.

Det gør det også nemmere at

# Perspektivering

# Litteraturliste

Reference til de event id’er som Winlogbeat transformerer i security modulet.

https://www.elastic.co/guide/en/beats/winlogbeat/7.7/winlogbeat-module-security.html

Microsoft Security Monitoring Recommendations

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4703#security-monitoring-recommendations

Basic security audit polices

https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies

# Ordliste

Her kan du se kort beskrivelse af forkortelser der er brugt i rapporten.

# Bilag

Manual for installering af Elk stack, manualen er delt op i nogle forskellige steps som man skal igennem før og under installering og opsætning af Elk stack’en.

Forberedelse til installation og opsætning af Elk stack

Step 1 - Forberedelse af server

Step 2 - Installering Java

Step 3 - Installering og opsætning af Elastic Search

Konfig til elasticsearch

path.data: /var/lib/elasticsearch

path.logs: /var/log/elasticsearch

network.host: 10.64.110.15

http.port: 9200

discovery.type: single-node

xpack.security.enabled: true

xpack.security.transport.ssl.enabled: true

xpack.security.transport.ssl.key: certs/siem.key

xpack.security.transport.ssl.certificate: certs/siem.crt

xpack.security.transport.ssl.certificate\_authorities: [ "certs/ca.crt" ]

xpack.security.http.ssl.enabled: true

xpack.security.http.ssl.key: certs/siem.key

xpack.security.http.ssl.certificate: certs/siem.crt

xpack.security.http.ssl.certificate\_authorities: certs/ca.crt

Step 4 - Installering og opsætning af Logstash

Step 5 - Installering og opsætning af Kibana

Konfig til Kibana

server.port: 5601

server.host: "10.64.110.15"

server.name: "siem.cgdev.dk"

elasticsearch.hosts: ["https://10.64.110.15:9200"]

elasticsearch.username: "kibana"

elasticsearch.password: "A4n9XLtHgV"

server.ssl.enabled: true

server.ssl.certificate: /etc/kibana/certs/siem.crt

server.ssl.key: /etc/kibana/certs/siem.key

elasticsearch.ssl.certificateAuthorities: [ "/etc/kibana/certs/ca.crt" ]

elasticsearch.ssl.verificationMode: 'full'

Step 6 – Opsætning af sikkerhed mellem Kibana og Elasticsearch

Lave certifikatter

root@scw-wizardly-joliot:/usr/share/elasticsearch# bin/elasticsearch-certutil cert --keep-ca-key ca --pem --in /root/instance.yml --out /root/certs/certs.zip

Step 7 - Installering og opsætning af Beats på "clineter"

Audit Beat

Winlogbeat

Konfigurationen af Windows AD