SOC
Security Operations Center

Lenny Hansson
Networkforensic.dk

Version 1.0 – FEB 2020

TLP: WHITE

Mange kan sige ordet ”SOC” men hvad dækker det over ?

Flere virksomheder siger de har en….Men har de nu det ?

Forord

IT sikkerhed har i dag en høj prioritet for de fleste virksomheder. Mange høj prioritets sikkerheds hændelser er sket i mange multinationale virksomheder udenlandske som Danske. En samlet række af hændelser har bevist at alle virksomheder står overfor disse forskellige trusler som IT medbringer.

Virksomheder søger derfor metoder til hvordan de bedst kan beskytte sig imod disse og reducerer "impact" af en given kompromittering. Det er generelt opfattet at det ikke længere er opfattelsen af om man bliver kompromitteret men mere om hvornår det vil ske.

God IT sikkerhed og sikkerheds kontroller kan gå langt imod at forhindre brud og dermed Incidents. Modstandernes taktikker og værktøjer er i en konstant udvikling og bliver brugt i avanceret malware som eks WannaCry og Notpetya som bl.a. ramte Mærsk. Disse angreb viser også at det ikke altid er muligt at forudsige forud i tiden hvordan man bliver ramt.

Derfor er virksomheder begyndt at tune sikkerheden imod en reaktiv mulighed og dette kan opnås igennem opbygningen af en SOC (Security Operations Center)

Dette dokument vil give et overblik over en SOC og beskrive roller og ansvar sammen med de overvejelser man bør gøre for om en SOC skal være intern eller ekstern, sammen med nogle spørgsmål man bør stille for at være sikker på om en SOC giver de nødvendige garantier for om denne opererer på det ønsket niveau.

Jeg vil drage egne erfaringer ind hvor jeg typisk ser det går galt under opbygninger af SOC enheder. Disse er baseret på mere en 10 års erfaringer med opbygninger af SAC/SOC/CERT enheder. Disse vil fremstå som bemærkninger.

1.1 Hvad er en SOC

En SOC er ansvarlig for at monitorere netværket på en given virksomhed for opståede angreb og trusler samt bringe fokus på disse overfor de rette personer i virksomheden og derved mindske effekten af et angreb eller at forbedre sikkerheden for den enkelte virksomhed så hurtigt som muligt.

En SOC består af et team af meget veluddannet og højt specialiserede IT kyndige personer, som arbejder omkring meget veldefinerede processer og supporteret af en høj grad Threat intelligence teknologier.

Et problem med at opsætte en SOC er at sikkerhed ofte ikke producerer nogen synlig effekt. Men et godt tegn på at sikkerhed virker, er at der ikke opstår nogen sikkerheds relaterede hændelser. Man skal betragte en SOC enhed på lidt samme måde som en brandstation. Hvis der ikke er nogen ildebrand hver dag betyder det ikke at man ikke har brug for den, da en ildebrand altid kan opstå i morgen.

I den anden ende at spektrummet findes "unknown unknowns". Det er former for angreb som foregår og ikke bliver opdaget, grundet manglende Threat intelligence eller fordi angriberne bruger metodikker der ligger uden for hvad den pågældende virksomhed kan opdage. Nogen kalder dette for "avancerede angrebs metodikker" hvilket de i virkeligheden sjældent er. Det er derfor vigtigt at en SOC forbliver ved med at have

træning og investeringer for at sikre de bedste muligheder for at kunne opdage de nyeste former for angreb.

Yderligere skal man skal "**bringe en SOC i stand til at kunne efterforske i eget net og infrastruktur"** Som er et af de mest vigtigste elementer i en SOC. Ekstern vendte SOC enheder kan meget sjældent dette, på kunde net. Tit skyldes dette manglende implementeret teknologier, samt en "MIS TRUST" fordi dette ville kræve at en SOC skal have fuld adgang til systemer som virksomheden ejer, herunder også til direktørens PC.

Såfremt en SOC eks. kun har adgang til netværkslogning, så efterlader det store huller i muligheden for at kunne validere alerts fra systemer. Her vil man mangle eks. Host logs (Se pkt 5.3)

Bemærkning: Det er min klare erfaring at man er godt på vej såfremt en virksomhed er i gang med implementeringen af CIS20. En succes for en SOC bliver nemmere såfremt man har forståelse for denne.

Yderligere kan man ved indkøb af ekstern SOC ydelser spørge ind til leverandørens implementering af bl.a. CIS20 kontroller i deres eget net. Såfremt leverandøren ikke har styr på disse kontroller, kan det være en af årsagerne til man bør overveje en anden leverandør. Yderligere kan man sjældent nøjes med at kun tilkøbe et SIEM system som nogen vil kigge på. Fordi man hele tiden vil blive mødt med at alerts skal valideres. Dette vil hele tiden falde tilbage på den pågældende virksomhed, og som tit ender i et sort hul, netop fordi den pågældende virksomhed ikke har personale til at validere disse alerts.

Man bør desuden forholde sig til antallet af ydelser en SOC yder i forhold til hvor meget personale der besætter en SOC. Yder en SOC alt for mange ydelser kan dette være tydelige tegen på at der bliver givet for lidt fokus til forskellige opgaver og analytiker er dagligt overbebyrdet. Dette er væsentligt når incidents opstår og derved ikke kan få den nødvendige fokus.

1.2 Hvad er en SOC's rolle

Dag til dag aktiviteter i en SOC er en konstant overvågning at alerts og undersøgelse af disse i dybden. Derudover er der stor kommunikation med team medlemmer og kunder.

En overordnet beskrivelse er er at en SOC arbejder målrettet og dedikeret for et kende til de nye trusler samtidigt med at man arbejder med risici og incident håndtering. Dette skal ske samtidigt med at man holder sig på linje med en kundes ønsker omkring deres ønskede risiko niveau.

Det er vigtigt at man har gjort sig det klart hvorfor man vil have en SOC, en SOC ofte er en brik i et meget større maskineri, og mens det er sjovt for en SOC at finde det næste store incident, så er målet at tjene forretningen. Det overordnede mål for en SOC er at bevare forretningens kontinuiteten.

SOC'en skal sammen med andre teams beskytte forretningen, og ud fra et sikkerheds perspektiv er det forretningens funktionalitet og data som er i højeste fokus. Dette skal gå forud for alle beslutninger for hvad en SOC vil og ikke vil.

1.3 Opbygningen af en SOC

Med en SOC's rolle i fokus så er næste step på hvordan man egentlig skal opbygge en SOC. Så er første mål hvad SOC'en skal og få dette på linje med hvad forretningen ønsker. Der skal ligge en klar strategi med klare mål fra forskellige afdelinger samt support fra ledelsen.

Det er vigtigt at kunderne prioriteres efter hvem der er vigtigst, således at der i tilfælde incidents kan prioriteres mellem kunderne. Ligeledes er det essentielt at der udpeges kritiske assets/infrastruktur for hver enkelt kunde, således at der kan etableres et overvågnings mæssig fokus for hver enkelt kunde. Kritiske assets/infrastruktur bør udvælges ud fra en risikovurdering/betragtning. Samt opbakning fra senior ledelse, dette er yderst vigtig hvis SOC'ens mission skal lykkedes, og skal sikre at alle forstår hvilken retning man skal bevæge sig i og hvorfor.

Selvom meget skal besluttes i starten er disse beslutninger IKKE en engangs aktivitet. En succesfuld SOC gennemgår valideringer og tilpasninger hen over tid. Vækst og ændringer i en organisation skal der planlægges for i en SOC. Som resultat skal en SOC tilpasse sig de nødvendige ændringer og tilpasse sig de nye trussels billeder der opstår. Det er vigtigt at man anerkender at eksisterende kontroller med tiden bliver mindre effektive, da angreb kontinuerligt finder nye måder hvorpå de eksisterende kontroller kan "bypasses". Som et resultat af dette SKAL en SOC hele tiden tilpasse sig nye generationer og typer af angreb.

1.4 Mennesker processer og teknologi

Et "White Paper" skrevet af SANS institute beskriver en SOC som et samarbejde via kommunikation og funktioner (mennesker) . Uanset sikkerheds produkter (teknologi) og forskellige processer (Processer) Samspillet imellem disse tre komponenter er hjørnestenen for en god SOC.

Alle komponenter skal afbalanceres i samarbejdet og manglende komponenter vil give væsentlig sikkerheds hul i muligheden for at opdage trusler. Når man opsætter en SOC, så kan man ofte blive afledt af at producenter lover mere end de kan holde. Uanset hvad der vælges kan det ikke stå alene uden mennesker og processer. Det er kritisk at man opnår basale muligheder for overvågning før man påbegynder avancerede analyser og overvågning (CIS20). Man skal bruge tid på at opbygge de basale nødvendigheder før de avancerede afprøves.

En anden måde at beskrive en SOC med succes er at den skal bygge på et stærkt fundament med veldesignet processer. Stærk governance, veluddannet personale og et konstant "drive" for at være på forkant med seneste Threat Intelligence.

1.5 Relationer med kunder

Alle SOC enheder uanset om de er interne eller tilbudt som en MMS (Managed Security Service) vil have kunder de skal rapportere til. Det er SOC'ens opgave at kontakte kunder og beskytte deres assets.

Gode relationer med kunder er yderst nødvendigt i tilfælde af incidents og efterforskninger samt muligheder for at rapportere sikkert til kunder. For alle kunder er det altid yderst dårlige nyheder som en SOC kommer med. Det betyder at MEGET kritisk information skal overdrages til kunder som de skal

håndtere. Man skal ikke antage at en kunde er klar til at lytte til en SOC om alle de kritiske ting som skal håndteres. Det er derfor vigtig med systemer i en SOC hvorved denne type information kan overdrages med mindst mulig adgang fra andre.

Dette kræver at der eksempelvis bliver opsat separate sagshåndterings systemer, mail system, mulighed for krypteret mails, samt dokumentations til brug for en SOC. Det er ikke en god ide at benytte allerede indterne sysemer som måtte være en del af en organisation for at "cutte en corners" og blive hurtigere klar til eks salg. Dette skyldes at dem en SOC skal hjælpe som i tilfælde af en indtern SOC, kunne være deres egen virksomhed som var kompromitteret eller personale var under efterforskning. Så hjælper det ikke meget at alle systemer som en SOC skal benytte var kompromitteret eller utilgængelige.

Bemærkning: Jeg har set meget tit at SOC enheder ikke kan finde ud af at klassificere informationer ud fra TLP principperne. Dette skyldes manglende træning og forståelse for hvordan information deles.

2.0 Mennesker

Et af de vigtigste aspekter man skal overveje i enhver SOC er mennesker. Det menneskelige element er ofte undervurderet og Alerts er meningsløse uden de kan blive vurderet og oversat til brugbar Threat intelligence som der kan blive handlet på. Det er her mennesker som arbejder i en SOC bliver vigtige.

Ansættelser af mennesker og sørge for de bliver ved med at have et ønske om at være en del af en SOC er ofte en udfordring. Det er fordi kompetencer og kvaliteter ofte er svære at læse ud fra et CV eller en job beskrivelse.

De kompetencer der er brug for i en SOC er ofte svære at skrive ned og dermed også svære at "forklare" via et stillingsopslag – Det er derfor ikke altid indlysende for de som ansætter, hvad de rigtige folk er for nogle. Analytikere skal, ud over de faglige kompetencer der kan læses på et CV, for eksempel være naturligt nysgerrige mennesker, som kan spotte mønstre i store mængder af data.

Det vil også være en naturlig del såfremt en SOC ønsker at være bemandet 24/7 at flere roller kan være afhængige af skiftehold og at en eller flere af disse roller vil være forbundet med tilkald, hvilket igen stiller store krav til ansættelsen og sammensætningen af mennesker i en SOC.

I følge Hewlett Packard (HP) vil en minimums fungerende SOC kræve 10 analytikere. Skiftehold er bedst udført med at hver analytiker arbejder 12 timer pr skift. Minimum 2 analytikere skal sidde på skift samtidigt. Derudover bør der være 1 eller flere level 2 analytikere med overlappende skift der kan overlappe de forskellige skift, således at kan fravær og sygdom dækkes ind under disse level 2 analytikere.

Globalt set er der mangel på analytikere herunder uddannede analytikere til SOC enheder. Derfor skifter mange ledere fokus til teknologi som firewalls og IPS systemer der kan forhindre angreb direkte. Men dette er kun de basale angreb og der er stigende brug for analytikere der er i stand til at lægge de mere avancered angreb i graven.

Som beskrevet af HP så er den store udfordring af finde de rigtige mennesker, og den rigtige bemanding er ofte sværd at opnå.

Analytikere såvel som ledere værende den daglige manager eller senior management skal fuldt ud kende til en SOC's mission, samt strategi, da en effektiv ledelse har en enormt betydning for en SOC.

2.1 Analytikere og teknisk stab

Størstedelen af medarbejderne i en SOC vil være analytikere og teknisk stab. Det er medarbejderne i SOC'en der håndterer daglige alerts, laver tickets, og overvåger trafik der flyder ind. De nøjagtige roller for medarbejderne i en SOC, kan inddeles i følgende 3 kategorier.

Level 1 (Tier one analyst)
Dette er junior analytikeren. Det er typisk personale der er nye inden for Cyber Security industri. Der opgaver er typisk at besvare kundekald, reagere på alerts og bestemme den rigtige "action" ved en given alert. De vil typisk blive meget erfarne i at reagere på de fleste alerts. Typisk vil der i 24/7 enheder også være en del skifteholdsarbejde i denne gruppe.

Level 2 (Tier two analyst)
Dette er de mere krævende tickets der skal håndteres. Såfremt Level 1 ikke kan besvare en ticket går den til Level 2. Denne gruppe består typisk af medarbejdere der har arbejdet et par år som Level 1 og som gennem løbende efteruddannelse udvikles til Level 2.

Level 2 dækker også en ledende rolle på det pågældende skift. Dette dækker også over at der bliver overdraget opgaver til næste skift som er igangværende.

Subject Matter Expert (SME)
Dette er typisk den mest erfarne analytiker der har speciel viden inden for vigtige områder, som er påkrævet i den pågældende SOC. Det kan være opgaver som forensic, network forensic, reverse engineering og malware analyser, Threat intelligence, hunters, SIEM engineers og indicent responders.

2.2 Management

Det overordnede ansvar for en SOC vil falde på SOC manageren som vil være indgangsvinklen hvis incidents skal eskaleres. Men det inkluderer også virksomheds management og support til resten af teamet samt planlægning af vækst og hvilke teknologier der giver mening. Dette er ofte i tæt samarbejde med analytikere grundet at SOC manageren ikke nødvendigvis har den nødvendige tekniske viden som også er nødvendig når der skal træffes beslutninger.

Det er vigtigt at en SOC manager har tillid til sit Team og omvendt ellers vil teamet ikke fungerer.

Bemærkning: Det er ofte set i Danmark at en SOC manager deler opgaver som eks daglig leder af en hel SOC og derved også sidder med andre typer personale ansvar, møder uden for SOC mm. Dette giver

yderst dårlig ledelse i forhold til incident håndteringer og fokus på daglige incidents, og som burde være der en SOC manager skal have sin fokus.

Ved indkøb af eksterne SOC ydelser er dette et klart område man kan spørge ind til. Det vil typisk give mange huller i incident håndteringer.

2.3 Senior/board level support

Det ses meget ofte at der er en undervurderet vital support fra den øverste ledelse (Senior management) specielt fra board level. Uden denne support er det sandsynligt at en SOC ikke kan opfylde sin mission. Senior management skal vise at virksomheden supporterer det højest level af sikkerhed og give en SOC autoritet til at gennemføre vigtige undersøgelser og bidrage til at en SOC bringes i stand til at kunne efterforske i eget net.

Senior management skal udvikle en klar forretnings strategi for sikkerhed og bistå denne udvikling der dækker , ”prevention” ”detection” og ”response” baseret på ønskede teknologier fra en SOC.

2.4 Træning og fremskridt

Som nævnt tidligere er det svært at tiltrække og fastholde ressourcer i dag da hele industrien mangler folk med de rette kompetencer målrettet til en SOC. Yderligere er det besværligt at bevare dem. Så det vil være vigtigt at have et roadmap klar til alle nye medarbejdere således at de kan blive uddannet i den rolle de skal udfylde.

Et godt tilrettelagt uddannelsesforløb hjælper i høj grad på at bevare personalet. Dette kan bindes op på kontrakter således at virksomhedens ressourcer ikke bliver spildt. Dette kan også mindske stress og ”Alarm fatigue” , da personalet føler sig bedre rustet til opgaverne.

Et veltilrettelagt trænings- og uddannelsesforløb bidrager til at personalet føler at de har en fremtid i. Personalet kan også følge med i den timeline der er lagt for dem og bl.a. også identificere svage sider der skal arbejdes med.

Nogen teams benytter eksempelvis tilrettelagte uddannelsesforløb, indkøb af hardware, software mm. Dette gør at man direkte ved hvad omkostningen er ved nyansættelser, samt hvornår en nyansat kan være klar til at indgå i et SOC team med de forventet kompetencer.

Alarm fatique
https://en.wikipedia.org/wiki/Alarm_fatigue

3. Processer

At have de rigtige mennesker er vigtigt for en SOC, men det er mindst ligeså vigtigt at de mennesker ved hvad de skal lave og hvordan de skal lave det. Dette kræver at der er nogle vel definerede processer så man kan kontrollere at ting bliver gjort korrekt og at SOC'en arbejder effektivt. I forhold til områder som compliance og jura er det særdeles vigtigt med gode og præcise processer.

Følgende er emner eksempler på hvad processer og procedure skal omhandle

- Monitorering
- Kontakt(hvordan kontakter vi kunder/andre afdelinger)
- Eskalation af sager
- Vagt overlevering
- Incident logning/dokumentering
- Compliance monitorering
- Rapporter
- Oprettelse af dashboards
- Incident investigation

Bemærkning: Her falder rigtig mange nye SOC enheder totalt igennem. Dette er en klar ting en kommende SOC kunde skal og bør spørge ind til. Disse punkter skal også være 100% på plads for man eks. Kan begynde at sælge ydelser som en SOC.

3.1 Hvordan får vi de rigtige processer og procedure

At måle succes er ikke nemt i en SOC. Mangel på alarmer og incidents kan skyldes at alt er sikkert og sikkerhedssystemerne er effektive eller at alt er i så dårlig stand at de ikke bliver opdaget.

Vi skal finde en måde at sikre vi har den rigtige modenhed samt at vores processer og procedure passer til vores forretningens behov, der er en lang række standarder der kan hjælpe med dette.

Bemærkning: Typisk sætter mange SOC managers analytiker til at udfærdige dette arbejde, hvilket det ikke bør være.

3.2 KPI'er/SLA'er

Key Performance Indicator/Kontrol Punkt indikatorer(KPI) er en række aftalte måle punkter der skal bruges til at vurdere ydeevnen inde for en given aktivitet. Nøje valgte KPI'er lan bruges til at måle om SOC'en yder som den skal.

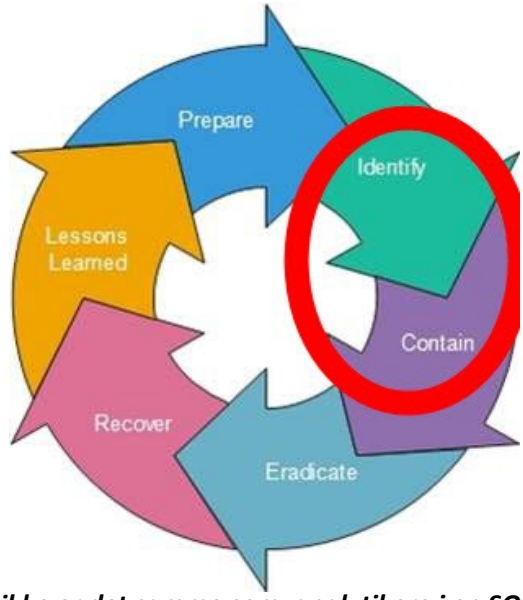
Service Level Agreements(SLA) er officielle forpligtelser som et firma skal overholde i en kontrakt med en kunde, det er typisk noget med oppe tid eller hvor lang tid det må tage at svare på en incident eller andre kommunikations tider.

Det er vigtigt at vi har fornuftige KPI'er så vi måler på det rigtige og dermed får den rette adfærd når det kommer til opgave løsning. Ligeså med SLA'er, de skal være på et niveau som kunden er glad for og SOC'en kan leve op til.

3.3 Håndtering af incidents

Når et incident er fundet og bekræftet, skal det overleveres til de rette response teams. Disse teams vil typiske sidde i flere steder af organisationen og består ikke kun af SOC folk. Et response teams opgave er at dokumentere og rydde op i et incident så man kan få forretningen oppe og køre igen så hurtigt som muligt, men også finde en "root cause" så man kan undgå det i fremtiden.

En SOC's vigtigste produkt, er at kunne beskrive og anskueliggøre hvordan lingende tilfælde i fremtiden kan forhindres også kaldet for "Leassons Learned". Hvorimod de i deres daglige arbejde vil befinde sig inden for "Identify" og "Contain" i hovedparten af deres opgaver.



Bemærk at et response teams ikke er det samme som analytikere i en SOC. Et response team kræver helt andre typer af kompetencer, træning og meget af det, metodikker, toolsets mm. Ønsker man et response team er dette en separate opbygning fra en SOC. Et respons team arbejder inde for området, for "Eradicate" ,"Recover" og bidrager til "Leassons Learned" Trækker man SOC personale ud som et del af response teams, hvem passer så SOC enheden ?

3.4 Metrikker

Der er et behov for at måle hvor effektivt SOC'en arbejder en Metrik kunne være hvor hurtigt en incident bliver opdaget, adresseret og løst. Dette kan være med til at anskueliggøre om der er behov for mere personale eller eksempelvis ny teknologi.

3.5 Use cases

Enhver SOC har kunder om det så er interne eller eksterne kunder, så vil kunderne have ting de er mere bekymrede over end andre. Samtidig har SOC'en også et begrænset antal ressourcer og kan umuligt analysere alle mails, alle netværks pakker og logs som findes i kundernes infrastruktur. Det er derfor vigtigt at SOC'en ved hvad der er vigtigst for kunden, så man kan målrette sine regler, dashboards, alarmer og filtre til kundens ønsker. Dette sker typisk på en workshop man holder sammen med kunden eller egen organisation.

-

3.6 Analyse

For at SOC'en er i stand til at fungere optimalt skal alle vide hvordan man håndterer en given situation og dokumenterer de rigtige informationer. Dette skal være med til at alle arbejder ens og at de rigtige informationer bliver overleveret ved vagtskifte. Dette skal tilsikre at vigtig information ikke bliver glemt, overset eller efterladt.

Metrikker til hvordan triage foretages bør derfor være på plads inden en SOC overhovedt kan arbejde efter hensigten for en SOC.

Bemærkning: Jeg har mage gange set at analytikker ikke kan videre give oplysninger til efterfølgende hold. Simplet hen fordi der ikke har fundet træning sted i hvordan overdragelser bør blive foretaget eller hvilket toolsets der skal benyttes til det. Jeg har set videregivelse af oplysninger via cloud løsninger som eks. Office365 med virkelig vigtig IOC informationer og givne angreb.

3.7 Andre frameworks

Ud over ITIL og COBIT er der også andre frameworks man med fordel kan se på. En populær model inden for incident response processer er DOE/CIAC som blandt andet indeholder de 6 incident stadier: Preparation, identification, containtment, eradication, recovery og lessons learned. Derudover er der også NIST Computer Security Incident Handling Guide.

Det er også en god ide at kører nogle "dry runs" så man ved hvordan SOC'en håndterer en presset situation og at man samtidig tester sine værktøjer. Dette kan gøres ved at bruge et såkaldt "red team" eller "purple team" så man kan trykprøve SOC'en under kontrollerede forhold. Bemærk på de første af disse øvelser må man forvente et dårligt resultat som dog hurtigt skulle blive bedre med mere træning og tilpasning af toolsets.

4 Teknologier

En anden vigtig ting for at en SOC kan få succes er de rigtige teknologier. Selv om der er en fare for at have et overforbrug at teknologier, så er der visse ting en SOC ikke kan undvære.

Disse teknologier vil variere ud fra SOC'ens opgaver, men de kan være alt fra store dyre tekniske komplekse løsninger til små open source løsninger som er billige eller gratis.

Når man skal finde de teknologier der skal benyttes i en SOC er det vigtigt at have fokus på at de mennesker der skal benytte dem først og dernæst de opgaver de skal løse og ikke omvendt. Og selvom der er mange forskellige teknologier på markedet så er der nogle få nøgle teknologier som en SOC ofte skal have.

Bemærk - Det er set i mange tilfælde at under opbygningen af en SOC , at der kommer et pres fra salgs folk med ønsker at at netop benytte deres teknologi. Dette er en farlig vej at bevæge sig ind på, da der typisk så vil blive anvendt utilstrækkelige ikke korrekte teknologier. Ønsket for salgs folk er ofte en forhøjet bonus salg til egen fordel og ikke for en SOC's fordel. Dette giver ofte en forsinket process i opbygnings fasen af en SOC.

Typisk ved salg af SOC ydelser når der er valgt en ekstern SOC , så ser jeg ofte at nogen gerne vil have kommercielle løsninger på hylden. Hver eneste gang jeg har set dette er det næsten umuligt at sælge viderer grundet for høje priser og den eneste der tjener på løsningen er typisk kun producenten.

4.1 SIEM

Security Information and Event Management System (SIEM) er en af de mest essentielle stykker værktøj der er i en SOC's værktøjskasse. Det bruges til at indsamle data fra en lang række kilder og sensorer. Det gør en analytiker i stand til at have et samlet overblik over samtlige data på tværs af systemer samt at holde øje med trends.

Men SIEMs skal tunes og justeres hele tiden i takt med kundernes infrastruktur vokser og ændre sig. For at være effektive. Som alle andre sikkerheds produkter er det kun så godt som de mennesker der vedligeholder og bruger det.

Bemærk. Ved valg af SIEM løsninger skal man være meget opmærksom på det rigtige valg af SIEM. Det er ofte mere nødvendigt at søgninger i store mængder date kan gøres hurtigt frem for mere "sexet" løsninger. Output / input fra TXT baseret IOC'er ofte meget vigtig for nemt at kunne få dette ind og ud til andre systemer og tools.

Database struktur skal være velegnet til netop logs fra forskellige systemer samt vigtigheden at muligheden for at kunne skalere løsningen uden dette vælter budgetter i en SOC vægter meget højt. Data base struktur skal kunne rumme udfasning af gamle logs til eks "cold storage" uden det bør kræve genindlæsninger til ny infrastruktur for at kunne læse ældre logs.

Der findes mange SIEM systemer som er baseret på ældre tankegange i database struktur, disse bør man undgå.

4.2 Dashboards

En SOC har behov for et system der visualisere alt den information der kommer ind. I bund og grund er det lige meget hvilket system det er, så længe det kan levere korrekt information rettidigt og stabilt. Typisk er det et SIEM eller log management system. Dog bør alle SOC ansatte selv kunne oprette de nødvendige dashboards efter behov.

Bemærk: Det ofte er vigtig med trænet personale der overvåger SIEM systemer dagligt tilstand mm. Dette personale er typisk ikke eksisterende i mange mindre SOC enheder. Resultatet er ofte at SIEM systemer der går ned grundet manglende daglig overvågning og daglig vedligehold. Det betyder kritiske tab af logs. Dette bør man især være fokuseret på såfremt man tilkøber SOC ydelser fra en ekstern leverandør. Her bør kunden forlange at alerts far overvågnings systemer om dens helbred bliver sendt direkte til kunden selv.

4.3 Ticket system

Ligegyldigt om en SOC har interne eller eksterne kunder, så er det vigtigt at SOC'en har et sted at dokumentere fremgangen i et incident, dette er vigtigt både for kvaliteten af arbejdet, men også fordi det giver kunden et sted at følge med i sagen (hvis man ønsker at åbne Ticket systemet for kunder).

Et Ticket system er uundværligt og er med til at sikre at intet bliver overset samt at danne en tidslinje for et givent incident. Men det kan også give indsigt og sindsro til en kunde. Det kan også hjælpe til med at fremtidige sager bliver løst hurtigere.

"Hastighed er vigtigt, men ikke på bekostning af kvalitet" Disse systemer bør ikke være en del af andre indterne systemer og bør blive beholdt adskilt, alene på baggrund af fortrolighed og integritet.

Bemærkning: Det er set at en SOC slet ikke har et ticket system eller dette ligger på delte cloud løsninger. Dette bør blive helt undgået. Jeg har set SOC enheder der benytter cloud løsninger på delte systemer hvor man ligger fortrolig information i ukrypteret stand. Det er helt NO GO.

4.4 Automated assessment tool

Det kan være svært at måle en SOC's ydeevne uden at simulere kendte angreb man kan køre igen og igen. Et Automated assessment tool som f.eks. SOCAlive, Metasploit, CANVAS eller Core IMPACT bruges til at sende simuleret angreb over netværket eller logs fra en PC. Man kan så måle hvor lang tid det tager SOC'en at finde og fjerne "truslen" Her bør man dog tilpasse værktøjer til de ønsket valideringer.

Bemærkning: Ved tilkøb at eksterne SOC ydelser bør kunder teste hvor hurtigt en SOC reagere på alerts der opstår fra deres eget net. Ligger disse uden for aftalte rammer bør disse blive tilrettet. Yderligere bør virksomheder fortage test med forskellige intervaller som kunden selv fastsætter, kun for a være sikker på at der til stadighed bliver levet op til de aftalte rammer.

4.5 CMDB

”Know your assets” Hvis man ikke kender infrastrukturen så kan man ikke beskytte den effektivt. Når man skal monitorere en infrastruktur er det ekstremt vigtigt at man ved hvad normalbilledet er. Dette kan man kun hvis man ved hvilke servere og protokoller der findes. Dette gør det hurtigere og nemmere at finde ud af om det man ser også burde være der eller ej. En CMDB (Configuration Management DataBase) er et uundværligt værktøj til hurtigt at vurdere om noget er normalt eller om der skal en nærmere undersøgelse til.

Bemærk: Som en del af modenhed så er punkt nr 1 i CIC20 netop at man har styr på egne assets. Man kan ikke beskytte noget, hvis man ikke ved hvad man skal beskytte.

4.6 Dokument arkiv

En SOC har mange dokumenter, alt fra processer og procedurer til playbooks og guides. Det er ekstremt vigtigt at alle folk i en SOC har adgang til den samme opdaterede information. Derfor skal alt den information man skal bruge være tilgængeligt online lokalt i en SOC. Samt være sikret på bedst mulige vis.

Bemærkning: Der findes systemer der kan indeholde SLA’er fra kunder samt playbooks mm. i dag.

Man kan ikke bruge mail systemer som dokumentations arkiv. Mail systemer bør i dag være ret tomme fordi de er en yndet mål for hackers, der netop godt ved at mange benytter mail systemer som netop dokumentations arkiv. Jeg har set uanet mængder af tilfælde hvor hacker har fået adgang til mailsystemer hvor al den kritiske information fra virksomheder ligger præsenteret på et sølvfad.

4.7 Special lavede værktøjer eller hyldevarer

Skal en SOC bruge special lavede værktøjer eller hyldevare - der er for og imod for begge. Det special lavede passer typisk bedre til SOC’ens behov men det tager lang tid at udvikle og er ofte meget dyrere mens man genopfinder den dybe tallerken.

Hyldevarer passer ikke altid til de behov en SOC har, men man er hurtigere i gang og det kan være hurtigere end at udvikle sit eget. Her behøver man typisk ikke mange kommercielle produkter. Her bør dette være ret begrænset.

Forskellige former for SOC tools er dog allerede udviklet og man behøver sjældent at indkøbe dyre løsninger. Der vil selvfølgelig være en nødvendighed i forhold til meget specielle værktøjer. Typisk er dette små tools og ikke kæmpe store løsninger.

5.0 Andre overvejelser

Mennesker, processer og teknologier er de 3 fokus områder i det fleste anbefalinger når der snakkes om en SOC's modenhed. Men der findes en række områder der ikke nødvendigvis passer ind i disse områder, Disse vil blive gennemgået her.

5.1 Arbejdsmiljø og områder

Det ligger i en SOC's natur at de kommer ofte i kontakt med sensitiv information, som eksempelvis fortrolig og hemmelig information der ikke kan deles med andre. Det kan være information fra interne der er under undersøgelse eller materialet kan være af en foruroligende karakter, som eksempelvis børneporno.

Ved siden af dette er det vigtigt at en SOC kan fungere som et hold og at information hurtigt kan deles imellem de forskellige analytikere. Derfor er fysisk nærhed imellem analytikere det der virker bedst.

Al adgang til hvad analytikere arbejder med og en fysisk separering imellem en SOC og resten af en virksomhed er derfor vigtig. Dette gælder for alle systemer til fysisk separering i kontormiljøer mm.

5.2 MSSP vs indtern SOC

En anden vigtig overvejelse er om en SOC skal være intern eller lagt ud til en ekstern leverandør en Managed Security Service Provider.

Begge dele har fordele og ulemper. Det er afhængigt at de individuelle ønsker og nødvendigheder. En intern SOC har nem adgang til centrale vigtige informationer i tilfælde af incidents og compromise.

Eksterne vil typisk spare på at have trænet personale der kan håndtere incident. Derudover kommer der besparelse på at have mange tunge systemer og teknologier implementeret. En MSSP har dog typisk en bredere billede af hvad der rør sig af trusler mm som de enkelte virksomheder kan være berørt af.

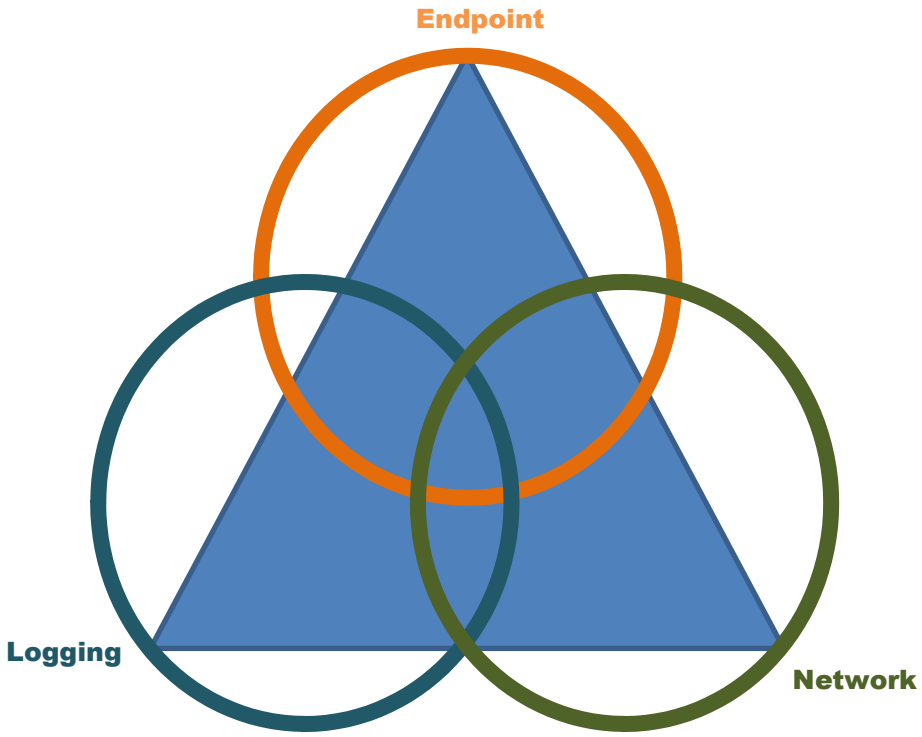
De vigtigste spørgsmål man skal overveje inden man vælger om en MSSP eller Interne SOC er følgende. "Hvor sikker er du på at teamet har resurser nok, samt teknisk kompetence til at kunne opdage, indramme, og respondere på en given data breach ? "

Har teamet ikke de nødvendige resurser eller kompetencer skal man altid gå efter en anden løsning / leverandør. Man bør gennemgå de forskellige punkter fra dette dokument. Det vil hurtigt give en fint billede af hvor moden i givet SOC måtte være.

5.3 Hunting

Intrusion detection og netværks overvågning sker typisk via ”known bad activity” eller ved unormal opførelse. Dette beror på det man også kalder for IOC’er (indicator of compromise) Det kan typisk være skadelige IP adresser, e-mail adresser, domæner, fil placeringer, MD5 summer på filer, certifikat informationer mm. Disse kommer typisk via forskellige former for ”threat inteligence” kilder.

Dog vil en tilgang med ”shared IOC’er” ikke finde nye ting som jo ikke allerede er kendt. For at finde disse ting kræver det at man påbegynder det man kalder for ”hunting” Hunting kræver at man begynder at kigge på alle de data man har, for at finde og jagte (hunte) for de anormale ting via mere generiske teknikker. For at muliggøre hunting skal man have følgende 3 kilder på plads, for at opnå resultater. Endpoints, Logning (Andre enheder) og netværk (Firewall, routers, switches mm.)



Det skal være muligt at lave en baseline for følgende aktiviteter som eks Netværks trafik, bruger aktivitet, mail systemer, applikationer installeret på systemer. Infrastruktur og systemer som eksempelvis printer og andet IOT udstyr, som køling systemer til server rum, adgangs kontrol på døre osv..

Selvom hunting kan finde ukendt kompromitteret udstyr med ukendte angrebs typer, så er en downside at det kræver en stor grad af falsk positiver der skal gennemgås af bl.a. andre afdelinger som netværk og infrastruktur hvor personale skal aktiveres i et vist omfang.

Succesen for ”hunting style” undersøgelser er også berørt af en given kundes ønsket tolerance level for hvor meget man kan inddrage 3 tredje part i undersøgelser herunder dem selv.

Yderligere findes der krav fra lovgivning for hvad der bliver muligt i hunting style undersøgelser, som også skal overholdes. Data beskyttelse og privacy love kan ikke tilsidesættes i forbindelse med hunting. Selvom det er en general bekymring i forbindelse med beskyttelse af en virksomhed eller andre forensic undersøgelser, så en der altid større tolerance såfremt man for hit på en allerede given kendt IOC fra et allerede dokumenteret angreb. Hele ideen med hunting er dog at være med til at skabe IOC’er for nye typer af angreb.

5.4 Øvelser og valideringer

Det er svært at benchmarke hvor godt en SOC performer, uden et forudsigeligt kendt angreb man kan måle ”detection rate” op imod. Hertil må man benytte kendte automatiseret angrebs tools der kan efterligne kendte angrebs metodikker. Til dette benyttes det man kalder for Red Teams der foretager angreb. Traditionelt vil en SOC være det man kalder for et Blue Team, som er beskyttende i natur.

Red Teams vil angribe så dybt som muligt og Blue Teams er dem der skal opdage de forskellige angreb. Såfremt angreb ikke bliver opdaget, vil en SOC anmode om ændringer i en give infrastruktur for at få foretaget ændringer således at oversete angreb kan opdages i fremtiden. På den måde kan sikkerheden i en infrastruktur målrettes og fokuseres på de svage områder.

Purple Teams er et forholdsvis nyt koncept, hvor man benytter et mix af Blue og Red Teams. For at have den bedste benyttelse er det påkrævet at begge Teams forstår begge Teams roller og metodikker i forbindelse med angreb. Dette er yderst vigtigt for at kunne beskytte og forsvare et givet netværk, man kan ikke isolere det ene teams roller i forbindelse med et godt forsvar af en infrastruktur.

5.5 NOC vs SOC

Network Operations Center (NOC) og SOC er 2 forskellige ting som dog har et nært fælles skab og typisk bliver kombineret sammen.

NOC er ansvarlig for selve netværkets oppetid og vedligeholdelse af enheder på netværket. NOC-en kan give oplysninger til SOC’en og kan forklare opførelse og give asset lister mm. At flytte personale imellem en SOC og en NOC kan give gode kombinationer af ”skill sets” til brug for en bedre sikkerhed.

5.6 Yderligere ansvarsområder

En SOC’s primære ansvarsområde er monitorering af netværks trafik og håndtering af incidents så bliver de ofte også ansvarlige for yderligere ansvarsområder.

Ofte bliver de ansvarlige for sårbarheds monitorering. Typisk falder disse under pentests teams. Men typisk

er dette teknologi som en SOC gør brug af for at overvåge sikkerheds tilsand på kritiske områder som angribere typisk vil gøre brug af eller målrette til brug for angreb.

Typisk vil en SOC lejlighedsvis benytte disse teknologier. Beslutninger om at gøre dette skal afbalanceres for ikke at fjerne fokus fra en SOC som er overvågning. Men bruges ofte for at afdække mulige sårbarheder der kan true virksomheden. Man skal tilsikre at normale "operations tasks" ikke bliver en del af hverdagen for en SOC. Andre opgaver er eksempelvis installationer af sikkerheds software som SIEM mm som ikke børe være at opgave for en SOC.

Beskyttelse imod "insider threats" i forbindelse med interne SOC's så skal adskillelse af funktioner være HØJT prioriteret. En insider trussel kan være en intern SOC medarbejder, der har dybdegående viden om hvordan en infrastruktur kan angribes uden at giver udslag i alerts mm. Dette er en af grundene til at analytikere bør arbejde på aflukket netværk der ikke har direkte adgang til kritiske systemer eller netværk.

En moden SOC der er fuldt bemandet, operationsklar som har en mission og en vision med dedikeret analytiker teams, skal kunne være i stand til at optage spikes i Alerts og incidents, skal kunne være i stand til at kunne vende tilbage til normal tilstande over en kort tids periode. Er analytikerne fyldt op med andre opgaver vil der ikke være "båndbredde" til at opdage angreb. En nedgang i opdagelse af angreb er typisk fordi analytikerne bliver sat til andre opgaver.

Bemærk. Det ses ofte at analytiker bliver sat til at lave eksempelvis udviklings opgaver af tools mm. Dette anses for at være yderst dårlig still, såfremt ledere begynder at tildele opgaver ud til analytiker der ligger uden for en SOC analytikers område. Også selvom en analytiker ville være i stand til at kunne løfte opgaven så fjerne det meget hurtigt en analytikkers fokus, for bla tanker vedrørende opdagelse af angrebs typer mm. Angreb vil typisk blive overset af den pågældende at analytiker som nu bruger tid og taker på andre opgaver.

5.7 Compliance

En typisk grund til at benytte en SOC service er fordi man ønsker at være complient med visse regulativer og en SOC genereret rapport kan tilsikre at disse bliver mødt og benchmarks bliver overholdt.

Dette er en valid grund til at benytte SOC servises, men compliance og sikkerhed er 2 forskellige ting og bliver typisk forvekslet med hinanden. Hvis en SOC bliver benyttet pga ønsket om compliance så skal sikkerheden betragtes separat for at tilsikre at sikkerheden også overholdes.

Angreb bliver mere og mere avanceret og den nuværende teknologier presses til kanten som kan opdage disse. Pålagt regulativer omkring compliance bebyrder derfor systemer administratorer og netværks administratorer i en sådan grad at sikkerhed ikke bliver overholdt.

5.8 Beskyttelse af en SOC

En sikker SOC beskytter sig selv. En SOC sidder med alle oplysninger omkring hvor data bliver opsamlet, omkring incidents osv. Givet dette vil den i sig selv være et primært mål for angreb, herunder meget

målrettede angreb. Ønsket om at målrette angreb imod en SOC for at kunne følge med i angreb er altså stort. Derfor er det essentielt at ønsket om og kravene til beskyttelse af en SOC skal være fastsat via politikker. Det kan f.eks. være krav til LOG overvågning på PC'er samt ensartet netværks overvågning på alle SOC'ens platforme.

Såfremt der udføres et vellykket angreb mod en SOC og at angrebet kan forblive uopdaget, betyder det at SOC'en ikke kan holde fortrolige data for kunder. Det betyder også at der kan rejses mange spørgsmål om hvor god en SOC reelt er.

Bemærk. Der findes allerede flere kendte og veldokumenteret angreb der er fortaget imod SOC enheder rundt om i verden. En SOC bør bør arbejde separeret net / lokaler mm.

Yderligere ser jeg typisk manglende overvågning af analytiker test udstyr og netværk.

5.9 Threat intelligence

Threat inteligense er defineret som detaljeret information omkring en angribers værktøjer, taktikker, metodikker samt associeret kendskab omkring anden viden omkring angribere.
Alt undtaget Hunting aktiviteter, så kan en SOC kun opdage hvad der er kendt. Så derfor spiller threat intelligence en vital rolle for at have en så bred viden som muligt til sin rådighed.

Der er mange kilder til Threat Intelligence som kan blive oprette via viden omkring angreb imod egen infrastruktur, informationer udefra, delte informationer via trusted kilder osv. Der er mange fordele i at dele viden med trusted kilder. Men der skal bruges mange kræfter på at beskytte denne viden.

Bemærk. Mange enheder gør i dag brug af MISP framework.
Dog skal man målerette Threat Intelligence til de dele hvor en virksomhed måtte befinde sig. Angreb der typisk rammer i udlandet er ikke altid det samme som rammer i Danmark. Dog skal man forvente at det man kalder "commodity malware" typisk rammer meget bredt osv.

6 Benchmarking

Denne sektion prøver at komme med forslag til hvordan man benchmarker en SOC og hvordan man kan lave målbare kriterier så man kan vise hvor en SOC forbedre sig samt de områder der ikke går så godt.

6.1 Exciterende modenheds modeller

Som sektion 3 også er inde på, så er der en masse ting der skal være på plads før en SOC er oppe og køre. "Rhodes University paper on Classification of Security Operation Centres", beskriver et framework der kan benyttes til måle modenheden af en SOC.

https://digifors.cs.up.ac.za/issa/2013/Proceedings/Full/58/58_Paper.pdf

6.2 Identificer kundekrav, nøgle kontaktpersoner og assets

Om en SOC er intern eller ekstern så vil den altid have mindst en kunde. For at opdage og bekæmpe et angreb hurtigere er det en god ide at have styr på kundekrav og assets på forhånd samt de kontaktpersoner som man skal notificere eller som skal gøre noget i forbindelse med et angreb.

En workshop med kunde er en god måde at identificere hvilke krav kunde måtte have samt hvilke assets der måtte være, disse afgørelser vil også være med til at afgøre hvem der skal kontaktes i forbindelse med en use case/alarm går af.

Det er også på dette stadie man burde snakke med kunde om de SLA'er der skal være, samt de assets der har højest prioritet og hvad de er. Dette er med til at hjælpe SOC'en med at vurdere trusler og falske positiver.

Bemærk. Der skal foretages test og afprøvninger af disse, på uforudsete tidspunkter for at kunne belyse eventulle behov der ikke er blevet afdækket.

6.3 Fysisk miljø

Der er et stort behov for samarbejde i en SOC hvis den også er intern. Der bliver håndteret følsom information som resten af firmaet ikke burde have adgang til. Det er vigtigt at have dette i baghovedet når man skal beslutte sig for hvor man fysisk skal placere en SOC. Det ideelle er at placere SOC'en et sted hvor de er afskærmet og hvor analytikerne kan sidde i samme rum og hvor de har adgang til den nødvendige teknologi. Dette er vigtigt fordi de også kan blive bedt om at lave undersøgelser på andre ansatte i firmaet hvor fortrolighed er alt afgørende.

Bemærk. Adgangs kontroller er vigtige så man kan dokumentere hvor der har haft adgang til SOC omgivelserne.

Yderligere bør man være opmærksom på sikkerheds godkendt personale ikke kan dele oplysninger med ikke sikkerheds godkendt personale. Typisk bliver ikke godkendt personale ofte placeret i samme rum/lokaler som sikkerheds godkendt personale. Dette vanskeliggøre det daglige arbejde da

samarbejdet imellem anlytikker gør at de eks ikke kan vende sig om og snakket åbent i lokalet såfremt ikke sikkerheds godkendt personale befinder sig i samme rum. Der bør blive fokuseret på de fysiske rammer ved tilkøb af eksterne SOC ydelser.

6.4 Antal af ansatte og plan for udvidelse

Antallet af ansatte i en SOC vil variere ud fra hvilke opgaver de skal arbejde med og hvor mange kunder de har. Man skal tage højde for hvor mange levels af analytikere der er behov for samt hvilke vagtplaner man vil gøre brug af 8-16, 24/7 samt syge dage, uddannelse, eksemer, ferie osv.

En fuldt bemandet SOC skal kunne håndtere en kraftig og uventet stigning i aktivitet som f.eks en malware udbrud eller en stort angreb i en kortere periode.

Der er også behov for at man gør det klart hvornår en SOC skal vokse på forhånd, dette kan gøres via KPI'er som kan være med til at måle om mængden af opgaver er højre end personalet kan håndtere.

Bemærk. Det ses meget ofte at der ikke findes en klar prioritet over hvilke kunder der skal håndteres først. Er man ny kunde i en SOC er dette altid en klar ting man bør spørge ind til.

6.5 Træning og udvikling af ansatte

En analytiker vil næppe arbejde som junior resten af livet og vil i de fleste tilfælde gerne specialisere sig inde for et område. Det er derfor en god ide at have klargjort en karrierevej i virksomheden så man ved hvilke muligheder for videreudvikling der er i firmaet. Derudover er det også vigtigt at man beslutter sige for hvilke egenskaber som er relevante for de forskellige roller i SOC'en samt synliggøre hvordan den ansatte tilegner sig den nødvendig viden, så de ansatte føler sig trygge i at der bliver investeret i dem og at der er den rette mængede ekspertise. En løsning kunne være at låse nyansatte med en kontakt så firmaet når at få værdi for investeringen.

6.6 Lederskab og topledelsen

Uden ordentlig ledelse og støtte fra topledelsen vil en SOC har ekstremt svært ved at udføre sin opgave, og vil mangle den nødvendige autoritet.

Det er ekstremt vigtigt at der er styr på ledelsen både hvad angår den daglig ledelse men også strategiske valg samt hvem der repræsenterer SOC'en i topledelsen som kan sikre budget og være med til at definere SOC'ens opgaver.

Bemærk. Det ses ofte at en indtern SOC placeres i en drift organastition. Dette er helt klart et forkert valg. En SOC bør være placeret direkte under topledelsen i en virksomhed, da det er dem den primært skal tjene. Der er en tendens til at en drift organasition ikke informaere topledelsen om vigtige hændelser for at dække over dem selv.

Det beviser også at topledelsen i en given virksomhed ikke har forståelse for deres egen sikkerhed når placeringen bliver lavet som beskrevet.

6.7 Processer og procedure

Det er ekstremt vigtigt at alle processer og procedure er lette at få adgang for at sikre at SOC'en reagere ens på alle hændelser samt at reaktionstiden på større eller sjældne hændelser bliver reduceret. Hændelser der kræver en proces/procedure skal identificeres og skal indeholde information som:

- Hvad skal der ske når noget opdages.
- Hvordan laver man en sag på det
- Hvilken information skal i sagen
- Hvornår og hvordan eskalere man en sag
- Hvad gør man i og uden for normal arbejdstid
- Hvordan overdrager man en sag til den næste vagt

Når disse ting er identificeret, skal processerne og procedurerne designes og dokumenteres på en måde så alle kan forstå dem, selv om man ingen forudsætning har. Og de skal placeres et sted hvor de er nemme at finde og få adgang til.

6.8 KPI'er

KPI'er skal være med til at lave et kvantificerbare måle punkter så man ved hvordan SOC'en klare sig med hensyn til dens opgaver samt vækst og forbedringer. Disse kan være forbundet med modenhedsmodellen som SOC'en bruger eller være sin egen.

En metric kunne være at måle "detection rate" og tiden til respons. Når at trussel bliver fundet så kan man måle på hvor lang tid den trussel har været i systemet får man fandt og fjernede den. Dette kan være med til at belyse om kvaliteten af arbejder er i orden, processer der skal ændres eller mangel på teknologi eller uddannelse.

En anden metric kunne være at beskyttelse skal holde længere end tiden brugt på detectering og fix. F.eks MTP > MTD + MTR, MTP (Mean Time to Protect); MTD (Mean Time to Detect); MTR (Mean Time to Repair) Dette kan man bruge på at bestemme et passende beskyttelsesniveau.

Andre KPI'er vil variere afhængig af mål og fokus men nogle eksempler kunne være:

- Personale rotations rate
- Audit resultat
- Overholdelse af SLA
- Ticket/sag løsnings rate
- Oppe tid
- Mængden af events, incidents, tickets som er blevet håndteret både antallet og type
- Løsnings tider
- Mængden af ansatte

- Ansatte per ticket/sag
- Events/incidents genereret per asset, usecase ect.

6.9 Identificering af nødvendig teknologi og hvorfor

Selvom teknologi er vigtigt for en SOC så kan det også være en hæmmesko, når der bliver købt teknologi ind som ikke er købt efter en SOC behov, men ud fra andre parameter, så kan det gøre mere skade end gavn.

Når ny teknologi skal købes ind så skal det dække et behov som ikke allerede er dækket af en anden teknologi. Og man skal være sikker på at det rent faktisk vil gavne den opgave man skal løse for kunden.

SOC'en og ledelsen skal sikre at den rigtige teknologi er på plads og at der ikke er nogle "huller" og at der er et formål med det man har købt ind.

Bemærk. MITRE attack framework kan benyttes til at identificere de nødvendige / manglende teknologier. Derved undgår man eventuel indkøb en forkert teknologi. Dete kunne være at det eksemplevis bare kræver tilpasninger i opsætninger på allerede indkøbt teknologi.

7 Test af SOC

Det er en god ide at finde en gentagelig måde hvor på man kan måle SOC'ens evne til at udføre sin opgave på. Dette kan være automatiske eller menneske styret tests som SOC'en er bekendt med eller ej.

Uanset vil det hjælpe med at for afdækket de områder hvor SOC'en mangler egenskaber og hvor man kan lave forbedringer, men det vil også belyse de ting der går godt.

8 Compliance, NOC og andre ansvarsområder

Som nævnt i afsnit 5 så kan SOC personalet ofte blive involveret i andre ansvarsområder såsom compliance eller være blandet ind i en NOC.

Mens det kan give mening at gøre det på denne måde til vil det tage ressourcer væk fra de opgaver der er SOC'en primære og det kan påvirke SOC'ens evne til at håndtere incidents negativt. På grund af dette er det vigtigt at finde ud af hvor ofte disse ekstra ting opstår og om SOC er det rigtige sted for at løse disse opgaver i firmaet. Det er ligeså vigtigt at firmaet er afklaret med den effekt disse ekstra opgaver kan have samt hvad det betyder hvis der er en major incident og om det er muligt at droppe disse ekstra opgaver hvis der skulle være et behov for det.

9 Ekstra services

Ekstra services kan være en værdifuld tilføjelse til en SOC, det kan hjælpe med at holde på personale ved at give den noget at specialisere sig i eller man kan bruge det til at tiltrække nye specialister. Men det er først noget man burde overveje når SOC'en har styr på sin kerne forretning.

Når man vurdere tiden er til det skal man finde ud af hvilke behov der er i market samt finde ud af hvad man vil satse på, dernæst skal der udarbejdes de nødvendige processer og procedure sammen med funktionsbeskrivelserne

De ekstra services kunne være, malware analyse, incident response, forensic, hunting, SIEM arkitekter og ingeniører, threat intel og meget mere.

10 Vækstplan

Trusselslandskabet ændre sig hele tiden, og SOC'en bliver nødt til at være i stand til at ændre med, for at kunne mitigerer truslerne.

Det er derfor der er behov for at forberede en vækstplan, gerne sammen med toplederen som SOC'en er tilknyttet, så der er støtte for de ændringer der er planlagt både kort sigtet og lang sigtet, men planen skal også indeholde ting som hvordan det forventes at SOC'en klare sig samt hvordan succes ser ud for SOC'en.

11 Beskyttelse af SOC'en

SOC'en er en guldmine for information og derfor også et værdifuldt mål, af disse over sager er det nødvendigt at man beskytter SOC'ens systemer forsvarligt. Det er en god ide at lave en plan for hvordan man vil sikre SOC'en, skal den overvåges og skal SOC'en selv gøre det? Hvordan sikre man sig at SOC'en er compliant med diverse standarder. Er det nødvendigt med pentest eller såbarheds scanninger?

Bemærkninger: Man bør mindst 1 gang pr år kræve rene straffeattester fra alt personalet i en SOC. Er der krav om sikkerheds godkendelser bør disse kunne blive opnået i hele arbejdsforholdets forløb.

Overvågning af PC'er fra en SOC der tilgår kunde systemer ser jeg meget ofte som værende mangelfuld eller ikke eksisterende.

Tilgang til SOC områder er ofte ikke beskyttet og tilgang til systemer kan ske via åbne kontorlandskaber med mangelfuld kontrol.

12 Konklusion

I forbindelse med at virksomheder udmelder public at man har en SOC, så skal man træde varsomt, da dette ofte ikke er tilfældet især hvis en SOC har mindre end 3 år på bagen.

Når man opbygger en SOC er der i dette dokument gennemgået de punkter der skal være på plads før man i virkeligheden kan sige at man har en egentlig og velfungerende SOC.

Ved udmeldinger om en SOC er kørende og velfungerende, kan give kunder det indtryk at de beskrevet punkter alle er på plads i SOC'en. Man bør være klar over at den danske IT-Sikkerheds verden inden for dette område (SOC) er meget bevidste om hvad det kræver at have en velfungerende SOC.

De kunder der typisk ikke ved hvad dette kræver, søger typisk råd om hvad det vil sige at have en SOC før ende de vil lægge sig fast på en leverandør af en SOC og SOC ydelser inden der bliver indgået kontrakter.

Så udmeldinger om en SOC kan have modsatte effekt og kan typisk bevirke at kunder finder andre leverandører af SOC ydelser, derved kan kunder på både SOC ydelser og andre områder være tabt i en rum tid fremover.

Der er mange punkter der bør blive taget fat på som er beskrevet igennem dette dokument. Disse punkter bør blive tilrettelagt og egentlige projekter omkring de forskellige emner bør bliver adresseret.

De vigtigste punkter at tage fat på til at starte med er at få tilrettelagt måle punkter for de enkelte delmål indlagt i faste tidsrammer for hvornår disse skal være gennemført for at kunne bevise at en SOC har fremgang og når de aftalte delmål.

Det ses meget ofte at virksomheder der opbygger SOC ydelser som en eksterne leverandør, går i gang med salg længe før end de egentligt er klar til salg. Det går kun ud over kunden der tror de får en billig SOC ydelse. Man skal som kunde forvente meget mangelfuld overvågning, da det sjældent er muligt at være en en SOC opbygnings fase og samtidigt være i gang med salg. På beggrund at netop dette har jeg set rigtig mange kunder komme galt afsted. Desuden taber virksomheden med denne for for tilgang kunder der næppe vender tilbage igen.

Investeringer samt en udviklings plan bør være forankret i ledelsen i virksomheder der ønsker en SOC. Ledelsen skal på status møder kunne spørge ind til fremdrift, samt have et overblik over de investeringer der bliver foretaget i udviklingen af en SOC. Men der skal også være en klar målsætning om hvornår salg på påbegyndes således at virksomheden der foretager disse kan have bare en lille ide om hvornår de kan forvente man begynder at tjene på investeringerne.

Bemærk. De SOC enheder jeg igennem tiden selv har været involveret i og som er fejlet og lukket. Så skyldes dette i bund og grund manglende investerings planlægning forankret i topledelsen. Manglende implementerings planer og målepunkter for implementeringer samt valget af kommercielle producenter, hvor der ikke kan tjenes på investeringerne.

Desuden ser jeg man har ansat lederer der rent faktisk slet ikke har haft en forståelse af hvad en SOC er og hvad det ikke er. Det er næsten den sikre vej til at SOC opbygningen ikke vil lykkedes.

En leder der ikke ved hvad der skal opbygges har meget svært ved at forstå de forskellige argumenter for hvorfor ting gøres som de gøres. Lederen får meget svært ved at fortælle topledelse hvad der rent faktisk sker og hvorfor det sker. Prioriteter af opgaver kommer meget hurtigt til kun at handle om hvad lederen kun lige har forstand på.

Jeg håber at virksomheder uanset om de vil bygge en SOC eller benytte en partner som leverandør af SOC ydelser, her har fået en lille forståelse for hvad en SOC er og hvad det ikke er. Samt vigtigheden for at spørge mere ind til de rigtige ting når en partner skal vælges som SOC leverandør.

Mit generalle råd er at undgå leverandører med for få ansatte, uden klare dokumentations muligheder eller man lige skal vente 4 dage på at modtage denne. En SOC med for under 3 års erfaring skal man være meget kritisk overfor. Typisk tager en SOC med rette mængde af ansatte 2 til 3 år at opbygge og så betragter jeg denne som værende meget ny, med meget at lære endnu og mange muligheder for fejl.

Man skal desuden være årvågen overfor for tilbud om at komme på med en ”rejse”. Det findes ikke i denne verden. Det er klare målsætninger der tæller, samt planer for implementeringer.