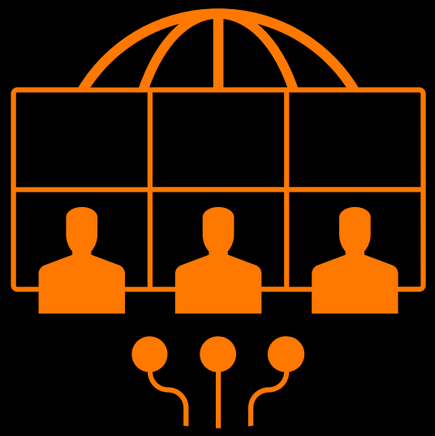
Guide

Upphandla en SOC

Det finns många viktiga delar att tänka på när man ska upphandla en SOC - oavsett ambitionsnivå.

orange™ Cyberdefense

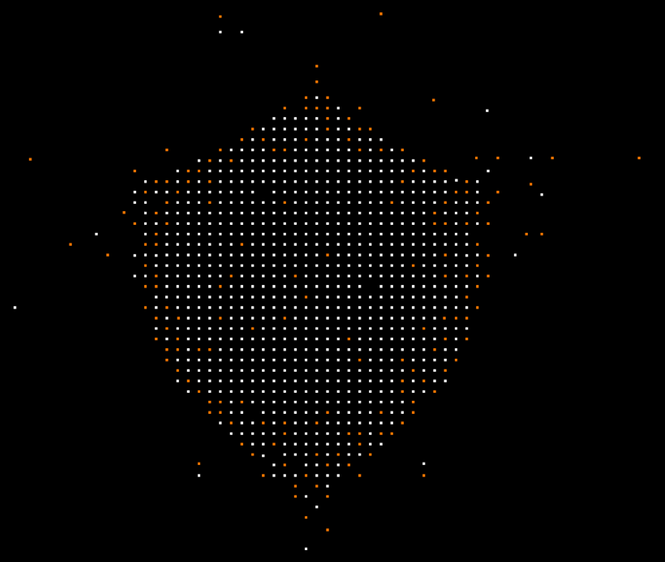
Innehåll



Security Operations Center

Ett Security Operations Center (SOC) är en säkerhetsavdelning och sambandscentral med ansvar för att aktivt identifiera, analysera och motverka cyberhot mot ett företag. I en SOC sitter team som arbetar dygnet runt med att övervaka och analysera data från olika källor i organisationen. När en incident sker och ett hot eller attackförsök upptäcks, tar teamet till åtgärder för att isolera händelsen, skydda organisationen och förhindra ytterligare skador, alternativt ta ärendet vidare till organisationen eller företagets egen beredskap för denna typ av incidenthantering.

En SOC utgörs oftast av ett team, vars medlemmar har olika ansvarsområden. Ett typiskt team består av incidenthanterare, olika nivåer av analytiker och hotjägare som jobbar uteslutande med att aktivt leta efter cyberhot. Dessa roller samverkar under ledning av väl upparbetade processer. För att arbeta proaktivt ska det också finnas personer som jobbar med research och aktiv hotintelligens (läs mer på sida 7-8). SOC-teamet är på plats dygnet runt, arbetar aktivt med att eftersöka hot och analysera data, och kan snabbt sätta in åtgärder. Kontinuerlig övervakning och snabba åtgärder är idag ett måste för varje organisation med kritisk information och/eller samhällsansvar.



SOC-guide

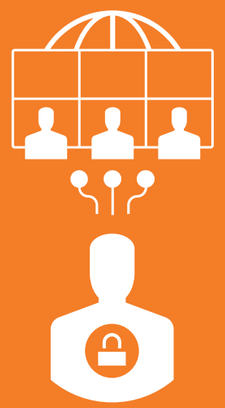
Som ett komplement till tekniken man investerar i väljer allt fler organisationer att investera i SOC (Security Operations Center). SOC kan beskrivas som en samlad säkerhetsfunktion, med både mänskliga resurser, avancerade tekniska lösningar är att detektera intrång och attacker, och processer för säker hantering av alla typer av cyberhot.

Det är ett säkerhetsteam vars huvuduppgift är att göra riskbedömningar i olika delar av den infrastruktur, IT- och verksamhetssystem som en organisation har. De ska skapa en bild av och ringa in sårbarheter för att sedan upptäcka och agera på potentiella attackförsök mot kända sårbarheter. Till SOC:ens uppgift hör också att rapportera till organisationen vilka sårbarheter som finns, omvärldsbevaka, kartlägga säkerhetsläget och föreslå åtgärder.

Den här texten syftar till att guida er i hur ni upphandlar en SOC. Det finns många viktiga delar att tänka på när man upphandlar en SOC-verksamhet – oavsett vilken ambitionsnivå ni väljer att lägga er på. Därför följer här de viktigaste stegen, våra bästa tips på vägen, vilka krav som bör ställas och hur ni bäst mäter framgång av en SOC-funktion.

Varför SOC?

De avancerade tekniska lösningarna och tjänsterna som tas fram och implementeras ger naturligtvis ett visst skydd. Brandväggar, antivirusprogram och XDR-verktyg (Extended Detection and Response) kan bromsa de mer uppenbara och konstaterade hoten, men det är samtidigt lätt att stirra sig blind på de tekniska verktygen och helt förlita sig på deras förmåga att förhindra attacker.



För att höja beredskapen och säkerställa att ni har den förmåga som krävs vid olika typer av incidenter behöver ni ha en total överblick över er IT-miljö, täppa igen eventuella säkerhetshål och anpassa er till nya, tänkbara hot. Dessutom bör alla säkerhetsinsatser som genomförs analyseras och mätas för att ni ska kunna utveckla och fördjupa ert säkertsarbete.

Myndigheter och organisationer som har vissa direktiv och krav att följa avseende hotupptäckt och incidentrapportering (exempelvis NIS2), bolag som driver hela eller delar av sin affär online eller har någon form av IP (Intellectual Property) bör ha ett avancerat och genomtänkt cybersäkerhetsarbete som inkluderar aktiv mänsklig analys. Oavsett om ni väljer att bygga full funktionalitet för säkerhetsanalys och responsprocesser internt, eller om ni tar in extern hjälp från en betrodd säkerhetspartner, ska det helt enkelt finnas där.

orange™ Cyberdefense

Vikten av den mänskliga analysen

Om ni inte har en SOC förlitar ni er på att de tekniska system ni har investerat i ska klara hela cybersäkerhetsarbetet. Arbetet sker då helt utan en mänsklig faktor som mer ingående analyserar händelser eller incidenter.

De säkerhetsprodukter som ni har investerat i stoppar antagligen de händelser som de är menade att stoppa, men kan av förklarliga skäl inte leverera där mänsklig bedömning är avgörande. Det kan dyka upp händelser som borde utredas eller undersökas vidare, som inte systemet eller tekniken klarar av. En SOC-analytikers uppgift är att analysera larm, anomalier och incidenter, bedöma allvaret av dessa och ta till åtgärd om det behövs. En sammanhållen rapportering är sedan av yttersta vikt för att säkerhetsarbetet ska vara effektivt och fruktsamt.

Ökad medvetenhet kring cybersäkerhet
Sverige som en högt digitaliserad ekonomi står inför alltmer sofistikerade hot och utmaningar inom cybersäkerhet. Hot som bara förväntas bli mer omfattande och komplexa framöver.

Cybersäkerhetsområdet växer i komplexitet hela tiden, och med det behovet av en breddning av omvärlds- och geopolitisk analys. En av de största utmaningarna Sverige står inför är cyberhot från främmande makt och icke-statliga aktörer. Dessa angrepp kan riktas mot allt från regeringsorgan till företag och kritisk infrastruktur såsom kraftverk, vattenförsörjning och transport.

Vi får också räkna med allt kraftigare försök till manipulation där syftet är att destabilisera det svenska samhället. Effekterna börjar redan bli synliga då såväl politiska partier, myndigheter och media tappar i tillit i allmänhetens ögon (enligt Radars rapport Cybersäkerhet 2023)

Under 2023 har antalet hacktivist-attacker mot Sverige ökat dramatiskt och Sverige har utsatts för näst flest attacker i världen. Under årets första månader är det bara Ukraina som utsatts för fler hacktivist-attacker än Sverige. Det framkommer av forskning och analyser som genomförts av Orange Cyberdefense Security Research Center.

Strängare lagstiftningar som reglerar hanteringen av data tillsammans med mer frekvent medierapportering om säkerhetsbrott och dess konsekvenser har drivit cybersäkerhet upp på dagordningen i ledningsrummen hos de flesta organisationer och företag.

I Radars rapport Cybersäkerhet 2023 kan data påvisa att verksamheter anser sig ha en låg mognad av förmågan att agera proaktivt och strukturerat i händelse av kris för att skydda sin verksamhet och affär, det vill säga att hantera sin digitala affärsrisk.

Antingen saknas detta arbete helt, är ad-hoc, reaktivt, eller under införande. Proaktivt säkerhetsarbete såsom automatisering av detektering, proaktiv jakt på cyberhot, samt användning av hotintelligens, är områden som avsevärt kan höja skyddsnivån och ska **ingå i en SOC.**

Uppbyggnaden av SOC

Att lägga ut sin SOC till extern part innebär att ni får tillgång till ett team av resurser som kan anpassas efter era specifika krav. Det låter er arbeta över organisatoriska gränser och få ut det mesta av era tekniska plattformar för säkerhetsnanalys. Innan en SOC implementeras är det viktigt att organisationen, tillsammans med den externa leverantören, diskuterar förväntningarna på SOC-teamet och att syftet och uppdraget sedan kommuniceras med hela organisationen. När allt är förberett och planerat är den allra viktigaste rekommendationen att sätta upp en SOC i etapper. För att ha en effektiv SOC behöver dessa tre – teknik, människor och processer – samspela och arbeta tillsammans.

Investera i rätt tjänster

Att investera i tjänster med bakomliggande verktyg är en god start i säkerhetsarbetet. Tekniken är viktig och det finns en rad innovativa tjänster och program för att stötta säkerhetsarbetet i en SOC. En stor del i teknikens utveckling på senare år har handlat om SOC-verktyg som automatiserar och effektiviserar.
Det vill säga att tekniken i allt högre grad ska kunna analysera ett säkerhetshot än djupare, och hjälpa analytikern med bättre sammanställt data och beroenden mellan händelser. Målet med samspelet mellan teknik och människa är att minska tiden från incident till åtgärd.

Rätt kompetens ger effektivare skydd

Att ha erfarna och kompetenta analytiker, som kan analysera inkommande data, detektera incidenter och ha en gedigen responsförmåga är en nyckel för att lyckas med säkerhetsarbetet. Att arbeta proaktivt med hotjakt och lägga till hotintelligens och research är avgörande, liksom att det kommer behövas människor på plats som kan förstå, förvalta och utveckla lösningarna för att möta de krav som ställs och den ständigt förändrade hotbilden. Det är även viktigt att SOC:en har konstant bemanning eftersom hotbilden inte bryr sig om traditionella arbetstider.
Attackerna sker från världens alla hörn och under dygnets alla timmar. En miljö kommer inte vara konstant och hotbilden kommer ändras, vilket innebär att en extern SOC måste vara en partner. Det är ett stort förtroende som läggs på extern part och att då få till ett tätt samarbete och förståelse är av yttersta vikt.

Sätt upp relevanta processer

Utöver tekniken som används och människorna som anställts för att analysera data, behöver ni ha effektiva processer för att säkerställa att rätt åtgärder görs när en incident väl inträffar. När något händer går det ofta snabbt och åtgärder kan behövas omgående. Till exempel bör det finnas processer för incidenthantering och för hur man uppdaterar detekteringsverktyget om en ny risk hittas, eller ett nytt system införs och ska tas i drift. När något nytt implementeras ska man alltid kunna svara på frågan: Vilka risker finns med detta och hur kan vi få en detektion snabbt på plats? Ett nära samspel med sin SOC-leverantör är därför helt avgörande för att uppnå önskat resultat.

Omvärldsbevakning och rapporter

Kortfattat hör dessa tre uppgifter till en SOC-analytikers vardag. Att dagligen noggrant bevaka sin omvärld och inte bara fokusera på den egna miljön är av yttersta vikt för att tidigt kunna upptäcka nya hot, kampanjer eller pågående attacker.
Att sedan kontinuerligt utveckla sin detektions- och responsförmåga genom att hela tiden mäta det som görs bidrar också till att fler incidenter kan stoppas innan de hinner orsaka verksamheten skada. Att få kontinuerliga rapporter från sin SOC-leverantör är viktigt. Detta för att hålla sig uppdaterad om vilka eventuella attacker man utsätts för och om incidenter som inträffat och som kan tas i beaktning för kommande utveckling, förbättring och inkluderas i interna riskanalyser. Rapporterna bör också innefatta allmän omvärldsbevakning och branschrelevanta threat research-analyser.

Vilka tjänster behövs?

Vilken typ av SOC-tjänst/er som upphandlas beror till stor del på företagets affär, riskaptit och resurser. De vanligaste är:

Logginsamlingstjänst

Ur ett compliance-perspektiv är det mest grundläggande att ha en logginsamlingsplattform som samlar in loggar från olika typer av system så att allt finns tillgängligt på ett ställe. Där kan sedan SOC-analytikerna se vad som händer på alla berörda servrar och klienter och snabbt få en överblick.

Detektionstjänst

Idag finns olika typer av detektionssystem som kan appliceras både på klienter, nätverk och system (exempelvis OT-miljöer) och som samtliga är till stor hjälp för en SOC. Dessa innehåller idag även maskininlärning, vilket underlättar det mänskliga analysarbetet.
Dessa benämns oftast som XDR (Extended Detection and Response), EDR (Endpoint Detection and Response) eller NDR (Network Detection and Response). De har alla sina olika styrkor vid olika typer av attackmönster, och ses i många fall som komplement till varandra för heltäckande detektering. Vilken som passar bäst beror på företagets tillgångar och risker, och rådgörs därför lämpligen med en SOC-leverantör.

Threat Intelligence

Threat Intelligence/hotintelligens är kunskap baserad på fakta om hotsituationen mot företaget utifrån. TI-kunskapen omfattar i första hand sammanhang, mekanismer, indikatorer, implikationer och rekommendationer för åtgärder av aktuella hot. Tjänster som gör denna information tillgänglig kallas Threat Intelligence Service.
Data om hot och attacker samlas in och utvärderas över hela världen. TI-information är en kontinuerlig dataström (feeds) i realtid som samlar in information relaterad till cyberrisker eller hot. Dessa feeds innehållande exempelvis ovanliga domäner, signaturer för skadlig programvara eller IP-adresser associerade med kända hotaktörer används i säkerhetslösningar och tjänster för att förbättra proaktiviteten.

Threat hunting

Hotjakt, ibland kallat cyberhotsjakt, är en proaktiv tjänst och process för att söka, isolera och utrota säkerhetshot som har lyckats kringgå befintliga säkerhetslösningar. Exempelvis kan det betyda ett hot som kringgått perimeterbrandväggar, sedan undvikit upptäckt av antivirus och andra säkerhetsåtgärder som finns på plats. Att arbeta proaktivt på detta sätt innebär att data samlas in från verksamheten dagligen och/eller veckovis. Uppgifterna bearbetas och extraheras till användbar, sökbar hotinformation och Threat Intelligence-feeds tas in för analys av insamlade data.

Incident response

Nyckeln till att mildra effekterna av alla cybersäkerhetsincidenter är reaktionstiden mellan upptäckt och åtgärd. I en SOC kan upptäckten av hotet göras, men vid ett införande av en SOC så måste processen för hantering av incidenten ingå. Antingen övergår ansvaret för hantering av incidenten till verksamheten, som då måste ha en beredskap för det. Saknar verksamheten den struktur som behövs för att reagera på ett snabbt och säkert sätt kan en Incident Response-tjänst som tillägg till SOC-tjänsten göra att cyberhot kan tas om hand snabbt och effektivt. En första åtgärd kan vara att SOC:en har förmågan att isolera enheter/resurser där incidenten uppdagats för att förhindra spridning. En komplett incident response-förmåga innebär att arbeta med ett ärende snabbt och effektivt. Att identifiera, analysera och utrota hotet, samt återställa för att få igång verksamheten i full kraft igen. Här krävs dokumenterad erfarenhet för bevisad effektivitet, då all tid då verksamheten står till kostar verksamheten pengar eller riskerar andra allvarliga konsekvenser.

Kundportal

En kundportal är en anpassad webbplats som erbjuder en samlad åtkomstpunkt till relevant information och möjlighet att följa upp och kommunicera med tjänsteleverantören. En portal för samlad översikt över ärenden, incidenter och statistik gör att uppföljningen förenklas och effektiviseras.

Drift

Om en SOC-tjänst upphandlas separat för exempelvis analys av data genererade av redan befintlig plattform (om man till exempel redan har en Microsoft säkerhetslösning på plats eller någon annan redan inköpt plattform), så kan man också fundera på att upphandla driftstjänst av den plattformen. Att ha en uppdaterad och driftsäker plattform är minst lika viktigt som detekteringsförmåga och analys av data för ett optimalt skydd. Många organisationer prioriterar tyvärr inte att underhålla sin säkerhetsteknik med den noggrannhet och proaktivitet som krävs. Detta kan bland annat leda till oönskade driftstopp och sårbarheter som öppnar upp för intrång.

Övriga funktioner att ha med vid utvärdering

När ni väl har bestämt er för att implementera en extern SOC är det mycket som ska komma på plats. För att utvärdera en partner så kan nedanstående funktioner, beroende på krav och risknivå, vara viktiga:

Business Continuity Plan (BCP)

BCP eller på svenska, plan för affärskontinuitet, kan definieras som “förmågan hos en organisation att fortsätta leverera tjänster på fördefinierade acceptabla nivåer efter en störande incident”. Det innefattar att man planerar för de troligaste scenariona och ser till att ha de tekniska lösningarna på plats för att kunna lösa situationerna så fort som möjligt. Det innefattar även ett därefter löpande arbete för att se om förhållanden inom företaget förändras som påverkar den plan man har utarbetat. Detta kan vara något att utvärdera hos en framtida leverantör.

Data Privacy/Dataskydd

Stöld eller manipulation av privat eller känslig information kan få förödande konsekvenser. I många fall är analys av data kopplat till känslig personinformation vilket medför att avtal och processer för hantering av detta måste finnas. Beroende på krav så kan data behöva säkerställas att det inte lämnar Sverige eller EU, samt att det bara hanteras svenskar eller EU-medborgare. Dokumentation och data privacy-hantering från SOC-leverantören är viktig.

Fysisk säkerhet

I en SOC är inte bara den digitala säkerheten viktigt. Den fysiska säkerheten i lokalen där SOC-arbetet bedrivs är av största vikt. Fysisk säkerhet ska skydda mot att obehöriga får tillträde till platser där säkerhetskänslig verksamhet bedrivs och mot skadlig inverkan på säkerhetskänslig verksamhet. Det finns olika nivåer av fysisk säkerhet där den högsta är kopplad till säkerhetsskyddslagen och säkerheten för Sverige och de verksamheter som har betydelse för Sveriges säkerhet. Exempelvis ska statliga myndigheter, kommuner eller regioner som avser att ingå ett avtal, ingå ett säkerhetsskyddsavtal om det förekommer säkerhetsskyddsklassade uppgifter eller leverantörerna har tillgång till säkerhetskänslig information.

Informationssäkerhet

Eftersom mycket och många gånger känsliga data hanteras i en SOC så är det av yttersta vikt att det finns ett ledningssystem för informationssäkerhet kring tjänsterna man avser att nyttja. ISO27000 är den internationella standarden för ledningssystem inom informationssäkerhet och det är därför vanligt att den används som krav vid upphandling av SOC-tjänster. I standarden omfattas bland annat hanteringen av informationssäkerheten, planeringsstyrning, ledningens engagemang, riskhantering, uppföljning och ständiga förbättringar.

Checklista för kravställning

Det är många som erbjuder SOC-tjänster. Hur ska man då veta vad som skiljer en SOC mot en annan och vad som passar kravbilden som satts upp? Här kommer exempel på områden/funktioner att ställa krav på:

Driftsättning – projektgenomförande

- Beskriv projektet för driftsättning, vem gör vad i projektet (kund/leverantör)?
- Vem leder och styr arbetet?
- Tidsplan?

Samverkansmodell

- Beskriv er samverkansmodell (strategiskt, taktiskt och operativt)
- Beskriv hur ni på operativ nivå rapporterar tjänseleveransen (SLA-uppfyllnad, incidenter, etcetera)
- Beskriv rapporter
- Beskriv kundportal
- Ställ krav på dedikerad Service Delivery Manager och Technical Delivery Manager

Teknik

- Beskriv partnerskap på utvald teknisk plattform
- Beskriv kundskap och certifieringar för vald teknisk plattform

Säkerhetsklassning/Data Privacy

- Beskriv hur data hanteras i de fall krav finns att det stannar inom Sverige och/eller EU
- Plarcing av SOC i Sverige 24/7, beskrivning av hur många resurser som sitter i Sverige
- Beskriv var er SOC är belägen, hur möter man säkerhetskraven på en modern SOC
- Beskriv processen för hur man arbetar med säkerhetsklassning

Beskriv...

Tjänster för SOC

- Er SOC, storlek och organisation
- Kompetens och kompetensutveckling hos säkerhetsanalytiker som arbetar i SOC.
- Hur ni arbetar med hotintelligens (Threat Intelligence) och hur den berikar er SOC-tjänst
- Hur ni säkerställer kvaliteten i leveransen av er SOC-tjänst (enligt ett kvalitets ledningssystem eller motsvarande)
- Hur ni säkerställer leverans vid en eventuell driftstörning i er SOC
- I kortform vilka övriga managerade säkerhetstjänster ni tillhandahåller
- På vilket sätt ni rapporterar incidenter till kund och hur de skiljer sig utifrån allvarlighetsgrad
- Hur ni jobbar med kontinuerlig förbättring av tjänsteleverans

SLA för tjänsten

- Beskriv hur SLA ser ut för tjänsten utifrån incidentens allvarlighetsgrad
- Tillgänglighet dygnet runt med bemanning av erfarna analytiker
- Beskriv kontinuitetsplan och hur man möjliggör vidarebefordring av larm till en annan SOC vid till exempel ett katastrofscenario
- Närvaro i Sverige ger närhet till kundens interna team och borgar för ett interaktivt samarbete

Kvalitet

- Beskriv hur man levererar en 24/7/365-tjänst med mätbara och nåbara mål och delmål
- Beskriv hur leverans ser ut med väldokumenterad erfarenhet för analytiker och resurser som jobbar med både omvärldsbevakning, analys och respons
- Tjänsten ska vara vertifierad enligt ISO270001
- Beskriv hur man använder Cyber Threat Intelligence i leveransen, hur insamling sker hur dessa integreras med tjänster
- Beskriv hur man jobbar med kontinuerlig förbättring av tjänsteleveransen
- Beskriv förmågan att snabbt kunna göra både triage och initial respons på allvarliga hot
- Beskriv förmågan av proaktiv och reaktiv Threat Hunting, kontinuerligt enligt antal SLA-timmar per månad eller initierat av kund på en specifik hotbild. Beskriv även hur det genomförs på ett strukturerat och dokumenterat sätt för att bemöta de senaste hoten
- Beskriv hur man på ett systematiskt sätt följer upp kundnöjdhet och NPS

Priser

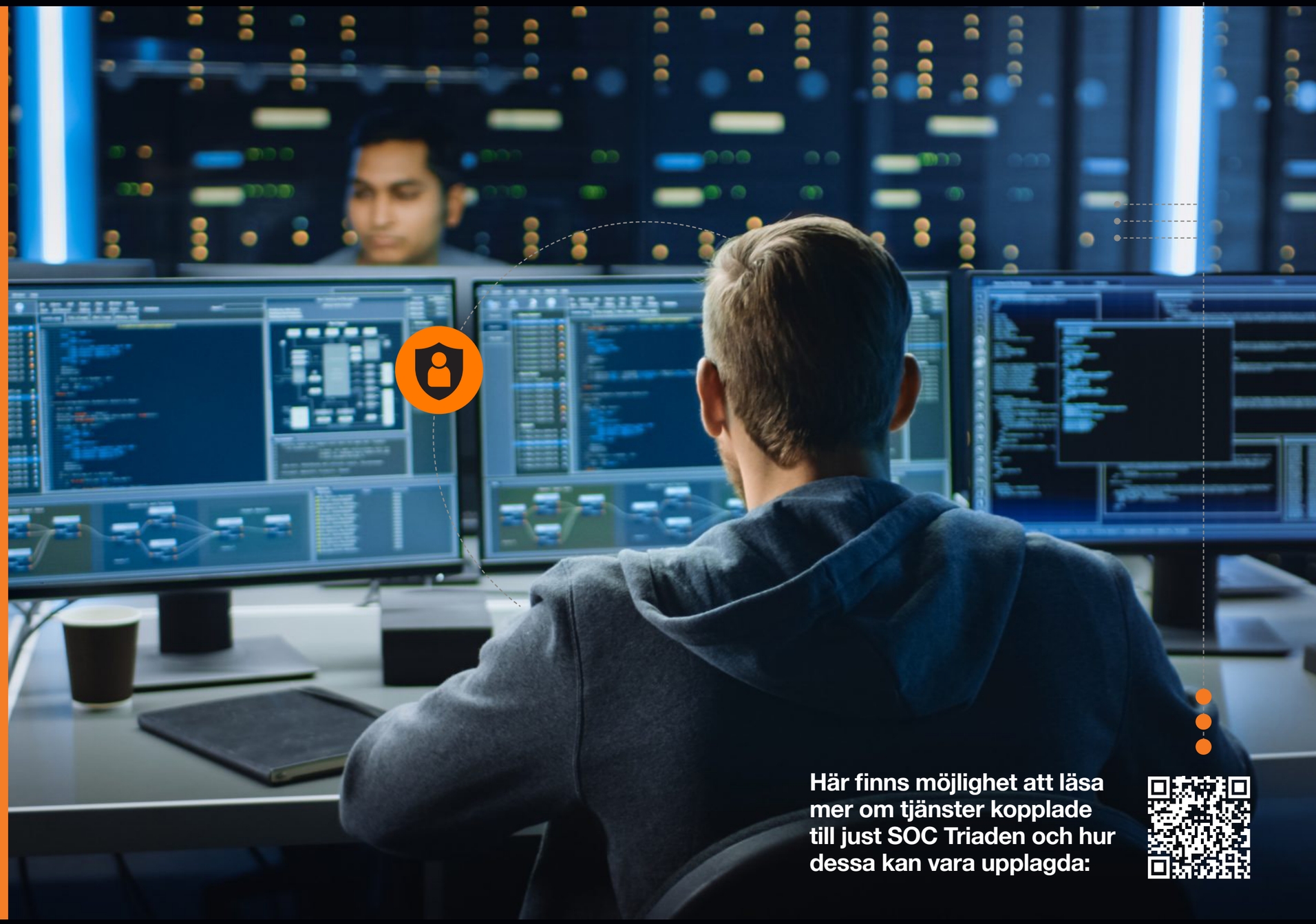
Tillkommande kostnader ska vara tydligt beskrivna

Framtidens SOC

Oavsett hur avancerad SOC-tjänst man behöver, är några av de viktigaste parametrarna att ha med er att hela tiden utveckla säkerhetsarbetet, omvärldsbevaka och se över era förmågor.

Många företag står inför en rejäl omställning i och med digitaliseringen och behöver ta ett helhetsgrepp runt sitt cybersäkerhetsarbete. En SOC:s uppgift är att vara spindeln i nätet – men hela organisationen måste inkluderas när det kommer till ansvaret som tas för cybersäkerheten.

Det finns extern hjälp att få. Antingen väljer ni att göra vissa delar av ert SOC-arbete själva och outsourcar resten, eller så väljer ni att lägga ut hela arbetet kring SOC:en på extern part som tar hand om larmen när de kommer. Ett annat sätt kan vara att lägga ut driften av vissa tjänster.



Här finns möjlighet att läsa mer om tjänster kopplade till just SOC Triaden och hur dessa kan vara upplagda:

Varför ska du välja Orange Cyberdefense?

Specialister inom cybersäkerhet

Orange Cyberdefense har specialiserat sig på cybersäkerhet och har 25 års erfarenhet av att leverera managerade tjänster till några av världens största företag.

Enastående expertis

Våra tjänster levereras från våra 14 CyberSOC och 18 SOC spridda över världen, vilket ger omedelbar tillgång under dygnets alla timmar till specialister som hanterar incidenter och säkerställer kontinuerlig tillgänglighet. I Sverige finns 2 CyberSOC och 1 SOC, bemannade 24/7.

14
SOC spridda över världen.

2
SOC i Sverige, bemannade 24/7

24/7/365
Tillgång till specialister

Insikter

Inom Orange Cyberdefense behandlas över 50 miljarder händelser varje dag, vilket ger oss oöverträffad tillgång till aktuella och framväxande hot. Våra experter är i framkant inom cybersäkerhet och har god insikt om hotbilden som finns. Vi använder denna information och alla insamlade data för att öka säkerheten för våra kunders verksamhet. Vi kallar det ”Intelligence led security approach”.

Partners

Vårt nära samarbete med många ledande leverantörer ger oss tillgång till deras tekniska experter och produktutveckling, vilket ger vår SOC värdefull kunskap och möjlighet att vara proaktiv

orange™ Cyberdefense