SIT CYBER EXPOSURE OPTIMIZATION

Bra säkerhetsarbete börjar med rätt information. Få ut mer av ert säkerhetsarbete.

SIT Cyber Exposure Optimization är för er med ett etablerat säkerhetsarbete som vill se mer, prioritera bättre och arbeta effektivare. Under tre månader jämför ni SIT med er befintliga lösning i samma IT-miljö. Resultaten avgör vad ni ska ersätta, konsolidera, komplettera och integrera. Därefter fortsätter tjänsten med oberoende, proaktiv kontroll före incidenten och uppföljning av er tekniska risk över tid.

FÖR ER SOM REDAN HAR KOMMIT LÅNGT

Ni har redan ett starkt säkerhetsarbete. Få större effekt av det.

Ni har verktygen, processerna och kompetensen på plats. Vi jämför vilken teknisk bild ni får, vilka relevanta sårbarheter som hittas, hur riskerna prioriteras och hur mycket manuellt arbete som krävs. Samma miljö. Samma förutsättningar. Resultaten får avgöra. När SIT ger det bättre samlade underlaget är målbilden att ersätta den traditionella interna sårbarhetsscanningen. Skydds-, detektions- och responssystem som fyller andra roller kompletteras med återkommande teknisk riskreduktion före incidenten.

Jämför hela kedjan i er egen miljö

Vi genomför tre scanningar parallellt med er befintliga lösning. Jämförelsekriterierna fastställs vid start: teknisk täckning och relevans, prioritering, arbetsinsats och uppföljningsvärde. SIT Appliances dedikerade fysiska hårdvara är en del av vår djupa fingerprinting och kräver ingen serverkapacitet i er befintliga IT-miljö. Ni jämför vilka allvarliga sårbarheter som identifieras, vad ni bör åtgärda och om åtgärderna ger effekt. SIT identifierar relevanta och kritiska sårbarheter som andra marknadsledande lösningar missar. Våra jämförelsetester visar dessutom att vi genomför scanningarna på mindre än halva tiden.

Skarpare prioritering

SIT Risk Score (0–10) väger samman teknisk allvarlighetsgrad med kända exploits, sannolikhet för exploatering, aktivt utnyttjande och verksamhetskritikalitet. Identifierade CVE:er matchas mot kända flerstegsattacker och kedjekontexten används i prioriteringen. Rapporten Top Priorities visar vilka Critical och High ni ska åtgärda först och rekommenderad åtgärd.

Mindre manuellt arbete

SIT kartlägger system, tjänster, produkter och versioner automatiskt, agentlöst och oautentiserat. Inga privilegierade konton krävs på målsystemen. Ni får en separat teknisk bild och lägger mindre tid på att sortera fynd. All intern analys sker lokalt i en härdad, nedlåst och krypterad SIT Appliance. Ingen information lämnar ert nätverk.

Optimera hela stacken

Ersätt eller konsolidera funktioner där SIT ger bättre resultat. Komplettera EDR, XDR, SIEM och SOC med proaktiv kontroll före incidenten. Våra experter hjälper er att jämföra resultaten och utforma målbilden. Vi kan integrera SIT med verktyg i er befintliga säkerhetsstack, så att förbättringarna blir enklare att införa.

Tre månader. Sida vid sida. Dubbelt expertstöd.

Tre scanningar ger ett gemensamt beslutsunderlag och en målbild för fortsatt användning. Våra experter hjälper er med jämförelse, verksamhetskontext och arbetssätt. Small, Medium och Large omfattar 8, 12 respektive 16 experttimmar per månad under etableringen, därefter 4, 6 respektive 8. Enterprise enligt offert. All tjänsteleverans och inkluderad expertkapacitet levereras från Sverige. Exitvillkor regleras i avtalet; annars fortsätter tjänsten löpande.

SÅ SKAPAR VI VÄRDE

Från jämförelse till långsiktig optimering.

Kartlägg → Prioritera → Rapportera → Åtgärda → Kartlägg igen. Kontrollcykeln upprepas och Delta Report validerar effekten av tidigare åtgärder i nästa scanning. Ni eller er IT-leverantör genomför förändringarna i er IT-miljö. SIT ger analys, rekommendationer och expertstöd. Hotmatchningen sker kontinuerligt mellan scanningarna.

1	2	3	4
NULÄGE	**KONTEXT**	**JÄMFÖR**	**MÅLBILD**
Scan 1 etablerar den tekniska nulägesbilden och jämförelsen enligt de kriterier vi fastställer tillsammans.	Scan 2 lägger till verksamhetskritikalitet och fördjupar jämförelsen av vilka risker som hittas och vad som bör åtgärdas först.	Scan 3 visar åtgärdseffekten och ger en samlad utvärdering av teknisk bild, prioritering, arbetsinsats och uppföljning.	Ni beslutar vad som ersätts, konsolideras, kompletteras och integreras i det fortsatta säkerhetsarbetet.

Efter de första tre månaderna: löpande optimering

- **Automatisk och återkommande kontroll. Scanningarna körs oövervakat i produktionsmiljön.** Kontrollerna är utformade för att inte störa systemen och kräver liten löpande insats från ert team.
- **Expertstöd för fortsatt optimering.** Våra experter hjälper er att tolka, prioritera och förbättra era arbetssätt. Expertkapaciteten följer vald tjänstestorlek.
- **Validera effekten och följ risktrenden.** Technical Report visar hela riskbilden. Delta Report visar vad som har åtgärdats, finns kvar och tillkommit. SIT Risk Index-historiken visar hur den samlade risknivån utvecklas och var den är högst.
- **Kontinuerlig hotmatchning.** Nya sårbarheter, zero-days och uppdaterad hotinformation matchas kontinuerligt mot den senast kända IT-miljön. Nya relevanta risker identifieras och ni notifieras.
- **Spårbart säkerhetsarbete.** SIT kopplar tekniska kontrollresultat till bland annat ISO 27001 och NIS2. Ni lägger till egna bedömningar. Rapporter och historik ger spårbart underlag för säkerhetsarbete och compliance.

Varför SIT i en mogen säkerhetsstack

- **Oberoende bild av er miljö.** Ni jämför faktiska resultat från samma miljö. Resultaten avgör vilka funktioner som ger bäst beslutsunderlag.
- **Lokal analys med bred räckvidd.** Appliance kontrollerar avtalade IP-baserade system som den når från sin nätverksposition, även på andra siter, hos leverantörer och i molnmiljöer.
- **Tekniska förutsättningar för intrång.** SIT Appliance visar när förutsättningarna finns utan att genomföra intrånget. Det ger återkommande kontroll med låg driftsrisk.
- **Utvecklat i Sverige.** SIT Appliance är utvecklat i Sverige. All intern analys sker lokalt. Ingen information lämnar ert nätverk.
- **Integrera där det ger värde.** SIT kan integreras med verktyg i er befintliga säkerhetsstack, inklusive tvåvägsintegration med ServiceNow. Det gör förbättringarna enklare att införa.

Komplettera den interna bilden med SIT Xternal

SIT Xternal är ett tillval som ger återkommande kontroll av er definierade internetexponerade attackyta. Ni ser exponerade system och tjänster, relevanta sårbarheter och tekniska förutsättningar för ett första fotfäste. Tillsammans med Appliance samlas resultaten och lagras lokalt hos er. Ni får både ett internt och ett externt exponeringsperspektiv.

Bättre information. Skarpare beslut. Lägre risk.

SIT Cyber Exposure Optimization ger er en bättre teknisk bild, skarpare prioriteringar och mindre manuellt arbete. Ni hittar fler relevanta sårbarheter, lägger tiden på rätt åtgärder och verifierar att de faktiskt minskar risken. När tjänsten integreras i ert löpande säkerhetsarbete får ni dessutom kontinuerlig hotbevakning, återkommande verifiering och en tydlig bild av hur er tekniska risk utvecklas över tid.

Resultatet är ett effektivare säkerhetsarbete, en enklare säkerhetsstack och en teknisk risknivå som pressas ned över tid.