

SIT CYBER EXPOSURE OPTIMIZATION

Bra säkerhetsarbete börjar med rätt information. Kan er bli bättre?

SIT Cyber Exposure Optimization är för er som redan har ett moget säkerhetsarbete och vill veta om ni kan se mer, prioritera bättre och arbeta effektivare. Under tre månader kör vi vår tjänst parallellt med er befintliga lösning i er egen IT-miljö. Ni jämför resultaten sida vid sida och får svart på vitt vad ni ska behålla, vad vår tjänst gör bättre och var ni kan konsolidera eller integrera för att få större effekt av ert säkerhetsarbete.

FÖR ER SOM REDAN HAR KOMMIT LÅNGT

Ni har redan ett starkt säkerhetsarbete. Nu ser vi om ni kan få ut ännu mer av det.

Ni har verktygen, processerna och kompetensen på plats. Därför ska ni inte behöva gissa vad som fungerar bäst. Under de första tre månaderna kör vi vår tjänst sida vid sida med er befintliga lösning i er egen IT-miljö. Vi jämför vilken teknisk bild ni får, vilka sårbarheter som faktiskt hittas, hur riskerna prioriteras och hur snabbt ni kommer från fynd till rätt åtgärd. Samma miljö. Samma förutsättningar. Resultaten får avgöra. De tre månaderna är starten, inte slutet. Därefter fortsätter tjänsten med återkommande analyser, prioritering och verifiering så att ni kan följa och förbättra er tekniska risk över tid.

Jämför hela kedjan i er egen miljö Under de första tre månaderna kör vi tre scanningar sida vid sida med er befintliga lösning. Ni ser vilken teknisk bild ni får, vilka sårbarheter som faktiskt hittas, hur riskerna prioriteras och hur snabbt ni kommer från fynd till rätt åtgärd.	Skarpare prioritering Det räcker inte att veta att en sårbarhet finns. Ni behöver veta vilken ni ska åtgärda först. SIT uppdaterar kritikaliteten utifrån om sårbarheten är nåbar, om det finns kända exploits, hur sannolik exploatering är, om den utnyttjas aktivt samt attackkedjor och verksamhetskritikalitet. Top Priorities visar vad ni ska börja med. Technical Report ger er samtidigt hela den identifierade riskbilden.
Mindre manuellt arbete Mer information är inte målet. Bättre beslut är målet. SIT kartlägger och analyserar automatiskt, agentlöst och oautentiserat och ger er ett koncentrerat underlag för vad som behöver åtgärdas. Ni lägger mindre specialisttid på att sortera fynd och mer tid på att minska den faktiska risken. All analys sker lokalt. Ingen information lämnar ert nätverk.	Optimera hela stacken De första tre månaderna visar inte bara hur SIT står sig mot dagens lösning. De ger er också ett konkret underlag för vad ni ska behålla, komplettera, ersätta eller integrera. Därefter fortsätter tjänsten löpande med den målbild ni valt. Målet är bättre säkerhetseffekt, mindre manuellt arbete och en enklare säkerhetsstack.

Tre månader. Sida vid sida. Dubbelt expertstöd.

Under de första tre månaderna genomförs tre scanningar parallellt med er befintliga lösning. Våra experter arbetar tätare tillsammans med er för att förstå skillnaderna, jämföra beslutsvärdet och ta fram en tydlig målbild för vad ni ska behålla, komplettera, ersätta eller integrera. Den inkluderade expertkapaciteten fördubblas så att ni snabbt får ett bra beslutsunderlag och kan etablera det arbetssätt som ska gälla framåt. Därefter fortsätter expertstödet som en del av den löpande tjänsten.

SÅ SKAPAR VI VÄRDE

Från jämförelse till långsiktig optimering.

De första tre månaderna visar vad som ger bäst resultat i er miljö. Tillsammans använder vi informationen till att bestämma hur tjänsten på bästa sätt integreras i ert fortsatta säkerhetsarbete. Därefter fortsätter SIT Cyber Exposure Optimization som en löpande tjänst med återkommande analyser, skarpare prioritering, verifiering av åtgärder och fortsatt effektivisering över tid.

1 NULÄGE Scan 1 bygger SIT:s tekniska nulägesbild och skapar utgångspunkten för jämförelsen med er befintliga lösning.	2 KONTEXT Scan 2 lägger till verksamhetskritikalitet och fördjupar jämförelsen av vilka risker som hittas och vad som bör åtgärdas först.	3 JÄMFÖR Scan 3 visar vad som förändrats och ger ett samlat underlag för vilken lösning som ger bäst resultat i er miljö, från teknisk bild och prioritering till manuellt arbete och uppföljning.	4 MÅLBILD Tillsammans bestämmer vi hur tjänsten på bästa sätt integreras i ert fortsatta säkerhetsarbete.
--	---	--	---

Efter de första tre månaderna: löpande optimering

- **12 scanningar per år.** Er IT-miljö analyseras återkommande så att ni ser vad som förändras, vilka risker som finns kvar och om genomförda åtgärder faktiskt minskar risken.
- **Expertstöd som hjälper er att få mer gjort.** I tjänsten ingår experttimmar som hjälper er att tolka resultaten, prioritera rätt och fortsätta utveckla ert säkerhetsarbete.
- **Rätt prioriteringar och tydlig utveckling över tid.** Top Priorities visar vad ni ska åtgärda först. Technical Report ger er hela den identifierade riskbilden. Delta Report och Risk Score-historiken visar vad som förändras och om den tekniska risken faktiskt minskar.
- **Hotbevakning mellan scanningarna.** Nya sårbarheter, zero days och kända exploits mappas kontinuerligt mot er senast kända IT-miljö. Ni meddelas när en ny risk upptäcks som berör er miljö.
- **Fortsatt optimering.** När er miljö och era behov förändras hjälper vi er att fortsätta förbättra arbetssättet, minska onödigt manuellt arbete och hitta nya möjligheter till konsolidering och integration.

Varför SIT i en mogen säkerhetsstack

- **Låt er egen miljö avgöra.** Ni jämför SIT med det ni redan använder utifrån faktiska resultat i er egen IT-miljö, inte utifrån produktblad och funktionslistor.
- **Bättre information ger bättre beslut.** SIT kartlägger system, tjänster, produkter och versioner med hög precision och bygger en bredare teknisk riskbild. Därefter vägs närbarhet, kända exploits, sannolik exploatering, aktivt utnyttjande, attackkedjor och verksamhetskritikalitet in för att visa vad ni ska åtgärda först.
- **Mindre manuellt arbete.** SIT Appliance arbetar automatiskt, agentlöst och oautentiserat. Ni får ett koncentrerat beslutsunderlag utan att skapa ännu en tung arbetsprocess för ert team.
- **Lokal analys. Full kontroll.** All intern analys sker lokalt. Ingen information lämnar ert nätverk. SIT är ett svenskt bolag och tekniken är utvecklad i Sverige.
- **Bygg in SIT där det ger mest värde.** SIT kan användas som en egen teknisk kontrollpunkt eller integreras med era befintliga system och arbetsflöden där det skapar ett bättre och effektivare säkerhetsarbete.

Komplettera den interna bilden med SIT Xternal

SIT Appliance visar vad som kan utnyttjas inne i er IT-miljö. SIT Xternal visar vad en angripare ser och kan nå från internet. Lägg till Xternal så får ni en automatiserad och återkommande kontroll av båda perspektiven. Resultaten samlas i SIT Appliance och ger er en sammanhängande bild av den externa exponeringen, möjliga vägar in och de interna risker en angripare kan möta efter ett första fotfäste.

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.