SIT CYBER EXPOSURE ASSURANCE

Cyberrisken är ert ansvar. Har ni kontroll?

Ni kan lägga ut IT-driften, men ansvaret för cyberrisken ligger fortfarande hos er. SIT ger er en oberoende teknisk bild av vilka risker som faktiskt finns i er IT-miljö, vad som ska åtgärdas först och hur risken utvecklas över tid.

BEHÅLL KONTROLLEN

Ni kan lägga ut IT-driften. Ansvaret för cyberrisken är fortfarande ert.

SIT Cyber Exposure Assurance ger er en egen, oberoende och återkommande teknisk kontroll oavsett om externa leverantörer ansvarar för delar av eller hela er IT-miljö, IT-drift eller säkerhetsarbete. SIT kartlägger miljön på djupet, visar vilka sårbarheter som faktiskt går att nå och utnyttja och ger er ett tydligt underlag för vad ni ska åtgärda själva och vad ni ska driva mot leverantören.

Se hela er IT-miljö

SIT Appliance kartlägger automatiskt och återkommande hela den IP-nåbara IT-miljön inom avtalat scope på djupet och identifierar system, tjänster, produkter och versioner med hög precision. Det ger en bredare och mer korrekt sårbarhetsbild som är oberoende av leverantörens egen rapportering. All analys sker lokalt och ingen information lämnar ert nätverk. SIT är ett svenskt bolag och tekniken är utvecklad i Sverige.

Prioritera på faktisk risk

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 vilka frågor ni och leverantören bör driva först och innehåller rekommenderade åtgärder. Den fullständiga tekniska rapporten ger samtidigt tillgång till hela den identifierade riskbilden.

Verifiera effekten

Nästa scanning visar vad som är nytt, vad som kvarstår och vad som försvunnit. Delta Report och Risk Score-historik gör utvecklingen mätbar i stället för att säkerhetsarbetet bara blir en följd av punktinsatser.

Stärk beställarrollen med expertstöd

SIT:s experter hjälper er att tolka resultaten, välja vad som ska drivas först, formulera rätt frågor och följa upp åtgärder tillsammans med er och IT-leverantören. Expertstödet är en del av tjänsten och hjälper er att få maximalt värde av kontrollen, från analys och prioritering till verifierad förbättring.

Cybersäkerhetslagen kräver ett systematiskt och återkommande säkerhetsarbete.

Det räcker inte att ha säkerhetsåtgärder på plats. Ni behöver veta att de fungerar. SIT ger er automatiska och återkommande analyser av er IT-miljö, visar vilka risker som finns kvar och vad ni ska åtgärda först. Ni följer effekten av genomförda åtgärder över tid och får ett tydligt, spårbart underlag för både ert eget säkerhetsarbete och uppföljningen av era IT-leverantörer. På så sätt hjälper SIT er att uppfylla de delar av cybersäkerhetslagen och MCFFS 2026:11 som handlar om teknisk kontroll, säkerhetstester och uppföljning av säkerhetsåtgärdernas effektivitet.

DEN LÖPANDE TJÄNSTEN

Automatiskt och återkommande - från nuläge till verifierad effekt

De första tre månaderna etablerar scope, baseline, verksamhetskontext och arbetssätt. Därefter fortsätter tjänsten med 12 scanningar per år, löpande mappning av nya sårbarheter, zero days och kända exploits mot er senast kända IT-miljö samt SIT:s experter som hjälper er från prioritering till åtgärd och verifierad uppföljning.

1	2	3	4	5
KARTLÄGG	**MATCHA**	**VALIDERA**	**PRIORITERA**	**VERIFIERA**
SIT Appliance scannar överenskommet scope och bygger en ny teknisk nulägesbild.	Observerad miljö kopplas mot relevanta sårbarheter och uppdaterad sårbarhetsinformation.	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 vilka Critical och High ni och leverantören ska driva först och innehåller rekommenderade åtgärder.	Nästa scanning och Delta Report visar vad som ändrats och om exponeringen faktiskt minskar.

SIT:s expertstöd genom hela cykeln

- **Maximera värdet.** Experttimmarna finns för att ni ska få så mycket effekt som möjligt av tjänsten. Vi lämnar inte bara över ett resultatpaket.
- **Från analys till åtgärd.** SIT hjälper till med tolkning, prioritering, tekniska frågor, åtgärdsstöd och konstruktiv leverantörsdialog.
- **Följ hela vägen.** Våra experter följer tillsammans med er vad som åtgärdats, vad som återstår och vad som tillkommit sedan senast.

Detta ingår löpande

- **12 scanningar per år.** En återkommande intern kontrollpunkt inom avtalat scope.
- **Expertstöd som hjälper er att få mer gjort.** Det ingår experttimmar i tjänsten som hjälper er att få ut så mycket som möjligt av ert säkerhetsarbete.
- **Hotbevakning mellan scanningarna.** Nya sårbarheter, zero days och kända exploits mappas kontinuerligt mot senast kända miljöbild och ni meddelas när en ny risk upptäcks.
- **Rapporter och historik.** Top Priorities med rekommenderad åtgärd, fullständig teknisk rapport över samtliga identifierade risker, Delta Report, Risk Score-historik och underlag för ledning och styrning.

Så kommer ni igång under de första tre månaderna

Månad 1: baseline och första Top Priorities. Månad 2: verksamhetskritikalitet och gemensam kontext läggs till. Månad 3: genomförda åtgärder verifieras och den fortsatta kontrollcykeln etableras. Under etableringen fördubblas den inkluderade expertkapaciteten så att ni snabbt får kontroll över er risknivå och etablerar ett arbetssätt för att åtgärda de mest kritiska riskerna först.

Komplettera den interna kontrollen med SIT Xternal

SIT Appliance visar den interna risken. SIT Xternal visar vad en angripare ser och kan nå från internet. Tillsammans ger de en automatiserad och återkommande helhetsbild, från möjliga vägar in till interna risker efter ett första fotfäste. Resultaten från båda tjänsterna samlas i SIT Appliance.

Egen kontroll. Rätt prioriteringar. Verifierad effekt.

Ni hittar de sårbarheter som faktiskt innebär störst risk, åtgärdar rätt saker först och verifierar att risken verkligen minskar. SIT ger er ett eget, oberoende beslutsunderlag och experter som hjälper er att driva rätt åtgärder hela vägen, internt och mot era leverantörer. Resultatet är färre kritiska risker, bättre kontroll och en teknisk risknivå som ni kan följa över tid.