

SIT CYBER EXPOSURE CONTROL

Få kontroll på cyberrisken. Åtgärda rätt först.

SIT Cyber Exposure Control är för er som vill få ett systematiskt säkerhetsarbete på plats snabbt. Vi kartlägger er IT-miljö på djupet, hittar de sårbarheter som faktiskt betyder mest och visar vad ni ska åtgärda först. Våra experter hjälper er att driva åtgärderna, verifiera effekten och bygga ett arbetssätt som pressar ned den tekniska risken över tid.

FÖR ER SOM VILL FÅ KONTROLL SNABBT

Se risken. Prioritera rätt. Få jobbet gjort.

Control ger er en tydlig startpunkt i den IT-miljö ni redan har. Under de första tre månaderna genomför vi tre scanningar, lägger till verksamhetskritikalitet, prioriterar de mest kritiska riskerna och etablerar ett arbetssätt för att få dem åtgärdade. Samtidigt ser vi var säkerhetsarbetet behöver stärkas runt den tekniska kontrollen. De tre månaderna är starten, inte slutet. Därefter fortsätter tjänsten med återkommande analyser, hotbevakning, expertstöd och verifiering så att ni kan följa och minska er tekniska risk över tid.

Se hela er IT-miljö SIT Appliance kartlägger automatiskt och återkommande hela den IP-nåbara IT-miljön inom avtalat scope och identifierar system, tjänster, produkter och versioner med hög precision. Det ger en bredare och mer korrekt sårbarhetsbild. All analys sker lokalt. Ingen information lämnar ert nätverk.	Åtgärda rätt först Det räcker inte att veta att en sårbarhet finns. Ni behöver veta vilken ni ska åtgärda först. SIT uppdaterar kritikaliteten utifrån nåbarhet, kända exploits, sannolik exploatering, aktivt utnyttjande, attackkedjor och verksamhetskritikalitet. Top Priorities visar vad ni ska börja med och rekommenderar åtgärd.
Bygg ett arbetssätt som håller Våra experter hjälper er att omsätta resultaten i tydliga prioriteringar, ansvar, åtgärdsplaner och uppföljning. Arbetssättet fungerar oavsett om åtgärderna genomförs av ert eget IT-team, en extern leverantör eller båda.	Stärk hela säkerhetsarbetet Under de första tre månaderna ser vi också var viktiga förmågor och arbetssätt behöver stärkas runt den tekniska kontrollen. Vi hjälper er prioritera nästa steg och kan rekommendera relevanta specialistpartners när behovet ligger utanför SIT:s egen leverans.

Tre månader för att få kontroll snabbare. Dubbelt expertstöd.

Under de första tre månaderna genomförs tre scanningar. Våra experter arbetar tätare tillsammans med er för att få kontroll på risknivån, prioritera de mest kritiska riskerna och etablera arbetssättet för åtgärd och uppföljning. Den inkluderade expertkapaciteten fördubblas så att ni snabbt kommer från nuläge till konkreta åtgärder. Därefter fortsätter expertstödet som en del av den löpande tjänsten.

SÅ SKAPAR VI KONTROLL

Från första nulägesbild till lägre risk över tid.

De första tre månaderna ger er en teknisk nulägesbild, tydliga prioriteringar och ett fungerande arbetssätt. Därefter fortsätter SIT Cyber Exposure Control som en löpande tjänst med återkommande analyser, hotbevakning, expertstöd och verifiering. Ni ser vad som förändras, vad som återstår och om den tekniska risken faktiskt går ned.

1 KARTLÄGG Scan 1 bygger en teknisk nulägesbild av hela den nåbara IT-miljön inom avtalat scope.	2 PRIORITERA Scan 2 lägger till verksamhetskritikalitet och visar vilka risker ni ska åtgärda först.	3 ÅTGÄRDA Ni eller er IT-partner genomför de prioriterade åtgärderna med stöd från SIT:s experter.	4 VERIFIERA Scan 3 visar vad som förändrats och om genomförda åtgärder faktiskt har minskat risken.	5 FÖRBÄTTRA Vi etablerar den löpande kontrollcykeln och stärker arbetssättet där nya behov uppstår.
--	--	--	---	---

Efter de första tre månaderna: löpande kontroll och förbättring

- **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, planera åtgärder och driva förbättringen vidare.
- **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 förbättring.** När er miljö och era behov förändras hjälper vi er att vidareutveckla arbetssättet, följa upp ansvar och prioritera nästa steg.

Varför Control gör skillnad

- **Teknik + människor.** Ni får automatisk teknisk kontroll och experter som hjälper er att omsätta resultaten i åtgärd.
- **Egen eller outsourcad IT.** Arbetssättet fungerar oavsett om åtgärderna genomförs av ert eget IT-team, en extern IT-leverantör eller båda.
- **Se hela behovet.** Vi identifierar viktiga luckor i säkerhetsarbetet runt den tekniska kontrollen och hjälper er prioritera nästa steg. För er som omfattas av cybersäkerhetslagen stödjer samma arbetssätt de tekniska delarna kring säkerhetstester och uppföljning.
- **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.
- **Rätt hjälp när den behövs.** När behovet ligger utanför Control hjälper vi er att definiera nästa steg och kan rekommendera relevanta specialistpartners.

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.

Kontroll. Rätt åtgärder. Lägre risk.

SIT Cyber Exposure Control ger er snabbt en korrekt teknisk bild, tydliga prioriteringar och ett arbetssätt som driver åtgärder hela vägen till verifierad effekt. Ni hittar de sårbarheter som faktiskt innebär störst risk, får rätt saker åtgärdade och ser om risknivån verkligen minskar. Våra experter fortsätter arbeta tillsammans med er när miljön och behoven förändras.

Resultatet är ett starkare och mer systematiskt säkerhetsarbete, färre kritiska risker och en teknisk risknivå som pressas ned över tid.