SIT CYBER EXPOSURE CONTROL

Få kontroll på cyberrisken. Åtgärda rätt först.

SIT Cyber Exposure Control är för er som behöver få ett systematiskt tekniskt säkerhetsarbete på plats och hålla det igång. Ni får oberoende, proaktiv kontroll före incidenten och expertstöd för att tolka resultaten, prioritera rätt och följa upp åtgärderna. Ni eller er IT-leverantör genomför förändringarna. Nästa scanning visar effekten och riskhistoriken visar utvecklingen 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, utan att ni först bygger en stor intern specialistfunktion. Under tre månaders etablering hjälper vi er att identifiera och prioritera tekniska risker, väga in verksamhetskritikalitet och få tydligt ansvar och uppföljning på plats. Vi går också igenom viktiga luckor i säkerhetsförmågor och arbetssätt. Därefter fortsätter tjänsten med återkommande teknisk kontroll, kontinuerlig hotmatchning och expertstöd. Arbetssättet fungerar med egen IT-drift, outsourcad drift eller en kombination.

Se vad som finns i er IT-miljö

SIT Appliance kartlägger avtalade IP-baserade system som den når från sin nätverksposition och identifierar system, tjänster, produkter och versioner. Det omfattar även andra siter, leverantörer och molnmiljöer när Appliance når dem. All intern analys sker lokalt. Ingen information lämnar ert nätverk.

Åtgärda rätt först

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.

Bygg ett arbetssätt som håller

Våra experter hjälper er att omsätta resultaten i tydliga prioriteringar, ansvar, åtgärdsplanering och uppföljning. Ni beslutar om risker och åtgärder. Ert IT-team eller er leverantör genomför förändringarna. Delta Report validerar effekten i nästa scanning.

Stärk hela säkerhetsarbetet

Under etableringen går vi igenom centrala säkerhetsförmågor och arbetssätt och identifierar de viktigaste luckorna. Vi hjälper er att prioritera nästa steg och rekommenderar relevanta specialistpartners när behovet ligger utanför Control. Större implementationsinsatser och specialistprojekt avtalas separat.

Tre månader för att få kontroll snabbare. Dubbelt expertstöd.

Tre scanningar etablerar teknisk nulägesbild, verksamhetskontext och den löpande kontrollcykeln. Small, Medium och Large omfattar 8, 12 respektive 16 experttimmar per månad under etableringen, därefter 4, 6 respektive 8. För Enterprise fördubblas avtalad kapacitet enligt offert. Tiden används för tolkning, prioritering, åtgärdsplanering och uppföljning. All tjänsteleverans och inkluderad expertkapacitet levereras från Sverige.

SÅ SKAPAR VI KONTROLL

Från första nulägesbild till lägre risk över tid.

Kartlägg → Prioritera → Rapportera → Åtgärda → Kartlägg igen. Cykeln upprepas och Delta Report visar vad som har åtgärdats, finns kvar och tillkommit i nästa scanning. SIT ger analys, rekommendationer och expertstöd. Ni eller er IT-leverantör genomför förändringarna. Kontinuerlig hotmatchning kompletterar cykeln mellan scanningarna.

1	2	3	4	5
NULÄGE	**KONTEXT**	**ÅTGÄRDER**	**UPPFÖLJNING**	**ARBETSSÄTT**
Scan 1 etablerar den tekniska nulägesbilden inom avtalat scope.	Scan 2 fördjupar verksamhetskontexten, prioriteringen och genomgången av processluckor.	Ni eller er IT-leverantör genomför prioriterade åtgärder med analysstöd från SIT.	Scan 3 visar vad som förändrats och validerar effekten av genomförda åtgärder.	Vi etablerar ansvar, uppföljning och den fortsatta återkommande kontrollen.

Efter de första tre månaderna: löpande kontroll och förbättring

- **Automatisk och återkommande kontroll. Scanningarna körs oövervakat i produktion.** Kontrollerna är utformade för att inte störa systemen och kräver liten löpande insats från ert team.
- **Expertstöd för att hålla arbetet igång.** Ni får hjälp att tolka, prioritera, planera åtgärder och följa upp ansvar. Arbetssättet utvecklas när er miljö och era behov förändras.
- **Rapporter som visar resultatet.** Top Priorities ger åtgärdsunderlaget. Technical Report visar hela riskbilden. Delta Report validerar åtgärdseffekten och SIT Risk Index-historiken visar riskutvecklingen.
- **Kontinuerlig hotmatchning.** Nya sårbarheter, zero-days och uppdaterad hotinformation matchas kontinuerligt mot den senast kända IT-miljön. Nya relevanta risker identifieras och ni notifieras.
- **Stöd i befintliga arbetsflöden.** Tvåvägsintegration med ServiceNow finns. Integrationer mot SOC, SIEM och andra arbetsflöden erbjuds som tillägg och avtalas separat.

Varför Control gör skillnad

- **En separat teknisk kontrollpunkt.** Agentlöst och oautentiserat. Inga agenter installeras på servrar eller klienter och inga privilegierade konton krävs på målsystemen.
- **Proaktiv kontroll före incidenten.** Appliance visar när de tekniska förutsättningarna för intrång finns utan att genomföra intrånget. SIT kompletterar EDR, XDR, SIEM och SOC.
- **Systematik och spårbarhet.** SIT kopplar tekniska kontrollresultat till regelverk och standarder, bland annat ISO 27001 och NIS2. Ni kompletterar med egna bedömningar och ser vad som behöver förbättras. Det stödjer regelefterlevnadsarbetet.
- **Utvecklat i Sverige.** SIT Appliance är utvecklat i Sverige. All intern analys sker lokalt. Ingen information lämnar ert nätverk.
- **Rätt hjälp för nästa steg.** Vi identifierar viktiga processluckor och kompletterande behov. Full gapanalys, större implementationsarbete och specialisttjänster avtalas separat.

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.

Cybersäkerhet ska inte vara en gissning.
Få en tydlig riskbild, åtgärda rätt först och följ upp effekten. Control hjälper er att etablera ett systematiskt tekniskt säkerhetsarbete och hålla det igång över tid.