SIT CYBER EXPOSURE ASSURANCE

Behåll kontrollen när ni lagt ut IT-driften

När IT-driften ligger hos en extern driftleverantör ligger ansvaret för cyberrisken fortfarande hos er. SIT Cyber Exposure Assurance ger er en egen, oberoende och återkommande teknisk kontroll, tydliga prioriteringar och expertstöd för att följa upp att rätt åtgärder genomförs och ger effekt.

SYFTET MED ASSURANCE

Ett eget tekniskt underlag - oberoende av driftleverantörens rapportering.

Driftleverantören kan göra ett bra jobb. Ni behöver ändå en egen teknisk kontroll av resultatet. SIT Cyber Exposure Assurance ger er en separat teknisk bild av de nät och system ni ansvarar för, så att ni och driftleverantören arbetar från samma fakta. Leverantörens uppdrag och angriparens attackyta är inte samma sak.

LOKAL ANALYS • INGEN INFORMATION LÄMNAR ERT NÄTVERK • UTVECKLAT I SVERIGE

Se hela den miljö ni ansvarar för

SIT Appliance kartlägger detaljerat de IP-baserade system som nås via ert interna nätverk - i era lokaler, på andra siter, hos IT-leverantörer och i molnmiljöer. Ni får en egen och mer korrekt teknisk bild av system, tjänster, produkter, versioner och relevanta sårbarheter.

Prioritera vad som ska åtgärdas först

SIT Risk Score sätter varje identifierad sårbarhet i er kontext och väger in teknisk allvarlighetsgrad, exploits, CISA KEV, EPSS, aktivt utnyttjande, attackkedjor och verksamhetskritikalitet. Rapporten Top Priorities visar vad ni och driftleverantören ska åtgärda först och vilken åtgärd SIT rekommenderar.

Verifiera att åtgärderna ger effekt

Nästa scanning visar vad som har åtgärdats, vad som finns kvar och vad som har tillkommit. Delta Report och SIT Risk Index visar hur den samlade risknivån utvecklas och var insatserna behövs mest.

En oberoende part i driftleverantörsdialogen

SIT:s experter hjälper er hela vägen - från att komma igång till att prioritera och följa upp åtgärder och föreslå förbättringar. Ni får också en oberoende part som hjälper er att formulera rätt frågor, bedöma svar och följa upp driftleverantörens genomförande.

Återkommande sårbarhetskontroll. Spårbar uppföljning.

Regelverk och standarder som cybersäkerhetslagen, NIS2 och ISO 27001 förstärker behovet av ett systematiskt och återkommande arbete med tekniska sårbarheter. SIT Cyber Exposure Assurance ger er återkommande säkerhetstester, prioriterade åtgärder, Delta Report och historik som visar vad som har förändrats och om åtgärderna ger effekt. Det ger ett spårbart tekniskt underlag för styrning, leverantörsuppföljning och regelefterlevnadsarbete. Tekniska kontrollresultat kopplas till bland annat ISO 27001 och NIS2 och kompletteras med era egna bedömningar.

DETTA INGÅR I SIT CYBER EXPOSURE ASSURANCE

En löpande tjänst - teknik, expertstöd och verifierad uppföljning

Tjänsten börjar med tre månaders etablering och fortsätter därefter som en återkommande kontroll. SIT Appliance visar när de tekniska förutsättningarna för intrång finns utan att SIT Appliance genomför intrånget. SIT Appliance scannar automatiskt och återkommande. Mellan scanningarna matchas nya sårbarheter, zero-days och uppdaterad hotinformation mot den senast kända IT-miljön. Nya relevanta hot identifieras och ni notifieras.

1	2	3	4
KARTLÄGG	**PRIORITERA**	**RAPPORTERA**	**ÅTGÄRDA**
SIT Appliance bygger en detaljerad teknisk bild av de nät och system som ingår och identifierar relevanta kända sårbarheter.	SIT Risk Score sätter riskerna i er kontext. Rapporten Top Priorities visar vad ni och driftleverantören ska åtgärda först.	Top Priorities, Technical Report och Delta Report ger underlag för åtgärd, leverantörsdialog och uppföljning.	Ni eller driftleverantören genomför åtgärderna. Nästa scanning verifierar effekten och startar nästa kontrollcykel.

MELLAN SCANNINGARNA: nya sårbarheter, zero-days och uppdaterad hotinformation matchas kontinuerligt mot den senast kända IT-miljön. Nya relevanta hot identifieras och ni notifieras.

SIT:s experter följer er hela vägen

- **Kom igång rätt.** SIT hjälper er att etablera baseline, verksamhetskontext, prioriteringar och ett fungerande arbetssätt.
- **Prioritera och förbättra.** SIT hjälper er att tolka resultaten, välja rätt åtgärder, följa upp arbetet och komma med förbättringsförslag.
- **Stärk driftleverantörsdialogen.** SIT är en oberoende part som hjälper er att formulera rätt frågor, bedöma svar och hålla fokus på de viktigaste åtgärderna.
- **Följ upp återkommande.** SIT går löpande igenom resultat, prioriteringar och åtgärder med er och stärker dialogen med driftleverantören. All inkluderad expertkapacitet och tjänsteleverans sker från Sverige.

Detta ingår löpande

- **12 automatiska scanningar per år.** SIT Appliance ger er en återkommande intern teknisk kontroll.
- **Hotmatchning och notifiering.** Nya relevanta hot identifieras mellan scanningarna och ni notifieras.
- **Rapporter och historik.** Top Priorities, Technical Report, Delta Report och SIT Risk Index-historik ger underlag för åtgärd, uppföljning och styrning.
- **Inkluderat expertstöd.** Small 3 h/mån, Medium 5 h/mån och Large 6 h/mån. Enterprise enligt avtal.
- **Dubbel expertkapacitet under etableringen.** De första tre månaderna får ni dubbelt antal inkluderade experttimmar.

Tre månader som etablerar kontrollen

Månad 1: baseline och första Top Priorities. Månad 2: verksamhetskontext läggs till och de första åtgärderna följs upp. Månad 3: genomförda åtgärder verifieras och den fortsatta kontrollcykeln etableras. Expertkapaciteten är dubblerad under hela etableringen.

Tillval: SIT Xternal

SIT Xternal kompletterar den interna kontrollen med återkommande kontroll av det som är exponerat mot internet. Resultaten samlas i SIT Appliance.

Behåll kontrollen när IT-driften ligger hos någon annan.

SIT Cyber Exposure Assurance ger er en egen teknisk faktabas, oberoende expertstöd i driftleverantörsdialogen och återkommande verifiering av att åtgärderna ger effekt.