SIT CYBERSECURITY

Cyberhoten förändras snabbt. Åtgärda de mest kritiska sårbarheterna först.

SIT kartlägger automatiskt och återkommande hela er IT-miljö på djupet och identifierar system, tjänster, produkter och versioner med hög precision. Det ger en bredare och mer korrekt sårbarhetsbild. Vi visar vilka sårbarheter som faktiskt går att nå och utnyttja, vad ni ska åtgärda först och hur er tekniska risk utvecklas över tid. All analys sker lokalt och ingen information lämnar ert nätverk. SIT är ett svenskt bolag och lösningen är utvecklad i Sverige.

VARFÖR SIT

Bättre bild av verkligheten. Bättre prioritering. Automatiskt och återkommande.

Bra prioritering börjar med rätt grunddata. SIT kartlägger hela er IT-miljö på djupet och identifierar system, tjänster, produkter och versioner med hög precision. I jämförande körning i verklig kundmiljö ger det en betydligt bredare och mer korrekt sårbarhetsbild än verktyg från andra leverantörer. Därefter uppdaterar SIT kritikaliteten genom att väga in om sårbarheten är nåbar, om det finns kända exploits, hur sannolik exploatering är, om den utnyttjas aktivt samt attackkedjor och verksamhetskritikalitet. Ni ser vad ni ska åtgärda först. Kontrollen upprepas automatiskt och återkommande över tid.

Se hela er IT-miljö

SIT Appliance kartlägger automatiskt och återkommande er interna IT-miljö på djupet och identifierar system, tjänster, produkter och versioner med hög precision. Det ger grunden för en bredare och mer korrekt sårbarhetsbild.

Se vad som är exponerat utifrån

SIT Xternal kartlägger automatiskt och återkommande er externa attackyta och visar vad som faktiskt är synligt från internet, vilka sårbarheter som är exponerade och vad som kan ge en angripare ett första fotfäste.

Prioritera utifrån verklig 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 vad ni ska åtgärda först.

Verifiera effekten över tid

Återkommande scanningar och rapporter visar vad som är nytt, vad som kvarstår och vad som är åtgärdat. Delta Report och Risk Score-historiken gör utvecklingen spårbar över tid.

Hotbilden förändras mellan scanningarna. SIT följer med.

Nya sårbarheter, zero days och kända exploits mappas löpande mot er senast kända IT-miljö. Ni ser snabbt om nya hot berör system och versioner som faktiskt finns hos er, utan att vänta på nästa scan.

Få en oberoende bild av vad som fortfarande kan utnyttjas.

SIT kompletterar de skydds- och övervakningssystem ni redan använder och visar vilka tekniska risker som fortfarande finns kvar. Ni ser vilka sårbarheter som faktiskt kan utnyttjas och var tid och budget gör störst nytta. SIT kan integreras med era befintliga system och arbetsflöden och bli en del av den samlade säkerhetskedjan.

FRÅN HELA BILDEN TILL RÄTT ÅTGÄRDER

Automatiskt. Återkommande. Spårbart.

SIT upprepar samma kontrollcykel automatiskt och återkommande. Vi kartlägger hela er IT-miljö, bygger sårbarhetsbilden, validerar vilka sårbarheter som faktiskt går att nå och utnyttja, prioriterar vad ni ska åtgärda först och verifierar resultatet. Ni ser både nuläget och hur er tekniska risk utvecklas över tid.

1	2	3	4	5
KARTLÄGG	**MATCHA**	**VALIDERA**	**PRIORITERA**	**VERIFIERA**
Kartlägg hela er interna IT-miljö på djupet och se vad som exponeras mot internet.	Bygg en bredare och mer korrekt sårbarhetsbild utifrån system, tjänster, produkter och versioner.	Bedöm om sårbarheten är nåbar, om det finns kända exploits, hur sannolik exploatering är, om den utnyttjas aktivt samt attackkedjor och verksamhetskritikalitet.	Lyft Critical och High som ni ska åtgärda först i Top Priorities.	Upprepa kontrollen och följ utvecklingen med nya scanningar, Delta Report och Risk Score-historik.

Konkreta resultat

- **Rätt åtgärder först.** Top Priorities lyfter Critical/High och ger er rekommenderade åtgärder, teknisk rapport och ledningsunderlag från samma analys.
- **Spårbar riskutveckling.** Automatiska och återkommande scanningar, Delta Report och Risk Score-historik visar hur er tekniska risknivå utvecklas över tid.
- **Tydlig ledningsrapportering.** Executive Reports och historik visar nuläge, trend och systematiken i ert säkerhetsarbete.
- **Tekniskt stöd för regelefterlevnad.** Kontroll och rapporter ger er tekniskt stöd i arbetet med ISO 27001, NIS2/cybersäkerhetslagen och uppföljning av säkerhetsåtgärdernas effekt.

Det som gör SIT annorlunda

- **Bättre teknisk bild.** SIT kartlägger hela er IT-miljö på djupet och identifierar system, tjänster, produkter och versioner med hög precision. Det ger en bredare och mer korrekt sårbarhetsbild.
- **Bättre prioritering.** 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. Prioriteringen bygger på faktisk risk, inte bara teknisk allvarlighetsgrad.
- **Automatiskt och återkommande.** Samma kontrollcykel upprepas över tid och ni ser hur er tekniska risk utvecklas.
- **Lokalt, oberoende och svenskt.** All analys sker lokalt och ingen information lämnar ert nätverk. Ni får en egen teknisk kontrollpunkt från ett svenskt bolag med svenskutvecklad teknik.

Se hela bilden. Åtgärda rätt först. Verifiera effekten.

Ni får en bredare och mer korrekt sårbarhetsbild, tydliga Top Priorities och en automatisk, återkommande kontroll som visar hur er tekniska risk utvecklas över tid. All analys sker lokalt. Ingen information lämnar ert nätverk.

Teknik och människor. Från sårbarhet till åtgärd.

SIT:s experter hjälper er att tolka resultaten, välja vad som ska åtgärdas först och följa upp att åtgärderna fungerar. Arbetssättet fungerar med egen eller outsourcad IT. När ni behöver andra förmågor identifierar SIT nästa steg och rekommenderar relevanta specialistpartners.