SIT APPLIANCE | PROAKTIV OCH ÅTERKOMMANDE TEKNISK KONTROLL

Ni kan inte åtgärda risker ni inte ser. SIT Appliance hittar dem.

SIT Appliance ger er en oberoende, proaktiv och återkommande teknisk kontroll före incidenten. Appliance kartlägger den IT-miljö den når, identifierar system, tjänster, produkter och versioner och matchar dem mot relevanta kända sårbarheter. SIT Appliance visar när de tekniska förutsättningarna för intrång finns utan att SIT Appliance genomför intrånget. Analysen sker lokalt. Ingen information lämnar ert nätverk.

BÄTTRE INFORMATION. BÄTTRE BESLUT.

Bra prioritering börjar med rätt bild av verkligheten.

Bra prioritering börjar med en detaljerad och korrekt bild av verkligheten. SIT Appliance identifierar de IP-baserade systemen i kontrollen och bygger en tydlig bild av vilka tjänster, produkter och versioner som faktiskt finns. Först därefter matchas miljön mot sårbarhetsunderlaget. En bättre verklighetsbild ger en bättre sårbarhetsbild och ett starkare underlag för prioritering.

Dedikerad fysisk hårdvara. Träffsäkrare analys. Automatisk kontroll.

Ni ansluter SIT Appliance till nätverket. Ingen programvara installeras på servrar eller klienter, inga privilegierade konton krävs och ingen serverkapacitet behöver avsättas för analysmotorn. SIT Appliance analyserar de IP-baserade system ni har valt att kontrollera – på samma site, andra siter, hos IT-leverantörer och i molnmiljöer – när nätverket ger åtkomst. Därefter körs kontrollen automatiskt och återkommande med liten löpande insats från ert team.

Se verkligheten bättre

SIT Appliances dedikerade fysiska hårdvara är en integrerad del av vår avancerade fingerprinting. Den ger kontrollerade förutsättningar för exakt identifiering av system, tjänster, produkter och versioner. Resultatet blir bättre sårbarhetsmatchning och tydligare prioritering, utan att vår analysmotor installeras på era servrar.

Hitta relevanta sårbarheter

SIT matchar den detaljerade miljöbilden mot ett brett och kontinuerligt uppdaterat sårbarhetsunderlag. Risker som inte identifieras kommer aldrig med i prioriteringen. Därför är en korrekt verklighetsbild avgörande: SIT hittar rätt sårbarheter och ger er ett starkare underlag för vad ni ska åtgärda först.

Prioritera rätt risker

SIT Risk Score (0–10) räknas fram för varje identifierad sårbarhet. I stället för att bara utgå från teoretiska CVSS-värden väger SIT samman teknisk allvarlighetsgrad med exploits, CISA KEV, EPSS, aktivt utnyttjande, attackkedjor och er verksamhetskritikalitet. Ni får en prioritering baserad på er egen kontext.

Visa förutsättningarna för intrång

SIT Appliance visar när de tekniska förutsättningarna för intrång finns och väger in kända flerstegsattacker i prioriteringen – utan att SIT Appliance genomför intrånget. SIT Appliance kör därför automatiskt och oövervakat i produktionsmiljön med låg driftsrisk.

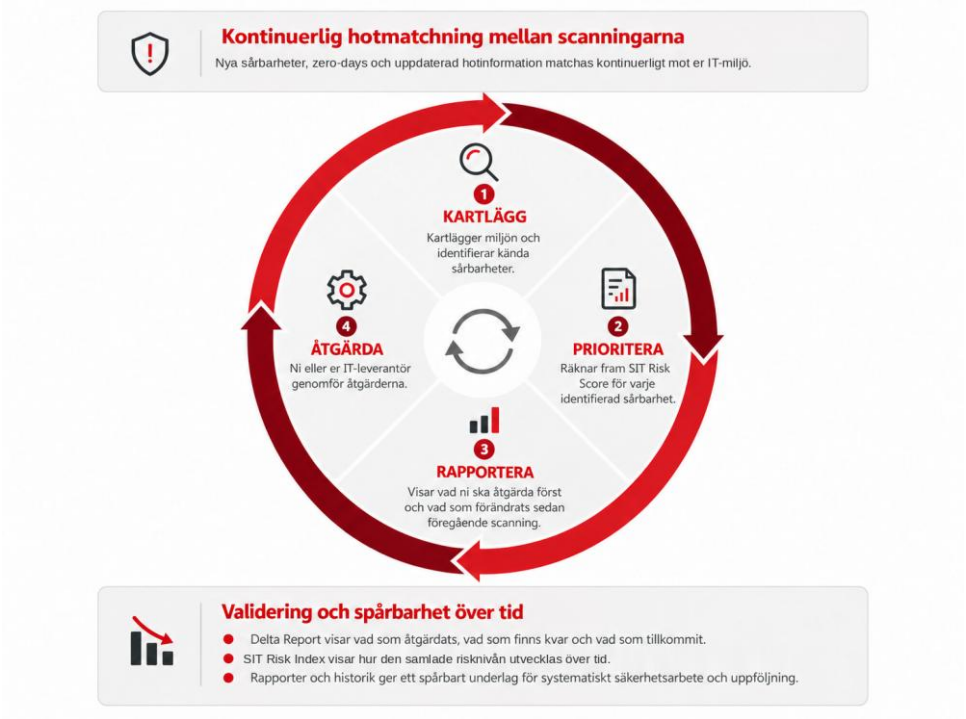
Från riskbild till rätt åtgärder först

Mer information är inte målet. Bättre beslut är målet. Rapporten Top Priorities visar vilka Critical och High ni ska åtgärda först och rekommenderad åtgärd. Technical Report behåller hela den identifierade riskbilden. SIT prioriterar det som minskar risken mest i just er miljö.

PROAKTIVT. AUTOMATISKT. ÅTERKOMMANDE.

Följ hotbilden. Åtgärda rätt. Verifiera effekten.

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. Nästa scanning visar vad som har förändrats och om genomförda åtgärder faktiskt gav effekt.



Från analys till verifierad effekt

- **Top Priorities.** Visar vilka Critical och High ni ska åtgärda först och rekommenderad åtgärd.
- **Delta Report.** Visar vad som har åtgärdats, vad som finns kvar och vad som har tillkommit sedan föregående scanning.
- **SIT Risk Index-historik. Visar hur den samlade risknivån utvecklas över tid och var den är högst.**
- **Technical Report.** Behåller hela den identifierade riskbilden för teknisk analys och uppföljning.
- **Spårbar uppföljning.** Rapporter, historik och undantag ger underlag för systematiskt säkerhetsarbete, teknisk compliance mot bland annat ISO 27001 och NIS2 samt egna bedömningar.

Varför SIT Appliance

- **Er miljö. Er data. Er kontroll.** Lokal analys i en härdad, nedlåst och krypterad Appliance. Ingen information lämnar ert nätverk. Utvecklat i Sverige.
- **Bred teknisk räckvidd.** SIT Appliance analyserar IP-baserade system på andra siter, hos IT-leverantörer och i molnmiljöer som nås via ert interna nätverk.
- **Agentlöst och oautentiserat.** Inga agenter och inga privilegierade konton på målsystemen. SIT bygger bilden utifrån det nätverket faktiskt visar.
- **Optimerar säkerhetsstacken.** SIT ersätter eller konsoliderar funktioner där SIT ger bättre resultat och kompletterar EDR, XDR, SIEM, SOC och andra system med andra roller. SIT Appliance kan integreras i befintliga arbetsflöden.
- **Tekniskt stöd för regelkrav.** Återkommande kontroll, Delta Report och historik ger spårbart underlag för riskanalys, säkerhetstest och uppföljning av åtgärders effekt, bland annat i arbetet med ISO 27001, NIS2 och cybersäkerhetslagen.

Se verkligheten bättre. Prioritera rätt. Pressa ned risken.

SIT Appliance ger er en bättre teknisk bild av er IT-miljö, visar vad ni ska åtgärda först, följer nya relevanta hot mellan scanningarna och verifierar effekten av genomförda åtgärder.

Bättre information. Bättre beslut. Verifierad riskreduktion över tid.

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