SIT APPLIANCE | AUTOMATED EXPOSURE VALIDATION

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

Bra säkerhetsarbete börjar med rätt information. SIT Appliance kartlägger automatiskt och återkommande er IP-nåbara IT-miljö på djupet och identifierar system, tjänster, produkter och versioner med hög precision. Det ger en bredare och mer korrekt sårbarhetsbild och ett bättre underlag för vad ni faktiskt ska åtgärda först. All analys sker lokalt. Ingen information lämnar ert nätverk.

BÄTTRE INFORMATION IN. BÄTTRE BESLUT UT.

Bra prioritering börjar med rätt bild av verkligheten.

Ni kan bara prioritera de risker ni faktiskt hittar. Om bilden av er IT-miljö är ofullständig blir också sårbarhetsbilden och prioriteringen ofullständig. SIT börjar därför med verkligheten: vad som faktiskt finns, vilka produkter och versioner som körs och vilka sårbarheter som hör till dem. Först därefter avgör vi vilka risker som kräver er uppmärksamhet.

En fysisk appliance. Enkel att införa. Byggd för återkommande kontroll.

SIT Appliance ansluts direkt till ert interna nät och analyserar det avtalade scopet utan agenter eller privilegierade konton. Ingen programvara installeras på era servrar eller klienter. När anslutning och scope är på plats kan kartläggning, analys och rapportering köras återkommande med mycket liten löpande insats från ert team.

Se vad som faktiskt finns

SIT kartlägger den IP-nåbara IT-miljön inom avtalat scope och identifierar system, tjänster, produkter och versioner med hög precision. Servrar, nätverksutrustning, klienter, skrivare, kameror och annan uppkopplad teknik blir en del av samma tekniska bild.

Hitta fler relevanta sårbarheter

Den tekniska miljöbilden matchas mot ett brett och kontinuerligt uppdaterat sårbarhetsunderlag. Resultatet är en bredare och mer korrekt bild av vilka kända sårbarheter som faktiskt berör de produkter och versioner som finns hos er.

Se vilken risk som faktiskt spelar roll

Det räcker inte att veta att en sårbarhet finns. SIT uppdaterar kritikaliteten utifrån nåbarhet, kända exploits, sannolik exploatering, aktivt utnyttjande, attackkedjor och verksamhetskritikalitet. Då ser ni vad ni ska åtgärda först.

Se attackvägen, inte bara fyndet

SIT visar när flera svagheter kan kombineras till attackkedjor och hur en angripare kan ta sig vidare genom IT-miljön. En till synes mindre sårbarhet kan då visa sig vara betydligt viktigare än den ser ut isolerat.

Från hela riskbilden till rätt åtgärder först

SIT Risk Score för samman teknisk exponering, aktuell hotinformation, exploaterbarhet, attackkedjor och er verksamhetskritikalitet. Top Priorities visar vilka Critical och High ni ska åtgärda först och vad ni bör göra åt dem. Technical Report ger er samtidigt hela den identifierade riskbilden.

AUTOMATISKT. ÅTERKOMMANDE. SPÅRBART.

Hotbilden förändras mellan scanningarna. SIT följer med.

SIT Appliance gör inte en punktmätning. Samma kontrollcykel upprepas automatiskt över tid så att ni ser vad som förändras, vilka risker som finns kvar och om genomförda åtgärder faktiskt minskar risken. Mellan scanningarna mappas nya sårbarheter, zero days och kända exploits kontinuerligt mot er senast kända IT-miljö. Ni meddelas när en ny risk upptäcks som berör er miljö.

1	2	3	4	5
KARTLÄGG	**MATCHA**	**VALIDERA**	**PRIORITERA**	**VERIFIERA**
Kartlägg system, tjänster, produkter och versioner i den IT-miljö Appliance når.	Matcha den faktiska miljön mot relevant och kontinuerligt uppdaterad sårbarhetsinformation.	Avgör vad som är nåbart och relevant utifrån exploits, aktuell hotbild, attackkedjor och verksamhetskritikalitet.	Top Priorities visar vilka risker ni ska åtgärda först.	Nästa scanning visar vad som förändrats och om den tekniska risken faktiskt minskar.

Från teknisk analys till beslut

- **Top Priorities.** De risker ni ska åtgärda först, med rekommenderad åtgärd.
- **Technical Report.** Hela den identifierade riskbilden när ni behöver gå på djupet.
- **Delta Report.** Vad som tillkommit, vad som finns kvar och vad som inte längre detekteras.
- **Risk Score-historik.** En tydlig bild av hur er tekniska risk utvecklas över tid och ett underlag för uppföljning och beslut.

Varför SIT Appliance

- **Bättre information ger bättre beslut.** Hög precision på system, tjänster, produkter och versioner ger en bredare och mer korrekt sårbarhetsbild innan prioriteringen börjar.
- **Automatiskt och återkommande.** Scanning, analys, hotmatchning och uppföljning körs över tid med mycket liten löpande insats från ert team.
- **Agentlöst och oautentiserat.** Inga agenter installeras och inga privilegierade konton krävs på systemen som analyseras.
- **Lokal analys. Svenskutvecklat.** All intern analys sker lokalt. Ingen information lämnar ert nätverk. SIT är ett svenskt bolag och tekniken är utvecklad i Sverige.
- **Byggd för återkommande körning i skarp driftsmiljö.** SIT validerar teknisk risk utan att göra den återkommande kontrollen till ett intrångstest och kan integreras med era befintliga system och arbetsflöden när det ger värde.

Se mer. Prioritera bättre. Pressa ned risken.

SIT Appliance ger er en bättre teknisk bild av er IT-miljö och ett skarpare underlag för vad som ska åtgärdas först. Ni hittar fler relevanta sårbarheter, lägger mindre tid på att sortera fynd och mer tid på rätt åtgärder. Den återkommande kontrollen visar sedan om åtgärderna faktiskt fungerar och hur er tekniska risk utvecklas över tid.
Resultatet är bättre säkerhetsbeslut, mindre manuellt arbete och en teknisk risknivå som pressas ned över tid.