

SIT XTERNAL | AUTOMATED EXTERNAL EXPOSURE VALIDATION

Se vad som är exponerat på internet. Åtgärda det innan någon utnyttjar det.

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 ni ska åtgärda först. Ingen intern installation, intern åtkomst eller inloggningsuppgifter krävs. SIT är ett svenskt bolag och tjänsten bygger på svenskutvecklad teknik.

UTIFRÅN OCH IN

Inventarielistan visar vad ni tror är exponerat. SIT Xternal visar vad internet faktiskt ser.

Nya system, tjänster, molnresurser och konfigurationsförändringar förändrar den publika attackytan hela tiden. SIT Xternal upprepar samma externa kontroll automatiskt och gör förändringar synliga över tid. När scopet är definierat körs kontrollen utan att ert team bemannar varje test eller installerar något i den interna miljön.

Extern discovery Identifierar internetnåbara system och exponerade tjänster inom definierat scope och bygger en aktuell bild av den publika attackytan.	Perimeter och sårbarheter Analyserar hur exponerade system, tjänster och perimeterkontroller svarar från internet och identifierar relevanta sårbarheter och felkonfigurationer.
Exploitkontext och ett första fotfäste Sätter fynd i relation till känd exploitinformation och bedömer hur exponeringen kan bidra till ett första fotfäste för en angripa.	Repeterbar kontroll Samma externa perspektiv kan återanvändas löpande så att ny eller förändrad exponering blir synlig, inte bara vid ett årligt pentest.

Automatisk och återkommande extern kontroll

När scopet är definierat körs SIT Xternal automatiskt och återkommande utan intern installation, inloggningsuppgifter eller åtkomst till ert interna nät. Ni följer en attackyta som förändras löpande med minimal insats från ert team.

FRÅN ATTACKYTA TILL ÅTGÄRD

Från extern exponering till rätt åtgärd

SIT Xternal ger er inte bara en lista över publika IP-adresser. Tjänsten hittar exponeringen, sätter den i exploitkontext, visar vad ni ska åtgärda först och verifierar återkommande att exponeringen förändras. Samma kontroll upprepas utan att skapa en ny intern testaktivitet varje gång.

1 KARTLÄGG Identifiera exponerade system, tjänster och den attackyta som syns från internet.	2 ANALYSERA Bedöm sårbarheter, felkonfigurationer och perimeterbeteende i det definierade scopet.	3 SÄTT KONTEXT Väg in relevant exploitinformation och betydelsen för ett första fotfäste.	4 PRIORITERA Gör tydligt vilka externa svagheter som bör hanteras först.	5 VERIFIERA Kör igen och se om exponeringen har försvunnit, förändrats eller återkommit.
--	---	---	--	--

När SIT Xternal ger störst värde

- **När ni vill veta vad som faktiskt är synligt.** Internetperspektivet visar vad som är nåbart utifrån, inte bara vad CMDB eller inventarielistor säger.
- **När attackytan förändras snabbt.** Nya tjänster, molnresurser, leverantörer och konfigurationer kan följas med samma återkommande metod.
- **När ni vill ha automatiserad och återkommande kontroll.** Efter att scopet är satt kan Xternal köras automatiserat utan intern installation, inloggningsuppgifter eller bemanning av varje körning.
- **När ni vill använda manuella pentest mer träffsäkert.** Xternal skapar kontroll mellan manuella penetrationstester och hjälper er att använda specialisttid där den ger mest värde.

Xternal + Appliance

- **Utsidan.** Xternal visar den internetexponerade attackytan och vad som kan bidra till ett första fotfäste.
- **Insidan.** SIT Appliance visar den interna tekniska exponeringen, attackkedjor och vilka risker som bör prioriteras inne i miljön.
- **Tillsammans.** Ni får ett sammanhållet internt och externt perspektiv och en betydligt starkare bild av var attackmöjligheterna faktiskt finns. Rapporterna innehåller den samlade informationen från båda produkterna.

Komplement till pentest, inte en ersättare

Xternal automatiserar de delar av extern säkerhetskontroll som tjänar på att göras ofta och likadant. Kreativ manuell penetrationstestning har fortsatt en viktig roll när djup, situationsanpassad angriparsimulering behövs. Xternal hjälper er att använda den typen av insats mer träffsäkert.