SIT CYBER EXPOSURE OPTIMIZATION

Better security starts with better information. Get more from your security work.

SIT Cyber Exposure Optimization is for teams with established security practices that want to see more, prioritise better and work more efficiently. Over three months, you compare SIT with your existing solution in the same IT environment. The results guide what to replace, consolidate, complement and integrate. The service then continues with independent, proactive checks before an incident occurs and ongoing tracking of technical risk.

FOR TEAMS WITH ESTABLISHED SECURITY PRACTICES

You already have a strong security programme. Make it more effective.

You have the tools, processes and expertise in place. We compare the technical insight, relevant vulnerabilities found, risk priorities and manual effort required. Same environment. Same conditions. Let the results decide. Where SIT provides a better overall basis for decisions, the aim is to replace traditional internal vulnerability scanning. Protection, detection and response systems with other roles are complemented by recurring technical risk reduction before an incident occurs.

Compare the full process in your environment

We run three scans alongside your existing solution. We agree the comparison criteria at the start: technical coverage and relevance, prioritisation, effort and follow-up value. SIT Appliance's dedicated physical hardware is part of our deep fingerprinting and requires no server capacity in your existing IT environment. Compare which serious vulnerabilities are found, which actions matter and whether those actions work. SIT identifies relevant and critical vulnerabilities that other market-leading solutions miss. Our comparative tests also show that we complete scans in less than half the time.

Sharper priorities

SIT Risk Score (0–10) combines technical severity with known exploits, exploitation likelihood, active exploitation and business criticality. Identified CVEs are matched against known multistage attacks, and attack chain context informs prioritisation. The Top Priorities report shows which Critical and High findings to address first and recommends actions.

Less manual work

SIT automatically maps systems, services, products and versions without agents or authentication. No privileged accounts are required on target systems. You gain a separate technical view and spend less time sorting findings. All internal analysis takes place locally in a hardened, locked-down and encrypted SIT Appliance. No information leaves your network.

Optimise your whole security stack

Replace or consolidate functions where SIT delivers better results. Complement EDR, XDR, SIEM and SOC with proactive checks before an incident occurs. Our experts help you compare results and define your future setup. SIT can integrate with tools in your existing security stack, making improvements easier to introduce.

Three months. Side by side. Double expert support.

Three scans provide a shared basis for decisions and a plan for continued use. Our experts support the comparison, business context and working practices. Small, Medium and Large include 8, 12 and 16 expert hours per month during onboarding, then 4, 6 and 8 respectively. Enterprise is defined in the quotation. All service delivery and included expert support are provided from Sweden. Exit terms are defined in the agreement; otherwise, the service continues on an ongoing basis.

HOW WE CREATE VALUE

From comparison to ongoing optimisation.

Map → Prioritise → Report → Remediate → Map again. The cycle repeats, and Delta Report validates the impact of earlier actions in the next scan. You or your IT provider make changes to your IT environment. SIT provides analysis, recommendations and expert support. Threat matching continues between scans.

1	2	3	4
BASELINE	**CONTEXT**	**COMPARE**	**NEXT STEPS**
Scan 1 establishes the technical baseline and the comparison against criteria agreed together.	Scan 2 adds business criticality and deepens the comparison of risks found and what to fix first.	Scan 3 shows the impact of remediation and supports an overall assessment of technical insight, priorities, effort and follow-up.	You decide what to replace, consolidate, complement and integrate into your ongoing security work.

After the first three months: ongoing optimisation

- **Automatic, recurring checks. Scans run unattended in production.** They are designed to avoid disrupting systems and require little ongoing effort from your team.
- **Expert support for ongoing optimisation.** Our experts help you interpret results, prioritise and improve working practices. Expert capacity follows your selected service size.
- **Validate the impact and track risk trends.** Technical Report shows the full risk picture. Delta Report shows what has been resolved, what remains and what is new. SIT Risk Index history tracks your overall risk level over time and identifies where it is highest.
- **Continuous threat matching.** New vulnerabilities, zero-days and updated threat intelligence are continuously matched against the last known state of your IT environment. New relevant risks are identified and you are notified.
- **Traceable security work.** SIT maps technical results to standards including ISO 27001 and NIS2; you add your own assessments. Reports and history support traceable security and compliance work.

Why SIT belongs in an established security stack

- **An independent view of your environment.** Compare actual results from the same environment. The results show which functions provide the best basis for decisions.
- **Local analysis with broad coverage.** Appliance checks the agreed IP-based systems it can reach from its network position, including other sites, providers and cloud environments.
- **Identify the conditions for a breach.** SIT Appliance identifies these technical conditions without carrying out the intrusion, enabling recurring checks with low operational risk.
- **Developed in Sweden.** SIT Appliance is developed in Sweden. All internal analysis takes place locally. No information leaves your network.
- **Integrate where it adds value.** SIT can integrate with tools in your existing security stack, including two-way ServiceNow integration. This makes improvements easier to introduce.

Add the external view with SIT Xternal

SIT Xternal is an optional addition that repeatedly checks your defined internet-facing attack surface. You see exposed systems and services, relevant vulnerabilities and the technical conditions for an initial foothold. Used with Appliance, results are combined and stored locally on your premises. You gain both an internal and an external view of exposure.

Better information. Sharper decisions. Lower risk.

SIT Cyber Exposure Optimization gives you better technical insight, sharper priorities and less manual work. You find more relevant vulnerabilities, focus on the right actions and verify that they reduce risk. Integrated into your ongoing security work, the service also provides continuous threat monitoring, recurring verification and a clear view of how technical risk changes over time.

The result is more effective security work, a simpler security stack and a technical risk level that is reduced over time.