SIT CYBER EXPOSURE CONTROL

Take control of cyber risk. Fix the right things first.

SIT Cyber Exposure Control is for teams that need to establish systematic technical security practices and keep them running. You get independent, proactive checks before an incident occurs and expert support to interpret results, set priorities and follow up on actions. You or your IT provider make the changes. The next scan shows the impact, and risk history tracks progress over time.

FOR TEAMS THAT NEED CONTROL QUICKLY

See the risks. Set priorities. Get the work done.

Control gives you a clear starting point in your existing IT environment, without first building a large in-house specialist team. During three months of onboarding, we help you identify and prioritise technical risks, consider business criticality and establish clear responsibilities and follow-up. We also review key gaps in security capabilities and working practices. The service then continues with recurring technical checks, continuous threat matching and expert support. It works with in-house IT operations, outsourced operations or a combination.

See what is in your IT environment

SIT Appliance maps the agreed IP-based systems it can reach from its network position, identifying systems, services, products and versions. This includes other sites, providers and cloud environments where Appliance has network access. All internal analysis takes place locally. No information leaves your network.

Fix the right things first

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.

Build a sustainable way of working

Our experts help turn results into clear priorities, responsibilities, remediation plans and follow-up. You make decisions on risks and actions. Your IT team or provider makes the changes. Delta Report validates the impact in the next scan.

Strengthen your overall security work

During onboarding, we review key security capabilities and working practices and identify the most important gaps. We help prioritise next steps and recommend relevant specialist partners where needs fall outside Control. Larger implementation efforts and specialist projects are agreed separately.

Three months to gain control faster. Double expert support.

Three scans establish the technical baseline, business context and ongoing cycle. Small, Medium and Large include 8, 12 and 16 expert hours per month during onboarding, then 4, 6 and 8 respectively. For Enterprise, agreed capacity is doubled as defined in the quotation. This time supports interpretation, prioritisation, remediation planning and follow-up. All service delivery and included expert support are provided from Sweden.

HOW WE ESTABLISH CONTROL

From an initial baseline to lower risk over time.

Map → Prioritise → Report → Remediate → Map again. The cycle repeats, and Delta Report shows what has been resolved, what remains and what is new in the next scan. SIT provides analysis, recommendations and expert support. You or your IT provider make the changes. Continuous threat matching complements the cycle between scans.

1	2	3	4	5
BASELINE	**CONTEXT**	**ACTION**	**FOLLOW-UP**	**PRACTICE**
Scan 1 establishes the technical baseline for the agreed networks and systems.	Scan 2 develops the business context, priorities and review of process gaps.	You or your IT provider carry out prioritised actions with analytical support from SIT.	Scan 3 shows what has changed and validates the impact of completed actions.	We establish responsibilities, follow-up and ongoing recurring checks.

After the first three months: ongoing control and improvement

- **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 to keep progress on track.** You get help to interpret findings, prioritise, plan actions and follow up on responsibilities. Working practices evolve as your environment and needs change.
- **Reports that show results.** Top Priorities guides action. Technical Report shows the full risk picture. Delta Report validates remediation, and SIT Risk Index history tracks risk over time.
- **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.
- **Support for existing workflows.** Two-way ServiceNow integration is available. Integrations with SOC, SIEM and other workflows are offered as separately agreed additions.

Why Control makes a difference

- **A separate technical assessment.** Agentless and unauthenticated. No agents are installed on servers or endpoints, and no privileged accounts are required on target systems.
- **Proactive checks before an incident occurs.** Appliance identifies the technical conditions for a breach without carrying out the intrusion. SIT complements EDR, XDR, SIEM and SOC.
- **Systematic work and traceability.** SIT maps technical findings to frameworks including ISO 27001 and NIS2. You add your own assessments and track gaps and improvements. This supports compliance work without guaranteeing full compliance.
- **Developed in Sweden.** SIT Appliance is developed in Sweden. All internal analysis takes place locally. No information leaves your network.
- **The right help for the next step.** We identify key process gaps and additional needs. Full gap assessments, larger implementation projects and specialist services are agreed separately.

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.

Cybersecurity should not be guesswork.
Get a clear view of risk, fix the right things first and verify the impact. Control helps you establish systematic technical security practices and sustain them over time.