# SIT CYBER EXPOSURE ASSURANCE

## Keep control when you outsource IT operations

When an external provider runs your IT, responsibility for cyber risk remains with you. SIT Cyber Exposure Assurance gives you your own independent, recurring technical security checks, clear priorities and expert support to verify that the right actions are taken and deliver results.

THE PURPOSE OF ASSURANCE

### Your own technical evidence, independent of your IT provider's reports.

Your IT provider may be doing a good job. You still need your own technical check of the results. SIT Cyber Exposure Assurance gives you a separate technical view of the networks and systems you are responsible for, so you and your provider work from the same facts. A provider's contracted responsibilities and an attacker's attack surface are not the same thing.

**LOCAL ANALYSIS • NO INFORMATION LEAVES YOUR NETWORK • DEVELOPED IN SWEDEN**

#### See the environment you are responsible for

SIT Appliance maps IP-based systems reachable through your internal network in detail, including your premises, other sites, IT providers and cloud environments. You gain your own, more accurate technical view of systems, services, products, versions and relevant vulnerabilities.

#### Decide what to fix first

SIT Risk Score puts each identified vulnerability in your context, considering technical severity, exploits, CISA KEV, EPSS, active exploitation, attack chains and business criticality. The Top Priorities report shows what you and your IT provider should address first and which action SIT recommends.

#### Verify that actions deliver results

The next scan shows what has been resolved, what remains and what is new. Delta Report and SIT Risk Index shows how your overall technical risk level changes and which areas need most attention.

#### Independent support in discussions with your IT provider

SIT's experts support you throughout, from getting started to prioritising, reviewing actions and identifying improvements. You also gain an independent party to help you ask the right questions, assess answers and follow up on your provider's implementation.

**Recurring vulnerability checks. Traceable follow-up.**

Regulations and standards such as Sweden's Cybersecurity Act, NIS2 and ISO 27001 reinforce the need for systematic, recurring work on technical vulnerabilities. SIT Cyber Exposure Assurance provides recurring security testing, prioritised actions, Delta Report and history showing what has changed and whether actions have worked. This provides traceable technical evidence for governance, supplier oversight and compliance work. Technical findings are mapped to frameworks including ISO 27001 and NIS2 and complemented by your own assessments.

WHAT SIT CYBER EXPOSURE ASSURANCE INCLUDES

# An ongoing service with technology, expert support and verified follow-up

The service starts with a three-month onboarding period, followed by recurring checks. SIT Appliance identifies the technical conditions for a breach without carrying out the intrusion. It performs scans automatically and on a recurring basis. Between scans, new vulnerabilities, zero-days and updated threat intelligence are matched against the last known state of your IT environment. New relevant threats are identified and you are notified.

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **MAP** | **PRIORITISE** | **REPORT** | **REMEDIATE** |
| SIT Appliance builds a detailed technical view of the networks and systems included and identifies relevant known vulnerabilities. | SIT Risk Score puts risks in your context. The Top Priorities report shows what you and your IT provider should fix first. | Top Priorities, Technical Report and Delta Report support action, discussions with your provider and follow-up. | You or your IT provider take action. The next scan verifies the impact and starts the next cycle. |

**BETWEEN SCANS: new vulnerabilities, zero-days and updated threat intelligence are continuously matched against the last known state of your IT environment. New relevant threats are identified and you are notified.**

## SIT's experts support you throughout

- **Start with a solid foundation.** SIT helps establish a baseline, business context, priorities and a practical way of working.
- **Prioritise and improve.** SIT helps you interpret results, choose the right actions, review progress and identify improvements.
- **Strengthen discussions with your IT provider.** SIT acts as an independent party to help you ask the right questions, assess answers and focus on the most important actions.
- **Review progress regularly.** SIT reviews results, priorities and actions with you and supports discussions with your IT provider. All included expert support and service delivery are provided from Sweden.

## Included on an ongoing basis

- **12 automatic scans per year.** SIT Appliance provides recurring internal technical security checks.
- **Threat matching and notifications.** New relevant threats are identified between scans and you are notified.
- **Reports and history.** Top Priorities, Technical Report, Delta Report and SIT Risk Index history support action, follow-up and governance.
- **Included expert support.** Small: 3 hours/month, Medium: 5 hours/month and Large: 6 hours/month. Enterprise as agreed.
- **Double expert capacity during onboarding.** You receive twice the included expert hours for the first three months.

### Three months to establish control

Month 1: baseline and the first Top Priorities. Month 2: business context is added and initial actions are reviewed. Month 3: completed actions are verified and the ongoing cycle is established. Expert capacity is doubled throughout onboarding.

### Optional addition: SIT Xternal

SIT Xternal adds recurring checks of your internet exposure to the internal assessment. Results are brought together in SIT Appliance.

**Keep control when someone else runs your IT.**

**SIT Cyber Exposure Assurance gives you your own technical evidence, independent expert support in discussions with your IT provider, and recurring verification that actions deliver results.**