Security Operations Centre

Security monitoring and incident response

SOC Service protects customer environment against cyber attack:

- **Threat detection and monitoring**
  Configuration of detection tools and 24/7 continuous monitoring.
- **Incident response**
  Resolve identified alerts and incidents. Performing defensive actions: containment, eradication and recovery.
- **SIEM system configuration**
  Implement, configure and maintain Microsoft Sentinel.
- **Threat hunting**
  Hunt for threats that are most likely to evade detection through traditional methods.
- **Threat Intelligence**
  Analyze current trends and understand future threats and attackers to better prepare security systems.

Why our clients decide to use Sii SOC services

- ➤ Significantly reduced successful attack risk.
- ➤ Faster detection and containment.
- ➤ Scalability and flexibility.
- ➤ Lower costs.

- ✓ Automated scans against common vulnerabilities
- ✓ Review and prioritize found vulnerabilities
- ✓ Oversee the process of fixes implementation (Vulnerability Management)

Vulnerability Assessment

- ✓ Performing penetration tests based on:
  - ✓ Penetration Testing Execution Standard
  - ✓ OWASP Web Application Penetration Testing Guide

Penetration tests

- ✓ Configurationof various security toolslike: MS Defender, CASB, IDS/IPS, MS Purview, and others
- ✓ Fine-tuning
- ✓ Upgrades

Security tools maintenance

The scope of our SOC service

SOC service implementation

- Analysis and improvement of existing process
- Security system 0 day audit
- Creation of workbooks and procedures for incidents handling
- SOC Team building

SIEM implementation

- Implementation of MS Sentinel
- Logs sourcing
- Configuration of queries and alerts
- Workbooks automation

Threat detection and monitoring

- Configuration of security detection tools (for example MS Defender)
- 24/7 or 8/5 security threats monitoring

Incident response

- Resolve identified alerts and incidents
- Triage identified incidents
- Performing defensive actions: containment, eradication and recovery

Threat hunting and intelligence

- Hunt for threats that are most likely to evade detection through traditional methods
- Analyze current trends and understand future threats and attackers to better prepare security systems

Security verification

- Vulnerability assessment
- Vulnerability management
- Penetration tests

Technologies

We use various technologies to meet your needs

Azure

Tangible Benefits / Desired Outcomes

✓ Significantly reduced breach risk thanks to faster detection and containment

✓ We can quickly scale up and down SOC service – depending on current need

✓ Cost effective – pay for needed activities, not for full team needed to cover 24/7

Microsoft Solution partner
Security

Microsoft Solution partner
Digital & App Innovation
Azure

Microsoft Solution partner
Data & AI
Azure

Microsoft Solution partner
Infrastructure
Azure
Specialist
Networking Services

Why Sii

150+ certified experts

OSCP, CEH, CISSP, GIAC GCIH, GIAC GCFE, CompTIA Security+

Secure project rooms

access control, 24/7 monitoring, security mantraps, and more

End-to-end support

from security assessment, solution design and implementation to verification, monitoring and incident response

Dedicated SOC team

If needed SOC team can be dedicated only for your project