SECURITY OPERATIONS CENTER

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.

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 Microsoft Sentinel
- Logs sourcing
- Configuration of queries and alerts
- Workbooks automation

Threat detection and monitoring

- Configuration of security detection tools (for example Microsoft 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

Why our clients decide to use Sii SOC services

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

Vulnerability Assessment

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

Penetration tests

✓ Performing penetration tests based on:

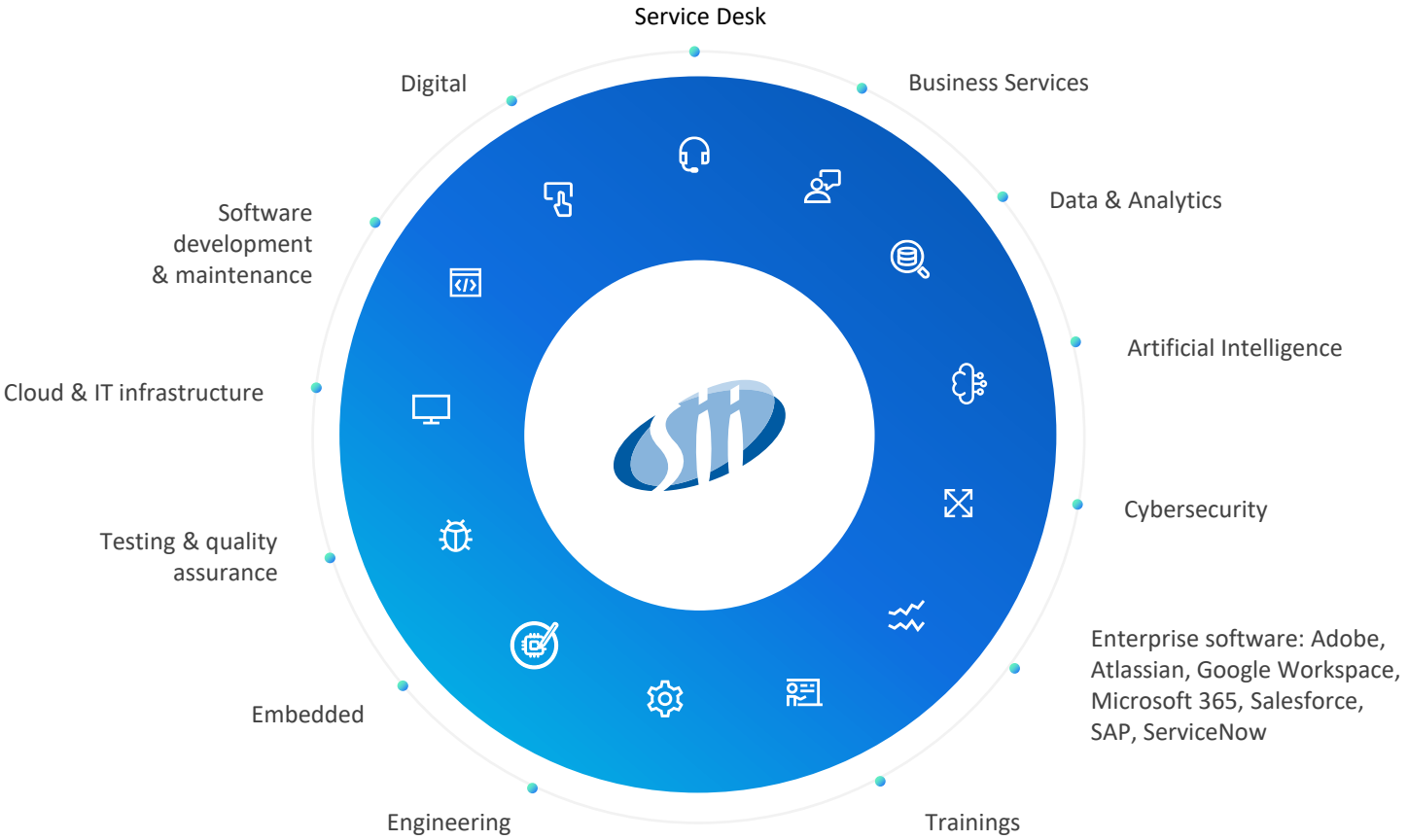
- Penetration Testing Execution Standard
- OWASP Web Application Penetration Testing Guide

Security tools maintenance

- ✓ Configuration of various security tools like: MS Defender, CASB, IDS/IPS, MS Purview, and others
- ✓ Fine-tuning
- ✓ Upgrades

Offer – One-stop shop

All services you need provided by one company



Tangible Benefits / Desired Outcomes

- ✓ You take care of your business development - we take care of the cloud
- ✓ Our architects will support you in the latest technologies
- ✓ We are ready to maintain your infrastructure with dedicated support team

Microsoft Solutions Partner

Microsoft Cloud

Why Sii

600 certifed experts

Solution Architects, Network Engineers, Security Engineers, DevOps Architects, Data Engineers, Azure Administrators, Azure Developer, Cybersecurity Artchitects, D365 Consultants, Power BI Analysts

Leading cloud services

Microsoft Azure, Microsoft 365, Dynamics 365, Power Platform

Innovative industry solutions

For manufacturing banking, healthcare, real estate and public sectors

End-to-end Project Support

Mrom preliminary data analysis, target model creation, implementation on dedicated devices to maintenance