axians

The best of ICT with a human touch

SECURITY OPERATIONS CENTER

Don't let cybercriminals compromise your business. Our SOC is your first line of defense, equipped with powerful tools and a dedicated team of security experts who work tirelessly to identify and neutralize threats.

Our SOC (Security Operations Center)

- International expert team
- Investigations and analysis
- 24/7 operation
- 10 x SOC in Europe
- Experience with 6 SIEM/SOC platforms

Our strong points

- Axians operates 10 SOC centers across the Europe
- Main focus on: **identification of incidents** and **threats** and their timely **resolution**
- Experience with the most widely used SIEM/SOC platforms
- Integration with HR systems, CMDB, ticketing systems, Asset and Risk Management
- Integration of physical security tools, access systems and use-cases combined with IT sources
- Use-cases for fraud detection in applications
- Integrated **threat intelligence** and on-going improvements

Do you know that?

- 43 % of cyber attacks are targeted at small businesses, but only 14 % are prepared to defend themselves
- 43 % of all breaches are caused by insider threats, either intentional or unintentional
- 66 % of small businesses have experienced a cyber attack in the past 12 months
- 95 % of cyber security breaches are caused by human error
- 54 % of companies say their IT departments are not advanced enough to handle sophisticated cyber attacks
- Approximately 70 % of breaches are financially motivated, while less than 5 % were motivated by espionage
- Nearly 40 % of breaches were caused by phishing, about 11 % by malware, and about 22 % by hacking

Security Operation Center

SERVICES PACKAGE

SOC SERVICES

Key service characterics

- 8x5 or 24x7 (web, phone, email)
- Access to experts (L1 to L3) included
- Initial setup and SIEM integration out-of-the-box connectors
- Use-cases definition
- Incident Response Plan

Added value

- Help with security monitoring and response process on customer side
- Proactive monitoring and adaptation to infrastructure changes
- Experience-driven scenarios approach

Services also includes

- Assessment before onboarding
- Incident Response Playbooks
- Customized report preparation
- Incident & threat identification
- Incident criticality identification
- Communication to remediation team
- Monthly report with incidents, threats, trends, and recommendations
- False positives tunning

Fixed price [per month]

SOC PROFESSIONAL SERVICES

Automation

- Customized connectors development
- Logs enhancement

SIEM Optimization

- License consumption optimization
- Storage and backup optimization
- Logging level optimization
- Traffic consumption optimization

Extras

- Architecture and design changes
- Migration projects
- Customized integrations
- Integration with ticketing systems
- Application analysis for use-cases preparation and SIEM integration
- Regulatory compliance assessment and integration to SIEM
- Other integrations via API

Variable price [per hour]

IBM Security SentinelOne FORTINET Microsoft Defender HUNTERS wazuh.

Contact:

Kryštof Oczadlý
Head of Sales
tel.: +420 720 761 981
e-mail: krystof.oczadly@axians.com

David Tůma
Sales Manager
tel.: +420 731 441 783
e-mail: david.tuma@axians.com

VINCI ENERGIES