Security Operations Centre (SOC)

The Security Operations Centre (SOC) is a solution to ensure the comprehensive central management of security situations and incidents at a single point with the aim of minimizing the response time to incidents and any damage that may arise.

www.aec.cz

AEC

The centre is based on the pillars of detection, analysis, investigation, response and post-incident activity. Continual real-time monitoring enables us to identify or possibly receive notification of potentially harmful activity within a protected infrastructure (detection). We determine whether this constitutes a security situation or incident that might have a negative impact on the infrastructure we protect (analysis). By examining the given security incident, we determine the specific impacts and method in which the attacker was able to penetrate the infrastructure (investigation). An immediate response minimizes the impact of the security incident (response). After a successful response, we ensure that lessons are learned from the incident (continual improvement), corrective measures are introduced, and all findings are reported to increase awareness (post-incident). This is all possible thanks to a robust combination of processes, technologies and human resources that are optimized to meet client needs.

Security Operations Centre (SOC)

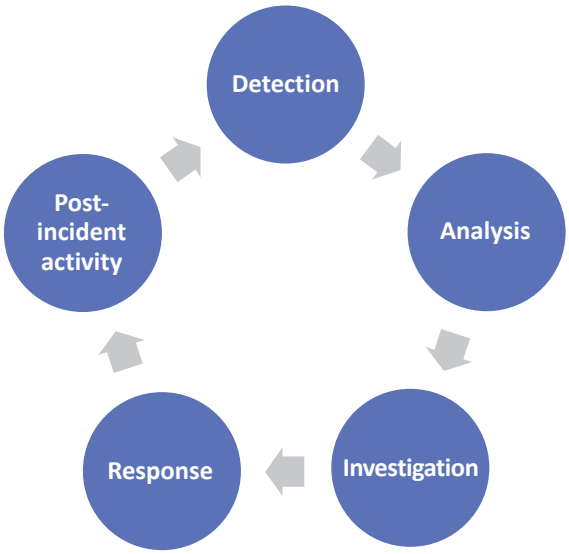
AEC offers two variants of the Security Operations Centre – onsite and as a service. The onsite SOC is completely built and administered by the client. The role of AEC for such types of SOCs is based primarily on a Support Agreement, where certain key security elements may be managed by AEC. SOC as a service is operated within the AEC infrastructure, to which the client is connected. AEC also offers related professional services such as: Cybersecurity Incident Response Team, Malware Analysis, Brand Protection, Cyber Threat Intelligence, Security Awareness, Continual Security Advisor and consulting services in various areas of security.

Reasons to acquire an SOC

- Reduced incident response times (increasing efficiency) and thus decreased incident impact (reducing replacement costs)
- Centralize security in a single place
- Gain real-time awareness of the security situation within the infrastructure
- Reduce human resource costs (SOC operators instead of technicians for individual technologies)
- Minimize operator errors (security automation) thanks to pre-defined incident resolution procedures
- Cover a comprehensive portfolio of security threats
- Respond to current and newly emerging threats

Key benefits

- Directly optimized for client infrastructure
- Reflects current security threats and Cybersecurity trends
- Increases level of security
- Reduces incident response time
- Provides an overview of the security situation within the infrastructure



Why choose AEC?

- We possess a team of experienced security consultants and specialists
- Our specialists are able to integrate a broad portfolio of technologies into a single point and create and set processes for these technologies to ensure the proposed solution functions properly
- We use penetration tests to test the design and function of the proposed solution
- We are a local company with a core group of employees that prioritizes an individual approach to every client
- We can supply references from large clients
- We have nearly 30 years of experience in information security across all sectors (banking, energy and utilities, telecommunications, manufacturing, media and trade, insurance, and the public sector)

AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283