Cyber Defense Center

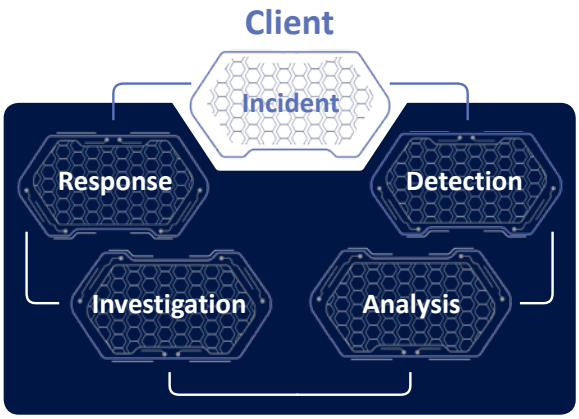
SOC as a Service

AEC

Monitor your infrastructure and prevent cyber attacks

The Cyber Defense Center (CDC) handles cyber security incidents on behalf of our clients. We help prevent incidents or detect them in time, eliminate or mitigate their impact and keep necessary records. The center uses the latest technologies and proven techniques and tactics for 24/7 security.

The center stands on the pillars of detection, analysis, investigation, response and post-incident activity. Through continuous real-time monitoring we identify or are notified of potential malicious behavior in protected infrastructure (detection). We determine whether this is a security incident that may have a negative impact on the protected infrastructure or just a false alarm that requires adjustment of detection mechanisms (analysis). By investigating security incidents, we determine the specific impacts and pathways used by attackers to penetrate the infrastructure (investigation). By responding immediately, we minimize the impact of security incidents (response). After a successful response, we learn from the incident and ensure the implementation of corrective measures and appropriate reporting for records and to increase awareness (post-incident activity).



Cyber Defense Center

aec-security.eu

Cyber Defense Center – SOC as a Service

Our team

The center is run by a veteran team of certified security analysts and administrators trained at global Security Operations Centers who have experience in deploying cutting-edge technologies and handling security incidents at the local and global levels.

CDC Services

- Security monitoring - Security monitoring tracks and resolves security incidents in real time. Key elements include the ability to differentiate incidents from false alarms, respond to incidents, and propose modifications to detection mechanisms.
- CSIRT - If an incident occurs, the Computer Security Incident Response Team is able to respond right at the place of origin, or possibly offer remote coordination to manage the situation.
- Vulnerability management – the process where we detect, evaluate, prioritize and provide recommendations on how to address vulnerabilities in the customer's infrastructure. Here we identify what must be addressed immediately and what can wait until the next patch cycle.
- Brand protection – where we scour the dark web looking for any signs of attack on our customers.
- Forensic analysis – in-depth analysis of security incidents that have already occurred and which require the collection of more data for continued investigation.
- Security consulting - the greatest value added of AEC, where we are able to cover nearly the entire cyber security portfolio.
- SOC - construction of a customized Security Operations Center directly within the client's environment to meet its needs and requirements.

Reasons to purchase an SOC

- Reduced incident response time (increased effectiveness) resulting in reduced incident impact and decreased recovery costs.
- Single point centralization of security.
- Real-time awareness of the security situation in the infrastructure.
- Reduced costs for human resources (security analysts are part of the service delivered).
- Minimal opportunity for operator error (automated security) thanks to predefined incident resolution procedures.
- Coverage of a comprehensive portfolio of security threats, both current and emerging.

Our strengths

- We are a leading Czech company that has been operating successfully for over 30 years, focusing on information security throughout this time.
- We have an experienced team of certified security consultants and specialists.
- Our specialists are able to integrate a broad portfolio of technologies into a single point and create and set up processes and comprehensive detection and correlation rules to ensure the proper functionality and visibility of the proposed solution.
- The solutions we offer are directly optimized for the client's infrastructure and reflect its architecture, current security threats and cyber security trends.
- We listen to clients and adapt our solution to meet their needs, requirements and capabilities.
- We have references from large clients across many sectors (banks, utilities, telecommunications, manufacturing companies, media and trade, insurance companies and the public sector).

Many years of experience and collaboration across AEC

Security Assessment Division
We use the experience of our penetration testers in real environments and adapt our detection and correlation rules accordingly. We regularly test our detection capabilities, including the work of our analysts.

Risk & Compliance Division
We work with process specialists to create and document processes between clients and the CDC.

Security Technologies Division
Our colleagues help us eliminate problems detected in client security systems and improve system development (NGFW, IDS/IPS, DLP, EDR configuration and more).

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