Cyber Defense Center

AEC

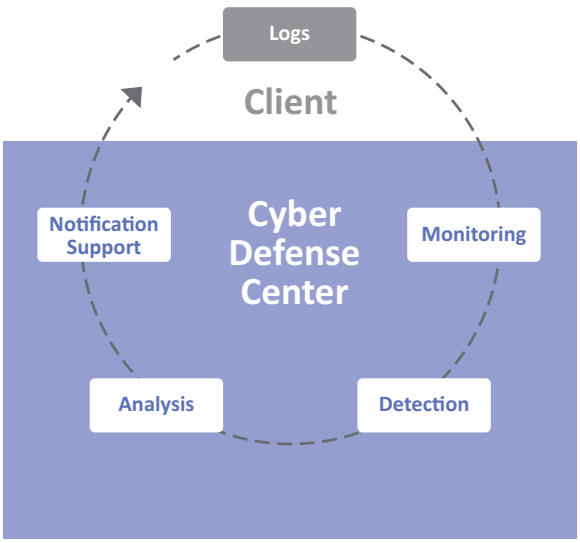
Securing the confidentiality, integrity and availability of data in modern enterprises comprises several tasks, ranging from systems management, change and configuration management, and also a cybernetic security strategy. An effective strategy must also cover detection and reaction to security incidents – no company that processes sensitive data can survive without such measures. The detection and reactionary abilities of a company are directly related to the knowledge, experience and quality of security tools and it is precisely these ingredients that our Cyber Defense Center has – and we are ready to provide them also to you.

www.aec.cz

Our team

The CDC is run by a team of experienced analysts and SIEM administrators with **practice from global SOC**, experience with the use of state-of-the-art technology and with **handling large-scale incidents as well as APT attacks** on local and global levels.

CDC services



Cyber Defense Center

CDC services

- **Security Monitoring** – implementation and development of detection rules, analysis of security events and incidents.
- **Incident Response** – recommendations on how to proceed in order to solve security incidents and help with handling them.
- **Threat Hunting** – active search for new threats and suspicious anomalies over collected events from the client's environments.
- **Threat Intelligence** – detection rules are enriched by IOC from external information sources/feeds.
- **Advanced Detection and Protection for Assets** – an agent-based solution with unique prevention and especially detection capabilities and reactionary functions which also allow for the remote solution of incidents on devices.
- **Cyber Brand Protection** – monitoring of external information sources with the aim of detecting leaks of defined sensitive data from the client's environment (login data, internal documents etc.).
- **Malware and Forensic Analysis** – analysis of the behavior and possible impacts of harmful code, forensic collection and analysis of data using procedures and outputs that are acceptable in court proceedings.
- **Professional Services** – impact analysis, proposal and support for the implementation of corrective measures after extensive cybernetic incidents or APT attacks (impact analysis is conditioned by the installation of agents on end devices).

Forms of service provision

- **Complete outsourcing** – you receive complete service, including not only CDC services but also the price of all required licenses and HW. CDC SIEM is operated in a so-called multi-tenant environment, where events from individual clients are strictly separated from each other. If you require logs to be saved in your own infrastructure, the data storage can be operated on your (the client's) side.
- **Hybrid model** – you own the licenses for SIEM and the hardware, we deliver the services.

The contributions of our solution

Cyber Defense Center provides stronger protection, with less things to worry about and lower costs

- **Significant reduction of risks** – Above-standard client protection thanks to continuous monitoring and development of detection rules. Our highly experienced CDC team efficiently and independently handles detected events.
- **Lower costs** –CDC services are of high quality but also allow clients to save operating costs compared to running the same services internally. No more worries with finding, raising and the retention of expert employees.
- **State-of-the-art technology** – the used tools are among TOP products on the market (SIEM, EDR, Threat Intelligence). We continuously keep track of the development of new products and deliver carefully tested and verified functionalities.

We make use of our many years of experience and collaborated through all AEC divisions

- **Security Assessment Division** – we utilize the experience of our pentesters from real environments and to this end adapt the composition of correlation rules; we also regularly test our detection capabilities including the work of our analysts.
- **Risk & Compliance Division** – we work with process specialists on the creation and documentation of processes on the interface between clients and the CDC.
- **Security Technologies Division** – our colleagues help you with fixing problems detected on the client's security solutions (configuration of the FW, IDS/IPS, DLP etc.).

Want to be sure you're not making a mistake? Try us!

- **We offer a trial mode for CDC services.**
- **We'll demonstrate our state-of-the-art detection and reaction capabilities on your selected asset. We can detect, among others:**
  - Infected servers and stations in your network,
  - Defective communication between your end devices and Command and Control servers on the internet (Botnets etc.),
  - Connections to Bitcoin miners from your network,
  - Misuse of privileged accounts.
- **We will show you the real threats you are facing and also propose ways to reduce them.**

Maturity assessment

- **We will carry out a quick maturity assessment of your SIEM/SOC.**
- **We will assess the level of your detection and reaction capabilities**

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