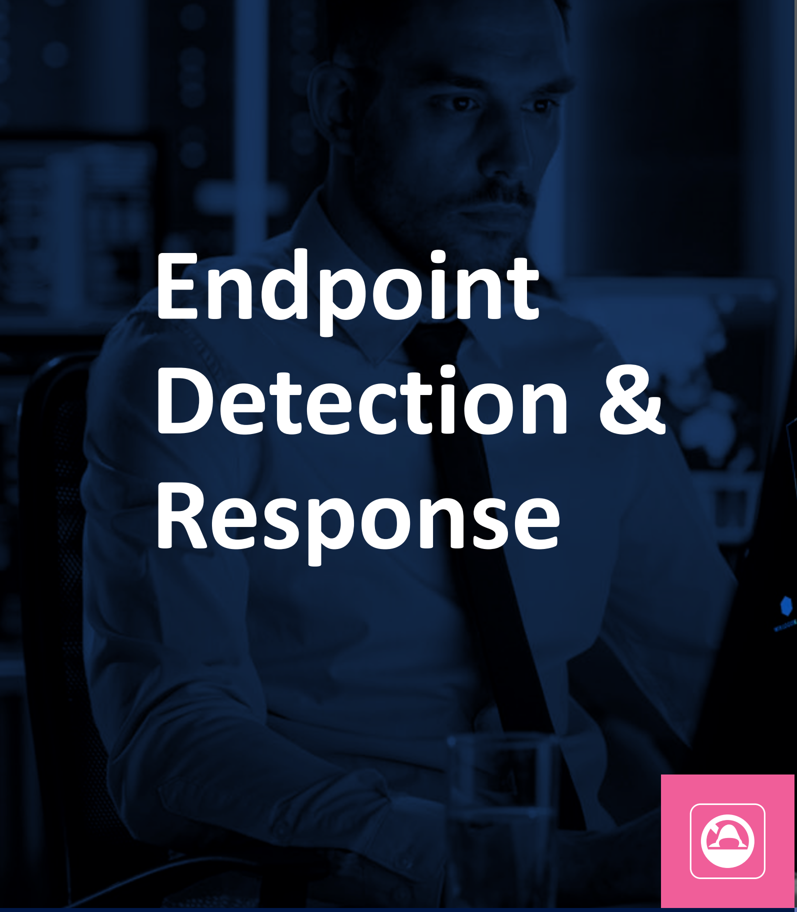


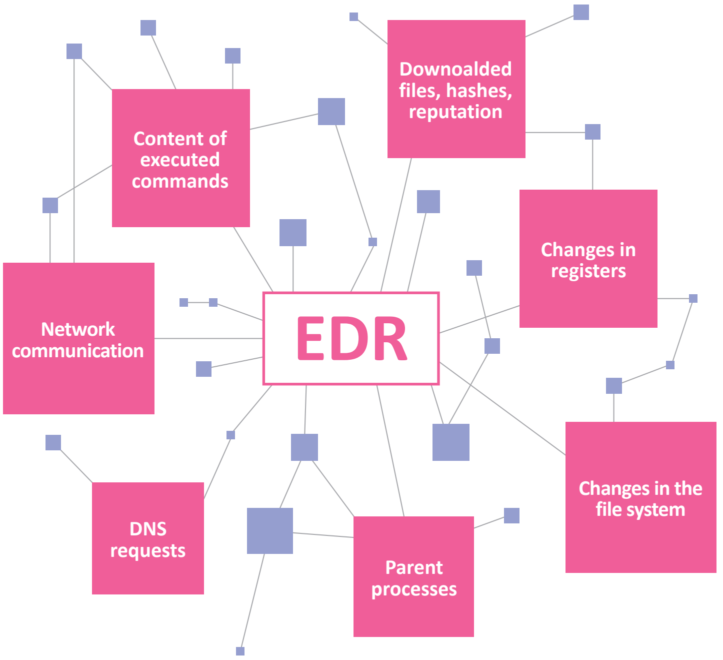
Endpoint Detection & Response

AEC

Endpoint Detection and Response (EDR) products are designed to protect endpoints from malicious code and penetration by attackers. Their difference from conventional anti-virus products lies in the logging of important activities on endpoints and a wide range of incident resolution options.

Collecting information

With EDR solution, it is possible to collect information about endpoint activities and thus provide efficient assessment of security incidents. There is no need to integrate log sources to the EDR tool, the endpoint agent has it all covered. Installation takes only several seconds, and it can be done centrally.



EDR

Downoalded files, hashes, reputation

Content of executed commands

Changes in registers

Network communication

Changes in the file system

DNS requests

Parent processes

www.aec.cz

Why EDR from AEC?

1

We analyse the incident

- How the attacker accessed the system
- What activities did the attacker execute
- How to prevent similar attack in the future

2

We respond immediately

- Security team arriving within 3 hours
- Monitoring the attacker and his real-time blocking
- Downloading suspicious files for analysis

3

We help to stop the attack

- Enforced termination of harmful processes
- Endpoint separation from the network
- Deleting all attacker’s residues

4

Continuous monitoring

- In 24/7 or 8/5 mode
- Security Analyst on stand-by
- Regular reporting of less serious activities

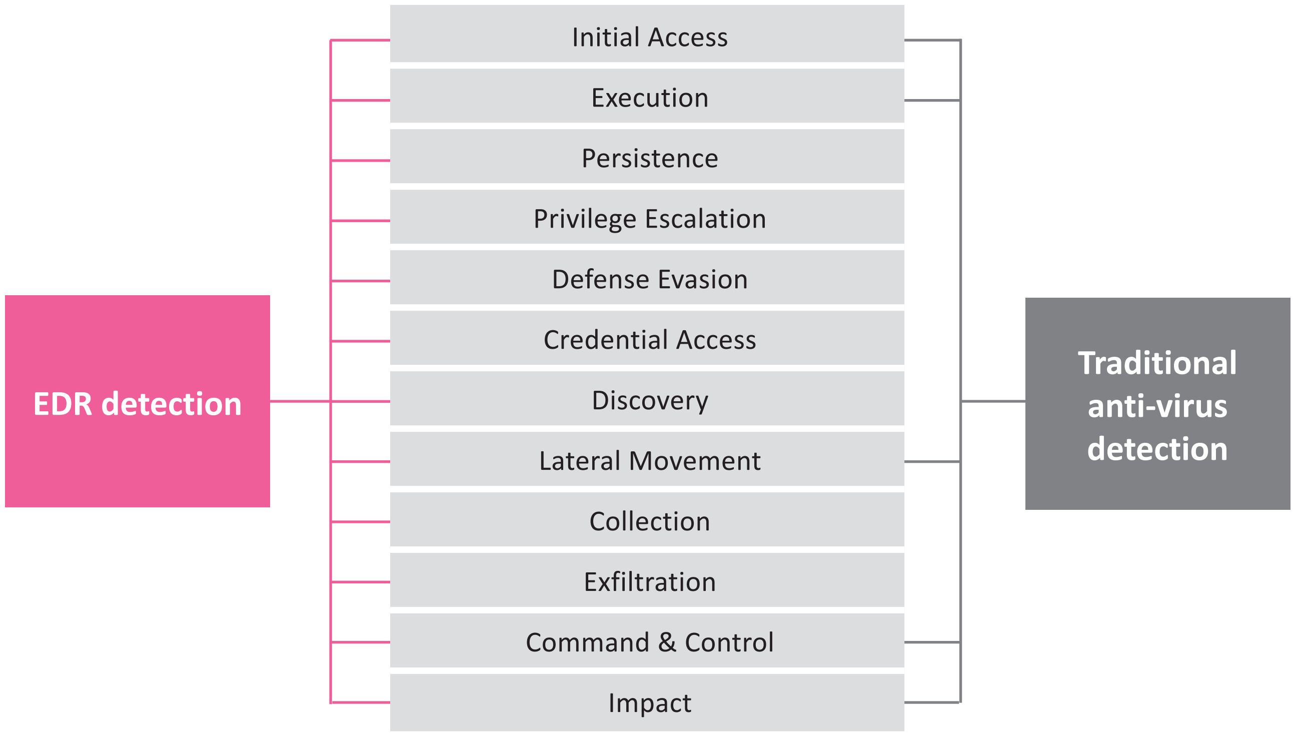
When it is hard to manage internally

Correct assessment of all security events can be time and capacity consuming. That is the reason why we also offer the services provided by Cyber Defense Center, our security operations centre. Our analysts investigate security incidents and can respond immediately in the event any issues occur.

What EDR has that AV has not?

- Collecting information on running processes
- Covering the whole spectrum of MITRE ATT&CK tactics used during attacks
- Making own YARA rules
- Enforced termination of a process or blocking network communication

MITRE ATT&CK tactics



EDR detection

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Exfiltration

Command & Control

Impact

Traditional anti-virus detection