EDR - response to ransomware, 0-day attacks and SOC requirements

Protection against modern cyber-attacks (incl. ransomware and 0-day) is possible thanks to signature-less identification of threats, and taking immediate responses to incidents and automated system recovery in the case of damage. Endpoint Detection and Response (EDR) is a new category of security systems that addresses these needs.

Verify how your systems are protected

EDR covers the entire cyber-attack handling process (below according to the NIST Cybersecurity Framework*). The multi-tenant EDR management system enables the provision of SOC services to many organizational units or many companies.

PHASE OF CYBER-ATTACK HANDLING PROCESS	FUNCTION SUPPORTING THE CYBER-ATTACK HANDLING PROCESS	EDR
IDENTIFY	Signature-less malware detection, incl. ML/behavioral	●
	Protection of virtual machines in the cloud, cloud workloads and containers (incl. Kubernetes)	●
PROTECT	Application inventory and vulnerability management	●
	Firewall controlling access to/from the network	●
	Control of USB and Bluetooth devices	●
DETECT	Incident identification based on ML/behavioral and Threat Intelligence	●
	Visualization of malware and other threats, including process operations map, network connections map	●
RESPOND	Incident response, incl. network quarantine	●
	Post-event forensic analysis, incl. remote PowerShell script execution	●
	Threat hunting, IoC search on all systems	●
RECOVER	Clearing the system after an incident, incl. automatic removal of changes made by malware	●
	System recovery after an incident, incl. automatic rollback from backup in case of ransomware	●

* Framework for Improving Critical Infrastructure Cybersecurity, NIST