Video transcript

Security monitoring

Cybersecurity threats can happen at any time. If you want your systems to be safe you must always be ready to find and react to an attack. Security monitoring involves continuously watching and analyzing the network, systems, and applications of an organization for potential threats and weaknesses. The goal is to identify and mitigate security threats before harm is done to an organization's data, systems, and reputation.

Effective cybersecurity requires skilled security professionals who analyze collected data and respond quickly to security incidents. But even the best security professionals can't be everywhere at all times. Monitoring cybersecurity also requires advanced tools and technologies. Security information and event management or SIEM monitors events in real time, analyzes them, and logs security data for compliance or auditing. SIEM solutions perform data collection, consolidation, and sorting to identify threats and adhere to data compliance requirements. They pinpoint unusual user behavior and then use artificial intelligence to automate processes of threat detection and incident response.

An intrusion detection system or IDS notifies an organization of attempts to hack into, disrupt, or deny service to the system. Specifically, intrusion detection involves gathering information about attacks arriving over the TCP/IP network. Most attackers try to get information about a system before attempting entry, so detecting these probes is a vital part of system security. An IDS also monitors for possible extrusions, where a system might be hijacked and used without an organization's knowledge as the source of an attack on another system.

Endpoint detection and response, or EDR, automatically protects an organization from cyberthreats that get past traditional endpoint security tools. This includes endpoint users, devices, and assets. EDR collects data continuously from all endpoints on the network: desktop and laptop computers, servers, mobile devices, and more. EDR analyzes this data in real time for evidence of cyberthreats and it can respond automatically.

Managed detection and response, or MDR, combines automated functions and human intelligence to provide continuous monitoring, threat detection, and incident response services. In short, MDR is EDR with added human intelligence. An EDR tool usually provides the monitoring information, tracking, and analysis. Then the system passes relevant threat information, advanced analytics, and forensic data to

human analysts, who assess alerts and determine appropriate responses to remove the threat and restore any damage.

Any time, day or night, malicious threats can appear. Good security monitoring systems ensure that you can relax knowing your infrastructure is safe.