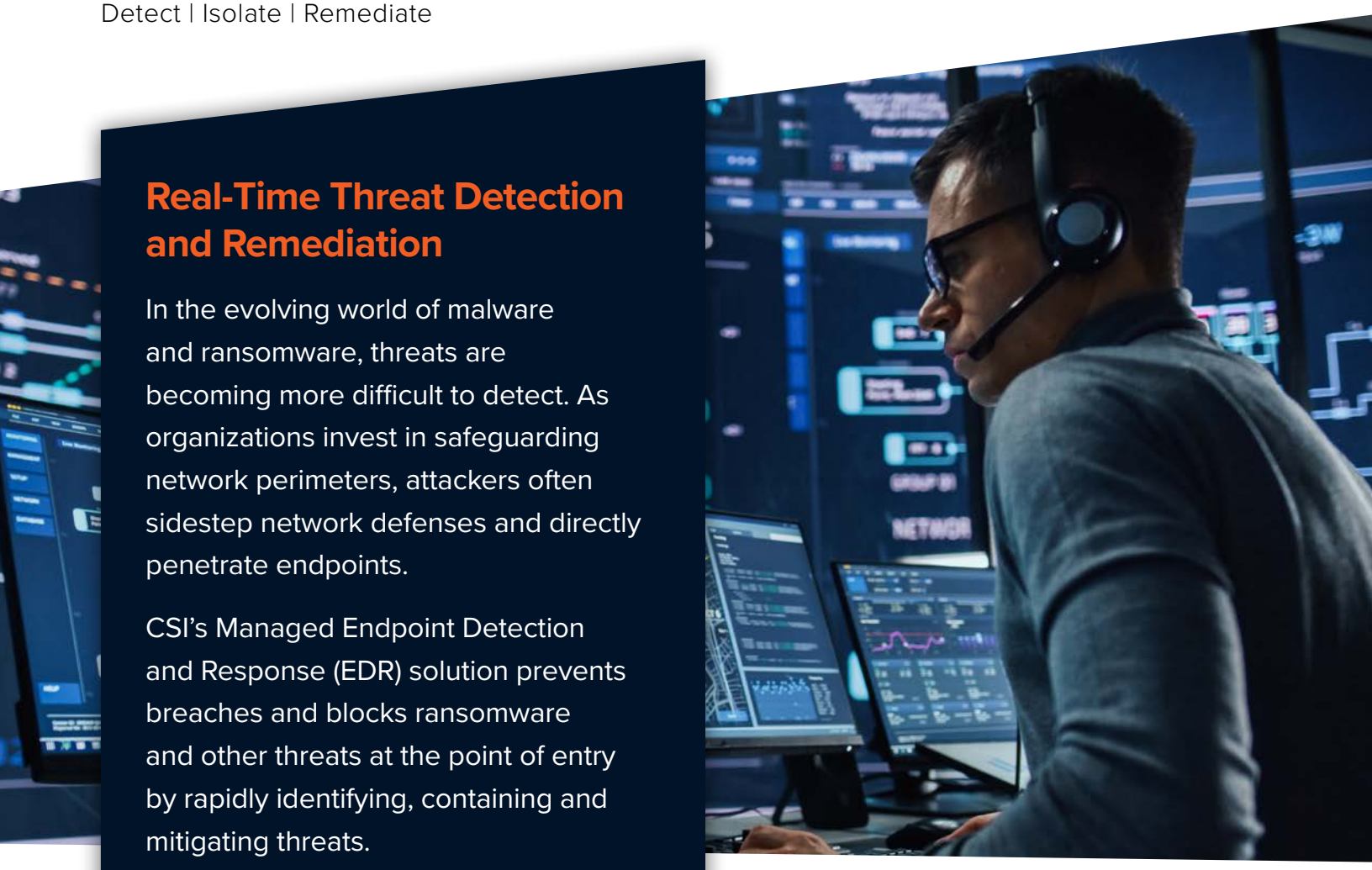
CSI Managed Endpoint Detection and Response

Detect | Isolate | Remediate



Real-Time Threat Detection and Remediation

In the evolving world of malware and ransomware, threats are becoming more difficult to detect. As organizations invest in safeguarding network perimeters, attackers often sidestep network defenses and directly penetrate endpoints.

CSI's Managed Endpoint Detection and Response (EDR) solution prevents breaches and blocks ransomware and other threats at the point of entry by rapidly identifying, containing and mitigating threats.

CSI Managed EDR: Advanced Threat Protection

EDR detects suspicious behavior and provides organizations with contextual information about incidents, delivering comprehensive protection by:

- **Leveraging behavioral analysis and actionable intelligence to prevent an incident from turning into a breach**
- **Protecting against zero-day exploits, which are vulnerabilities with no available patches**
- **Providing continuous, real-time visibility into activity on endpoint devices**
- **Delivering around-the-clock monitoring and remediation from CSI's security operations center (SOC)**

How CSI Managed EDR Keeps Your Organization Protected

Integrated with CSI SIEM-as-a-Service (SIEMaaS), CSI Managed EDR produces logs of endpoint activity that are captured in the SIEM to provide a more holistic analysis of attacks in an environment, thereby enhancing defenses against internal and external threats.

CSI provides end-to-end management of the service, including deployment, management and updating of endpoint agents combined with alert remediation, infected system isolation and remote removal of threats. CSI Managed EDR delivers real-time visibility into an organization's system using technology to prevent, detect and respond to attacks.

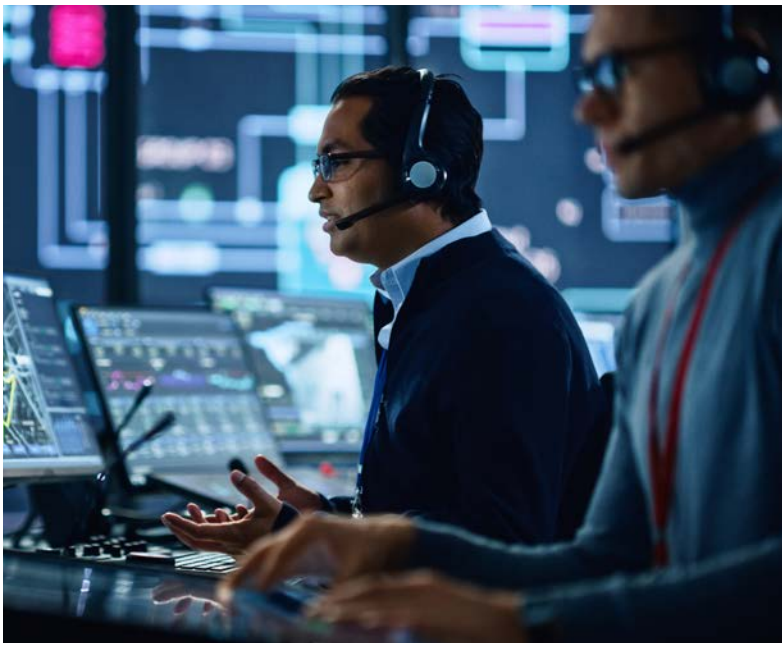
Prevention

By preventing malware and ransomware in real time, CSI Managed EDR protects endpoints against today's most common attacks with:

File Reputation: EDR contains a comprehensive database of files, allowing known malware and ransomware to be quickly quarantined at the point of entry.

Machine Learning Analysis: EDR is trained by algorithms to "learn" to identify malicious files and activity based on the attributes of known malware and ransomware.

Behavioral Protection: Enhanced behavioral analysis continually monitors all user and endpoint activity, offering real-time protection against malicious behavior.



Detection

CSI Managed EDR continuously monitors endpoints to detect new and unknown threats using:

Malicious Activity Protection: EDR monitors all endpoint activity, providing run-time detection and blocking abnormal behavior of running programs on the endpoint.

Cloud-Based Indicators of Compromise: EDR constantly analyzes malware to uncover new threat types and build behavioral and forensic profiles for emerging threats, known as Indicators of Compromise, which help administrators identify breached systems.

Vulnerability Identification: EDR identifies vulnerable software across environments to help reduce the attack surface.

Response

In addition to 24/7 monitoring from our SOC, CSI Managed EDR offers response tools to handle security breaches quickly and efficiently, accelerating time to detection and reducing the spread of malware and ransomware through:

Retrospective Security: EDR automatically uncovers advanced threats in an environment and correlates new threat information with history to automatically quarantine files when they exhibit malicious behavior.

Endpoint Isolation: By allowing one-click isolation of an infected endpoint along with the ability to whitelist trusted network resources, EDR stops threats from spreading.

Advanced Insight: Integration with CSI SIEMaaS enables deeper visibility on what happened to any endpoint at any given time, delivering additional alerts and response capabilities to streamline remediation of incidents.

Contact us to learn more about how CSI Managed EDR enhances protections for your organization.

LET'S TALK!

CSI