Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) services are available for U.S. State, Local, Tribal, and Territorial (SLTT) government entities, offered in partnership with CrowdStrike. For protecting U.S. SLTT election systems and endpoints, this solution is federally funded and available at no cost. It is deployed on endpoint devices to identify, detect, respond to, and remediate security incidents and alerts. See page 2 for all capabilities.

Device-Level Cyber Defense

EDR offers device-level protection and response to strengthen an organization's cybersecurity program. It includes various ways to protect endpoints, and provides active defense against cybersecurity threats, blocking both known (signature-based) and unknown (behavioral-based) malicious activity, as well as effective defense against encrypted malicious traffic.

The solution doesn't just block malicious activity; it can stop an attack in its tracks by taking an active role in mitigating and remediating malware, and killing or quarantining files. It's also capable of tracking actions that resulted in system compromise, enabling entities to learn how to help prevent future incidents.

Protection 24×7×365

Organizations using EDR have a full-time cybersecurity defense partner in the CIS Security Operations Center (SOC). Our SOC provides 24x7x365 monitoring and management, including analyzing malicious activity and escalating actionable threats. The SOC provides consolidated, actionable insights from expert analysts with industry-leading response times.

Additionally, any organization protected by this service can request the assistance of our Cyber Incident Response Team (CIRT) if they experience a cyber incident. Our CIRT analysts can reach directly into an affected system and conduct digital forensics remotely, acquiring evidence and performing analysis to determine the root cause, the scope of the incident, attack methodologies, and more.

Expand Your Multi-Tiered Defense Strategy

Adding EDR to an organization's defense-in-depth portfolio helps ensure a layered approach to cybersecurity while significantly increasing the time and complexity required for bad actors to compromise its network. EDR capabilities are integrated into our existing defense-in-depth cybersecurity offerings for U.S. election entities, and complement other security measures, including the CIS Critical Security Controls, Albert Network Monitoring and Management, Managed Security Services (MSS), and Malicious Domain Blocking and Reporting (MDBR).

Scalable to Meet Your Needs

EDR can be configured to meet the unique cybersecurity needs of the smallest to the largest election organization. The chart on page 2 outlines the endpoint protection offering available from the industry-leading vendor of this service, CrowdStrike.

Why Use EDR?

- Federally funded and available at no cost to protect election computers and systems
- Easy to deploy, low impact software solution for devices like servers and workstations
- Endpoint protection both on and off network
- Signature-based detections to identify known threats
- Rules-based logic to discover and learn about unknown threats
- Fully managed and monitored by our SOC
- Remote digital forensics support by our CIRT
- Compatible with on-premise, cloud, and remote systems
- Assists with implementation of CIS Critical Security Controls:
  - Control 01: Asset Inventory
  - Control 02: Software Inventory
  - Control 04: Secure Configuration of Enterprise Assets and Software
  - Control 05: Account Management
  - Control 06: Access Control Management
  - Control 07: Continuous Vulnerability Management
  - Control 10: Malware Defense
  - Control 13: Network Monitoring and Defense
  - Control 17: Incident Response Management

Contact Us

elections@cisecurity.org
www.cisecurity.org
518.880.0699

Key Service Capabilities

Next Generation Antivirus (NGAV)

- Cloud integrated endpoint protection
- Signature and behavioral malware prevention
- Ransomware protection
- Threat intel and threat indicators
- Exploit blocking

Endpoint Detection & Response (EDR)

- Custom detection rules
- Threat hunting
- Remote system quarantine
- Optional secure remote system access

Advanced Capabilities

- Asset inventory
- Application inventory
- User account monitoring
- Rogue device detection

CIS EDR Advanced

Powered by CrowdStrike

Fully Managed Solution

- 24×7×365 monitoring and management by CIS SOC
- Cyber incident response team
- World-class cybersecurity experts
- Robust SLTT threat database

Customizable Device Control

- Access to management portal
- Host-based firewall control
- USB device control
- Protection on and off network

Alignment with Industry Standards

- MITRE ATT&CK framework aligned
- FedRAMP certified
- Assists with CIS Critical Security Controls implementation

Learn More

U.S. election entities can learn more or request more information about Endpoint Detection and Response (EDR) services by contacting us at elections@cisecurity.org or 518-880-0699.

This solution is available at no cost to protect all U.S. SLTT election systems and endpoints through funding provided by the Cybersecurity and Infrastructure Security Agency (CISA). For U.S. SLTT government organizations interested in acquiring EDR protection for systems not covered by funding from CISA, additional coverage can be purchased through CIS Endpoint Security Services from CIS Services. Please contact services@cisecurity.org or 518-880-0699 for more information.