INTRODUCTION

The Essential Guide to Election Security

MATURITY

Maturities

Determining Your Maturity Level

Prioritizing Best Practices for the Level 1 maturity

Prioritizing Best Practices for the Level 2 and Level 3 maturities

BEST PRACTICES

Index of Best Practices

Addressing Physical Threats

Join the EI-ISAC

Asset Management

Encrypt Data at Rest

Encrypt Data in Transit

Managing Infrastructure with Secure Configurations

User Management

Backups

Incident Response Planning

Building and Managing Staff

Patching and Vulnerability Management

Remediate Penetration Test Findings

Perform Internal Penetration Test

v: latest

Network Monitoring and Intrusion Detection

Intrusion Detection Systems (IDSs) monitor network traffic traveling into and out of networks for malicious activity. These sensors passively monitor network data traffic but do not block traffic and cannot directly affect a member network or change the actual data traversing the network. Other technologies, called Intrusion Prevention Systems (IPSs), can also block traffic that the sensors deem a threat.

IDSs monitor traffic as it flows across a network to look for matches against a set of threat signatures. If a match is found, an alert is sent for analysis and, if warranted, further action. In this way, an IDS can provide protection against both traditional and advanced network threats by helping organizations identify malicious activity.

The EI-ISAC offers an IDS called Albert to election offices. Albert sensors reside on the local network, providing security alerts for cyber threats, helping organizations identify malicious cyber activity. The sensor passively monitors network data traffic; it does not block traffic and cannot negatively affect a member network or read or change the actual data traversing the network.

Under this service, the EI-ISAC receives any alerts, analyzes them, and works with your office to take any recommended action. The EI-ISAC can also be used to analyze historical data to retroactively search for malicious activity. While the Albert sensor is optimized for use in the state, local, tribal, and territorial governments, commercial IDS and IPS systems are also available.

Goals

1. Understand what an IDS is and why it’s important (Level 1 maturity)
2. Deploy an IDS (Level 2 maturity)

Actions

For Network Monitoring and Intrusion Detection, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

We don’t recommend investing in an IDS at the Level 1 maturity.

While it can provide protection in any network environment, there are more fundamental steps to take, as described in the best practice prioritization for Level 1.

Level 2 and Level 3 Maturities

1. Consider investing in an IDS or IPS.
   - The Albert sensor and service is a free or low-cost way to do this that is optimized for use in the election offices and other state, local, tribal, and territorial governments. Contact elections@cisecurity.org to get information about Albert.

Cost-Effective Tools

- Zabbix: Monitoring tool for IT infrastructure
- Quad9®: Domain Name System (DNS) filtering service
- OpenDNS®: Domain Name System (DNS) filtering service
- Snort: Open source IDS/IPS maintained by Cisco
- Suricata: Open source intrusion detection system
- Zeek NIDS: Open source network analysis tool with an IDS
- Security Onion: Linux distribution dedicated to network security monitoring
- Skybox Network Assurance: Network security posture management

Learn More

- NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)

Mapping to CIS Controls and Safeguards

- 13.3: Deploy a Network Intrusion Detection Solution
- 13.4: Perform Traffic Filtering Between Network Segments
- 13.8: Deploy a Network Intrusion Prevention Solution

Mapping to CIS Handbook Best Practices

- 7

Previous
Malicious Domain Blocking and Reporting

Next
Managing Wireless Networks

Made with Sphinx and @pradyunsg's Furo
Last updated on Jan 12, 2023