Elections Infrastructure ISAC®

Essential Guide to Election Security

Search

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

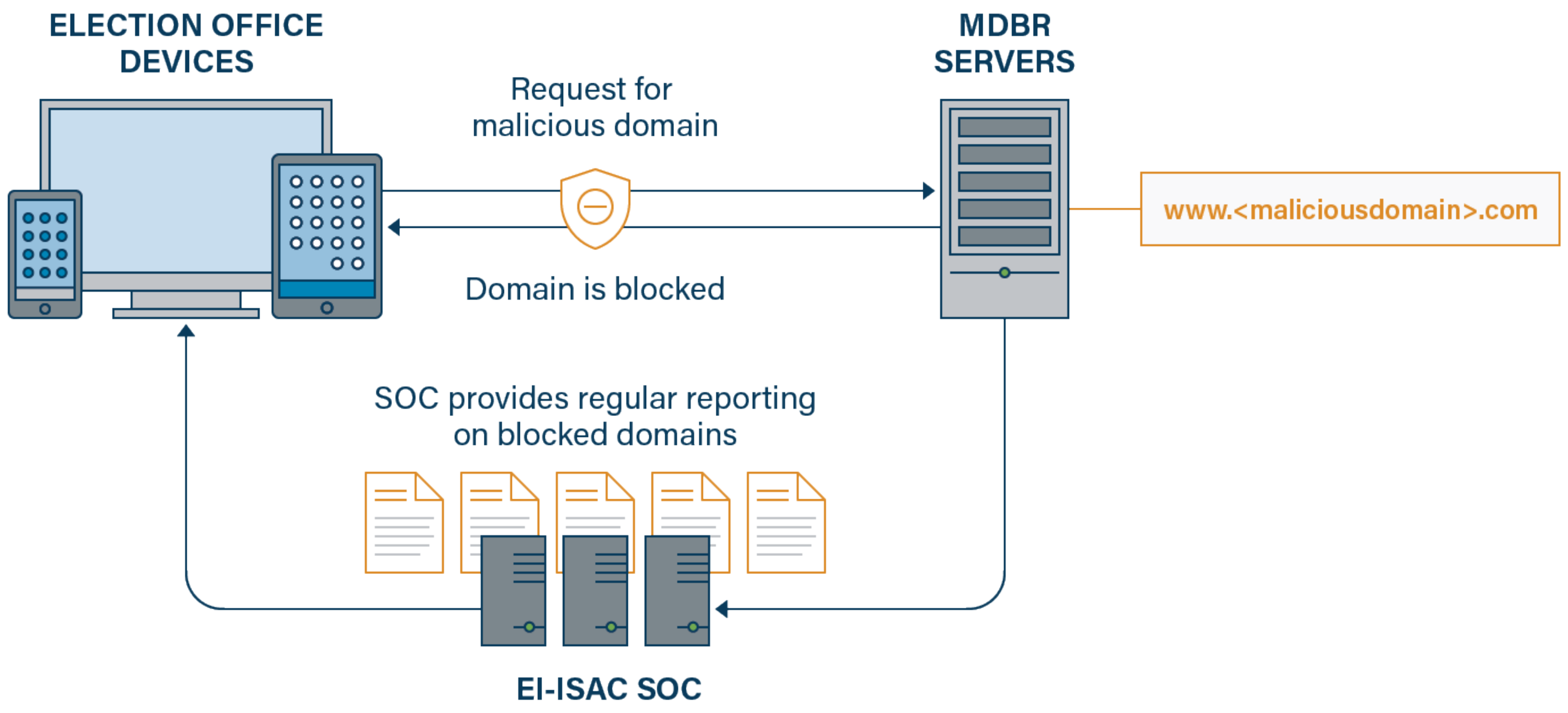
Perform Internal Penetration Test

v: latest

# Malicious Domain Blocking and Reporting

Malicious Domain Blocking and Reporting, or MDBR, technology prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats. This capability can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.

Once an organization points its domain name system (DNS) requests to the MDBR DNS server IP addresses, every DNS lookup will be compared against a list of known and suspected malicious domains. Attempts to access known malicious domains such as those associated with malware, phishing, and ransomware, among other threats, are blocked and logged.


ELECTION OFFICE DEVICES
MDBR SERVERS
Request for malicious domain
Domain is blocked
www.<maliciousdomain>.com
SOC provides regular reporting on blocked domains
EI-ISAC SOC

MDBR in an election office environment #

## Goals

1. Deploy MDBR for all internet-facing assets (Level 1 maturity)

## Actions

For Malicious Domain Blocking and Reporting, the necessary actions are the same for all maturity levels.

1. If you're an EI-ISAC member, you can sign up for no-cost MDBR by registering at https://mdbr.cisecurity.org. You will be asked to provide the following information:
   - Your contact information
   - Technical contact(s) for MDBR setup, troubleshooting, and general technical support
   - Reporting contact(s) for receiving reports on your MDBR service
   - Public IP addresses or CIDR netblocks from which your organization's DNS queries are sent
2. If you aren't an MS-ISAC or EI-ISAC member, join today – then complete action #1 of this best practice.

The EI-ISAC provides members with a free MDBR service. Members sign up and configure their DNS server, and the EI-ISAC will then provide reporting that includes log information for all blocked requests and assist in remediation if needed.

The service is easy to implement and requires virtually no maintenance as EI-ISAC and its provider fully maintain the systems required to provide the service.

The EI-ISAC hosts all reporting data, including both successful and blocked DNS requests. It will then perform detailed analysis and reporting for the organization and the election community writ large. The EI-ISAC will provide regular reporting and intelligence services for SLTT members.

## Cost-Effective Tools

- EI-ISAC MDBR service: A no-cost, lightweight MDBR solution for EI-ISAC members.

## Mapping to CIS Controls and Safeguards

- 9.2: Use DNS Filtering Services
- 9.3: Maintain and Enforce Network-Based URL Filters

## Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices

‹ Previous
Endpoint Protection

Next ›
Network Monitoring and Intrusion Detection

Last updated on Mar 06, 2023