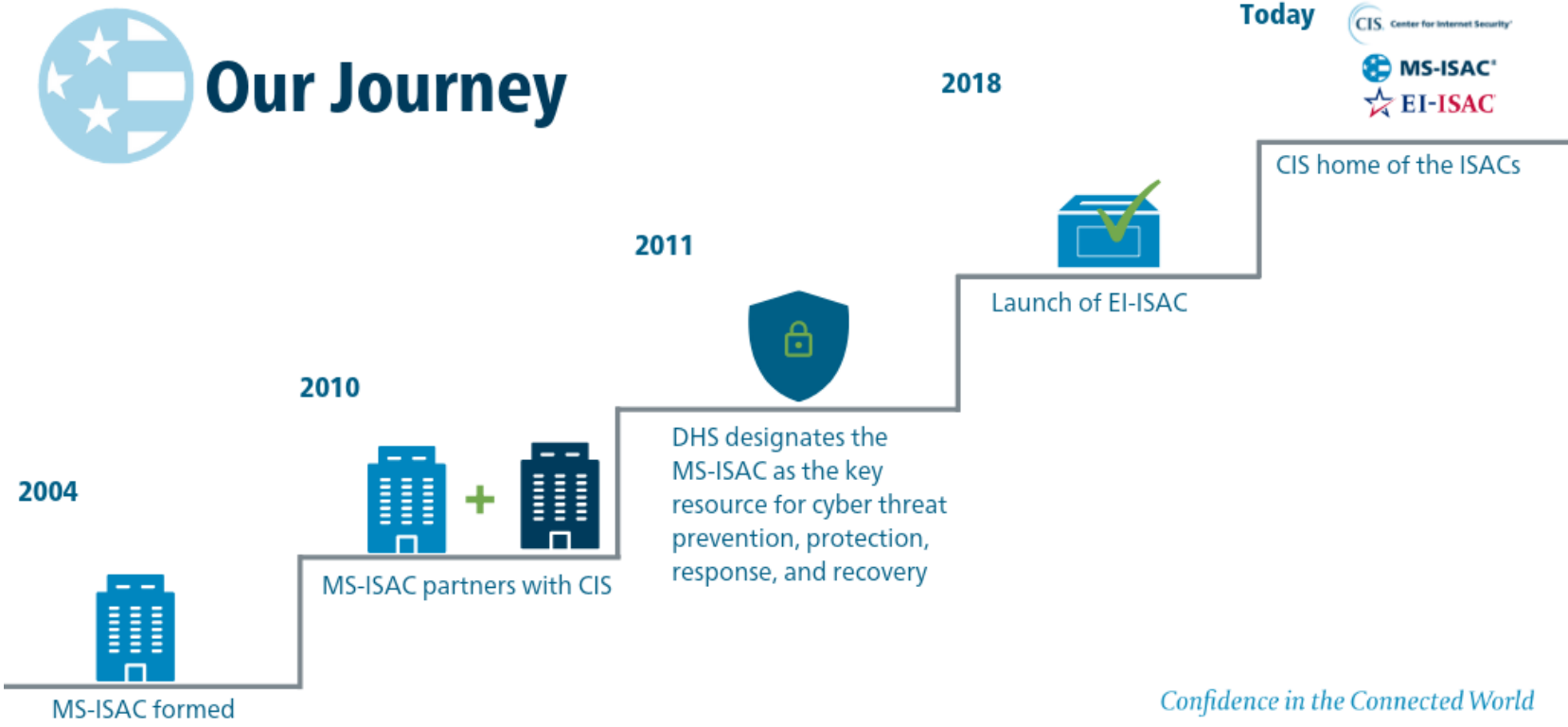
No-Cost Resources With the MS-ISAC

Kyle Bryans

Senior Program Specialist

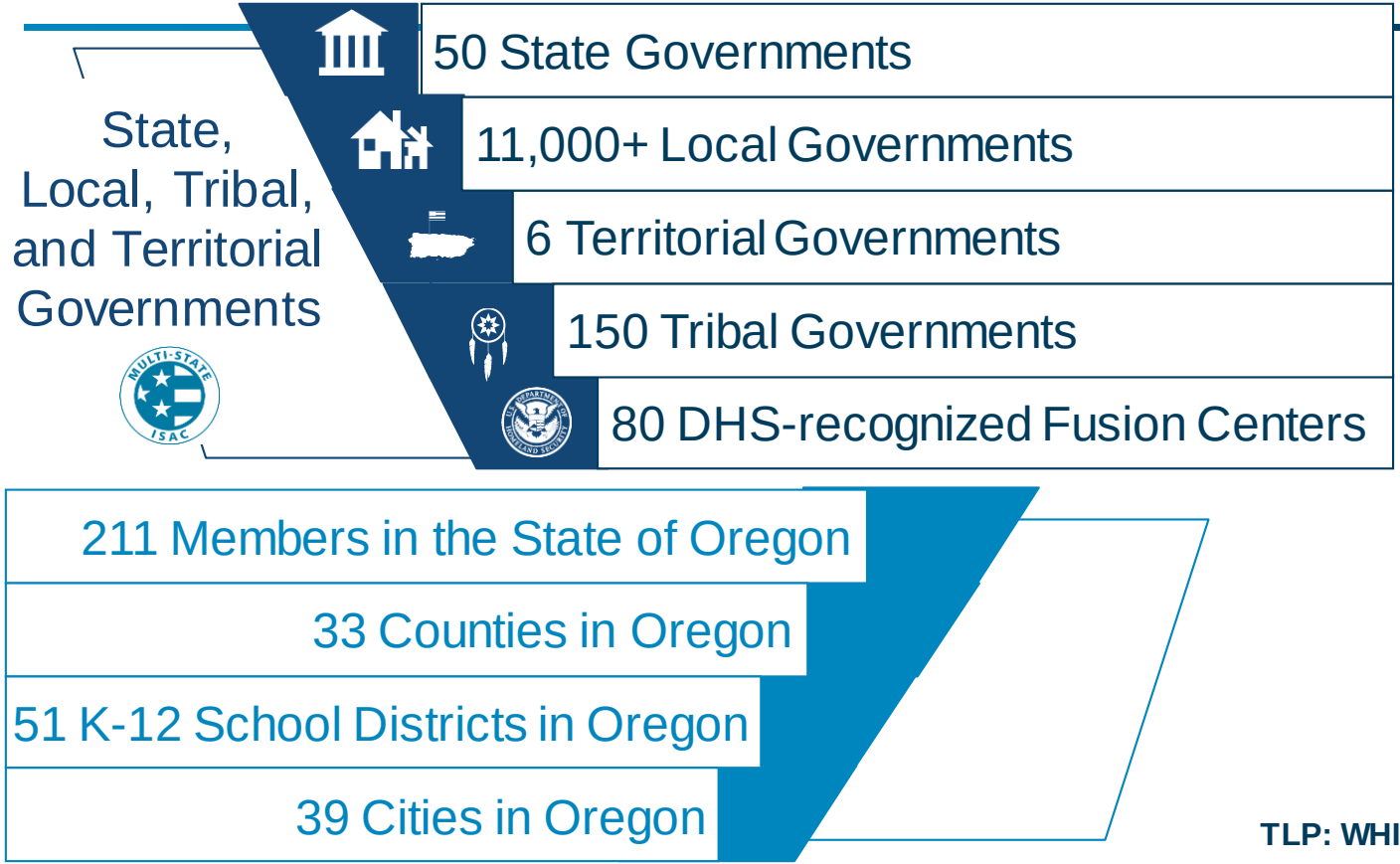
MS-ISAC®
EI-ISAC®

Our Journey



Confidence in the Connected World

Who We Serve


State, Local, Tribal, and Territorial Governments
50 State Governments
11,000+ Local Governments
6 Territorial Governments
150 Tribal Governments
80 DHS-recognized Fusion Centers
211 Members in the State of Oregon
33 Counties in Oregon
51 K-12 School Districts in Oregon
39 Cities in Oregon

How to access MS-ISAC resources

- **Register for the MS-ISAC's services here:**

https://learn.cisecurity.org/ms-isac-registration

- **The MS-ISAC Stakeholder Engagement team will provide you with next steps:**
  - Register your HSIN account
  - Submit public IPs, domains, and subdomains
  - Register for MDBR
  - Add additional staff to your account

Security Operations Center

24/7 support for:

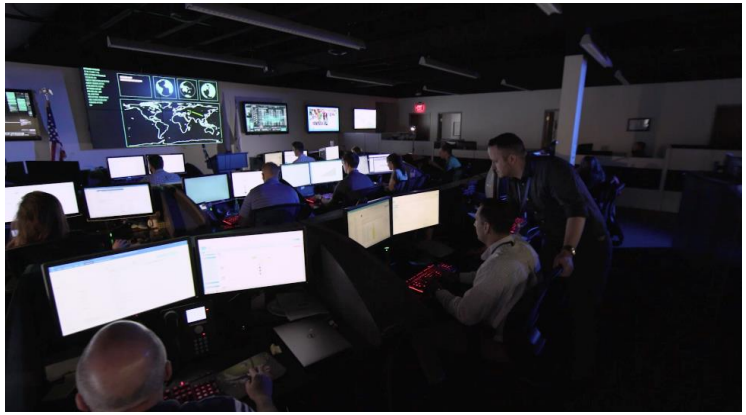
- ✓ Network Monitoring Services
- ✓ Research and Analysis

24/7 analysis and monitoring of:

- ✓ Threats
- ✓ Vulnerabilities
- ✓ Attacks

24/7 reporting:

- ✓ Cyber Alerts & Advisories
- ✓ Web Defacements
- ✓ Account Compromises
- ✓ Hacktivist Notifications



To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Services Snapshot

- CERT (Computer Emergency Response Team)
- 24/7/365 Security Operations Center
- Network Monitoring (Albert)
- Monitoring of IP Range & Domain Space
- MCAP (Malicious Code Analysis Platform)
- CIS SecureSuite®
- Malicious Domain Blocking and Reporting (MDBR)

Disseminations & Alerts

MS-ISAC Advisory Michael Aliperti

MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Various Cisco Products Could Allow for Administrator Privileges - PATCH: NOW - TLP: WHITE

Retention Policy Default 2 year move to archive (2 years) Expires 7/3/2022

This message was sent with High importance.

TLP: WHITE
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2020-089

DATE(S) ISSUED:
07/03/2020

SUBJECT:
Multiple Vulnerabilities in Cisco Products Could Allow for Administrator Privileges

OVERVIEW:
Multiple vulnerabilities have been discovered in Cisco products, the most severe of which could allow for an attacker gaining administrator pr
exploitation of the most severe of these vulnerabilities could result in an attacker gaining administrator privileges. Depending on the privileges
data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be les

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Cisco AnyConnect Secure Mobility Client for Mac OS releases earlier than 4.9.00086
- Cisco Digital Network Architecture Center releases earlier than 1.2.10
- Cisco Identity Services Engine releases earlier than 2.6 Patch 7
- Cisco 250 Series Smart Switches

Volume 15, Issue 7 • July 2020 Monthly Security Tips Newsletter

From the desk of
Michael Aliperti
MS-ISAC Chair

6 Common Elderly Scams to Watch Out For and How to Stay Safe

A scam can be initiated via the computer (email, internet, social media), text, postal mail, in person, or a phone call. No matter the origin of the scam, the characteristics are the same:

- First, there is something to pique your interest – someone in trouble, big discount offers, lottery win.
- Second, the individual contacting you seems trustworthy, super friendly, and seems to care about you.
- Third, there's a deadline associated with the offer – act fast, act now.

There will always be scams, particularly those targeted at seniors. This month's newsletter identifies some common scams and some tips to help you take control of the situation and stay safe and stay in control.

Grandparent Scam

One of the most common scams presented to seniors is the Grandparent Scam. The caller claims to be a relative, a grandson or granddaughter, and the call is urgent. Typically, the grandchild is out of

Nationwide Cybersecurity Review

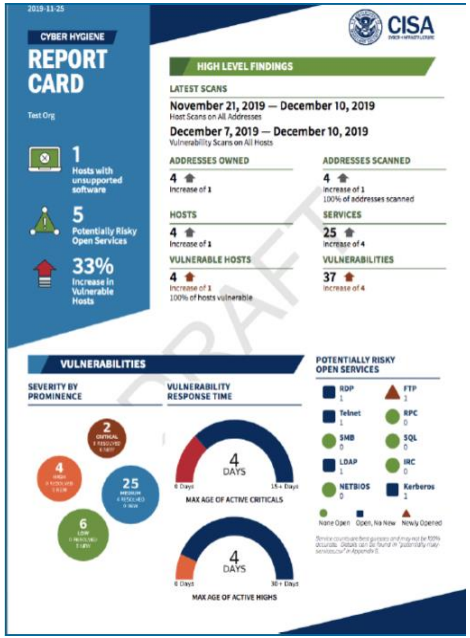
- **Annual Self-Assessment**
  - No Cost
  - Anonymous
- **NIST Framework**
- **Cybersecurity Roadmap**
  - Identify Areas for Improvement
  - Justify Investments

Maturity Levels

Score	Maturity Level *The recommended minimum maturity level is set at a score of 5 and higher*
7	**Optimized:** Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified:** Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process:** Your organization has formally documented policies, standards, and procedures, and is in the process of implementing and aligning this documentation to a formal security framework and/or methodology.
4	**Partially Documented Standards and/or Procedures:** Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy:** Your organization has a formal policy in place.
2	**Informally Performed:** Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed:** Activities, processes and technologies are not in place to achieve the referenced objective.

https://www.cisecurity.org/ms-isac/services/ncsr

CISA Cyber Hygiene Program



- No cost, network evaluation through CISA.
  Near continuous scans for open ports and vulnerabilities.
- Vulnerabilities checked against a large library that an internet-based threat actor could exploit.
  Alert notifications sent to organization within 24 hours.
- Scans performed based on the criticality of the vulnerability.
  (Between 24 hours and 1 week)
- Provide a detailed report card outlining key new findings, as well as historical data.

CISA Cyber Hygiene Program

How to Enroll

- Request your initial assessment with CISA at Vulnerability_Info@cisa.dhs.gov
- Complete the Service Request form along with other required legal documents
- Complete the Data Sharing Form
- Elect to share your reports with the MS/EI-ISAC

Malicious Domain Blocking and Reporting (MDBR)

Security Focused DNS service:

Blocks malicious domain requests before a connection is even established!

Simple Implementation:

No new hardware or software required

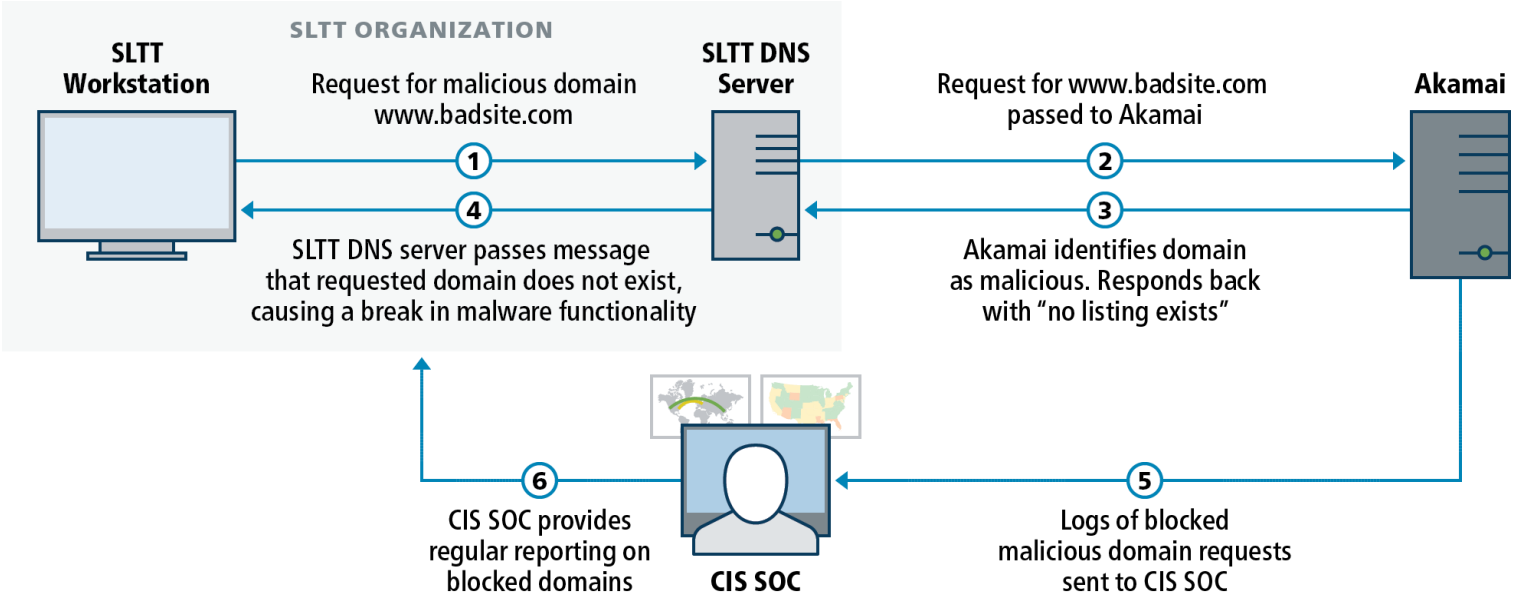
Helps limit infections related to:

- Known Malware
- Ransomware
- Phishing
- Other cyber threats

How MDBR Works

1. Organization points DNS requests to Akamai's DNS server IP addresses
2. Every DNS lookup will be compared against a list of known malicious domains
3. Attempts to access known malicious domains such as those associated with malware, phishing, and ransomware, among other threats, will be blocked and logged
4. CIS will then provide reporting that includes information related to the blocked requests and assist in remediation if needed

How MDBR Works



MDBR Reporting

- Summary PDF reports and associated blocked logged data will be sent on a weekly basis, identifying both high-level and detailed information on blocked requests, broken down by:
  - Severity
  - Threat type
  - Confidence level (known or suspected)
  - Top domains blocked
  - Reasons malicious domains are believed to be malicious

How to Sign Up

1. Visit https://mdbr.cisecurity.org
2. Enter your email address, which will confirm your organization is either an MS-ISAC member
3. Once membership is confirmed an email will be sent to you with a link to the signup form. We will need 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

How to Sign Up (Continued)

4. Submitting the form will trigger a confirmation email to your organization's primary member, requesting that they review and approve the information provided and accept to the terms and conditions
5. Once the information is reviewed for accuracy and submitted, and the MDBR terms and conditions are accepted, information will be provided on MDBR setup instructions

Important Links

How to Sign Up: https://mdbr.cisecurity.org

FAQ: https://www.cisecurity.org/ms-isac/services/mdbr/mdbr-faq/

To Learn More: https://www.cisecurity.org/ms-isac/services/mdbr

Questions and Answers

Thank you!

Contact Us

Security Operations Center
24/7 Phone Number
1-866-787-4722
soc@cisecurity.org

Kyle Bryans
Senior Program Specialist
518-880-0747
Kyle.Bryans@cisecurity.org