WELCOME TO THE ISOAG MEETING

VIRGINIA
IT AGENCY

Information Security Officers Advisory Group

September 4, 2024

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Kendra Burgess/ VITA
MS-ISAC's Cybersecurity Resources and Tools	Megan Incerto/ MS-ISAC CIS
Google Chrome Browser Entrust Distrust / Vita Review and Go-Forward for COV Servers Update	John Del Grosso/VITA
Components and Concepts of a Risk Assessment	Matthew Steinbach / VITA
Agency Data Points	Erica Bland/VITA
Announcements / Upcoming Events	Kendra Burgess/ VITA
Adjourn	

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

September ISOAG Meeting

Megan Incerto

Regional Engagement Manager, MS-ISAC

Megan.Incerto@cisecurity.org | 518-640-3655

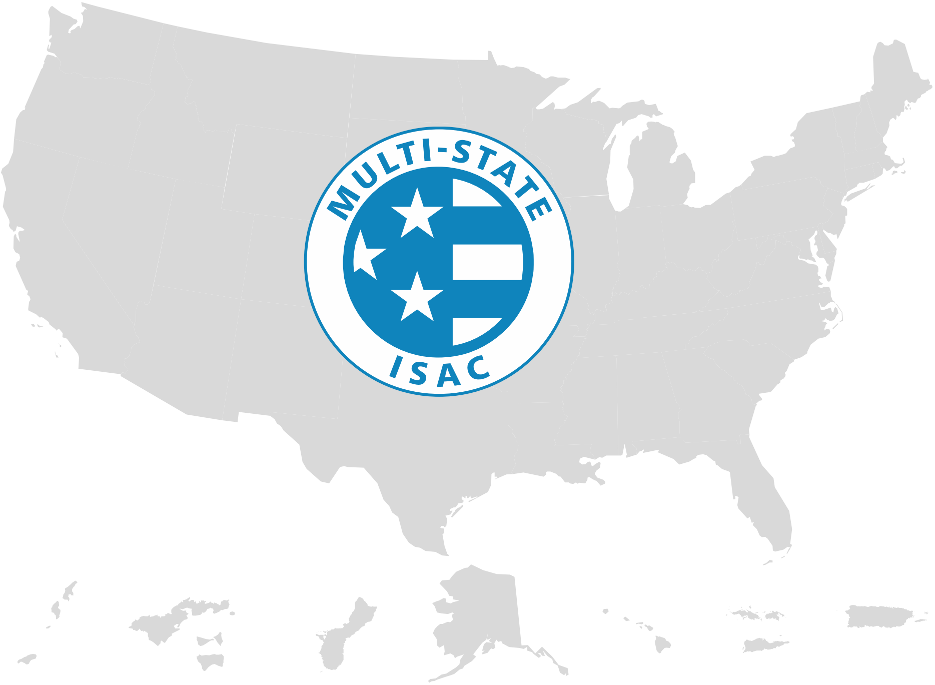
Multi-State Information Sharing & Analysis Center®

The MS-ISAC®

- Designated by the Cybersecurity & Infrastructure Security Agency (CISA) as a key resource for cyber threat prevention, protection, response and recovery for all U.S. State, Local, Tribal and Territorial (SLTT) governments.

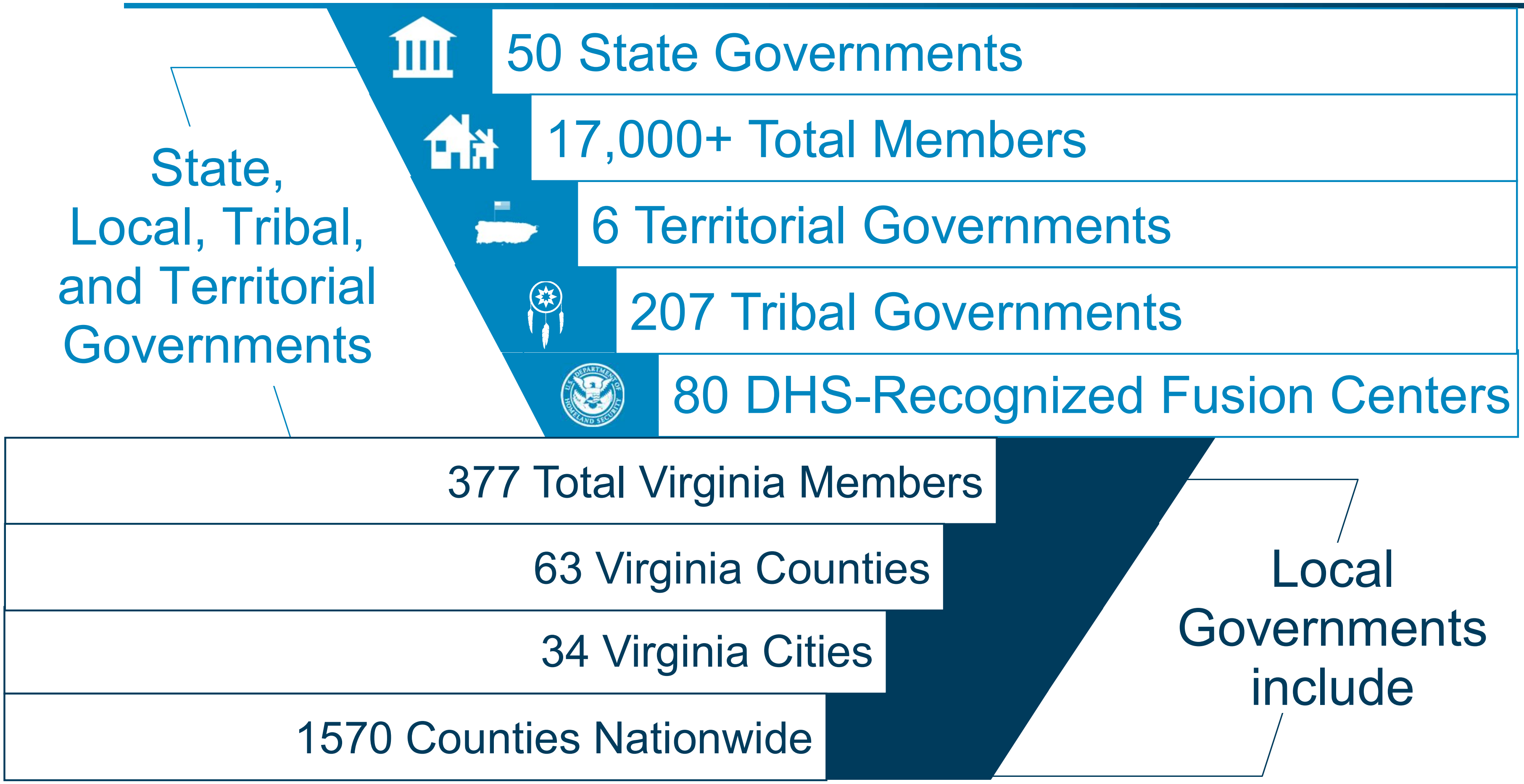
- A division of the Center for Internet Security® (CIS®), a 501(c)(3) nonprofit.

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



MS-ISAC®

Who We Serve



State, Local, Tribal, and Territorial Governments

50 State Governments

17,000+ Total Members

6 Territorial Governments

207 Tribal Governments

80 DHS-Recognized Fusion Centers

Local Governments include

377 Total Virginia Members

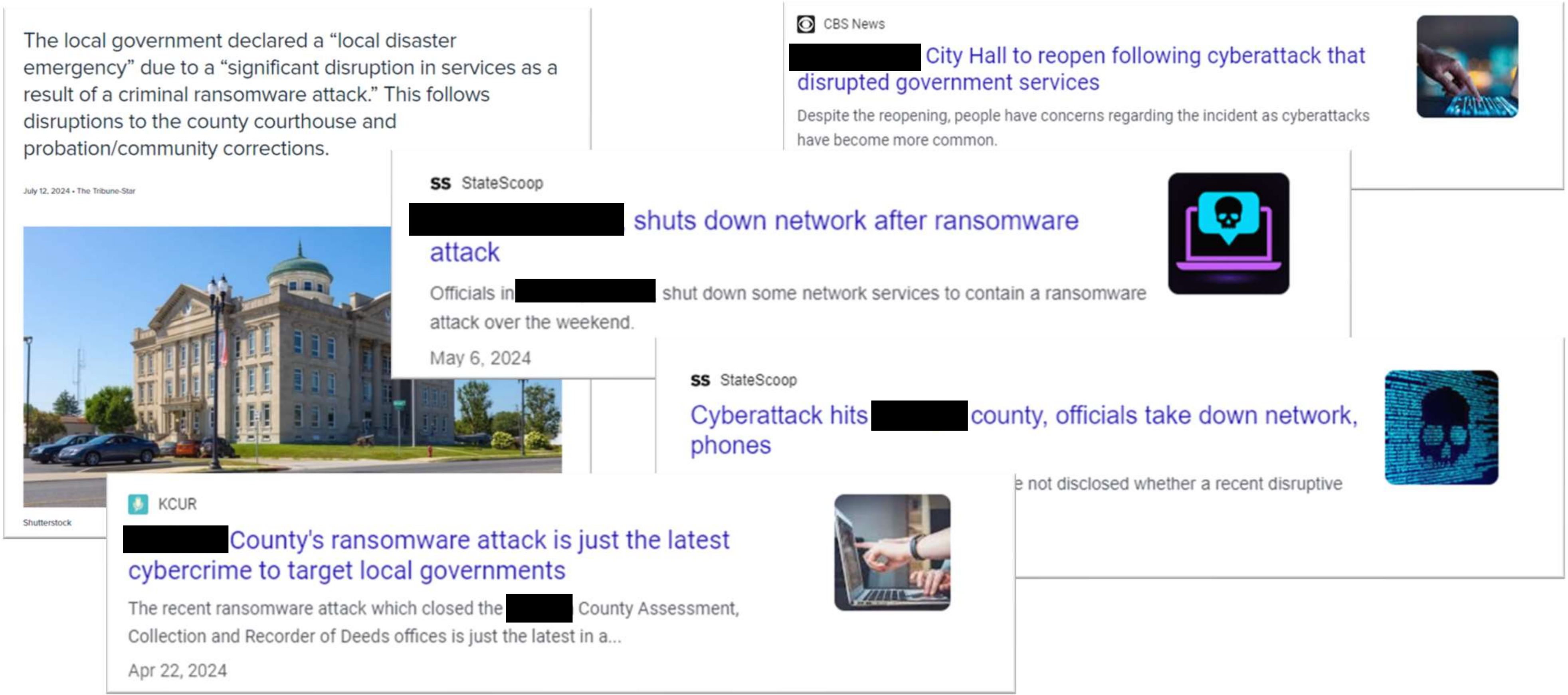
63 Virginia Counties

34 Virginia Cities

1570 Counties Nationwide

Local Government Targeted by Cybercriminals

Examples in the Headlines



The local government declared a "local disaster emergency" due to a "significant disruption in services as a result of a criminal ransomware attack." This follows disruptions to the county courthouse and probation/community corrections.

July 12, 2024 • The Tribune-Star

Shutterstock

CBS News

[redacted] City Hall to reopen following cyberattack that disrupted government services

Despite the reopening, people have concerns regarding the incident as cyberattacks have become more common.

SS StateScoop

[redacted] shuts down network after ransomware attack

Officials in [redacted] shut down some network services to contain a ransomware attack over the weekend.

May 6, 2024

SS StateScoop

Cyberattack hits [redacted] county, officials take down network, phones

e not disclosed whether a recent disruptive

KCUR

[redacted] County's ransomware attack is just the latest cybercrime to target local governments

The recent ransomware attack which closed the [redacted] County Assessment, Collection and Recorder of Deeds offices is just the latest in a...

Apr 22, 2024

Recommendations

Implement Best Practices

- **CIS Critical Security Controls**
  - provide a prioritized set of actions to protect your organization and data from known cyber-attack vectors.

CIS Controls

https://www.cisecurity.org/controls/

- **CISA/MS-ISAC Joint Ransomware Guide**
  - Best practices and incident response guidance
  - https://www.cisa.gov/stopransomware/ransomware-guide
  - https://www.cisa.gov/stopransomware

RANSOMWARE GUIDE

SEPTEMBER 2020

MS-ISAC Multi-State Information Sharing & Analysis Center

- **Use free and low-cost security services**

No-Cost MS-ISAC Benefits to SLTTs

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

Cyber Threat Intelligence

- Cyber Alerts & Advisories
- Quarterly Threat Report
- Regular Indicators of Compromise (IOCs)
- White Papers
- Cyber Threat Briefings
- Real-Time Intelligence Feeds

Cybersecurity Services

- 24x7x365 Security Operations Center (SOC)
- Cyber Incident Response Team (CIRT)
- ISAC Threat Notification Service (IP & Domain Monitoring)
- Malicious Domain Blocking & Reporting (MDBR)

Cyber Framework & Best Practices

- Nationwide Cybersecurity Review (NCSR)
- CIS SecureSuite Membership
  - ○ *Tools to implement the CIS Critical Security Controls and CIS Benchmarks*

Other Member Resources

- MS-ISAC Webinars
- MS-ISAC Working Groups
- CIS CyberMarket
- Virtual Service Reviews
- Homeland Security Information Network (HSIN)

Security Operations Center

24x7x365

Support

Network Monitoring Services
+
Research and Analysis

Analysis & Monitoring

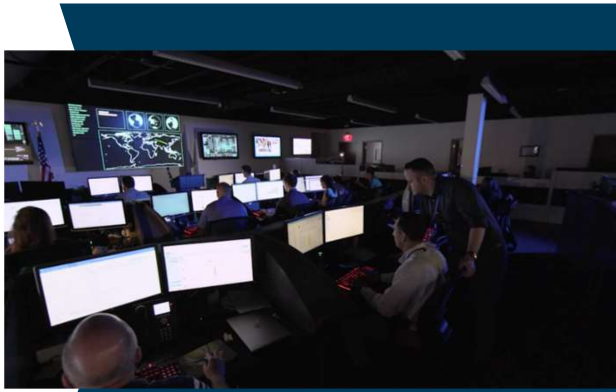
Threats, Vulnerabilities
+
Attacks

Reporting

Cyber Alerts & Advisories

Web Defacements

Account Compromises



To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Confidential & Proprietary

Cyber Incident Response Team (CIRT)

Incident Response

Malware Analysis

Log Analysis

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@cisecurity.org

Monitoring of IP Range & Domain Space

IP Monitoring

- Signs of Compromise
- Malicious Activity

Domain Monitoring

- Notifications on compromised user credentials

Send Public IPs and Domains to soc@cisecurity.org

MS-ISAC®

Malicious Domain Blocking and Reporting (MDBR)

https://mdbr.cisecurity.org/

Security Focused DNS service:

Blocks malicious domain requests before a connection is even established!

Simple Implementation:

No new hardware or software required

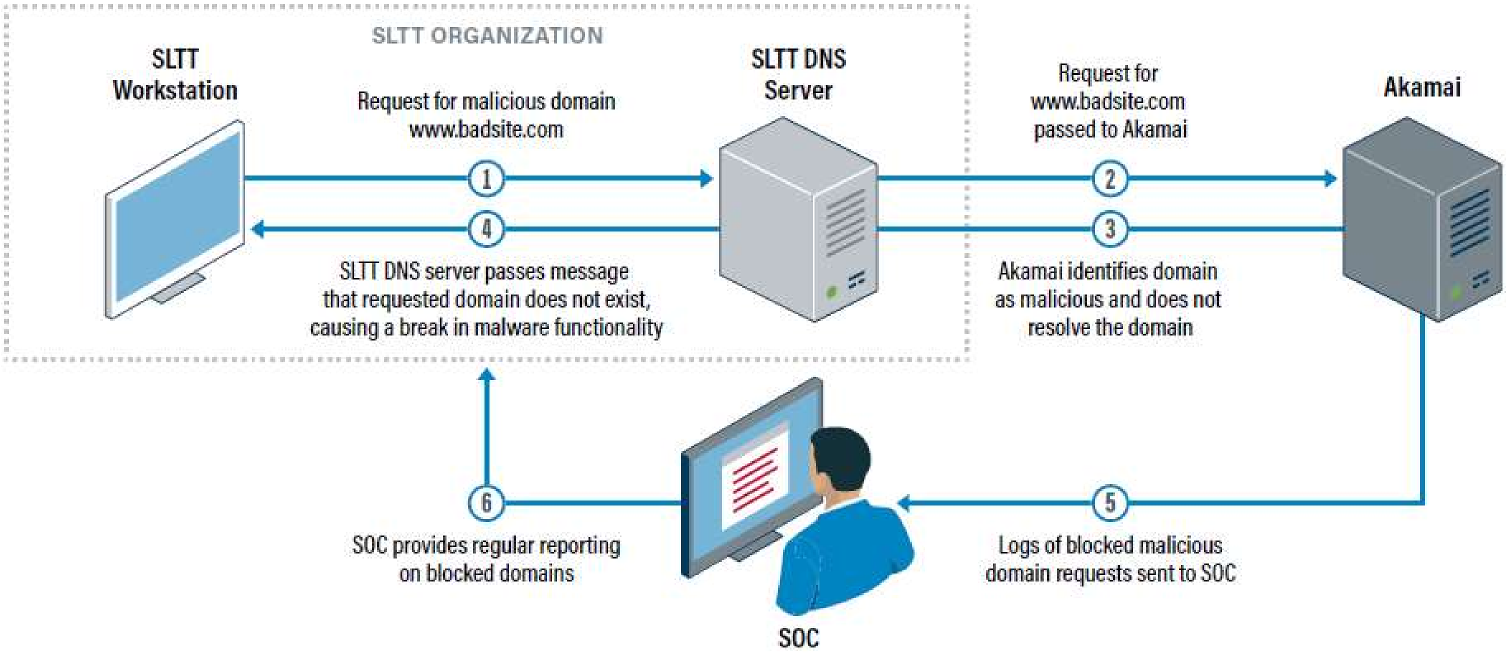
Helps limit infections related to:

- Known Malware
- Ransomware
- Phishing
- Other cyber threats

Malicious Domain Blocking and Reporting (MDBR)

https://mdbr.cisecurity.org/

↓ Malicious Domain Blocking and Reporting Data Flow



SLTT ORGANIZATION

SLTT Workstation

SLTT DNS Server

Akamai

SOC

1 Request for malicious domain www.badsite.com

2 Request for www.badsite.com passed to Akamai

3 Akamai identifies domain as malicious and does not resolve the domain

4 SLTT DNS server passes message that requested domain does not exist, causing a break in malware functionality

5 Logs of blocked malicious domain requests sent to SOC

6 SOC provides regular reporting on blocked domains

Nationwide Cybersecurity Review (NCSR)

- Annual, self-Assessment
- NIST Framework
- Cybersecurity Roadmap

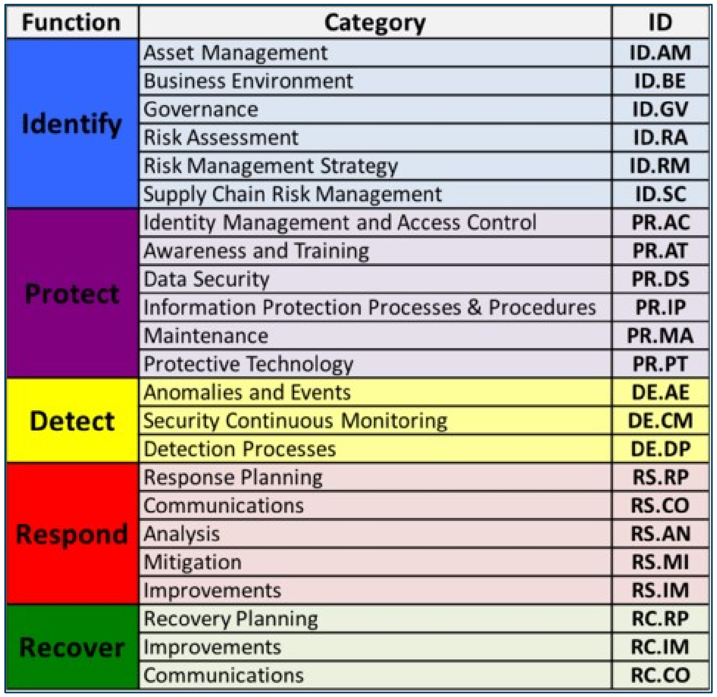
For More Information:

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

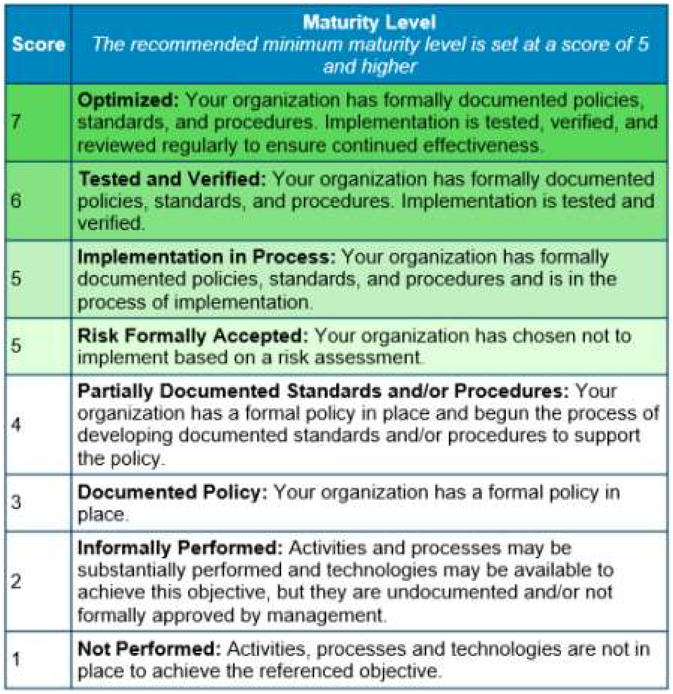
- **2023 NCSR**
  - Currently Open for Registration
  - Available to Complete through February 28, 2024
- **Registration & Resources**
  - Located on NCSR Webpage
  - End-User Guidance
  - Results & Reporting Templates

https://www.cisecurity.org/insights/white-papers/2022-nationwide-cybersecurity-review

NCSR Question Set – NIST Sections & Answer Scale



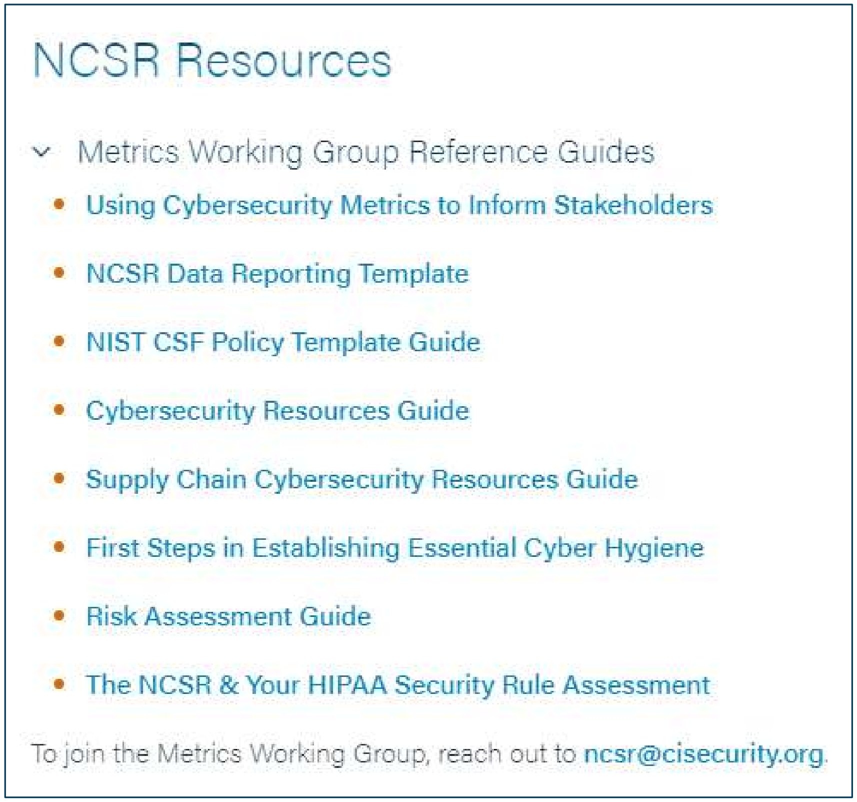
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO



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 implementation.
5	**Risk Formally Accepted:** Your organization has chosen not to implement based on a risk assessment.
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.

NIST Cybersecurity Framework - https://www.nist.gov/cyberframework/framework

Best Practice Resources



NCSR Resources

Metrics Working Group Reference Guides

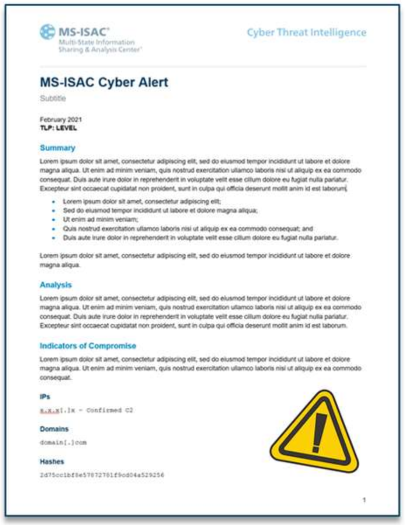
- Using Cybersecurity Metrics to Inform Stakeholders
- NCSR Data Reporting Template
- NIST CSF Policy Template Guide
- Cybersecurity Resources Guide
- Supply Chain Cybersecurity Resources Guide
- First Steps in Establishing Essential Cyber Hygiene
- Risk Assessment Guide
- The NCSR & Your HIPAA Security Rule Assessment

To join the Metrics Working Group, reach out to ncsr@cisecurity.org.

Cyber Threat Intelligence Products

Advisories & Alerts

- Ad Hoc
- Urgent Actions
- Prevalent Threats



MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Cyber Threat Intelligence

MS-ISAC Cyber Alert

Subtitle

February 2021
TLP: LEVEL

Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

- Lorem ipsum dolor sit amet, consectetur adipiscing elit;
- Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua;
- Ut enim ad minim veniam;
- Quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat; and
- Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Analysis

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Indicators of Compromise

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

IPs

`x.x.x[.]x - Confirmed C2`

Domains

`domain[.]com`

Hashes

`2d75cc1bf8e57872781f9cd04a529256`

1

Reports

- Assessment Based
- Probability Focused
- Analytic Confidence

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Cyber Threat Intelligence
Long-Form Analytic Report

Cyber Threats to the Healthcare Industry

Analysis Across Trends from 2019-2021

February 2021 • LFAR-2021-0002
TLP: WHITE

Executive Summary

Protected health information (PHI) represents highly valuable data for cybercriminals on dark web markets. Constrained financial resources, system sprawl, and varied cybersecurity awareness among staff are primary factors for the majority of healthcare-related breaches. In 2019, attacks against healthcare institutions increased by 75%, and these trends will likely increase due to pandemic-related telework vulnerabilities; increasing integration of innovative technology into legacy systems; and profitable return for exfiltrated data within the healthcare sector. This publication aims to illuminate current targeted data and identify key cybersecurity trends between 2019-2020 to highlight major threats and vulnerabilities for healthcare industries in 2021.

Key Findings

An increase in ransomware campaigns and secondary infections, through long-term campaigns against digital healthcare supply chains, marks a notable shift from 2019-2020. COVID-19 vaccine research makes an attractive target for nation-state cyber threat actors (CTAs), while COVID-19-themed phishing lures offer cybercriminals an opportunity to capitalize on hospitals in need of personal protective equipment (PPE), such as N95 masks.

- Estimated total financial losses for U.S. health systems and facilities at $323.1 billion in 2020. [1]
- Seventy-five percent increase in reports of ransomware attacks on healthcare entities in 2019.[2]
- Stolen medical records can sell for 10 to 20 times more than credit card or social security numbers. [3]
- COVID-19-related phishing attempts increased by 700% worldwide in 2020.[4]

Substantive Analysis

Most successful data breaches stem from human error or adversaries preying upon human behavioral patterns of trust, fear, and urgency. [5] With hospitals and healthcare providers rushing to acquire PPE, contain COVID-19 within their facilities; and minimizing staff to reduce spread, cybercriminals are provided many windows of opportunity to leverage human error. Errors can range from misconfigured systems, susceptibility to phishing, and improperly secured data. The Multi-State Sharing and Analysis Center's (MS-ISAC) Cyber Threat Intelligence (CTI) team assesses with high confidence cybercriminals will likely increase targeting hospitals and healthcare providers in 2021. The CTI team bases this assessment on current reported profitable returns for PHI; [6] wider attack surfaces due to integration of legacy systems with internet-of-things (IoT) devices; increased telemedicine practices; and the cost associated with an inability to care for patients[7] or store limited vaccine supply. [8]

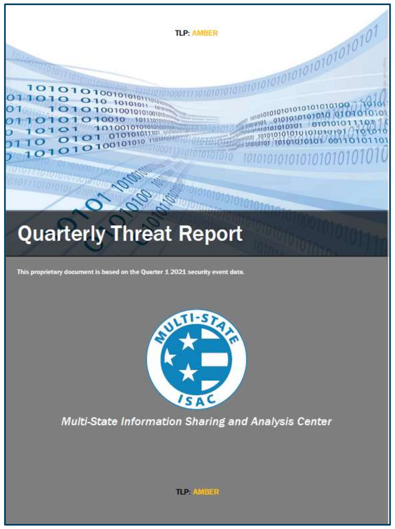
Targeted Data

Medical identity theft, which includes using a victim's personal information to fraudulently obtain medical services or prescriptions alongside standard identity theft actions, represents a critical threat to patients and providers

1

Strategic Assessments

- Deeply Researched
- Forward Looking
- Trends & Patterns



TLP: AMBER

Quarterly Threat Report

This proprietary document is based on the Quarter 1 2021 security event data.

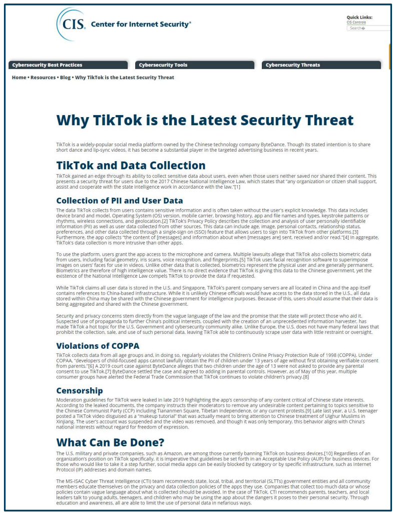
MULTI-STATE ISAC

Multi-State Information Sharing and Analysis Center

TLP: AMBER

Briefs & Blogs

- Simple or Complex
- Technically Focused
- Threat Driven



CIS. Center for Internet Security®

Home • Resources • Blog • Why TikTok is the Latest Security Threat

Why TikTok is the Latest Security Threat

TikTok is a widely-popular social media platform owned by the Chinese technology company ByteDance. Though its stated intention is to share short dance and lip-sync videos, it has become a substantial player in the targeted advertising business in recent years.

TikTok and Data Collection

TikTok gained an edge through its ability to collect sensitive data about users, even when those users neither saved nor shared their content. This presents a security threat for users due to the 2017 Chinese National Intelligence Law, which states that "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law."[1]

Collection of PII and User Data

The data TikTok collects from users contains sensitive information and is often taken without the user's explicit knowledge. This data includes device brand and model, Operating System (OS) version, mobile carrier, browsing history, app and file names and types, keystroke patterns or rhythms, wireless connections, and geolocation.[2] TikTok's Privacy Policy describes the collection and analysis of user personally identifiable information (PII) as well as user data collected from other sources. This data can include age, image, personal contacts, relationship status, preferences, and other data collected through a single-sign on (SSO) feature that allows users to sign into TikTok from other platforms.[3] Furthermore, the app collects "the content of [messages] and information about when [messages are] sent, received and/or read."[4] In aggregate, TikTok's data collection is more intrusive than other apps.

To use the platform, users grant the app access to the microphone and camera. Multiple lawsuits allege that TikTok also collects biometric data from users, including facial geometry, iris scans, voice recognition, and fingerprints.[5] TikTok uses facial recognition software to superimpose images on users' faces for use in videos. Unlike other data that is collected, biometrics represent the physical user and are generally permanent. Biometrics are therefore of high intelligence value. There is no direct evidence that TikTok is giving this data to the Chinese government, yet the existence of the National Intelligence Law compels TikTok to provide the data if requested.

While TikTok claims all user data is stored in the U.S. and Singapore, TikTok's parent company servers are all located in China and the app itself contains references to China-based infrastructure. While it is unlikely Chinese officials would have access to the data stored in the U.S., all data stored within China may be shared with the Chinese government for intelligence purposes. Because of this, users should assume that their data is being aggregated and shared with the Chinese government.

Security and privacy concerns stem directly from the vague language of the law and the promise that the state will protect those who aid it. Suspected use of propaganda to further China's political interests, coupled with the creation of an unprecedented information harvester, has made TikTok a hot topic for the U.S. Government and cybersecurity community alike. Unlike Europe, the U.S. does not have many federal laws that prohibit the collection, sale, and use of such personal data, leaving TikTok able to continuously scrape user data with little restraint or oversight.

Violations of COPPA

TikTok collects data from all age groups and, in doing so, regularly violates the Children's Online Privacy Protection Rule of 1998 (COPPA). Under COPAA, "developers of child-focused apps cannot lawfully obtain the PII of children under 13 years of age without first obtaining verifiable consent from parents."[6] A 2019 court case against ByteDance alleges that two children under the age of 13 were not asked to provide any parental consent to use TikTok.[7] ByteDance settled the case and agreed to adding in parental controls. However, as of May of this year, multiple consumer groups have alerted the Federal Trade Commission that TikTok continues to violate children's privacy.[8]

Censorship

Moderation guidelines for TikTok were leaked in late 2019 highlighting the app's censorship of any content critical of Chinese state interests. According to the leaked documents, the company instructs their moderators to remove any undesirable content pertaining to topics sensitive to the Chinese Communist Party (CCP) including Tiananmen Square, Tibetan Independence, or any current protests.[9] Late last year, a U.S. teenager posted a TiKTok video disguised as a "makeup tutorial" that was actually meant to bring attention to Chinese treatment of Uighur Muslims in Xinjiang. The user's account was suspended and the video was removed, and though it was only temporary, this behavior aligns with China's national interests without regard for freedom of expression.

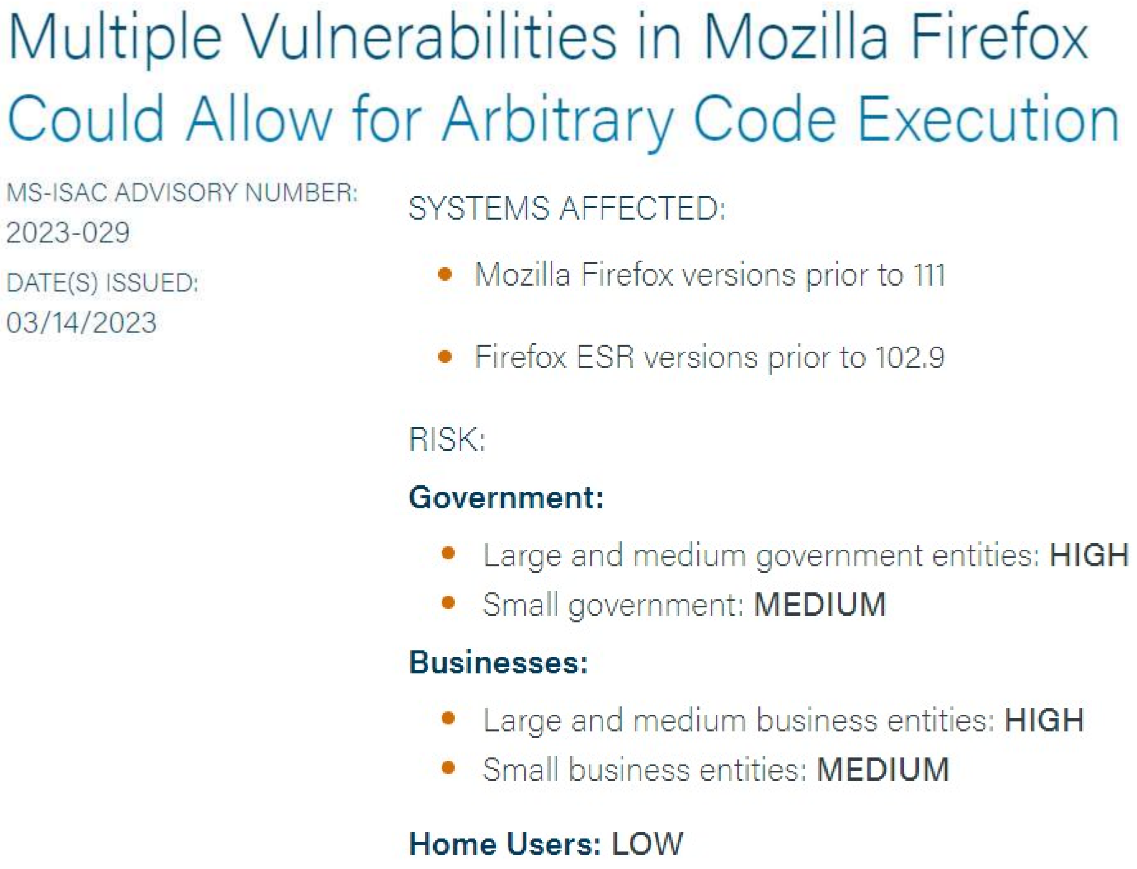
What Can Be Done?

The U.S. military and private companies, such as Amazon, are among those currently banning TikTok on business devices.[10] Regardless of an organization's position on TikTok specifically, it is imperative that guidelines be set forth in an Acceptable Use Policy (AUP) for business devices. For those who would like to take it a step further, social media apps can be easily blocked by category or by specific infrastructure, such as Internet Protocol (IP) addresses and domain names.

The MS-ISAC Cyber Threat Intelligence (CTI) team recommends state, local, tribal, and territorial (SLTTs) government entities and all community members educate themselves on the privacy and data collection policies of the apps they use. Companies that collect too much data or whose policies contain vague language about what is collected should be avoided. In the case of TikTok, CTI recommends parents, teachers, and local leaders talk to young adults, teenagers, and children who may be using the app about the dangers it poses to their personal security. Through education and awareness, all are able to limit the use of personal data in nefarious ways.

Alerts and Advisories

- Overview
- Threat Intelligence
- Systems Affected
- Risk Level
- Technical Summary
- Associated CVEs
- Recommendations



Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

MS-ISAC ADVISORY NUMBER:
2023-029

DATE(S) ISSUED:
03/14/2023

SYSTEMS AFFECTED:

- Mozilla Firefox versions prior to 111
- Firefox ESR versions prior to 102.9

RISK:

Government:

- Large and medium government entities: **HIGH**
- Small government: **MEDIUM**

Businesses:

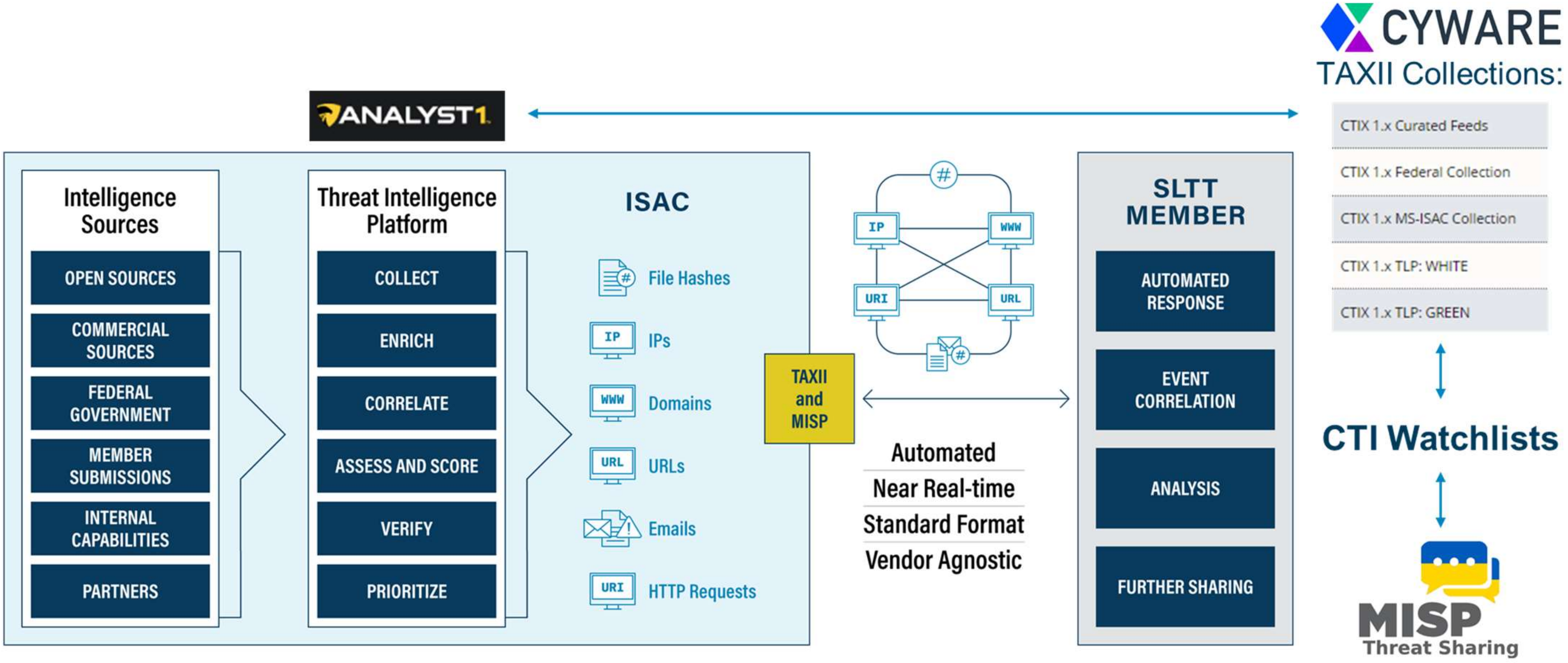
- Large and medium business entities: **HIGH**
- Small business entities: **MEDIUM**

Home Users: LOW

MS-ISAC®

Indicator Sharing Program

OperationsSupport@cisecurity.org



CYWARE

TAXII Collections:

- CTIX 1.x Curated Feeds
- CTIX 1.x Federal Collection
- CTIX 1.x MS-ISAC Collection
- CTIX 1.x TLP: WHITE
- CTIX 1.x TLP: GREEN

ANALYST1

Intelligence Sources

- OPEN SOURCES
- COMMERCIAL SOURCES
- FEDERAL GOVERNMENT
- MEMBER SUBMISSIONS
- INTERNAL CAPABILITIES
- PARTNERS

Threat Intelligence Platform

- COLLECT
- ENRICH
- CORRELATE
- ASSESS AND SCORE
- VERIFY
- PRIORITIZE

ISAC

- File Hashes
- IPs
- Domains
- URLs
- Emails
- HTTP Requests

TAXII and MISP

Automated

Near Real-time

Standard Format

Vendor Agnostic

SLTT MEMBER

- AUTOMATED RESPONSE
- EVENT CORRELATION
- ANALYSIS
- FURTHER SHARING

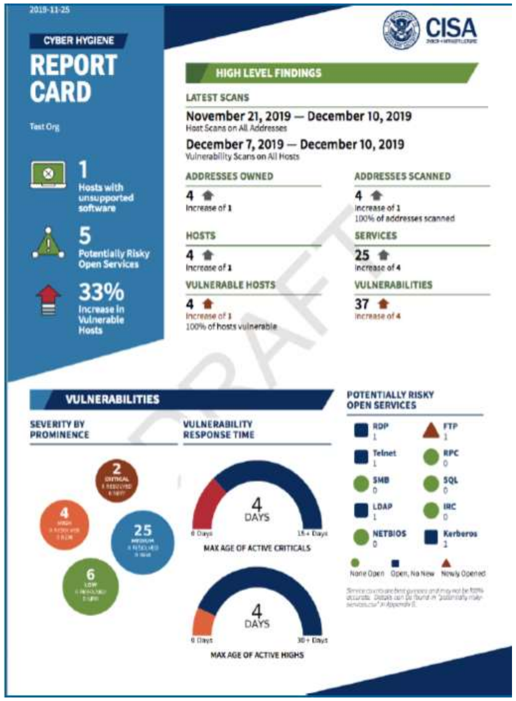
CTI Watchlists

MISP Threat Sharing

https://www.cisecurity.org/ms-isac/services/real-time-indicator-feeds

CISA Cyber Hygiene Program

Avoid a Cyber Disaster



2019-11-25

CYBER HYGIENE

REPORT CARD

Test Org

1 Hosts with unsupported software

5 Potentially Risky Open Services

33% Increase in Vulnerable Hosts

CISA

HIGH LEVEL FINDINGS

LATEST SCANS

November 21, 2019 — December 10, 2019
Host Scans on All Addresses

December 7, 2019 — December 10, 2019
Vulnerability Scans on All Hosts

ADDRESSES OWNED
4
Increase of 1

ADDRESSES SCANNED
4
Increase of 1
100% of addresses scanned

HOSTS
4
Increase of 1

SERVICES
25
Increase of 4

VULNERABLE HOSTS
4
Increase of 1
100% of hosts vulnerable

VULNERABILITIES
37
Increase of 4

VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME

MAX AGE OF ACTIVE CRITICALS

MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

■ RDP 1	▲ FTP 1
■ Telnet 1	● RPC 0
● SMB 0	● SQL 0
■ LDAP 1	● IRC 0
● NETBIOS 0	■ Kerberos 1

● None Open ■ Open, No New ▲ Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix B.

- 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.

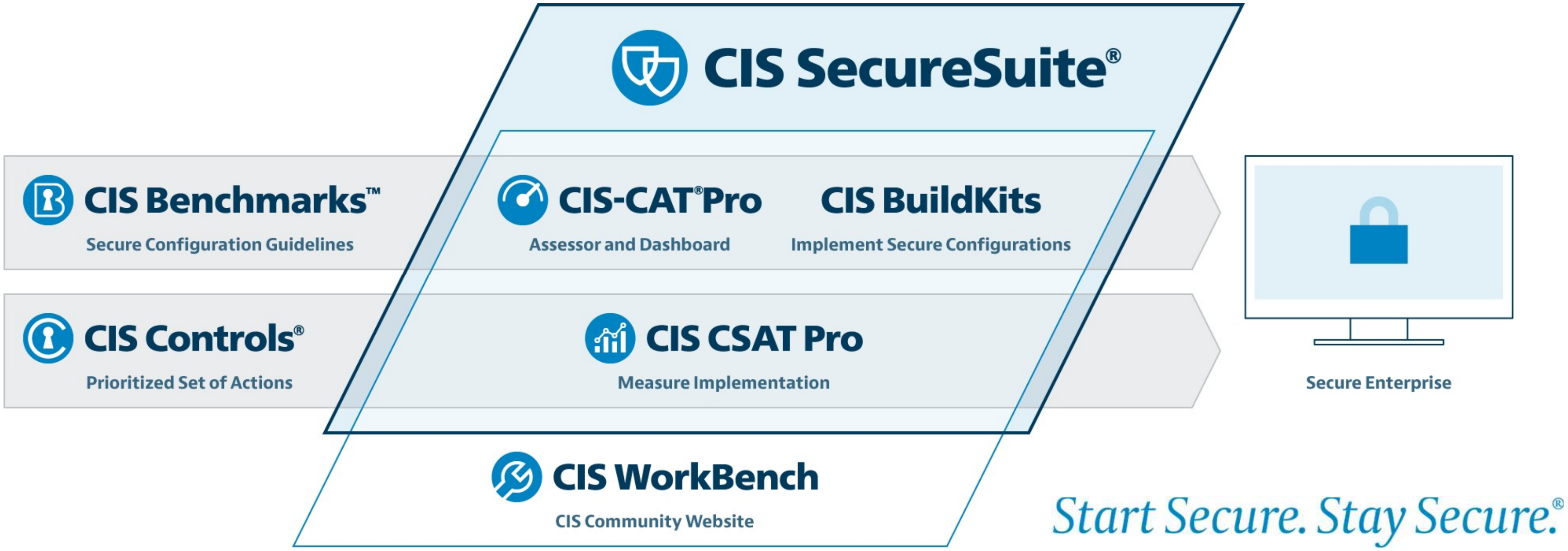
MS-ISAC®

SecureSuite Introduction

MS-ISAC®

CIS SecureSuite®

FreeSecureSuite@cisecurity.org

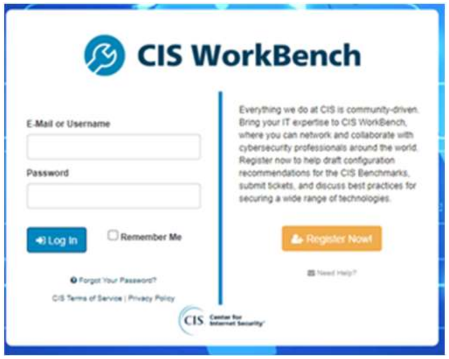


https://www.cisecurity.org/cis-securesuite/member-webinars

CIS WorkBench

Collaborative platform

- **Access CIS WorkBench:** https://workbench.cisecurity.org
- **Platform for creating and maintaining resources**
  - Access to member only downloads
    - CIS-CAT Pro
    - CIS CSAT Pro
    - CIS Benchmarks (PDF, Word, Excel, XML/OVAL)
    - CIS Build Kits (GPOs/Scripts for implementing CIS Benchmarks)
  - Join the consensus process

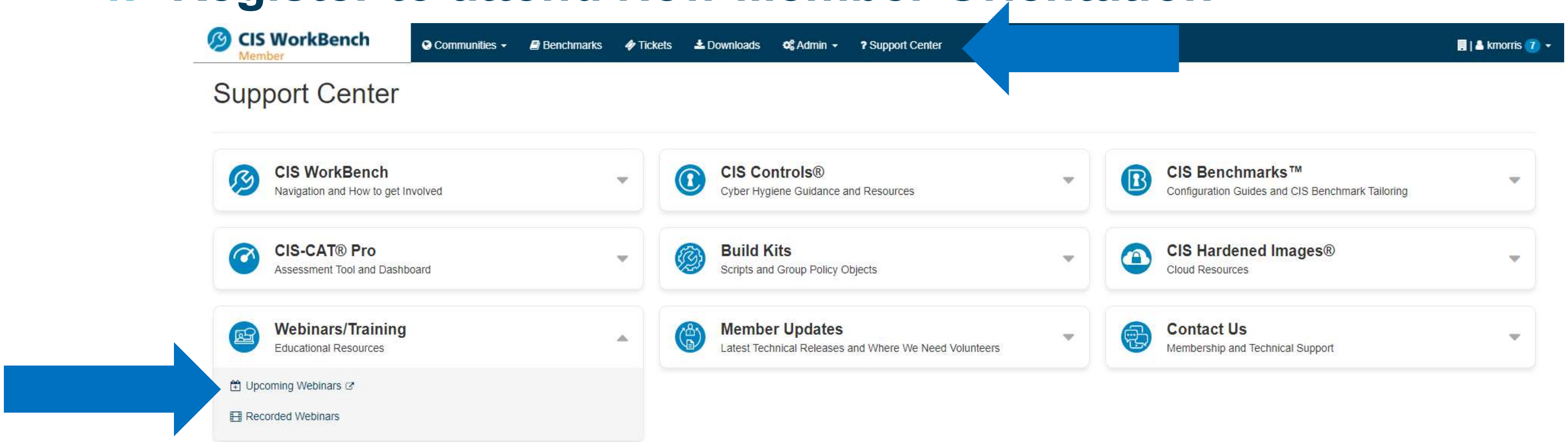


Everything we do at CIS is community-driven. Bring your IT expertise to CIS WorkBench, where you can network and collaborate with cybersecurity professionals around the world. Register now to help draft configuration recommendations for the CIS Benchmarks, submit tickets, and discuss best practices for securing a wide range of technologies.

CIS SecureSuite® Membership

Getting Started Checklist

1. **Log into CIS Workbench:** https://workbench.cisecurity.org
2. **Visit the Support Center:** https://workbench.cisecurity.org/support-center
3. **Visit Upcoming Webinars link**
4. **Register to attend New Member Orientation**

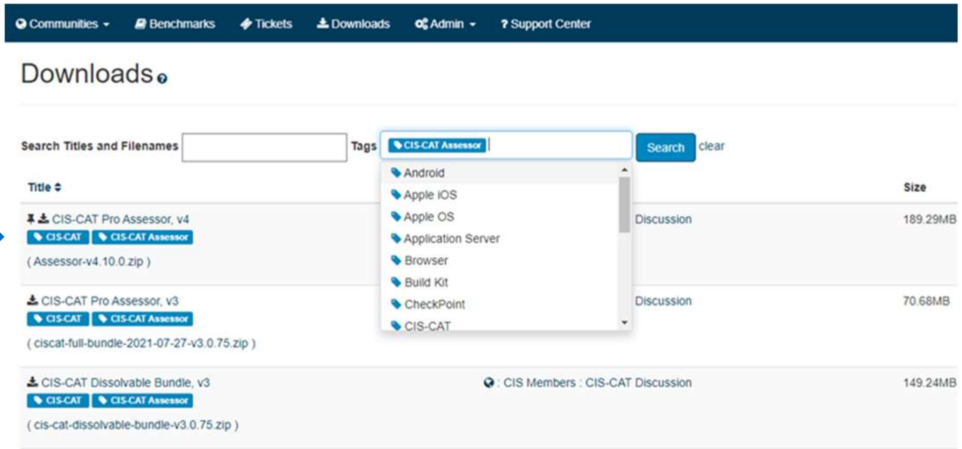


CIS SecureSuite® Membership

Getting Started Checklist

5. **Join CIS-CAT Discussion community**
6. **Schedule on-boarding call with me:** Jody.Tarshis@cisecurity.org

- ➢ Download CIS-CAT Pro Assessor: https://workbench.cisecurity.org/files/2151
- ➢ Run a scan
- ➢ Review Report



Downloads

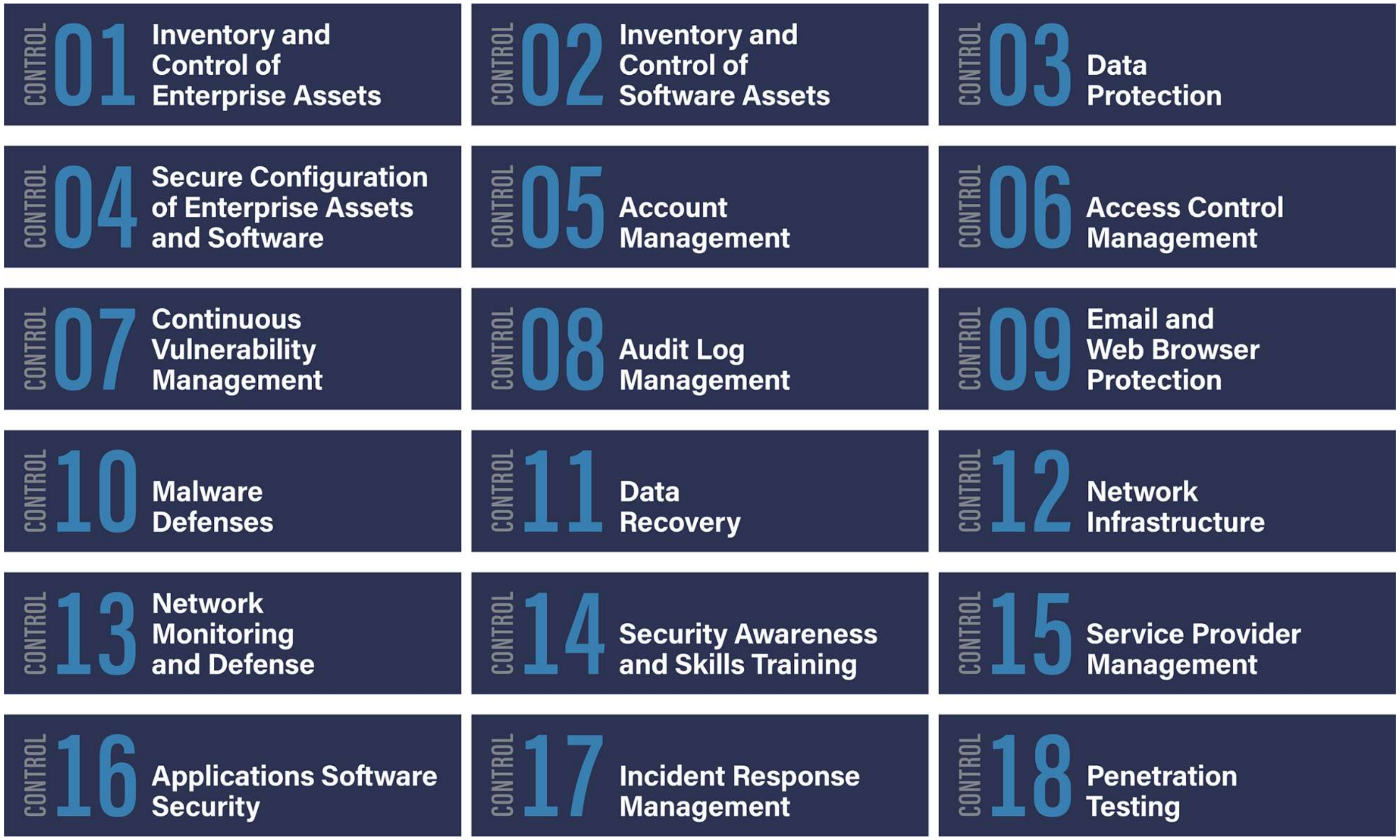
Search Titles and Filenames: [ ] Tags: CIS-CAT Assessor — Search — clear

Title		Size
CIS-CAT Pro Assessor, v4 CIS-CAT · CIS-CAT Assessor (Assessor-v4.10.0.zip)	Discussion	189.29MB
CIS-CAT Pro Assessor, v3 CIS-CAT · CIS-CAT Assessor (ciscat-full-bundle-2021-07-27-v3.0.75.zip)	Discussion	70.68MB
CIS-CAT Dissolvable Bundle, v3 CIS-CAT · CIS-CAT Assessor (cis-cat-dissolvable-bundle-v3.0.75.zip)	: CIS Members : CIS-CAT Discussion	149.24MB

MS-ISAC®

CIS Controls – Security Best Practices

CIS Controls v8

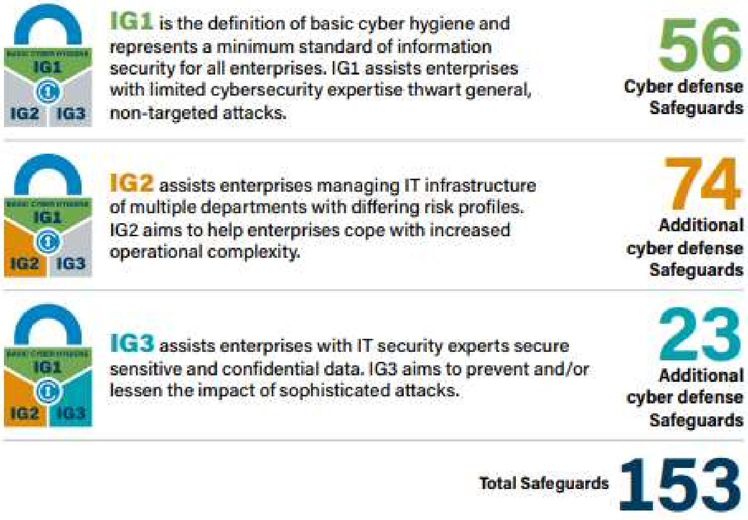


- CONTROL 01 Inventory and Control of Enterprise Assets
- CONTROL 02 Inventory and Control of Software Assets
- CONTROL 03 Data Protection
- CONTROL 04 Secure Configuration of Enterprise Assets and Software
- CONTROL 05 Account Management
- CONTROL 06 Access Control Management
- CONTROL 07 Continuous Vulnerability Management
- CONTROL 08 Audit Log Management
- CONTROL 09 Email and Web Browser Protection
- CONTROL 10 Malware Defenses
- CONTROL 11 Data Recovery
- CONTROL 12 Network Infrastructure
- CONTROL 13 Network Monitoring and Defense
- CONTROL 14 Security Awareness and Skills Training
- CONTROL 15 Service Provider Management
- CONTROL 16 Applications Software Security
- CONTROL 17 Incident Response Management
- CONTROL 18 Penetration Testing

MS-ISAC®

CIS Controls™

- **Implementation Groups (IG) to the CIS Controls:**
  - IG's – are the recommended guidance to prioritize implementation of the CIS Controls.
  - IGs are divided into three groups, based on the risk profile and resources an enterprise has available to them to implement the CIS Controls



IG1 is the definition of basic cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56 Cyber defense Safeguards

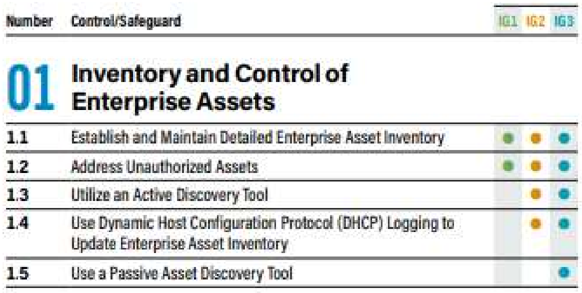
IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74 Additional cyber defense Safeguards

IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23 Additional cyber defense Safeguards

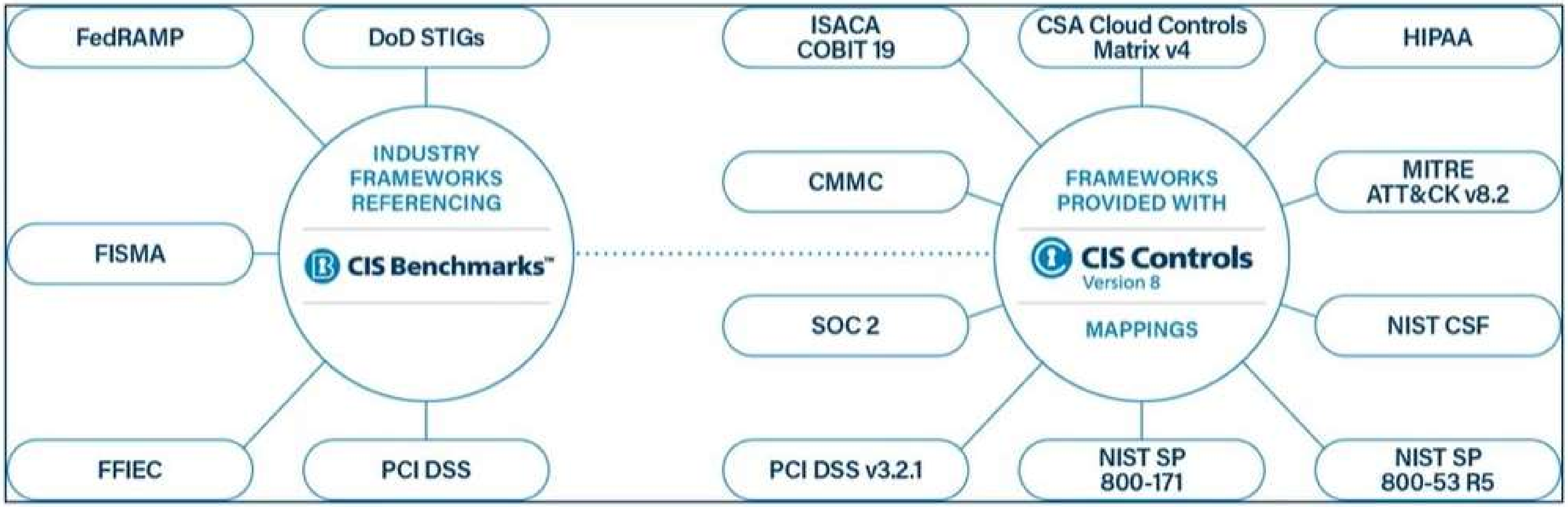
Total Safeguards **153**



Number	Control/Safeguard	IG1	IG2	IG3
01	**Inventory and Control of Enterprise Assets**			
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●

Referenced by Industry Standards

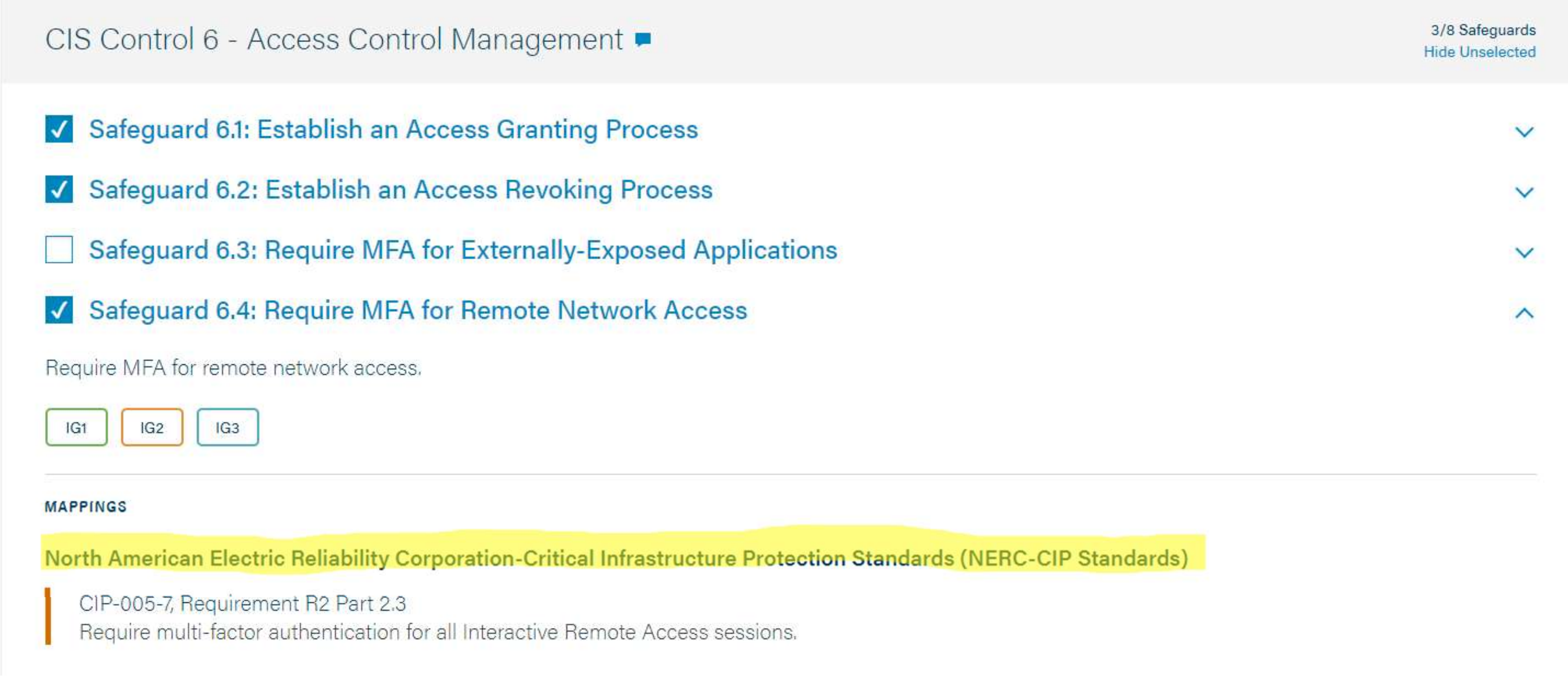
Assisting Organizations That are Working Towards Compliance



Controls Navigator Tool

https://www.cisecurity.org/controls/cis-controls-navigator

- Explore how the Controls map to your broader security program
- Broken down by Implementation Group



CIS Control 6 - Access Control Management

3/8 Safeguards
Hide Unselected

☑ Safeguard 6.1: Establish an Access Granting Process

☑ Safeguard 6.2: Establish an Access Revoking Process

□ Safeguard 6.3: Require MFA for Externally-Exposed Applications

☑ Safeguard 6.4: Require MFA for Remote Network Access

Require MFA for remote network access.

IG1 IG2 IG3

MAPPINGS

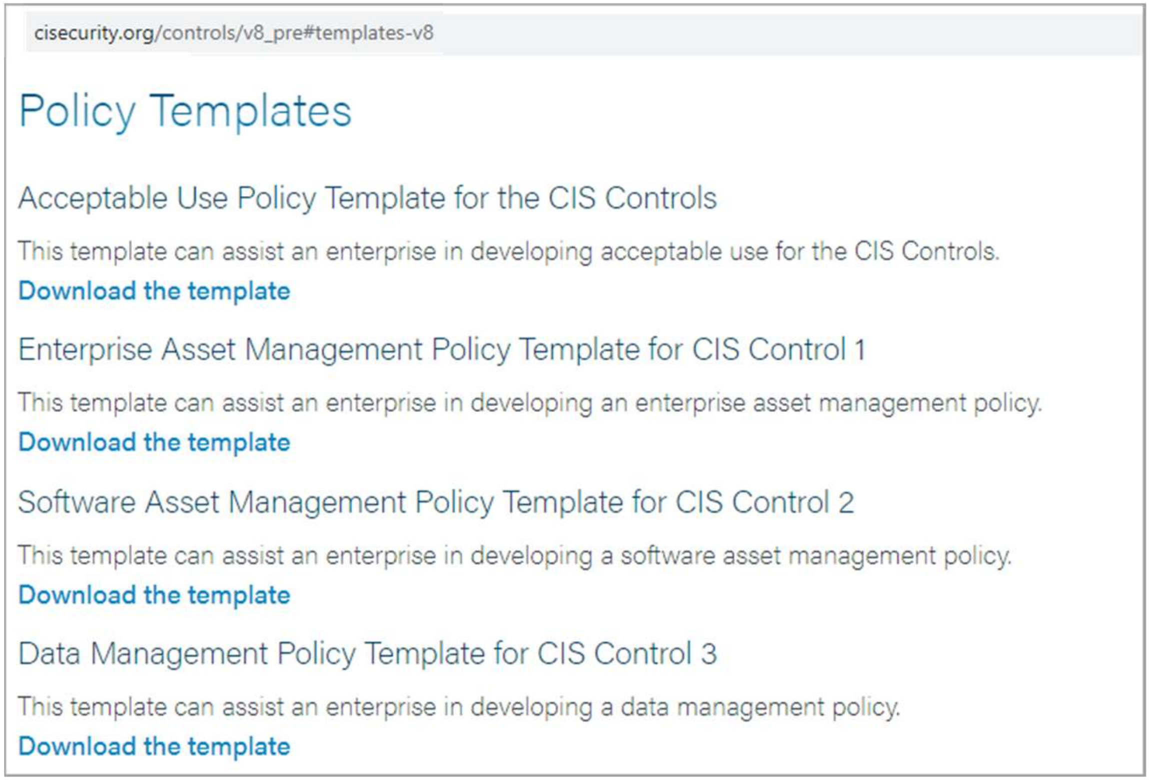
North American Electric Reliability Corporation-Critical Infrastructure Protection Standards (NERC-CIP Standards)

CIP-005-7, Requirement R2 Part 2.3
Require multi-factor authentication for all Interactive Remote Access sessions.

Introduction: CIS Critical Security Controls

Policy Templates

- **Policy templates available to help organizations get started**



cisecurity.org/controls/v8_pre#templates-v8

Policy Templates

Acceptable Use Policy Template for the CIS Controls

This template can assist an enterprise in developing acceptable use for the CIS Controls.

Download the template

Enterprise Asset Management Policy Template for CIS Control 1

This template can assist an enterprise in developing an enterprise asset management policy.

Download the template

Software Asset Management Policy Template for CIS Control 2

This template can assist an enterprise in developing a software asset management policy.

Download the template

Data Management Policy Template for CIS Control 3

This template can assist an enterprise in developing a data management policy.

Download the template

Controls Resources

Workbench

- **MS-ISAC Establishing Essential Cyber Hygiene Guide**
  - NIST Mappings, step-by-step guidance, open-source tools and resources
- **The Cost of Cyber Defense**
  - Budgeting guidance for Implementation Group 1
- **CIS Community Defense Model**
  - See how the Controls and Benchmarks defend against top attack tactics using MITRE ATT&CK Framework
- **A Guide to Defining Reasonable Cybersecurity**

MS-ISAC®

Introduction to CSAT Pro
Controls Self Assessment Tool

Confidential & Proprietary

V2.0

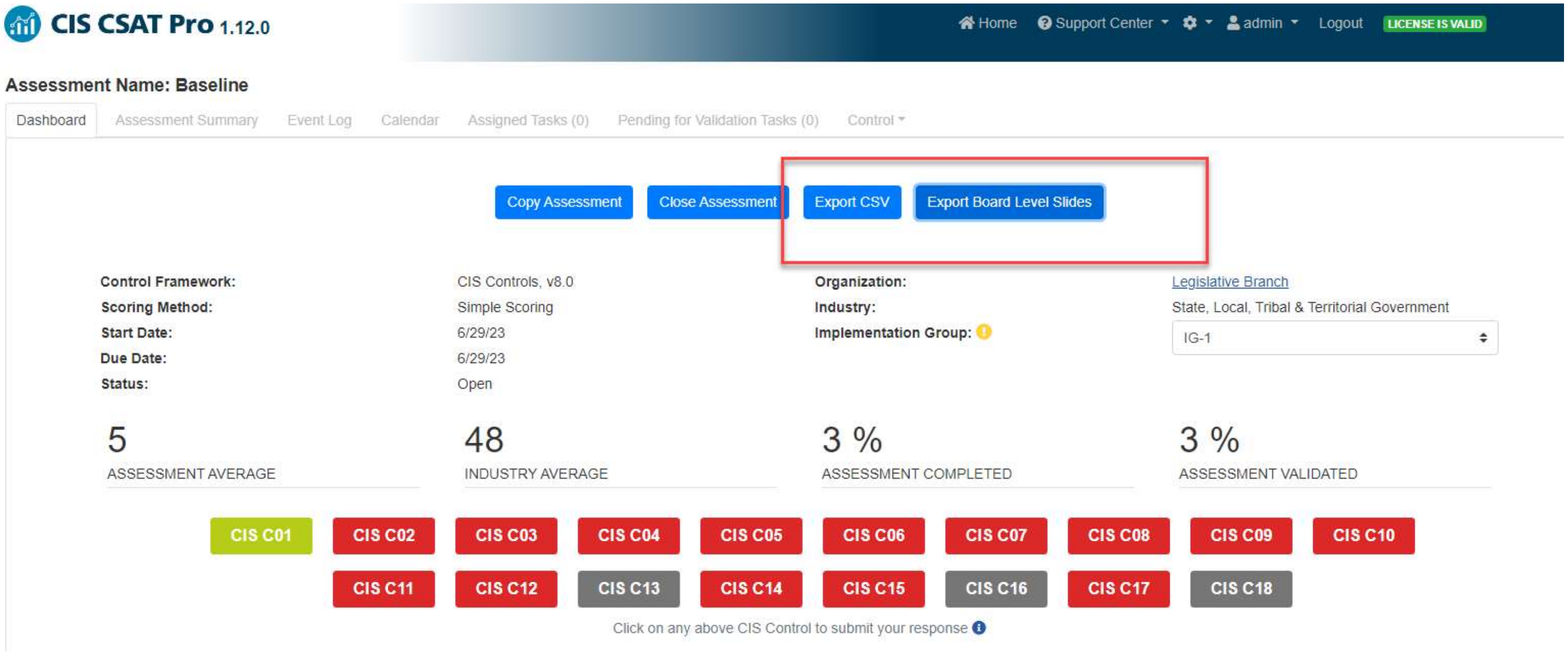
CIS Controls Self Assessment Tool Pro (CSAT Pro)

High-Level Features

- **Easy web interface to view CIS Controls**
- **Provides scored assessment of an organization's implementation of the CIS Controls**
  - Based on organization's input *(self-assessment)*
  - At the Safeguard level *(Supports Implementation Groups)*
  - Pro version is on premises *(CIS Hosted version also available)*
  - Flexible scoring per organizational policies
- **Optionally compares scores over time and against others in the same industry**
- **Flexible reporting**
- **Enables organizations to assess and track their implementation of the CIS Controls for Versions 8 and 7.1**

Controls Self Assessment Tool (CIS CSAT Pro)

Report Exports



Assessment Name: Baseline

Control Framework:	CIS Controls, v8.0	**Organization:**	Legislative Branch
Scoring Method:	Simple Scoring	**Industry:**	State, Local, Tribal & Territorial Government
Start Date:	6/29/23	**Implementation Group:**	IG-1
Due Date:	6/29/23		
Status:	Open		

5	48	3 %	3 %
ASSESSMENT AVERAGE	INDUSTRY AVERAGE	ASSESSMENT COMPLETED	ASSESSMENT VALIDATED

Click on any above CIS Control to submit your response

- Export stakeholder reports in multiple formats such as PowerPoint, and Excel

MS-ISAC®

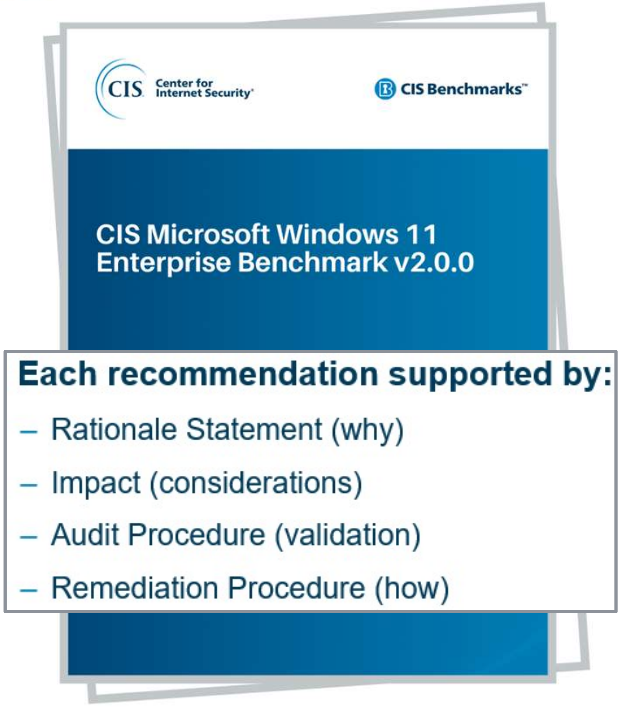
CIS Benchmarks

CIS Benchmarks

Consensus-developed secure configuration guidelines

- **100+ CIS Benchmarks**
  - Recommendations for system state
- **Covering 25 vendor product families**
  - Operating Systems, Server Software, Cloud Providers, Network Devices, Desktop Software
- **Recognized by industry frameworks**
  - FISMA, FedRAMP, PCI, DoD Cloud Computing SRG
- **Community developed**
  - CIS members, subject matter experts, security community experts, and technology vendors

CIS Benchmarks™



CIS Center for Internet Security®

CIS Benchmarks™

CIS Microsoft Windows 11 Enterprise Benchmark v2.0.0

Each recommendation supported by:

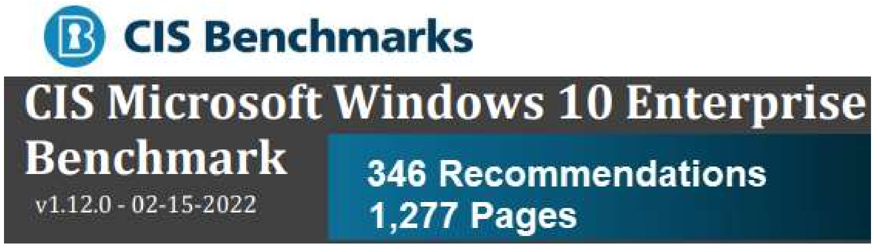
- Rationale Statement (why)
- Impact (considerations)
- Audit Procedure (validation)
- Remediation Procedure (how)

CIS-CAT: Best Practice in Action

What exactly does CIS-CAT Assessor do?

No CIS-CAT – Weeks of Human Effort

Manual comparison



CIS Benchmarks

CIS Microsoft Windows 10 Enterprise Benchmark

v1.12.0 - 02-15-2022

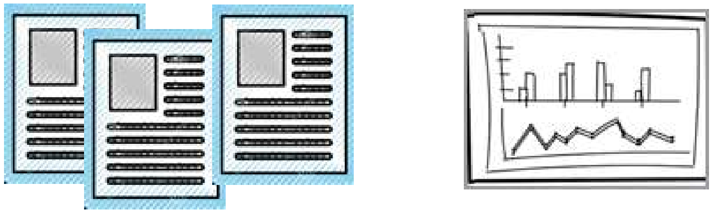
346 Recommendations

1,277 Pages

CIS-CAT – 2 Minutes Machine Effort

Automatic comparison

Result Output: Reports and Dashboard



CIS-CAT: Components

CIS-CAT Main Components

CIS-CAT Pro

Assessor

Reports a configuration result score

Dashboard

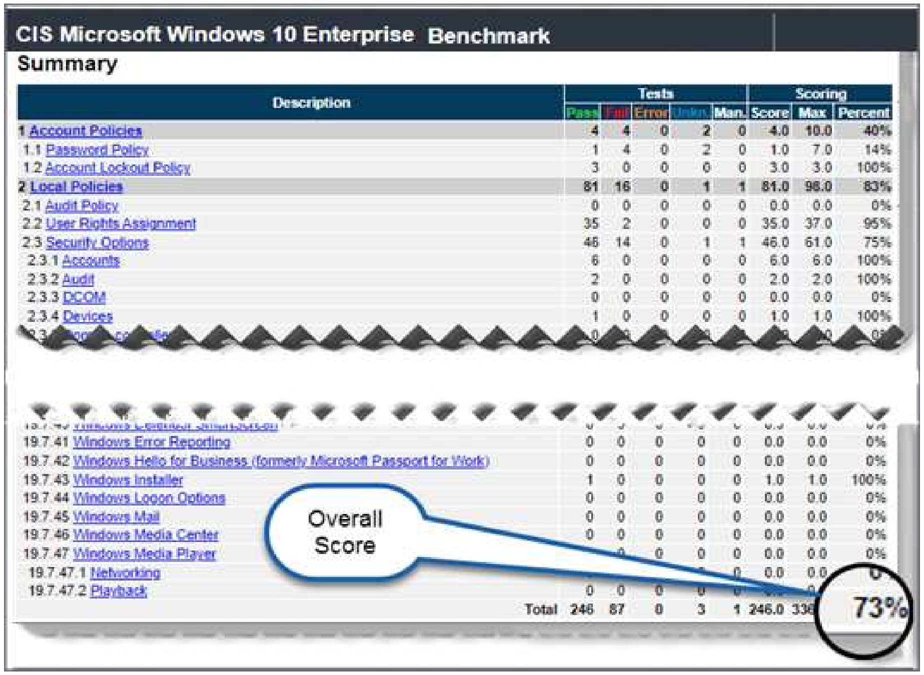
Graphical Display of Results

- On-premise (self-managed) applications under your control (cloud, VM, Server)
- Utilized in testing CIS Benchmarks
- Easy graphical user interface (GUI) in Assessor
- Local or remote system assessment

CIS-CAT Actionable Results

Configuration Result Output

- **Organization cyber security policy will dictate accepted score**
- **Out of the box systems** score **< 30%**
- **Aim for a score between 85%-95%**
- CIS-CAT® Pro Assessor evaluates the cybersecurity posture (**configuration**) of a system against recommended configuration policy settings (**CIS Benchmarks**).



CIS Microsoft Windows 10 Enterprise Benchmark

Summary

Description	Tests					Scoring		
	Pass	Fail	Error	Unkn.	Man.	Score	Max	Percent
1 Account Policies	4	4	0	2	0	4.0	10.0	40%
1.1 Password Policy	1	4	0	2	0	1.0	7.0	14%
1.2 Account Lockout Policy	3	0	0	0	0	3.0	3.0	100%
2 Local Policies	81	16	0	1	1	81.0	98.0	83%
2.1 Audit Policy	0	0	0	0	0	0.0	0.0	0%
2.2 User Rights Assignment	35	2	0	0	0	35.0	37.0	95%
2.3 Security Options	46	14	0	1	1	46.0	61.0	75%
2.3.1 Accounts	6	0	0	0	0	6.0	6.0	100%
2.3.2 Audit	2	0	0	0	0	2.0	2.0	100%
2.3.3 DCOM	0	0	0	0	0	0.0	0.0	0%
2.3.4 Devices	1	0	0	0	0	1.0	1.0	100%
[illegible]	0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
19.7.41 Windows Error Reporting	0	0	0	0	0	0.0	0.0	0%
19.7.42 Windows Hello for Business (formerly Microsoft Passport for Work)	0	0	0	0	0	0.0	0.0	0%
19.7.43 Windows Installer	1	0	0	0	0	1.0	1.0	100%
19.7.44 Windows Logon Options	0	0	0	0	0	0.0	0.0	0%
19.7.45 Windows Mail	0	0	0	0	0	0.0	0.0	0%
19.7.46 Windows Media Center	0	0	0	0	0	0.0	0.0	0%
19.7.47 Windows Media Player	[illegible]	0	0	0	0	0.0	0.0	0%
19.7.47.1 Networking	[illegible]	[illegible]	[illegible]	[illegible]	0	0.0	0.0	0
19.7.47.2 Playback	0	0	0	0	0	[illegible]	[illegible]	[illegible]
Total	246	87	0	3	1	246.0	336	73%

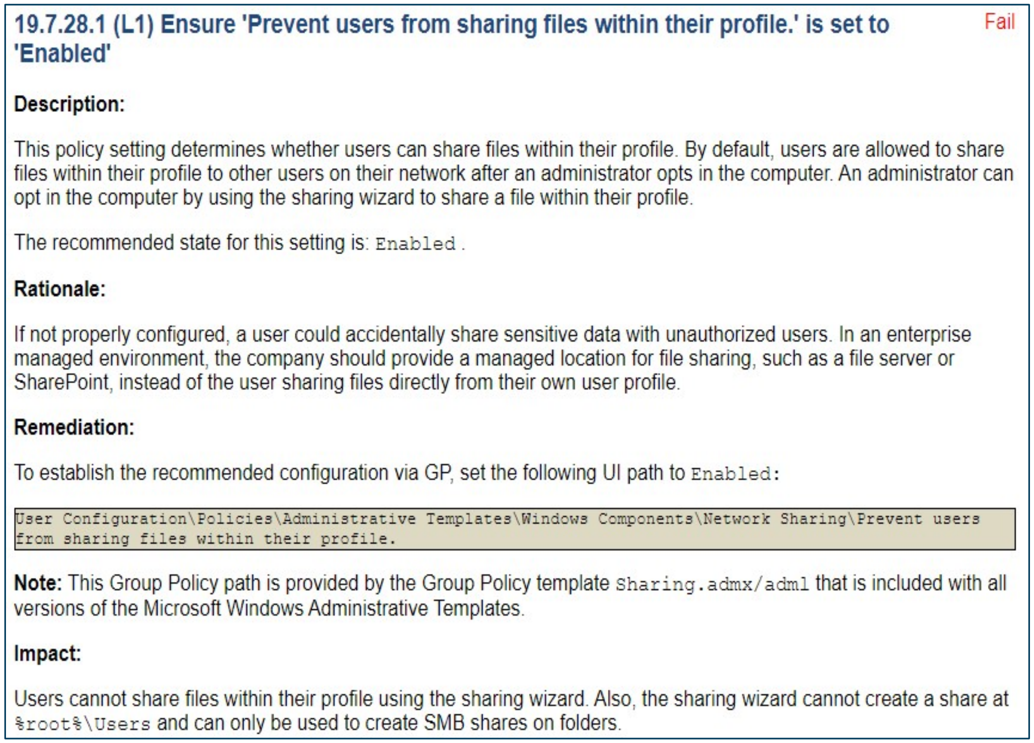
Confidential & Proprietary

CIS-CAT: Actionable Results

Key configuration information to inform recommendation adoption

CIS Benchmarks™

- **Description:** about the configuration
- **Rationale:** the importance
- **Remediation:** how to modify the configuration
- **Note:** special information about this remediation
- **Impact:** the potential considerations of adjusting this configuration



19.7.28.1 (L1) Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' Fail

Description:

This policy setting determines whether users can share files within their profile. By default, users are allowed to share files within their profile to other users on their network after an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile.

The recommended state for this setting is: `Enabled` .

Rationale:

If not properly configured, a user could accidentally share sensitive data with unauthorized users. In an enterprise managed environment, the company should provide a managed location for file sharing, such as a file server or SharePoint, instead of the user sharing files directly from their own user profile.

Remediation:

To establish the recommended configuration via GP, set the following UI path to `Enabled:`

```
User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users
from sharing files within their profile.
```

Note: This Group Policy path is provided by the Group Policy template `Sharing.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

Impact:

Users cannot share files within their profile using the sharing wizard. Also, the sharing wizard cannot create a share at `%root%\Users` and can only be used to create SMB shares on folders.

MS-ISAC®

Build Kits – Remediation

Confidential & Proprietary

V2.0

Automated Remediation

CIS Build Kits

- **Pre-configured templates used to implement the recommendations from the benchmark to the target system (for Windows and Linux primarily)**
  - Pre-configured GPOs for Windows
    - Import via Group Policy Management
  - Basic Shell Scripts for Linux/Unix
    - Run using scripting tool of choice

ANY QUESTIONS?

MS-ISAC®

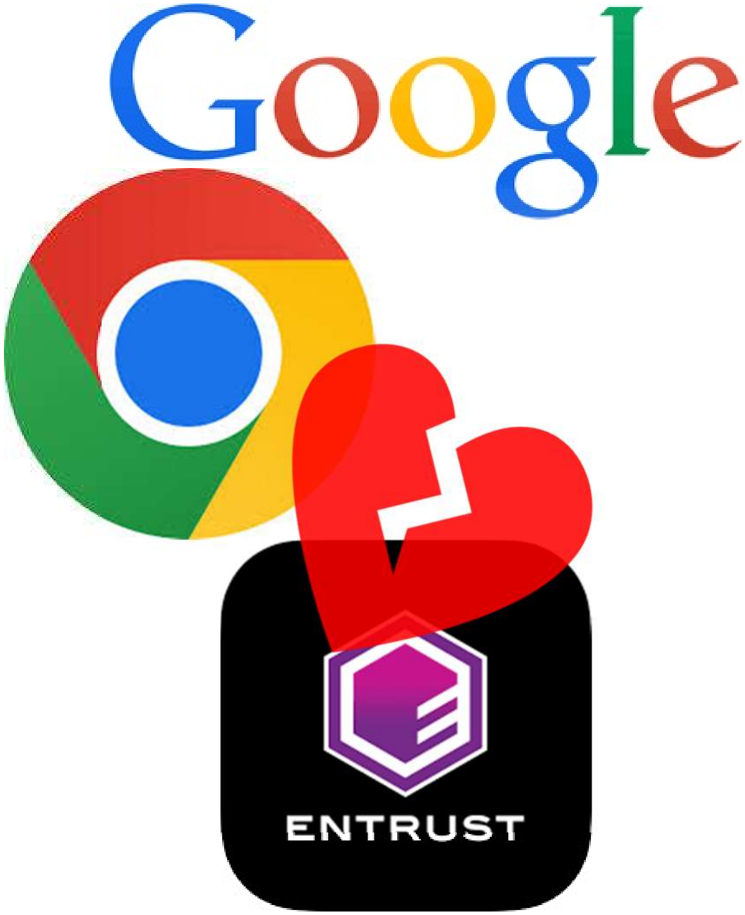
Multi-State Information Sharing & Analysis Center®

Thank You!

Megan Incerto

Regional Engagement Manager, MS-ISAC

Megan.Incerto@cisecurity.org | 518-640-3655



VIRGINIA
IT AGENCY

Google Chrome browser Entrust Distrust

VITA Review and Go-Forward for COV Servers - UPDATE

John C Del Grosso
VITA SSDC Service Owner

September 4, 2024

Google distrust of Entrust certificates starting Oct. 31

Google Chrome will no longer support Entrust certificates installed *after* Oct. 31 **AND** those installed before Oct. 31 that *do not* meet the Entrust root certification authority Signed Certificate Timestamp (SCT).

COV has used Entrust as the primary vendor for all certificates for many years.

778 active certificates impacting 52 agencies

Please see the Entrust webpage for additional detail: TLS Certificate Information Center | TLS Support | Entrust

As such, the change does not adversely affect VITA, agencies, or Customers

All existing Entrust certs will operate without affect to users or systems past Oct. 31 until expiration

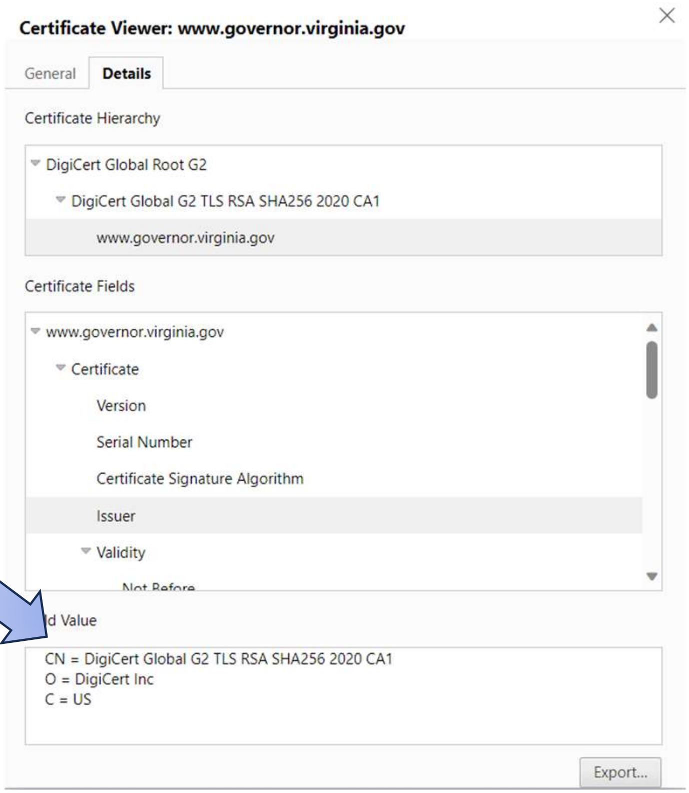
- Complete: DigiCert will be the new CA vendor.
- Entrust certificates will be removed/replaced from environment as they expire over the next year starting when the new certificate authority (CA) is on-boarded (September)

Immediate and Long-Term Planning

- Immediate goal: Replace Entrust with a new certificate authority by the end of August, start using new CA before October for new/replacement certs.
  - Entrust certificates will be removed/replaced from environment as they expire over the next year starting when the new CA is on-boarded (September)
  - DigiCert is the new CA vendor.
    - Initial goal is to keep the service in place as it exists today and get to a steady state, then move to the long-term goal of full-service using automation, notification and business processes.
- Long-term goal: An end-to-end full service CA that utilizes automation, notification, and business processes built-in for true modernized certificate management by end-of-year.

Certificate attribute changes with new authority vendor

The Issuer will show a new CA vendor (TBD).



Certificate Viewer: www.governor.virginia.gov

Certificate Hierarchy

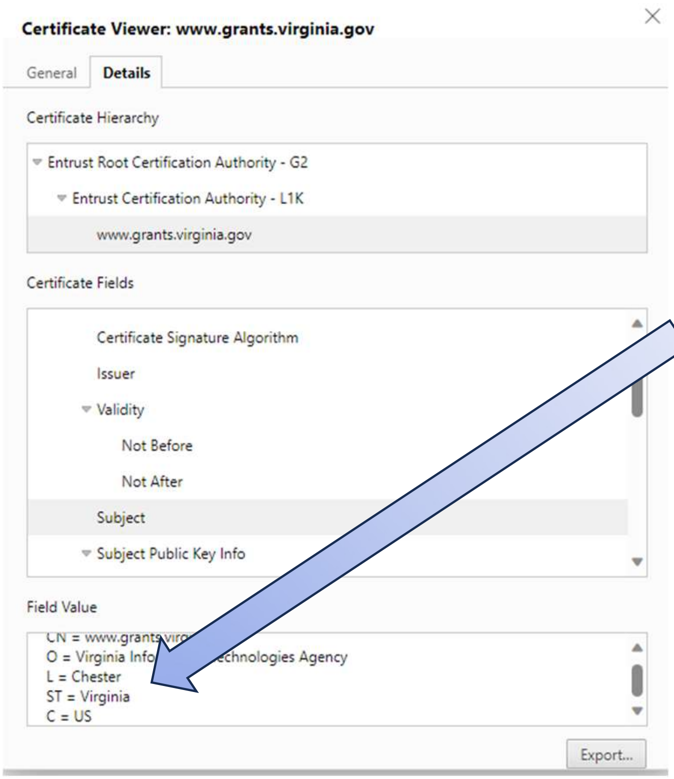
- DigiCert Global Root G2
  - DigiCert Global G2 TLS RSA SHA256 2020 CA1
    - www.governor.virginia.gov

Certificate Fields

- www.governor.virginia.gov
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

d Value

CN = DigiCert Global G2 TLS RSA SHA256 2020 CA1
O = DigiCert Inc
C = US



Certificate Viewer: www.grants.virginia.gov

Certificate Hierarchy

- Entrust Root Certification Authority - G2
  - Entrust Certification Authority - L1K
    - www.grants.virginia.gov

Certificate Fields

- Certificate Signature Algorithm
- Issuer
- Validity
  - Not Before
  - Not After
- Subject
- Subject Public Key Info

Field Value

CN = www.grants.virg
O = Virginia Info echnologies Agency
L = Chester
ST = Virginia
C = US

The (L) attribute will be changed from 'Chester' to 'Sandston' to reflect the new datacenter location (CESC to QTS-Sandston)

The start of something new!...

Questions?
Thank you!

VIRGINIA IT AGENCY

Components and Concepts of a Risk Assessment

VITA Risk Management

Matt Steinbach

Risk Assessment completion requires input and collaboration from business and agency leadership

What is a Risk Assessment

- Address the potential adverse impacts to organizational operations and assets arising from the operation and use of information systems and the information processed, stored, and transmitted by those systems
- Organizations conduct risk assessments to determine risks that are common to the organization's core missions, business processes, infrastructure services, or information systems

Risk Assessments can support a wide variety of risk-based decisions and activities including:

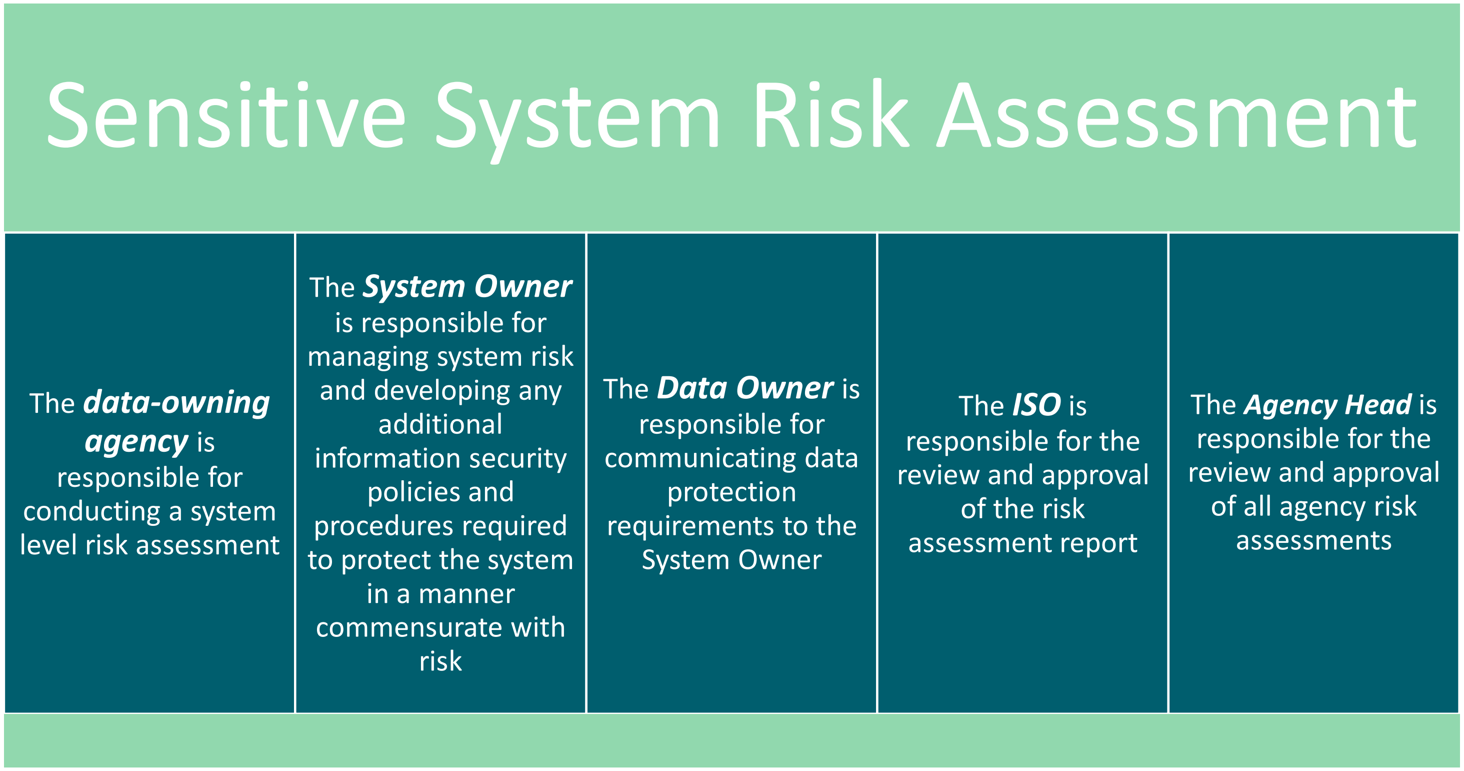
- Design of security solutions for information systems and environments of operation
- Authorization (or denial of authorization) to operate information systems
- Implementation of security solutions including continuous monitoring strategies and ongoing authorizations
- Development of an information security architecture

Negative Impacts of Incomplete or Incorrect RA:

- ➢ *Organization risk appetite undefined*
- ➢ *Unidentified risks communicated to leadership*
- ➢ *Unprotected assets*
- ➢ *Underestimated threats*

NIST Special Publication 800-30

Roles and Responsibilities

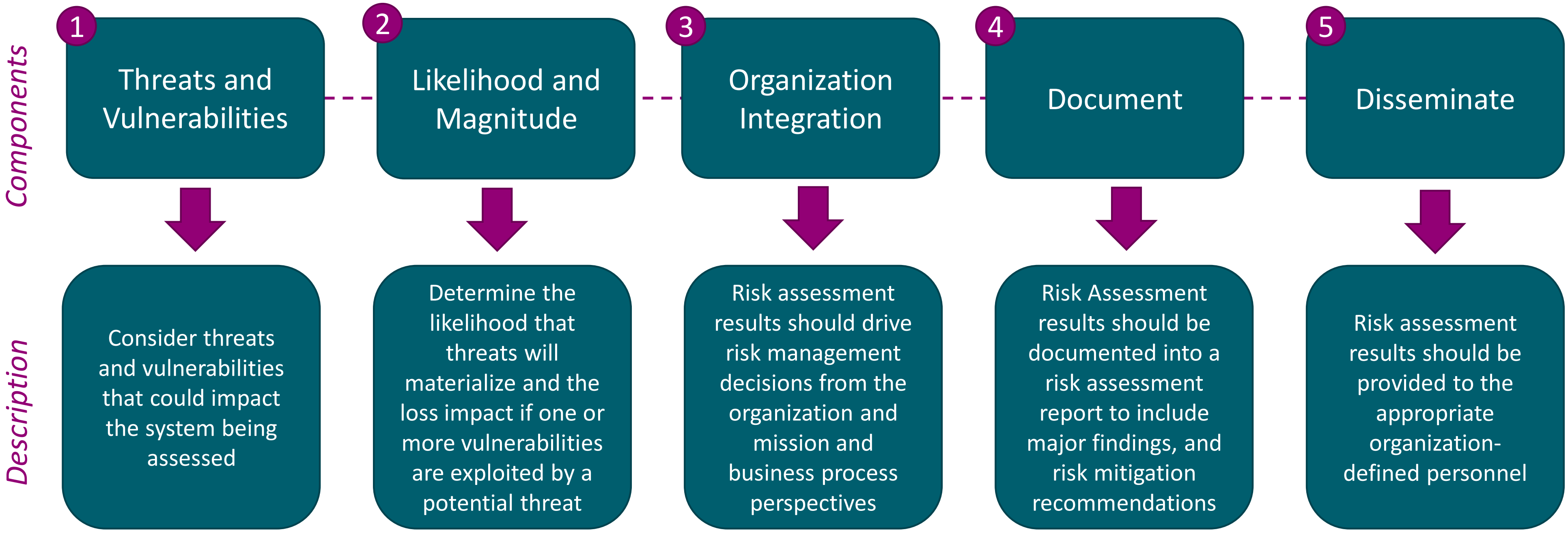


Sensitive System Risk Assessment

- The ***data-owning agency*** is responsible for conducting a system level risk assessment
- The ***System Owner*** is responsible for managing system risk and developing any additional information security policies and procedures required to protect the system in a manner commensurate with risk
- The ***Data Owner*** is responsible for communicating data protection requirements to the System Owner
- The ***ISO*** is responsible for the review and approval of the risk assessment report
- The ***Agency Head*** is responsible for the review and approval of all agency risk assessments

SEC530-01.0 , RA-3

Requirements of a Risk Assessment



Components

1. Threats and Vulnerabilities
2. Likelihood and Magnitude
3. Organization Integration
4. Document
5. Disseminate

Description

1. Consider threats and vulnerabilities that could impact the system being assessed
2. Determine the likelihood that threats will materialize and the loss impact if one or more vulnerabilities are exploited by a potential threat
3. Risk assessment results should drive risk management decisions from the organization and mission and business process perspectives
4. Risk Assessment results should be documented into a risk assessment report to include major findings, and risk mitigation recommendations
5. Risk assessment results should be provided to the appropriate organization-defined personnel

RAs should be reviewed on an annual basis, and fully revised every three (3) years.

SEC530-01.0 , 6.1

Threats and Vulnerabilities

A threat is any potential danger or harm that could compromise the confidentiality, integrity, or availability of an organization's information systems, data or networks

- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
- PASTA (Process for Attack Simulation and Threat Analysis)
- MITRE ATT&CK

A vulnerability is a weakness or flaw in a system, application, or network that could be exploited by a malicious actor to gain unauthorized access, disrupt operations, or steal data

- OWASP Top Ten
- CIS Top Eighteen

Measuring Magnitude of Impact

Rating	Magnitude of Impact Definition
Critical	Direct high impact such as mission essential functions unavailable and/or complete breach of sensitive information
High	Direct minimal impact such as a temporary suspension of services or the loss of a subset of information
Moderate	Indirect high impact
Low	Indirect minimal impact

- System owner is likely the best equipped to determine the magnitude of impact
- Key areas to look for when determining magnitude of impact would include business process analysis and data set analysis.
- System containing sensitive data or mission essential functions will likely have critical to high magnitudes of impact

Measuring Probability of Occurrence

Rating	Probability of Occurrence
Critical	There are no other controls in place that mitigate the risk and existing threats capable of exploiting the gap
High	Few, if any, internal controls are in place to reduce the risk
Moderate	Internal controls reduce the threat; however, additional controls should be implemented to further mitigate the risk where feasible
Low	There are sufficient controls in place to substantially reduce the risk posed

Key areas to analyze when determining probability of occurrence would include SEC530 control compliance, vulnerability management and remediation, vendor performance and compliance, and overall information security maturity of the organization

SEC520-05

Calculating Total Risk

Probability of Occurrence	Magnitude of Impact			
	Low	Moderate	High	Critical
Critical	High	High	Critical	Critical
High	Moderate	High	High	Critical
Moderate	Low	Moderate	High	High
Low	Low	Low	Moderate	High

Risks identified in the risk assessment with a severity greater than a value of low create a risk finding

Documenting Risk Assessment Results

Risk Assessment Report

- Prepare a report of each risk assessment that includes:
- Executive summary
- The identification of all vulnerabilities discovered during the assessment
- Major findings, and risk mitigation recommendations.
- This report must be reviewed and approved by the ISO or ISO designee.

For each risk identified with total risk greater than low, a Risk Treatment Plan shall be submitted to the CISO (CSRM) within 30 days of the final risk assessment report.

Open Risk Findings require quarterly updates until remediation

SEC520-05

VIRGINIA IT AGENCY

Agency Data Points

Erica Bland, Manager IT Security Governance and Compliance

Sept 4, 2024

What are Agency Data Points

They are compliance metrics that revolve around agency's audit and risk programs. These metrics help to demonstrate how an agency is managing its IT security program.

- VITA is required to report annually to the Governor and General Assembly on the state of the Commonwealth's IT security per **§** ***2.2-2009 Additional duties of the CIO relating to security government information***.
- Agency data points are captured from January 1st to December 31st of each calendar year.
- Each metric is converted to a numeric score, added up, averaged, and then reported as a letter grade.
- Agencies can keep track of their score throughout the year using Archer. A report detailing your agency datapoints can found here Agency Data Points

Overall Audit Score

- The ***audit score*** is essentially the average of three data points:

  1) Audit plans. Each agency must submit an **audit plan** *annually*. The only requirement is that it lists all the agency's sensitive systems and includes a scheduled audit date within three years of the date of the last audit. The metric will be either pass or fail (numerically that means 100% or 0%). It can be re-submitted anytime your plan changes.

  2) Audits. Each sensitive system should be audited at least *once every three years*. The metric is a percentage of sensitive systems audited. If the agency is reporting 10 sensitive systems and eight were audited over the last three years period, it's a score of 80%.

  3) Quarterly updates. Remediation steps need to be reported for *all open audit findings on a quarterly basis*. If a finding is open all year long, we are expecting at least four updates for the finding. The metric is a % of quarterly updates received for each finding. If an agency cannot remediate a finding in 90 days, please submit an exception request.

- The final audit metric is **[(Audit plan) + (% of audits completed) + (% of quarterly updates)] / 3**

Overall Risk Score

The **risk score** consists of eight different metrics:

1. **Risk assessment plan** (must be submitted annually/ Pass or Fail)
2. **Risks assessments performed** (% of RAs submitted over the last three years)
3. **Quarterly updates of risk assessment findings** (works the same way as audit findings, reported as a %)
4. **BIA** (All reported business processes must be updated annually. Archer calculates a %)
5. **Applications certified** (all applications must be "certified", i.e., associated with at least one business process, one dataset and at least one device (or product/service).
6. **IDS reporting** each quarter (for enterprise managed agencies, this is always a pass. For independent agencies, we expect quarterly updates to be sent to Commonwealth Security)
7. **ISO certification** (agency primary ISO must meet the certification requirement, this is reported as (Pass/Fail)
8. **ISO must report to the agency head** (required by OSIG audit of security in the Commonwealth in 2019)

The final risk metric is **[(risk assessment plan) + (% of risk assessments completed) + (% of quarterly updates) + (% business processes updated) + (% of applications certified) + (% of IDS reports submitted) + (ISO certification) + (ISO reports to agency head)] / 8**

Agency Data Points Reminder

Beginning January 1, 2024, we only accept agency deliverables using the templates found on our website or by providing updates directly into Archer.

- However, Agency Head approved audit and risk plans should be sent to the CSRM mailbox, commonwealthsecurity@vita.virginia.gov
- We encourage agencies to not wait until the fourth quarter to submit deliverables for the calendar year.
- Routinely check Archer to ensure your audit and risk scores are accurate.
- If you have any questions, please contact your CSRM analyst and/or the Commonwealth Security mailbox.

Announcements

ISOAG September 4, 2024

Renea Dickerson is Retiring this Month

We want to take a moment to thank Renea for all she has done and wish her all the best in retirement!

VIRGINIA
IT AGENCY

- SPLUNK UPDATE August 2024

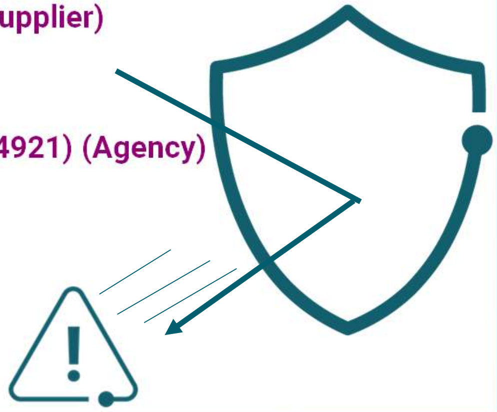
WE WANT YOUR LOGS:

VITA is starting to work with agencies to ingest their application logs in to the VITA Splunk instance. We ask that all agencies start identifying what logs you would like to have ingested. We are always happy to schedule a call to review your options.

5 Key Vulnerabilities

For the Month of September, the Top 5 Key Vulnerabilities are:

- KB5039294: Windows Server 2012 R2 Security Update (June 2024) (Plugin ID: 200338) (Supplier)
- KB5039217: Windows 10 version 1809 / Windows Server 2019 Security Update (June 2024) (Plugin ID: 200349) (Supplier)
- KB5039227: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (June 2024) (200336) (Supplier)
- Splunk Universal Forwarder 9.0.0 < 9.0.9, 9.1.0 < 9.1.4, 9.2.0 < 9.2.1 (SVD-2024-0304) (Plugin ID: 194921) (Agency)
- Apache 2.4.x < 2.4.60 Multiple Vulnerabilities (Plugin ID: 201198) (Agency)



Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

Splunk Lunch & Learn – Investigating with Splunk

Join us at the Boulders on September 5th.

Training is onsite only and space is limited. First come first served.

Register at https://forms.office.com/g/WmNiWQc1Dt

Investigating with Splunk is a modular, hands-on workshop designed to familiarize participants with how to investigate incidents using Splunk and open source. This workshop provides users a way to gain experience searching in Splunk to answer specific questions related to an investigation. These questions are similar to what would be asked in their own organizations. The workshop leverages the popular Boss of the SOC (BOTS) dataset in a question and answer format. Users will leave with a better understanding of how Splunk can be used to investigate in their enterprise.

COVITS

Save the Date!

September 11 / Richmond, VA
2024
COVITS
government technology

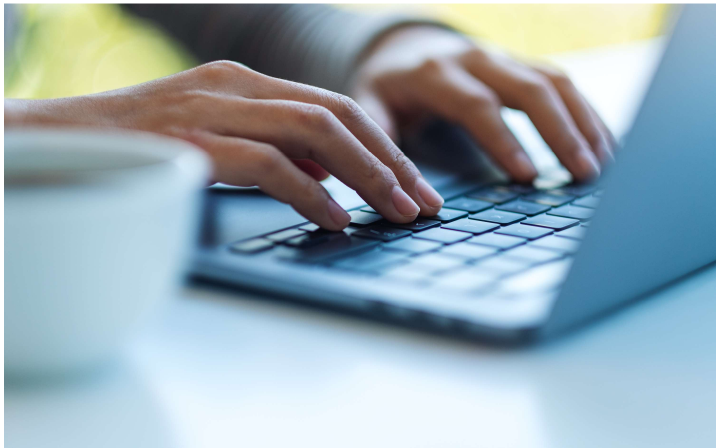
Registration link.

IS Orientation

The next IS Orientation is being held on September 25th

- It will be held virtually via WebEx from 1pm-3pm
- Please register at the link below:

https://covaconf.webex.com/weblink/register/ra80c2228f9b560704b5193640d78b1a5



October 2nd ISOAG

The Mandatory October 2, 2024, ISOAG meeting will be an In-person/Hybrid Event

Location will be the Reynolds Community College

In the Workforce Development and Conference Center

This is an opportunity to catch up with your fellow Information Security Officers in person, enjoy informative presentations, and mingle. Seating is limited to 150, so reserve your place at the in-person event. If you are unable to attend in person, and need someone to attend in your place, please notify Commonwealth Security, as attendance is mandatory for ISO’s.

Link to register **in person**:
https://covaconf.webex.com/weblink/register/r0809a97ccffc9550fed4f1325179cb89

Link to register **remote**:
https://covaconf.webex.com/weblink/register/r527efc3bfe8a72d8eb29a04d0b988714

Reynolds
COMMUNITY COLLEGE

1651 East Parham Road
Richmond, Virginia 23228

October is Cybersecurity Awareness Month

October is Cybersecurity Awareness Month

- Theme: Secure Our World

- Four Simple Ways to Stay Safe Online:
  - 1. Use Strong Passwords and a Password Manager
  - 2. Turn on multifactor authentication
  - 3. Recognize and report phishing
  - 4. Update software

Cybersecurity Awareness Month Resources

- https://staysafeonline.org/
- Cybersecurity Awareness Month Kit 2024 (knowbe4.com)
- https://www.govtech.com/blogs/lohrmann-on-cybersecurity/secure-our-world-cybersecurity-awareness-month-2024

Service Tower SOC Report Review Sessions

The upcoming SOC review session is October 10, 2024, and will be held remotely via WebEx. Please register at the link below

To register for this meeting, please click on the link below:
https://covaconf.webex.com/weblink/register/r9c8cb1394982eb22a7fa276a7f04fb91

MEETING ADJOURNED

VIRGINIA IT AGENCY