North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Supplier Sharing Call

October 26, 2022

Please Participate

- Raise your hand
  - We will unmute you
  - Make sure you are identified in the participant list
- Put a question or comment in the chat
- Put a question or comment in the Q&A

If you put a question or comment in the chat or Q&A but want to remain anonymous, please open with your request

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Opening Remarks

Tom Galloway, NATF President and CEO

Purpose of the sharing calls

Chris Fitzhugh, Siemens Energy

- Provide an opportunity for suppliers to talk about cyber security issues and practices ranging from
  - How to set up a program, to
  - In-depth discussions on a specific technical challenge
- Leverage knowledge from lessons learned
- Share information
- Calls will be limited to suppliers

Contributing Organizations

Chris Fitzhugh, Siemens Energy

- Hitachi Energy
- International Society of Automation (ISA)
- National Electrical Manufacturers Association (NEMA)
- Schneider Electric
- Schweitzer Engineering Labs (SEL)
- Siemens Energy
- US Chamber of Commerce
- With support from:
  - Nebraska Public Power District
  - Southern Company
  - North American Transmission Forum (NATF)

Today's Agenda and Presenters

Chris Fitzhugh, Siemens Energy

- Comments - Jennifer Couch (Southern Co)
- Future calls – Steve Griffith (NEMA)
- Where we're at and what you can do today – Frank Harrill (SEL)
- Future Topics – Frank Harrill (SEL)

Participants Available for Discussion/Questions

- Andre Ristaino (ISA)
- Steve Griffith (NEMA)
- Mike Pyle (Schneider Electric)
- Andy Turke (Siemens)
- Chris Fitzhugh (Siemens Energy)
- Frank Harrill (SEL)
- Heath Knakmuhs (US Chamber of Commerce)
- Jon Terrell (Hitachi Energy)

Please remember to either raise your hand to ask a question or you can put your question into the chat or Q&A.

Comments from a Customer

Jennifer Couch, Southern Company

- View from the customer
- Value of the partnership
- We are in this together
- We're all suppliers to someone

Future Calls

Steve Griffith, NEMA

- Currently Planned for approximately every 2 months from 1-2:30pm ET
  - Oct 26, 2022
  - Dec 7, 2022
  - Jan 25, 2023
  - March 22, 2023
  - May 24, 2023
  - July 19, 2023
  - Sept 27, 2023
  - Nov 29, 2023
- Could keep a main topic for the call to 1 hour with a special group break-out (e.g., small suppliers) for the last half hour
  - There will be a poll at the end of the call
- Calls are not recorded
- Slides will be available

slido

Join at slido.com
#2702596

ⓘ Start presenting to display the joining instructions on this slide.

slido

What is your end-use market?

ⓘ Start presenting to display the poll results on this slide.

slido

What is the annual revenue of your company?

ⓘ Start presenting to display the poll results on this slide.

slido

How many employees does your company have?

ⓘ Start presenting to display the poll results on this slide.

slido

In what country(ies) does your company sell products or provide services?

ⓘ Start presenting to display the poll results on this slide.

Managing Cybersecurity Risk

Frank Harrill, SEL

OCTOBER 2022

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-277A

October 4, 2022

Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization

SUMMARY

From November 2021 through January 2022, the Cybersecurity and Infrastructure Security Agency (CISA) responded to advanced persistent threat (APT) activity on a Defense Industrial Base (DIB) Sector organization's enterprise network. During incident response activities, CISA uncovered that likely multiple APT groups compromised the organization's network, and some APT actors had long-term access to the environment. APT actors used an open-source toolkit called Impacket to gain their foothold within the environment and further compromise the network, and also used a custom data exfiltration tool, CovalentStealer, to steal the victim's sensitive data.

Actions to Help Protect Against APT Cyber Activity.

- Enforce multifactor authentication (MFA) on all user accounts.
- Implement network segmentation to separate network segments based on role and functionality.
- Update software, including operating systems, applications, and firmware, on network assets.
- Audit account usage.

This joint Cybersecurity Advisory (CSA) provides APT actors tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified during the incident response activities by CISA and a third-party incident response organization. The CSA includes detection and mitigation actions to help organizations detect and prevent related APT activity. CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) recommend DIB sector and other critical infrastructure organizations implement the mitigations in this CSA to ensure they are managing and reducing the impact of cyber threats to their networks.

All organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to FBI via your local FBI field office or FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.

TLP:WHITE

Open Distribution for Supply Chain Materials

APRIL 2022

JOINT CYBERSECURITY ADVISORY

UNCLASSIFIED / NON CLASSIFIÉ

Co-Authored by:

TLP:WHITE

Product ID: AA22-110A

April 20, 2022

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure

SUMMARY

The cybersecurity authorities of the United States[1][2][3], Australia[4], Canada[5], New Zealand[6], and the United Kingdom[7][8] are releasing this joint Cybersecurity Advisory (CSA). The intent of this joint CSA is to warn organizations that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity. This activity may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and U.S. allies and partners.

Evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the

Actions critical infrastructure organizations should implement to immediately protect against Russian state-sponsored and criminal cyber threats:

- Patch all systems. Prioritize patching known exploited vulnerabilities.
- Enforce multifactor authentication.
- Secure and monitor remote desktop protocol and other risky services.
- Provide end-user awareness and training.

U.S. organizations: to report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov. Australian organizations: visit cyber.gov.au/acsc/report or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories. Canadian organizations: report incidents by emailing CCCS at contact@cyber.gc.ca. New Zealand organizations: report cyber security incidents to ncscincidents@ncsc.govt.nz or call 04 498 7654. United Kingdom organizations: report a significant cyber security incident: ncsc.gov.uk/report-an-incident (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

TLP: WHITE

MAY 2022

JOINT CYBERSECURITY ADVISORY

TLP:WHITE

Product ID: AA22-131A

May 11, 2022

Co-authored by:

Protecting Against Cyber Threats to Managed Service Providers and their Customers

SUMMARY

The cybersecurity authorities of the United Kingdom (NCSC-UK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ), and the United States (CISA), (NSA), (FBI) are aware of recent reports that observe an increase in malicious cyber activity targeting managed service providers (MSPs) and expect this trend to continue.[1] This joint Cybersecurity Advisory (CSA) provides actions MSPs and their customers can take to reduce their risk of falling victim to a cyber intrusion.

This advisory describes cybersecurity best practices for information and communications technology (ICT) services and functions, focusing on guidance that enables transparent discussions between MSPs and their customers on securing sensitive data. Organizations should implement these guidelines as appropriate to their unique environments, in accordance with their specific security needs, and in compliance with applicable regulations. MSP customers should verify that the contractual arrangements with their provider include cybersecurity measures in line with their particular security requirements.

The guidance provided in this advisory is specifically tailored for both MSPs and their customers and is the result of a collaborative effort from the United Kingdom National Cyber Security Centre (NCSC-UK), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), the United States' Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) with contributions from industry members of the Joint Cyber Defense Collaborative

Tactical actions for MSPs and their customers to take today:

- Identify and disable accounts that are no longer in use.
- Enforce MFA on MSP accounts that access the customer environment and monitor for unexplained failed authentication.
- Ensure MSP-customer contracts transparently identify ownership of ICT security roles and responsibilities.

TLP:WHITE

MARCH 2022

National Security Agency
Cybersecurity Technical Report

Network Infrastructure Security Guidance

March 2022

PP-22-0266
Version 1.0

APRIL 2022

JOINT
CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22–103A

April 13, 2022

APT Cyber Tools Targeting ICS/SCADA Devices

SUMMARY

The Department of Energy (DOE), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) are releasing this joint Cybersecurity Advisory (CSA) to warn that certain advanced persistent threat (APT) actors have exhibited the capability to gain full system access to multiple industrial control system (ICS)/supervisory control and data acquisition (SCADA) devices, including:

- Schneider Electric programmable logic controllers (PLCs),
- OMRON Sysmac NEX PLCs, and
- Open Platform Communications Unified Architecture (OPC UA) servers.

The APT actors have developed custom-made tools for targeting ICS/SCADA devices. The tools enable them to scan for, compromise, and control affected devices once they have established initial access to the operational technology (OT) network. Additionally, the actors can compromise Windows-based engineering workstations, which may be present in information technology (IT) or OT environments, using an exploit that compromises an ASRock motherboard driver with known vulnerabilities. By compromising

Actions to Take Today to Protect ICS/SCADA Devices:

- Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible.
- Change all passwords to ICS/SCADA devices and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks and to give defender monitoring systems opportunities to detect common attacks.
- Leverage a properly installed continuous OT monitoring solution to log and alert on malicious indicators and behaviors.

JANUARY 2022

Canada

Canadian Centre for Cyber Security

Home → Publications

→ Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awar…

Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity

The Canadian Centre for Cyber Security encourages the Canadian cybersecurity community—especially critical infrastructure network defenders—to bolster their awareness of and protection against Russian state-sponsored cyber threats. The Cyber Centre joins our partners in the US and the UK in recommending proactive network monitoring and mitigations.

FEBRUARY 2022

JOINT CYBERSECURITY ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-047A

February 16, 2022

Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

SUMMARY

From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources. These CDCs support contracts for the U.S. Department of Defense (DoD) and Intelligence Community in the following areas:

- Command, control, communications, and combat systems;
- Intelligence, surveillance, reconnaissance, and targeting;
- Weapons and missile development;
- Vehicle and aircraft design; and
- Software development, data analytics, computers, and logistics.

Historically, Russian state-sponsored cyber actors have used common but effective tactics to gain access to target networks, including spearphishing, credential harvesting, brute force/password spray techniques, and known vulnerability exploitation against accounts and networks with weak security. These actors take advantage of simple passwords, unpatched systems, and unsuspecting employees to gain initial access before moving laterally through the network to establish persistence and exfiltrate data.

Actions to Help Protect Against Russian State-Sponsored Malicious Cyber Activity:

- Enforce multifactor authentication.
- Enforce strong, unique passwords.
- Enable M365 Unified Audit Logs.
- Implement endpoint detection and response tools.

JANUARY 2022

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: A22-011A

January 11, 2022

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

SUMMARY

This joint Cybersecurity Advisory (CSA)—authored by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)—is part of our continuing cybersecurity mission to warn organizations of cyber threats and help the cybersecurity community reduce the risk presented by these threats. This CSA provides an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.

CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations listed below and detailed in the Mitigations section. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation.

Actions critical infrastructure organizations should implement to immediately strengthen their cyber posture.

- Patch all systems. Prioritize patching known exploited vulnerabilities.
- Implement multi-factor authentication.
- Use antivirus software.
- Develop internal contact lists and surge support.

JULY 2021

National Security Agency | Cybersecurity & Infrastructure Security Agency | Federal Bureau of Investigation | Cybersecurity Advisory

Chinese State-Sponsored Cyber Operations: Observed TTPs

Summary

The National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China state-sponsored malicious cyber activity is a major threat to U.S. and Allied cyberspace assets. Chinese state-sponsored cyber actors aggressively target U.S. and allied political, economic, military, educational, and critical infrastructure (CI) personnel and organizations to steal sensitive data, critical and emerging key technologies, intellectual property, and personally identifiable information (PII). Some target sectors include managed service providers, semiconductor companies, the Defense Industrial Base (DIB), universities, and medical institutions. These cyber operations support China's long-term economic and military development objectives.

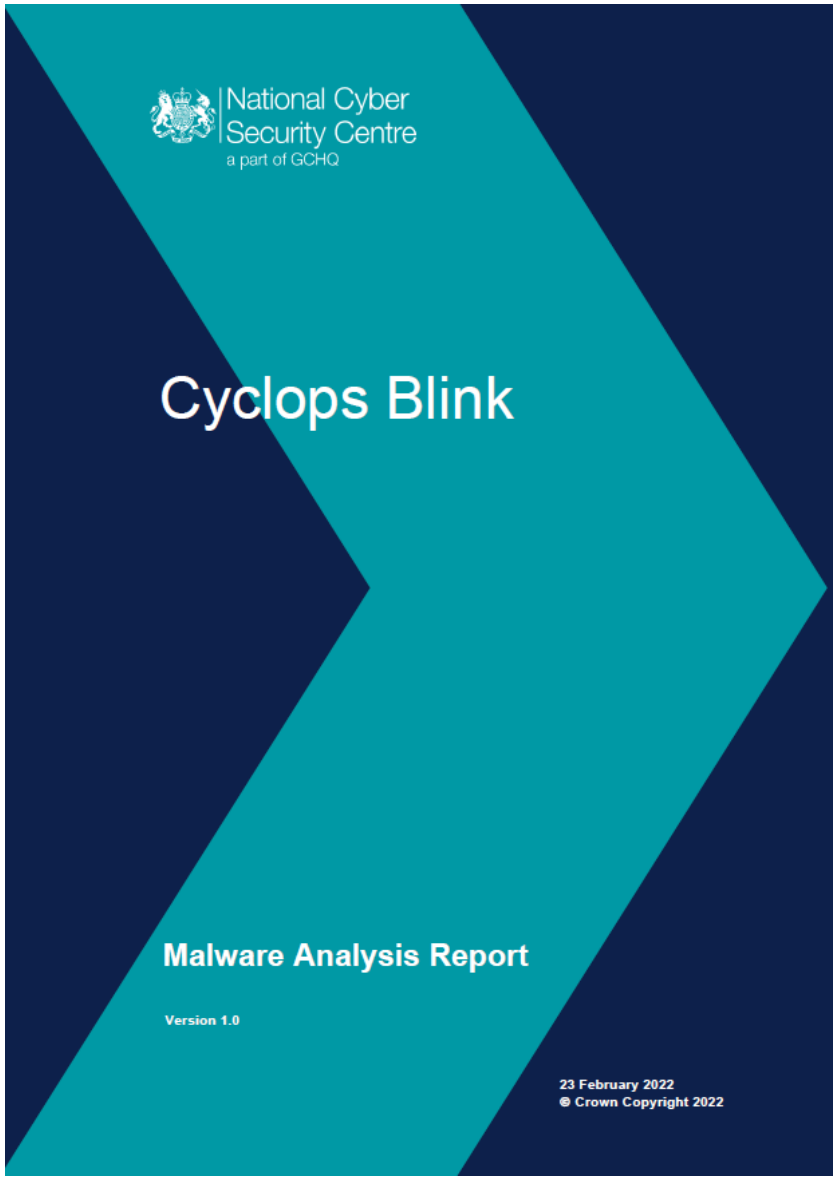
This Joint Cybersecurity Advisory (CSA) provides information on tactics, techniques, and procedures (TTPs) used by Chinese state-sponsored cyber actors. This advisory builds on previous NSA, CISA, and FBI reporting to inform federal, state, local, tribal, and territorial (SLTT) government, CI, DIB, and private industry organizations about notable trends and persistent TTPs through collaborative, proactive, and retrospective analysis.

This advisory uses the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework, version 9, and MITRE D3FEND™ framework, version 0.9.2-BETA-3.

See the ATT&CK for Enterprise framework for all referenced threat actor tactics and techniques and the D3FEND framework for referenced defensive tactics and techniques.

FEBRUARY 2022

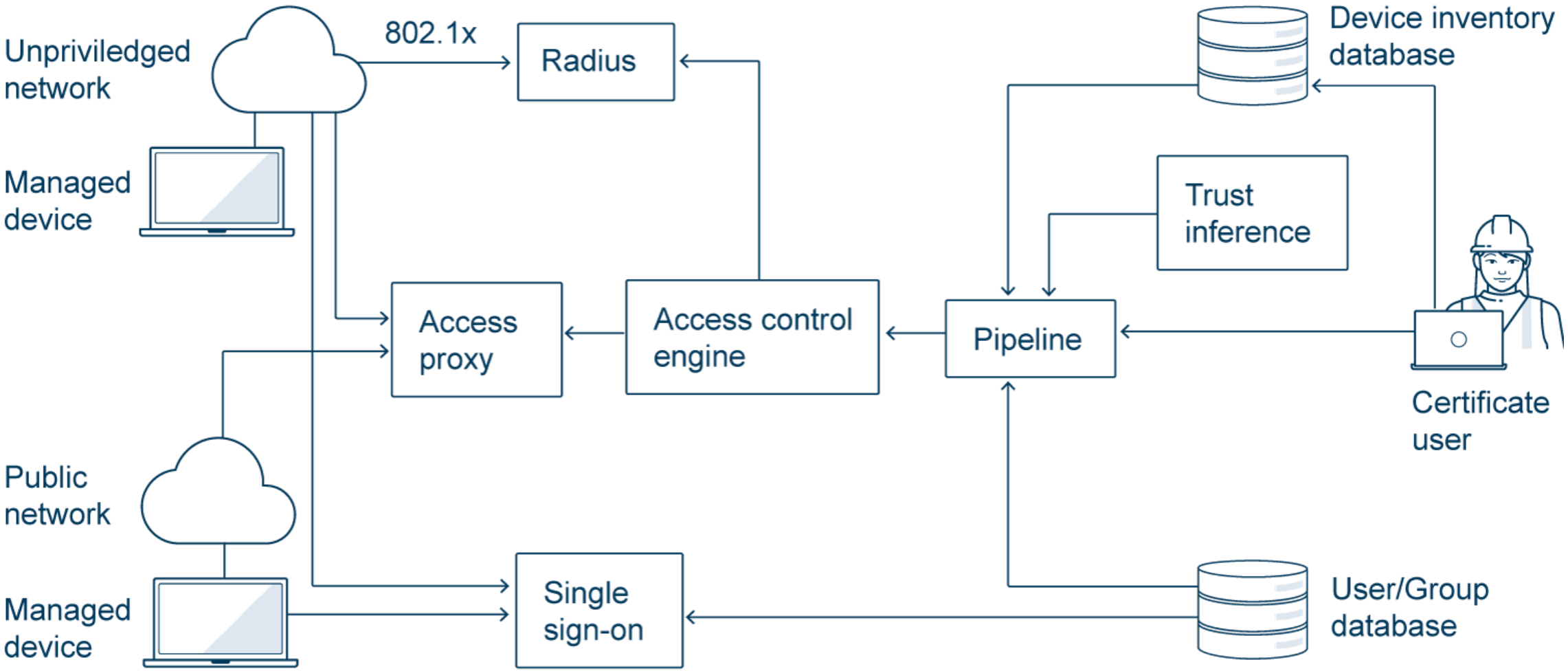
FEBRUARY 2022



We are all prime targets.

The trust we place in
each other is a weapon
that will be turned against us
if fundamental safeguards
are not present

Defender context



Attacker Context

Mid-level finance team member

IT employee likely to have privileged access

HR manager with access to employee records

Time devoted to probe entire internet continues to shrink

2013

MINUTES

TODAY

MINUTES

Vital safeguards

- Multifactor authentication
- Patch constantly
- Monitored EDR/XDR platform
- Employee training
- Begin supplier vetting
- Certification preparation

Industry Resources

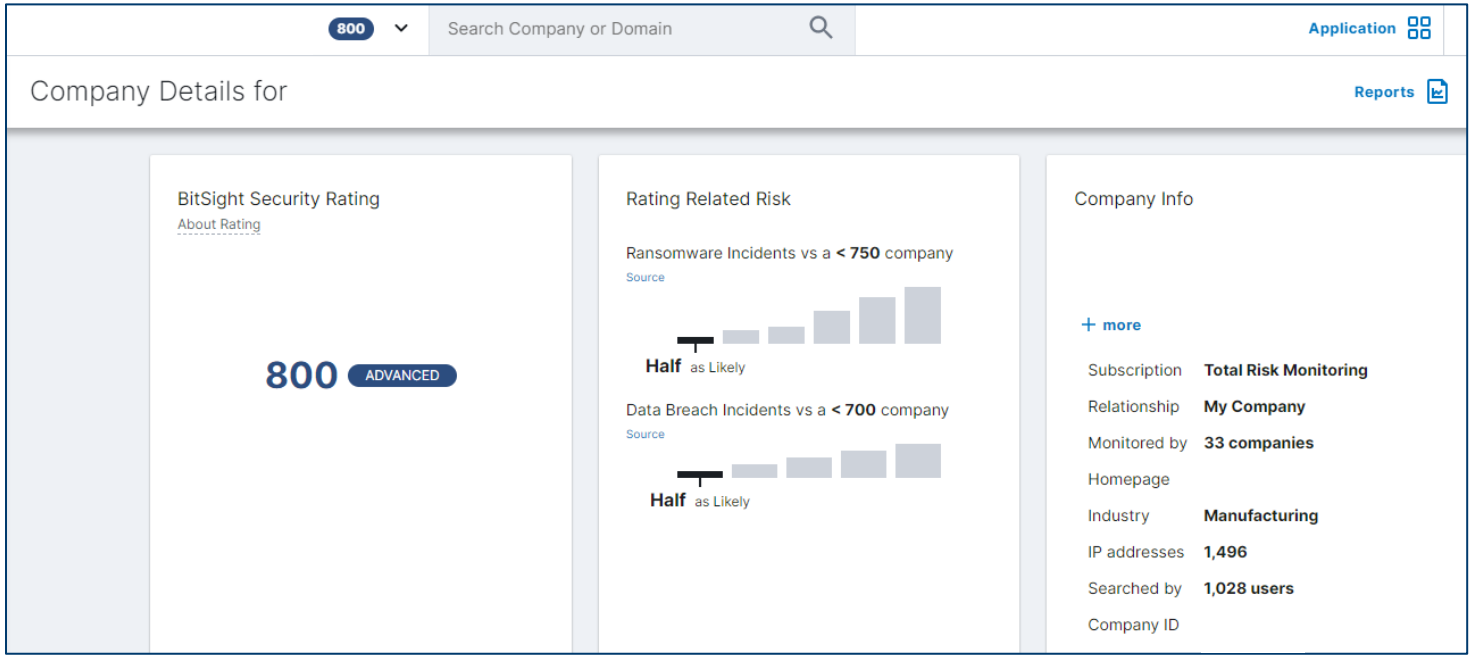
Security and Supply Chain

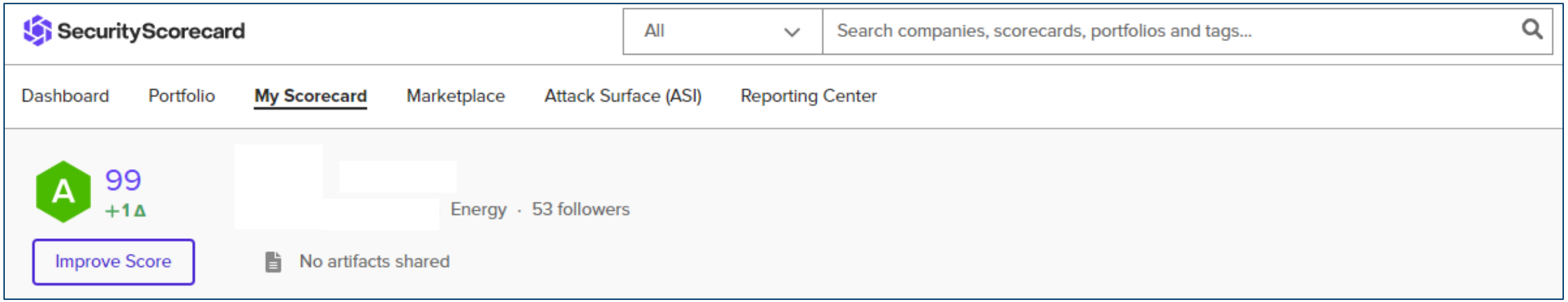
Cyber Security – Vendor Support via Web Conferencing - Implementation Guidance for CIP-005-6 Parts 2.4 and 2.5
Energy Sector Supply Chain Risk Questionnaire - Formatted V3.0
Energy Sector Supply Chain Risk Questionnaire - Unformatted V3.0
NATF CIP-013 Supply Chain Risk Management Plans (ERO Endorsed)
NATF CIP-013 Using Independent Assessments of Vendors (ERO Endorsed)
NATF Cyber Security Supply Chain Risk Management Guidance
NATF Implementation Guidance for CIP-010-3 Software Integrity
NATF Industry Collaboration - Using Solution Providers for Third-Party Risk Management
NATF Practices Document for CIP-014-2 R4
NATF Practices Document for CIP-014-2 R5
NATF Supply Chain Security Criteria V3.0
Revision Process for the Energy Sector Supply Chain Risk Questionnaire and NATF Supply Chain Security Criteria
Supply Chain Security Assessment Model

Questionnaire and ERO Endorsements

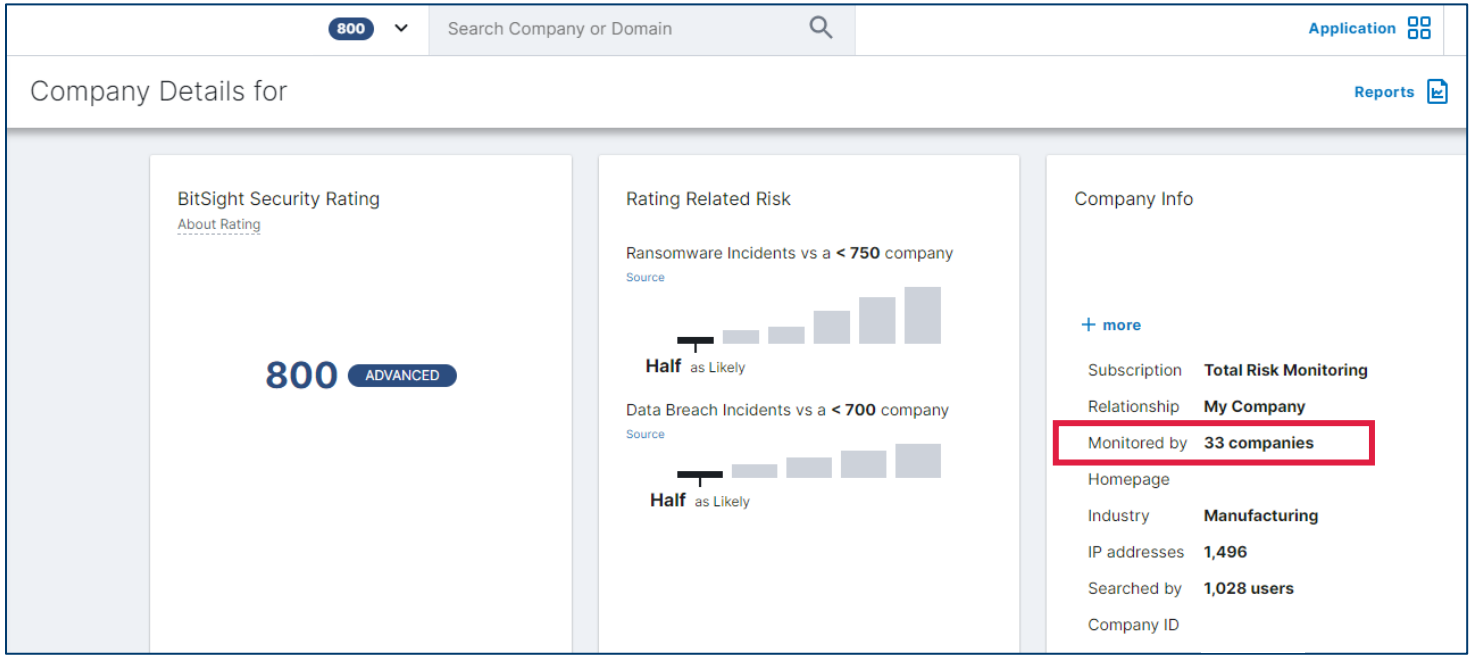
North American Transmission FORUM

Customers count on each of us

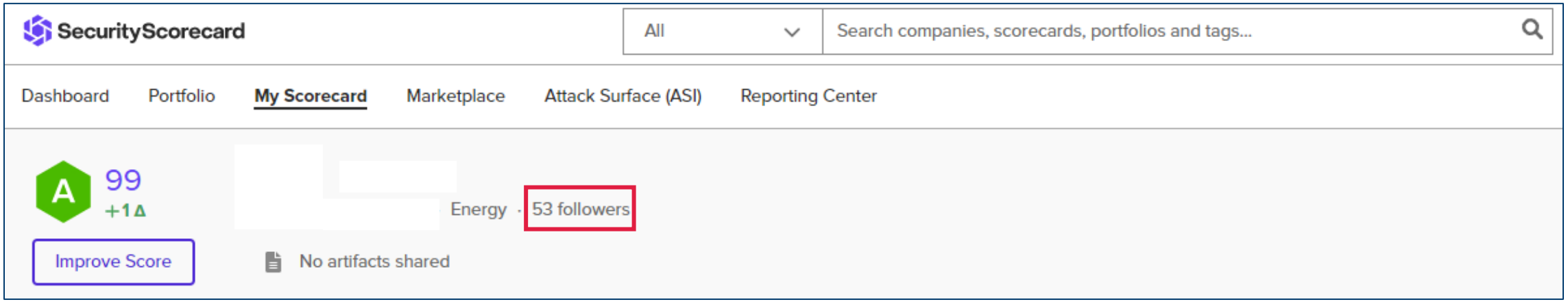




Customers count on each of us…



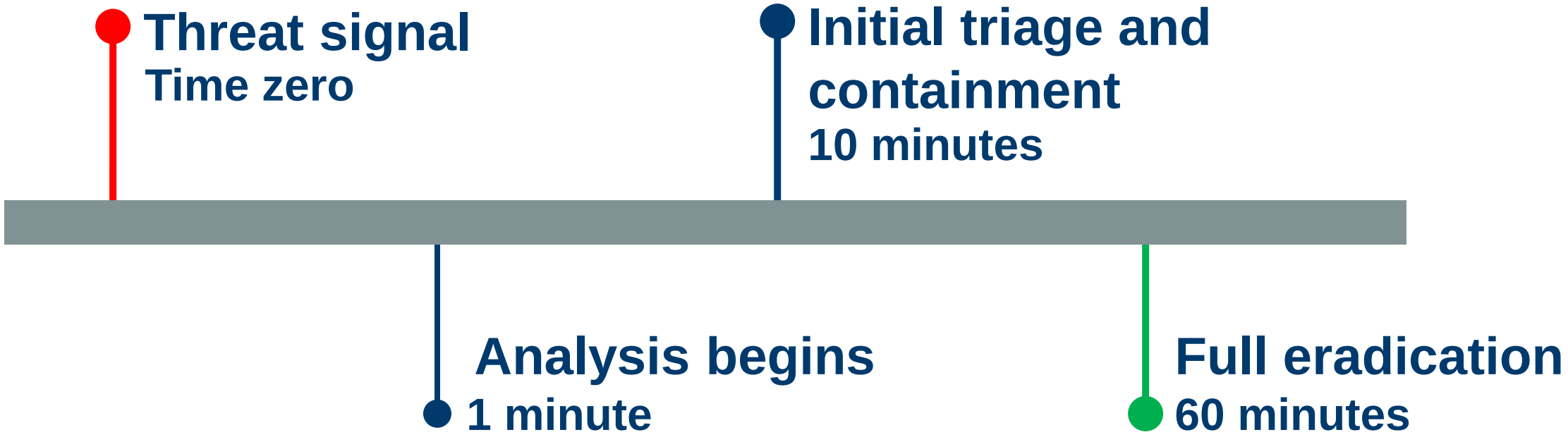
and WATCH



Free external assessment tools

- securityscorecard.com/free-account
- security.microsoft.com/securescore
- observatory.mozilla.org
- webscan.upguard.com
- iss-cyber.com/signup
- search.censys.io

Constant vigilance is required

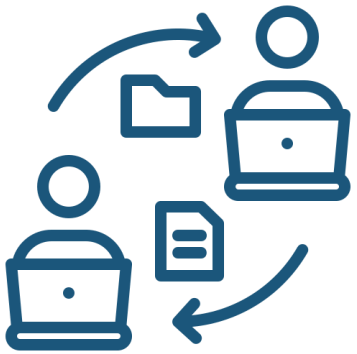


Training and government resources

- www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance
- www.cisa.gov/free-cybersecurity-services-and-tools
- www.cisa.gov/known-exploited-vulnerabilities
- https://learnsecurity.amazon.com/en/index.html
- https://www.cisa.gov/shields-up

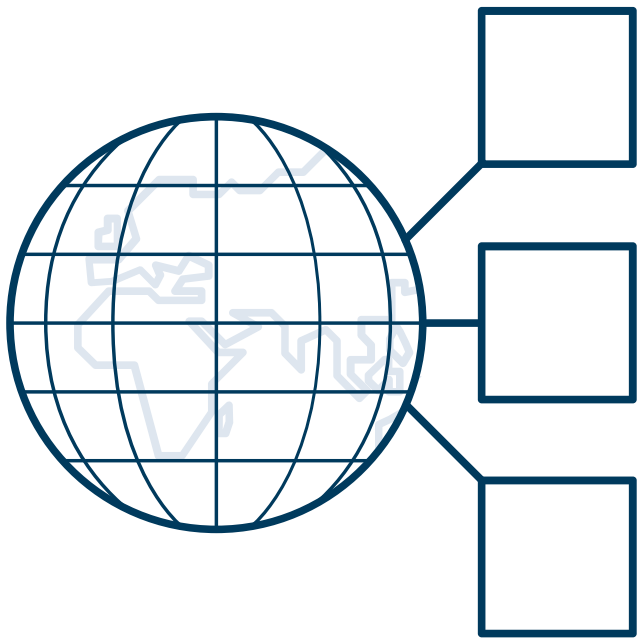
Information Sharing Opportunities

- E-ISAC and other Information Sharing and Analysis Centers
- Homeland Security Information Network (HSIN)
- National Cyber Awareness System (NCAS)
- CISA Automated Indicator Sharing (AIS)
- FBI Infragard



Managing provenance across mutual supply chains is increasingly vital

- “Executive Order No. 14028, Improving the Nation’s Cybersecurity”
- “Executive Order No. 14017, America’s Supply Chains”
- Department of Energy directives



slido

What certifications or assessments offered by qualified third parties does your company have?

ⓘ Start presenting to display the poll results on this slide.

slido

If you responded "other" to the prior question, please identify the certification or assessment.

ⓘ Start presenting to display the poll results on this slide.

Move beyond compliance

Develop a risk-based security management system using a recognized standard.

- CIS Critical Security Controls
- NIST Cybersecurity Framework
- ISO 27001
- IEC 62443

Auditable, Certifiable, and Recognized Globally

Questions?

Future Calls

Frank Harrill, SEL

- What would you like to talk about during the next call or a future call? Deeper dive
- Would you like to have a separate break out for small suppliers? Or a different subgroups?
- Several ways to respond to these questions:
  - Respond to the Slido poll
  - Join the conversation (raise your hand or put a comment in the chat or Q&A)
  - Send an email to one of the NATF staff members or to your NEMA or US Chamber of Commerce representatives

slido

What topics would you like to have discussed in depth on future calls?

ⓘ Start presenting to display the poll results on this slide.

slido

If you responded "other" to the previous question, please provide your topic(s) of interest

ⓘ Start presenting to display the poll results on this slide.

slido

Would you like to have specific sessions for the following types of suppliers?

ⓘ Start presenting to display the poll results on this slide.

Questions

North American Transmission FORUM

Community *Confidentiality* *Candor* *Commitment*

Thank you for attending!

NATF Contact Information

supplychain@natf.net

dearley@natf.net

rstewart@natf.net

vagnew@natf.net

Links and comments provided during the call

OMB memo M-22-18 for what is included:, link available in this article: https://energycentral.com/c/pip/advice-software-vendors-prepare-omb-m-22-18-requirements

From M-22-18: The term "software" for purposes of this memorandum includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software

The Internet Engineering Task Force (IETF) is working on supply chain standards to address specific supply chain use cases:, that may be of interest: https://www.ietf.org/archive/id/draft-birkholz-scitt-software-use-cases-00.txt

https://www.isa.org/intech-home/2021/december-2021/departments/two-standards-one-integrated-industrial-cybersecur

CISA is leading 4 different SBOM workstreams: https://www.cisa.gov/sbom