HOW TO REDUCE CYBER RISK

Part II: Information and Operational Technology Networks

SEVEN STATES® POWER CORPORATION

SEVEN STATES POWER

Vision and Mission

- Energy solutions **cooperative**
- 100% owned and operated by **153** power utilities across seven states in the Tennessee Valley
- **Vision:** Leverage innovative technology to design, develop and deploy solutions for our member utilities
- **Mission:** Empower member utilities to meet consumer demand for renewable energy in an evolving marketplace

DESIGN, DEVELOP, DEPLOY

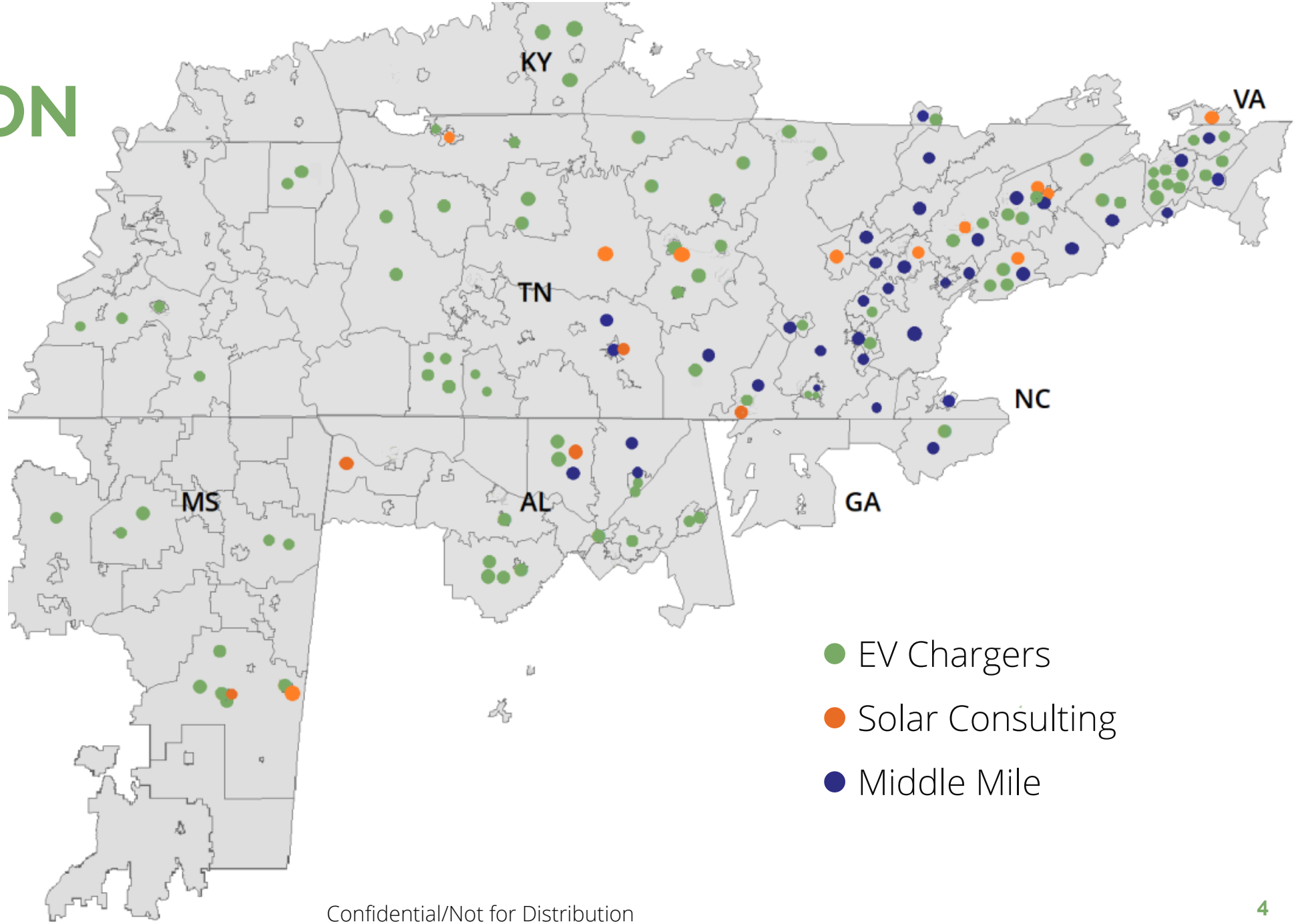
Focus Areas

Design Innovative Solutions through Collaborative Research

Develop Best Pricing through Strategic Partnerships

Deploy Technology with Sustainable Revenue Streams

VALLEY INNOVATION MAP



CYBER SECURITY AWARENESS WEBINAR

Agenda

CHUCK SPEAKS

Sr. Program Advisor

Intuitive Research and Technologies

RON MCLEROY

Technical Services Director

Huntsville Utilities

ANDREA BRACKETT

VP and CISO

TVA

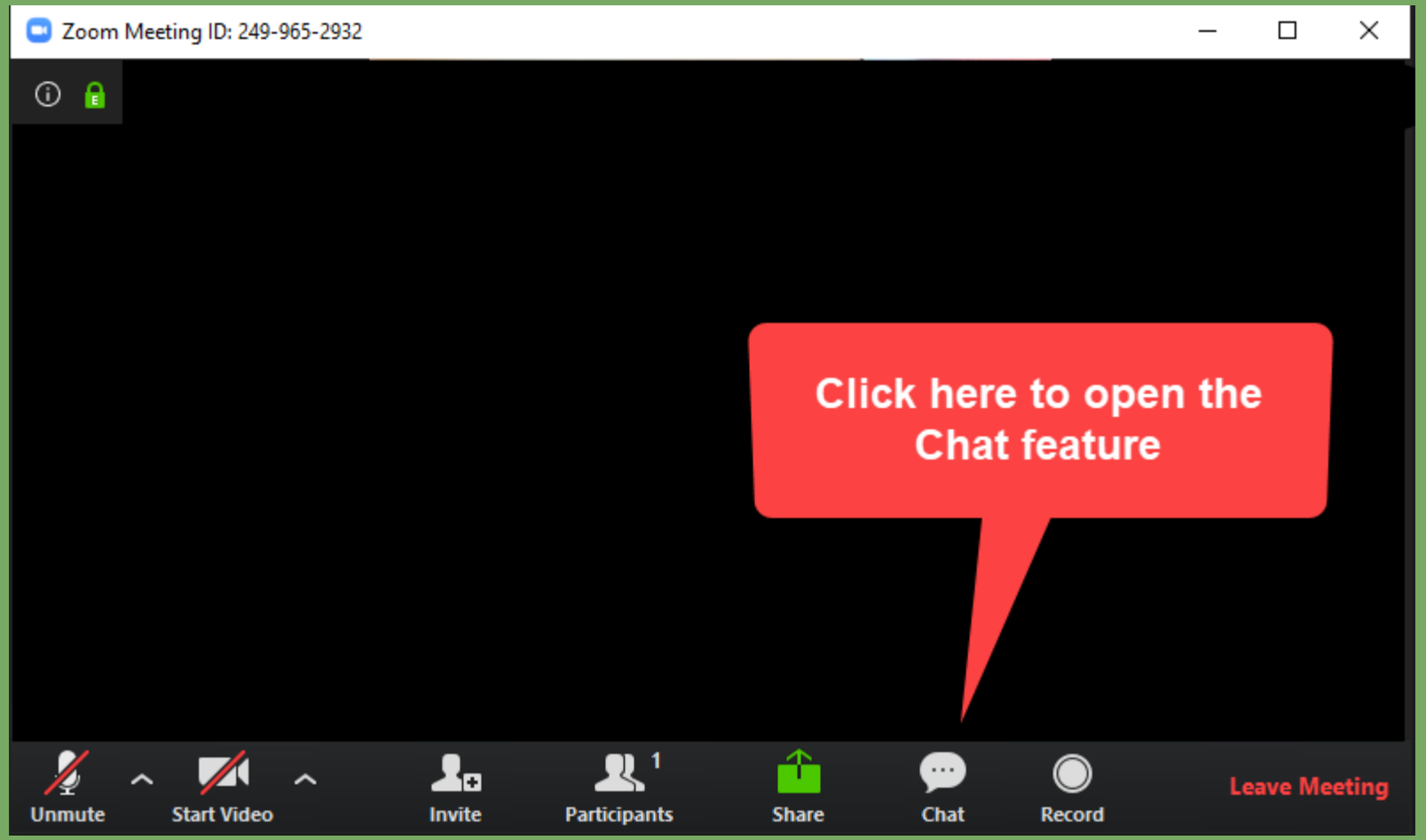
RYAN NEWLON

Principal

NRECA Cyber Security

SEVEN STATES POWER CORPORATION

Q&A in chat please



Reduce Cyber Risk
Operationalizing Threat Intelligence

Threat Intelligence – Finding Signal in the Noise

INTUITIVE®

E-ISAC
A DIVISION OF NERC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

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

INFRAGARD
PARTNERSHIP FOR PROTECTION

INTERNET STORM CENTER

OSINT

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA
CYBER+INFRASTRUCTURE

VirusTotal

NDCA

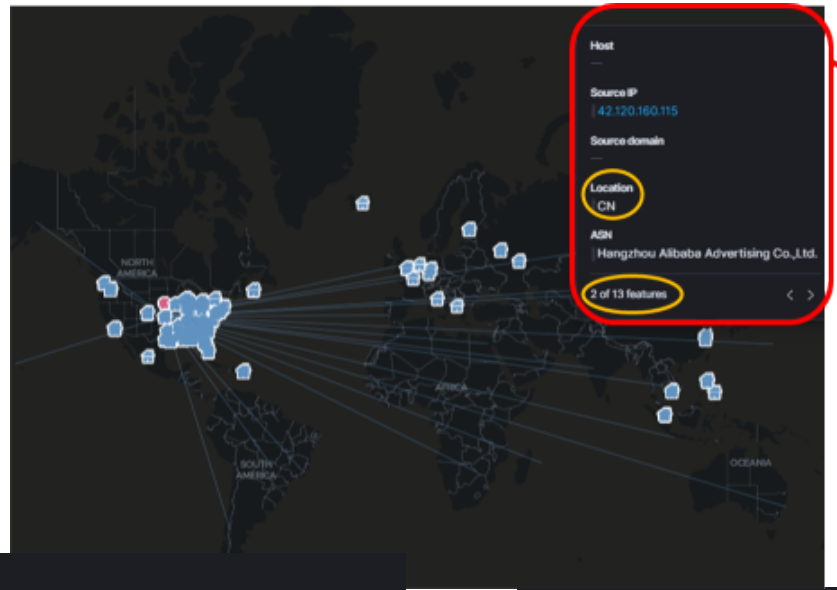
DECIDE
MANAGED CYBERSECURITY

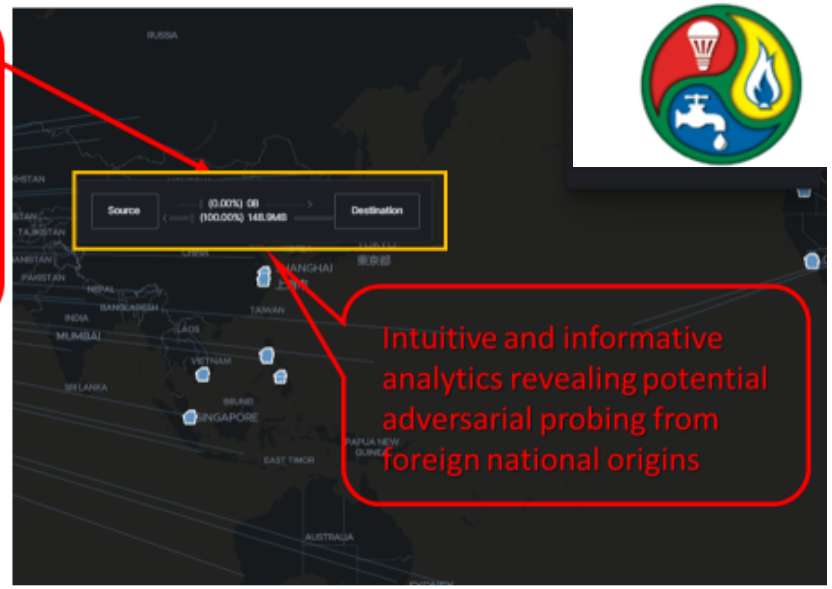
Operationalizing Threat Intelligence –Use Case

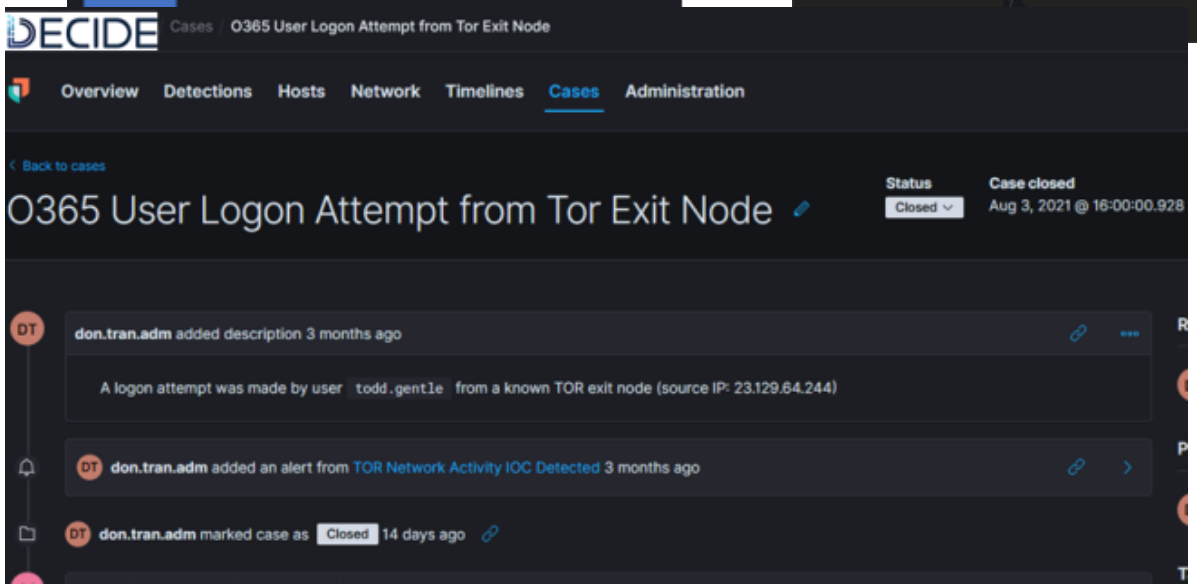
INTUITIVE®

HUNTSVILLE UTILITIES
ELECTRICITY • NATURAL GAS • WATER

[redacted]	Los Angeles	United States
[redacted]	Los Angeles	United States
[redacted]	Los Angeles	United States
[redacted]	Los Angeles	United States
[redacted]	Los Angeles	United States
[redacted]	Los Angeles	United States
[redacted]	-	United States
[redacted]	Birmingham	United States







Email payloads to lookout for

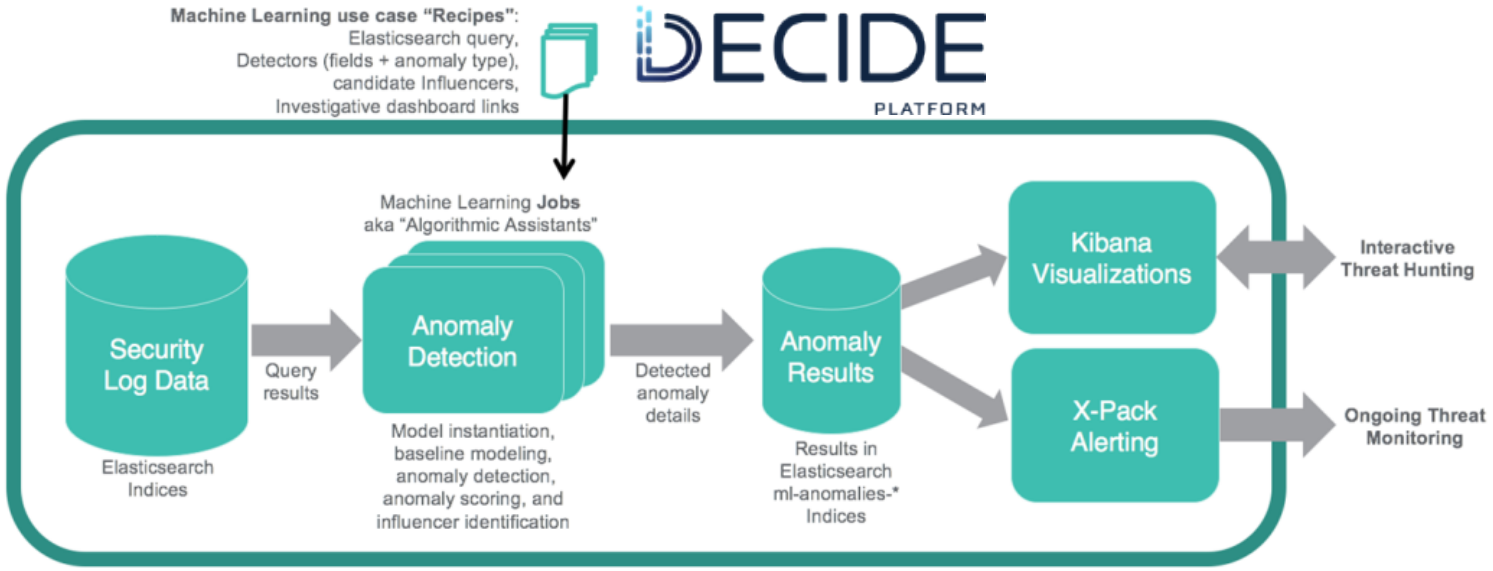
Time	o365.audit.Item.Attachments	o365.audit.Item.Subject
Apr 19, 2021 @ 08 : 58 : 20.000	IMG_0219.jpg (1542367b)	Test
Apr 17, 2021 @ 12 : 46 : 17.000	image001.png (346b)	PAYMENT CONFIRMATION STATUS 002021
Apr 17, 2021 @ 12 : 46 : 10.000	image001.png (346b)	PAYMENT CONFIRMATION STATUS 002021
Apr 16, 2021 @ 12 : 38 : 26.000	(44591b)	Undeliverable: Sign in & confirm:
Apr 16, 2021 @ 12 : 38 : 19.000	(44569b)	Undeliverable: Sign in & confirm: AQE30
Apr 16, 2021 @ 12 : 37 : 50.000	image008.jpg (737b); image010.jpg (756b)	Sign in & confirm: AQE30
Apr 16, 2021 @ 12 : 37 : 44.000	image008.jpg (737b); image010.jpg (756b)	Sign in & confirm:
Apr 16, 2021 @ 12 : 34 : 31.000	image001.png (337b)	PAYMENT CONFIRMATION STATUS 002021
Apr 16, 2021 @ 12 : 33 : 59.000	image001.png (337b)	PAYMENT CONFIRMATION STATUS 002021

Next Generation Threat Detection

Automated Insights & Forecasting Unusual Behavior

Identifying the Off-Nominal

- DECIDE provides forecasting based on observed behavior over time
- Exceptions are identified when behavior exceeds threshold
- These exceptions create alerts and are investigated
- Threats are mitigated through direct defensive action or configuration changes
- DECIDE Platform then gives security engineers an environment to develop and deploy responses



Save time. Save money. Stay ahead of cyber adversaries.

Seven States Webinar: How to Reduce Cyber Risk

March 23, 2022

Cyber Security at Huntsville Utilities– brief description

- Huntsville Utilities adopted the NIST Cyber Security Framework in early 2014, soon after it was published
- Worked through several workshops (both with partners and on our own) refining our maturity levels, goals and milestones
- Active in local Cyber Security meetings and events
- Somewhat regular reviews of our Cyber Security programs and initiatives
- Third party Pentesting, security assessments of existing and new programs and systems

Cyber related team

Information Security Manager, Network Security Analyst
(dedicated to Security tasks)

Network team (2), Admins (2), team of Analysts
(part time Security tasks and responsibilities)

Technical Services Director *(+/- 50% security related)*

Risk Assessment Analyst (under General Counsel)
(also part time Security tasks)

- Now conducting cyber reviews for ALL IT projects prior to approval

We need help !!

Day to day, normal security tasks (updates, config, web and email security)

- 720 users, 700+ servers, workstations, 400+ mobile devices
- Multiple networks and business systems
- Monitor and respond to alerts and log events, etc…

Evaluate and perform triage as needed for multiple threat feeds, including

- US CERT,
- CISA / DHS
- MS-ISAC, Water ISAC, DNG ISAC, Electric ISAC, MS-ISAC,
- FBI/Infragard and others…

We had a goal of finding a partner for continuous monitoring of our networks and systems

Intuitive Research - Pilot Project

- Began a Pilot Project in April 2021 with Intuitive, designed to ingest our logs, correlate with threat feeds and provide custom detection rules
- As part of this project, we wanted to provide both FBI and NDCA feeds of our firewall logs, as both had come to us asking if we could share this information for joint projects they were considering
- Initially- just sent firewall logs, syslogs and public website logs. Soon we added Office 365 connector to add these logs as well
- By August, we were developing a contract to continue this engagement with Intuitive, as we were seeing more benefits

Intuitive Research Project

- Continue to enhance and increase the breadth of information we are sharing into this new system while we reduce our internal needs and products required for visibility into our systems and network
  - Windows Defender / Microsoft ATP logs and alerts
  - Endgame – endpoint protection

  (we were able to replace McAfee subscription with these 2 products)

- Continue to scale up for more logs and better performance

- Intuitive providing multiple KPI/ scoresheets, dashboards and custom alerts based on input and observed network activities

- Next Step – SCADA systems and logs

Intuitive Research – Early Wins

- Successful phishing attempt gathered one users' credentials, followed by multiple additional phishing attempts using his email account
  - Intuitive able to immediately assist us with reconnaissance and confirm the location/actor originating these attempts, and assist us in blocking further exposure of user accounts and/or systems.

- See near instant alerts on any users outside US trying to connect to our O365 instance

- Several instances of foreign entities trying to access our systems from countries we thought we already blocked (better GEO referencing of IP addresses through multiple sources)

Examples - suspicious activity report

Detection Rule: Secure Shell to the Internet

Description: This rule detects network events that may indicate the use of SSH traffic to the Internet. SSH is commonly used by system administrators to remotely control a system using the command line shell. If it is exposed to the Internet, it should be done with strong security controls as it is frequently targeted and exploited by threat actors as an initial access or back-door vector.

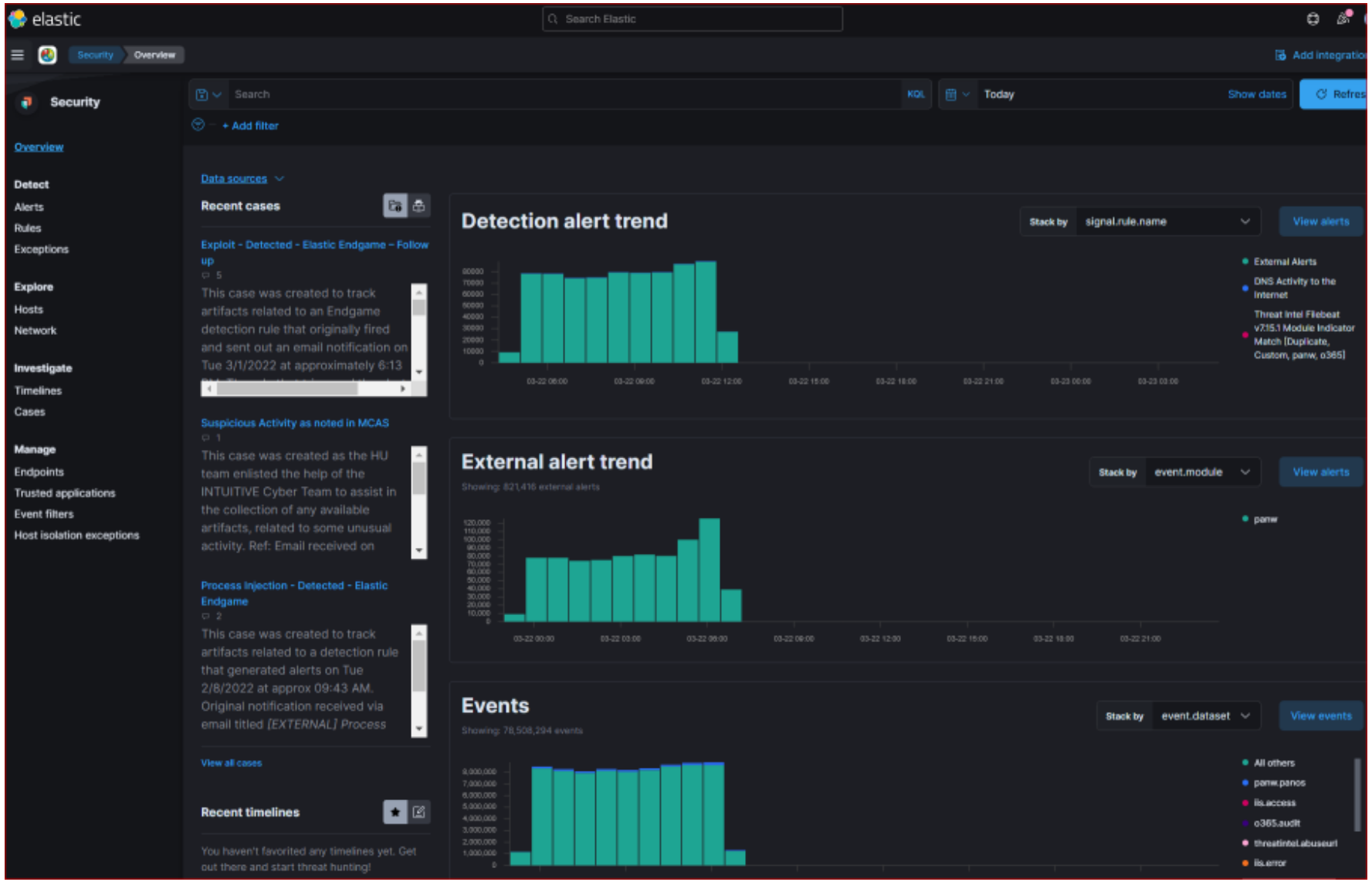
Does any traffic listed above fit the following descriptions?

- SSH connections may be made directly to Internet destinations in order to access Linux cloud server instances. Such connections are usually made, only by engineers. In such cases, only SSH gateways, bastions or jump servers may be expected Internet destinations and can be exempted from this rule.
- SSH may be required by some workflows such as remote access and support for specialized software products and servers. Such workflows are usually known and not unexpected.
- Usage that is unfamiliar to server or network owners can be unexpected and suspicious.

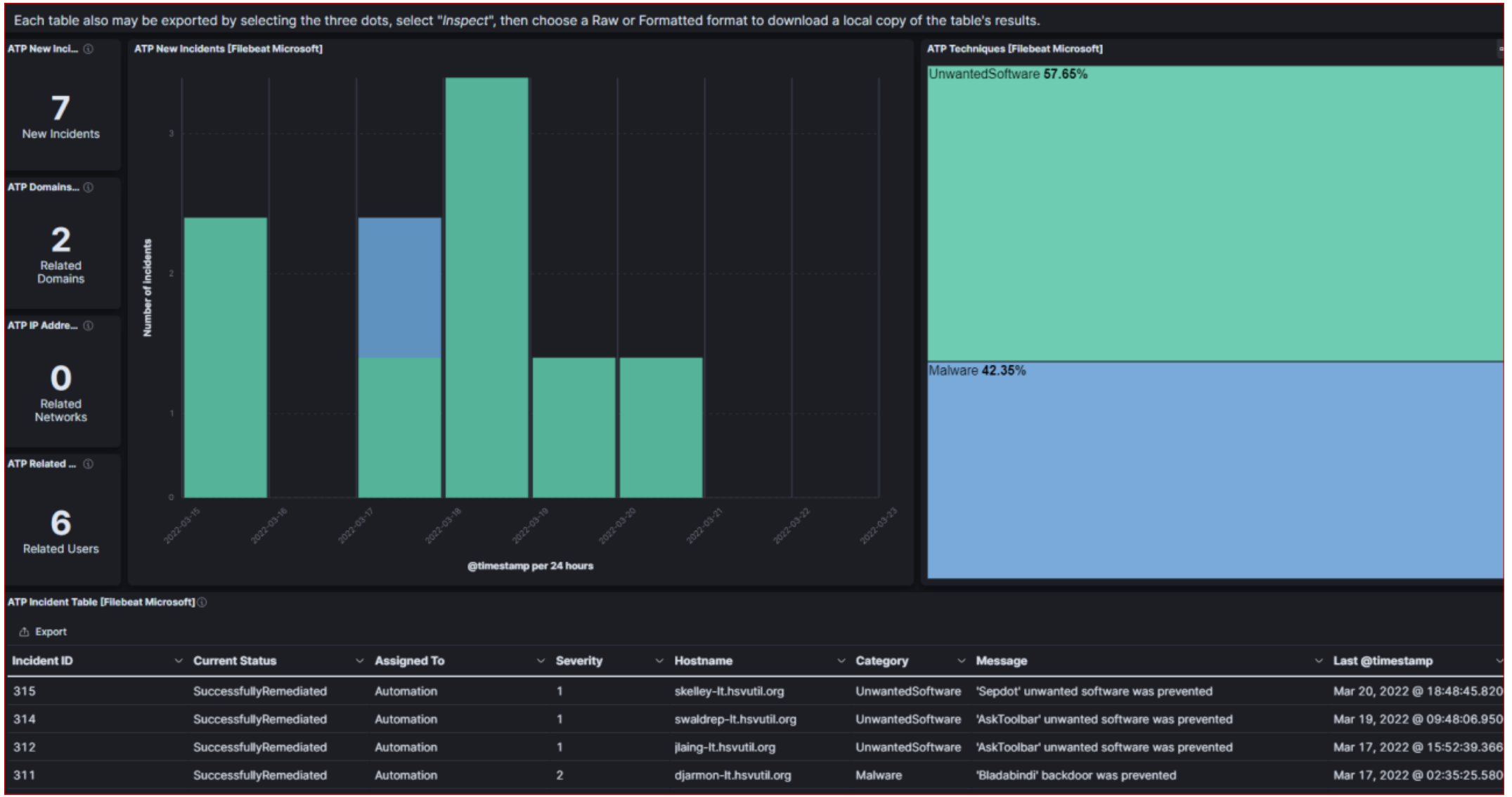
Source IPs

Source IP	Whitelist	Notes (optional)
111.111.111.111	☐	
222.22.2.20	☐	
101.33.333.59	☐	

Examples - Security overview



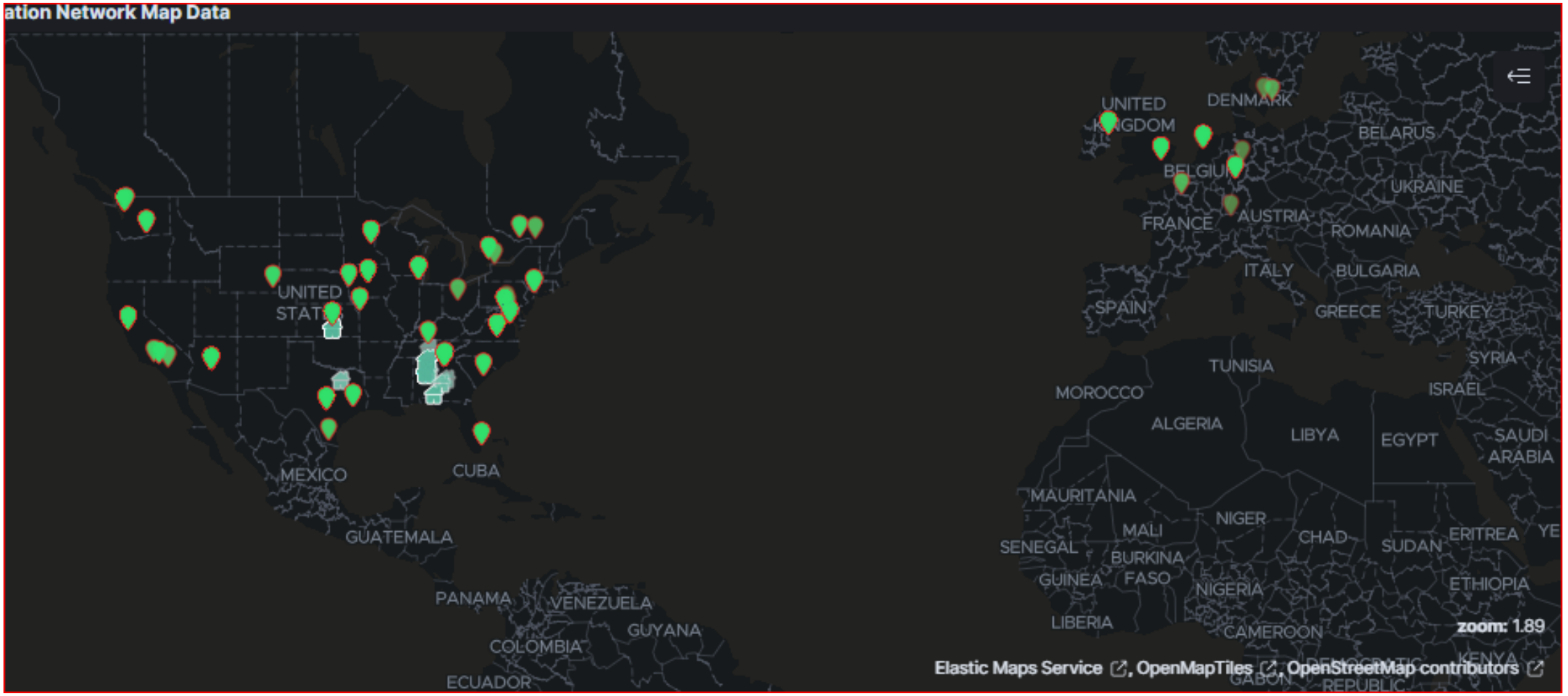
Examples - ATP report (phishing)



Incident ID	Current Status	Assigned To	Severity	Hostname	Category	Message	Last @timestamp
315	SuccessfullyRemediated	Automation	1	skelley-lt.hsvutil.org	UnwantedSoftware	'Sepdot' unwanted software was prevented	Mar 20, 2022 @ 18:48:45.820
314	SuccessfullyRemediated	Automation	1	swaldrep-lt.hsvutil.org	UnwantedSoftware	'AskToolbar' unwanted software was prevented	Mar 19, 2022 @ 09:48:06.950
312	SuccessfullyRemediated	Automation	1	jlaing-lt.hsvutil.org	UnwantedSoftware	'AskToolbar' unwanted software was prevented	Mar 17, 2022 @ 15:52:39.366
311	SuccessfullyRemediated	Automation	2	djarmon-lt.hsvutil.org	Malware	'Bladabindi' backdoor was prevented	Mar 17, 2022 @ 02:35:25.580

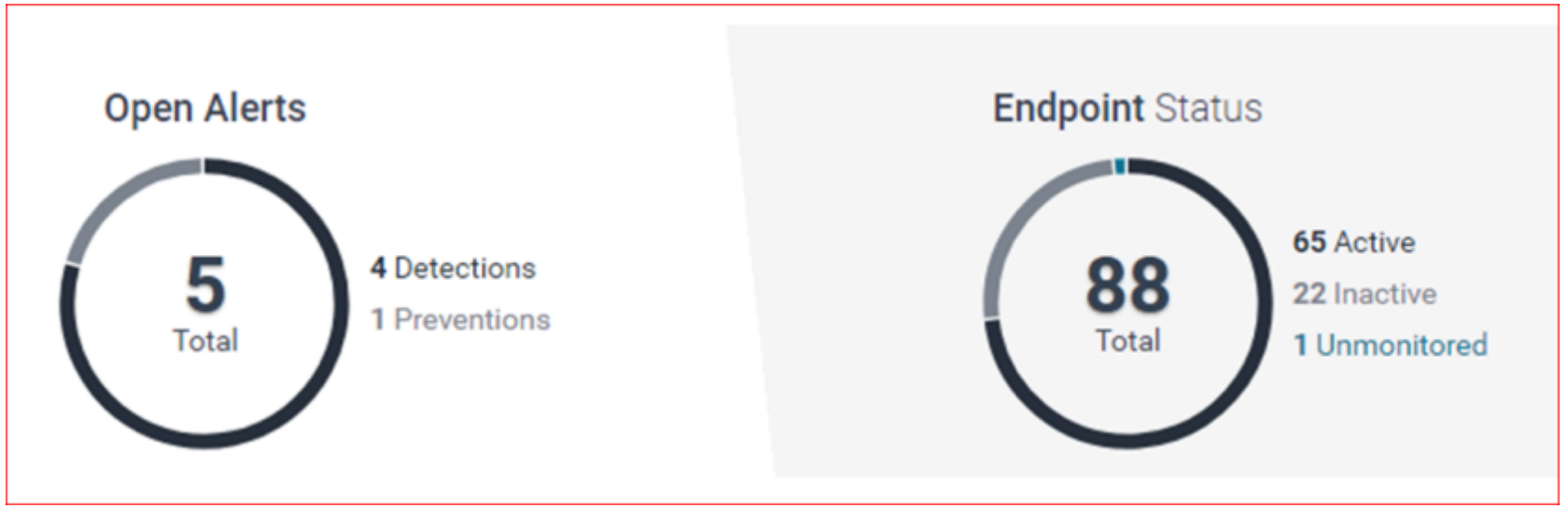
Examples - User activity

Examples - Drill down into user activity

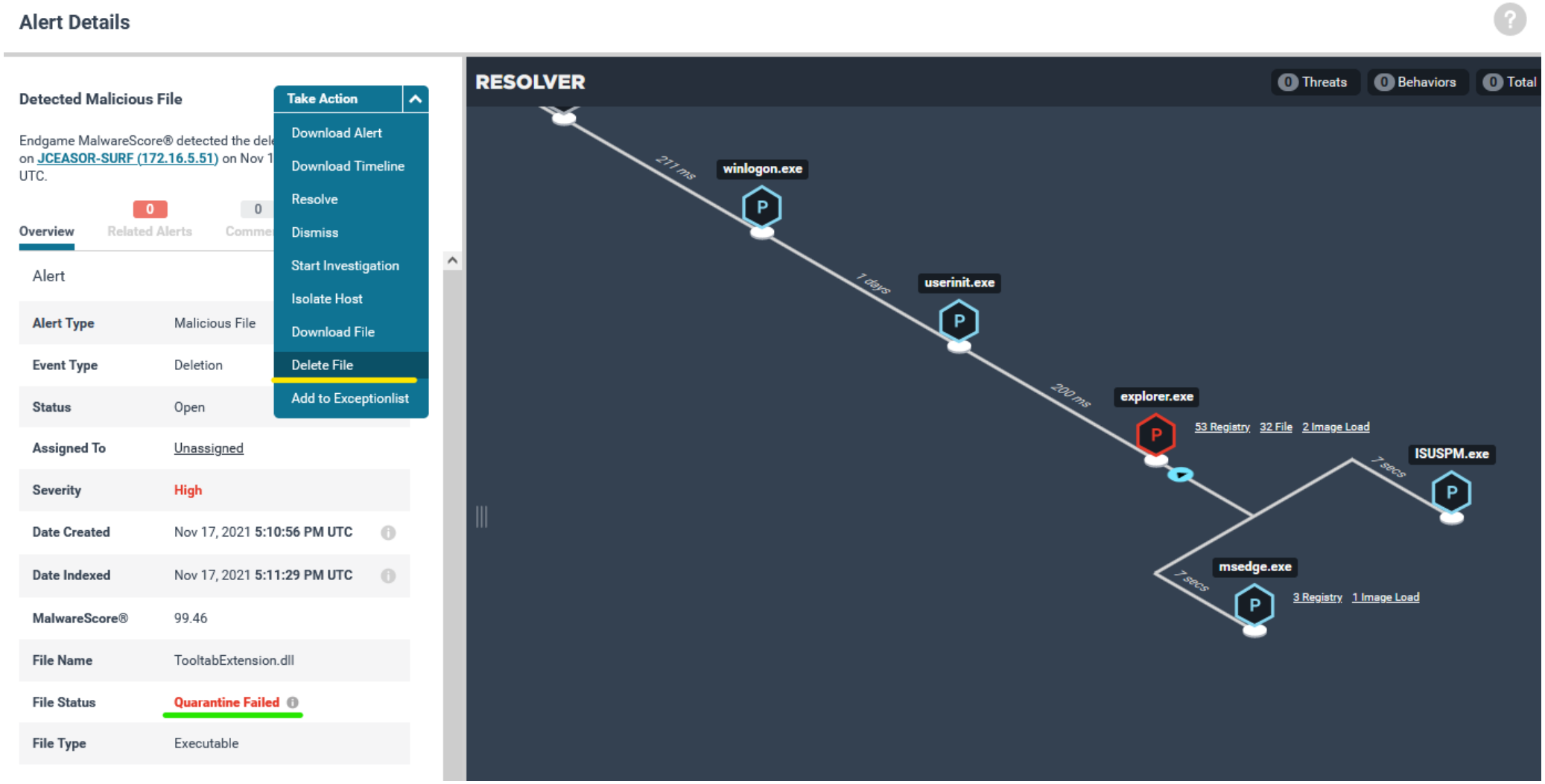


Examples - Threat indicators

Examples - EndGame rollout dashboard



Examples – EndGame report – malicious file found



TENNESSEE VALLEY AUTHORITY

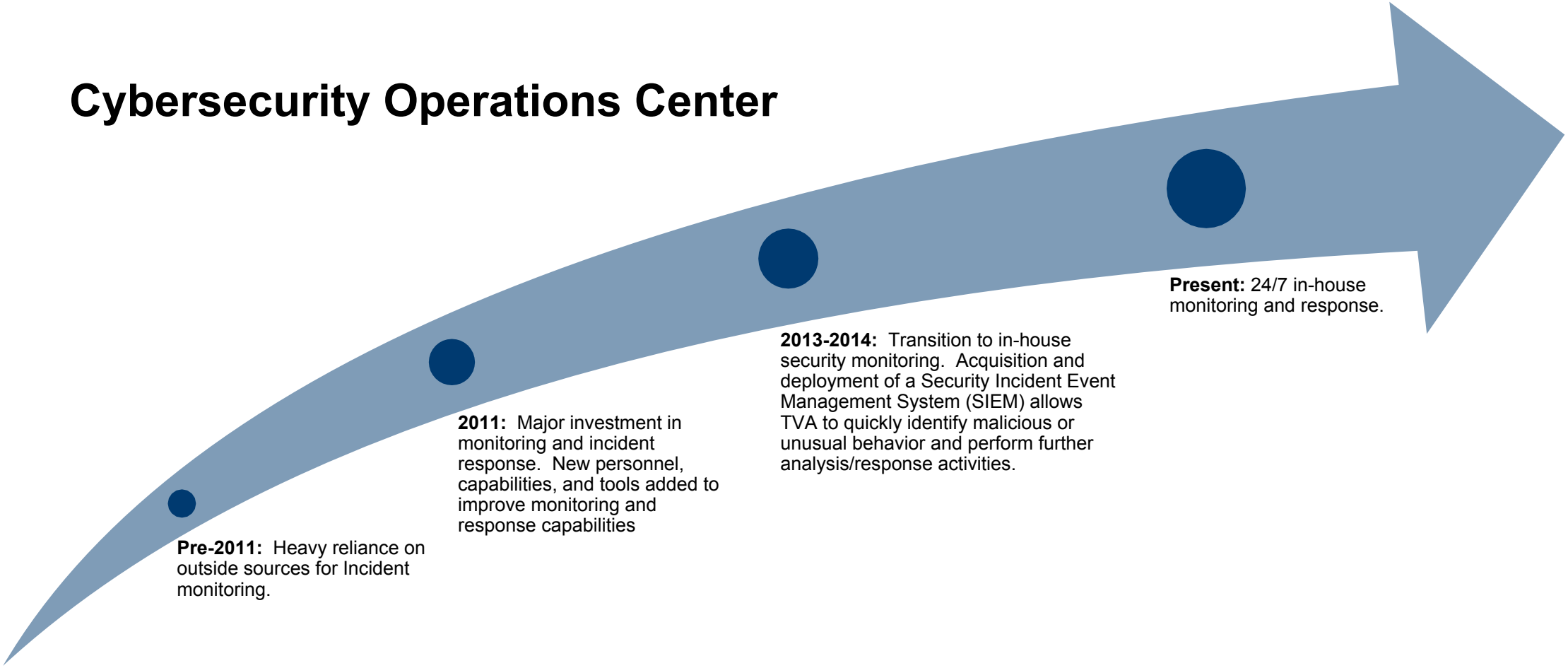
TVA Cybersecurity

Todd McCarter
Director, Cybersecurity Engagement

March 23, 2022

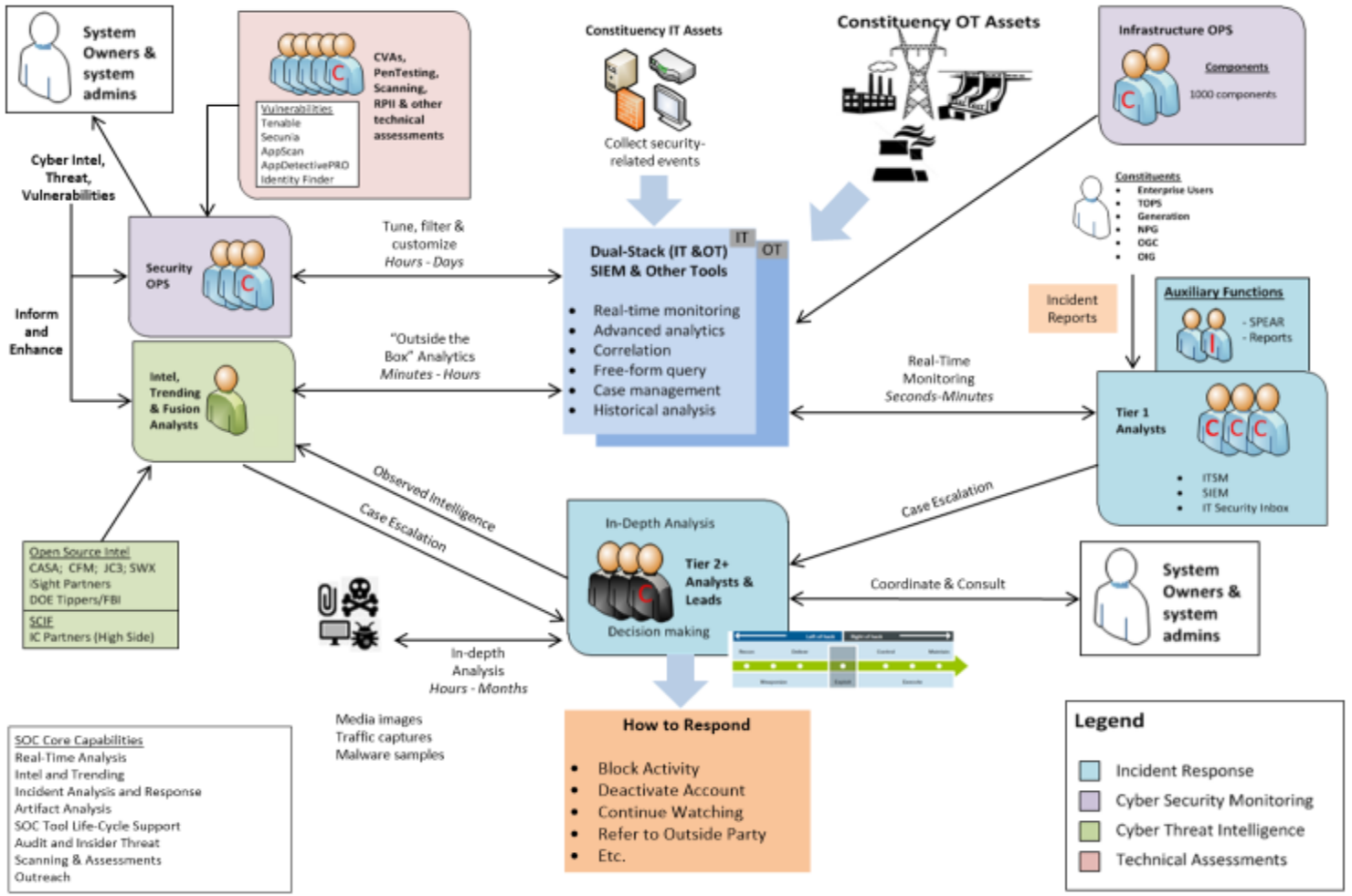
TVA CSOC Journey

Cybersecurity Operations Center



TENNESSEE VALLEY AUTHORITY

TVAC CSOC Functional Chart



TENNESSEE VALLEY AUTHORITY

TVA MSSP Experience

Pros

- 24/7 monitoring
- 24/7 alerting
- MSSP resource onsite
- Responsible for finding staff
- Services offered—training and awareness, threat research, forensics

Cons

- “Out of the box” tuning
- False positives
- Did not understand TVA’s unique architecture
- Lack of visibility on OT
- Lack of familiarity with unusual protocols
- Missed callout procedures
- Lack of coverage for Saas/Cloud
- Limited Threat Intelligence
- Mergers

Upcoming TVA Cyber Webinars

- How to Build a Cyber Program - Thursday, March 31 11:00 – 12:30 PM ET
- Testing & Evaluating Cyber Posture - Thursday, June 30 11:00 – 12:30 PM ET
- Phishing Awareness Training - Thursday, September 29 11:00 – 12:30 PM ET

Contact:

Greg Jackson: ggjackson@tva.gov
Brandy Barbee: babrown1@tva.gov
Todd McCarter: temccarter@tva.gov


TVA
TENNESSEE
VALLEY
AUTHORITY

NRECA Cyber Program

Ryan M. Newlon

Principal Cyber Security Solutions

March 1, 2022

NRECA
America's Electric Cooperatives

Mission Statement and ME

- NRECA's Cyber Program is founded on the concept of mutual assistance and service. By strengthening the cyber defenses of one cooperative, we improve the collective strength of all cooperatives.

- Ryan as a bullet point:
  - Co-op space - 5 years going on 6 in March
    - Co-Mo - 3 years as a Systems and Network Administrator for Co-Mo Connect -Tipton, Mo.
    - Co-Mo - 2 years as the IT Manager of Infrastructure and Cyber Security
    - NRECA – 4 months as the Principle Cyber Security Solutions (Oct 2021)
  - Missouri Army National Guard
    - Chief Warrant Officer 3 (255A) in the Signal Corps
    - Several deployments and countless missions to help defend our country
    - 20+ years in some sort of IT or Cyber capacity

NRECA
America's Electric Cooperatives

What is NRECA Doing

Helping Cooperatives Improve Their Cybersecurity Posture

Representing Co-op Perspective In Key Industry Forums

- Advocacy
- Legal Resources
- Partnerships
- Coordination of Efforts

Providing Resources

- Research & Development
- Tools, Exercises, and Resources
- Technology Planning & Roadmap
- Engagement and Training

NRECA BTS Cybersecurity – Mission Statement

- NRECA's Cyber Program is founded on the concept of mutual assistance and service. By strengthening the cyber defenses of one cooperative, we improve the collective strength of all cooperatives.

- People:
  - Emma Stewart, Chief Scientist
  - Ryan Newlon, Principal Cyber Solutions
  - William Hutton, Principal Cyber Security
  - Doug Lambert, Senior Principal Grid Operations
  - Meredith Miller, Data Scientist
  - Contractors, Incident Support, MSPs, MSSPs

NRECA
America's Electric Cooperatives

What are we and what are we doing?

- **Unique** model for operational research in cybersecurity—merging the cooperative spirit with federal research.
- Program is **growing,** as is the threat to our cooperatives.
- Delicate **balance**—meet you where you are vs. the large scale threat.
- **Constant challenge**: How to battle an enemy that is anonymous and invisible to operators?
- All aspects approach—member directed, public-private partnerships
  - Information **sharing**–Federal, state, and local level via IRMS.
  - CaaS: **Cyber-as-a-service**
  - Cyber security maturity **assessments** and directions to prioritize resources
  - Novel business model for cyber operations

Why?

- For US the Co-op environment
- Solving hard problems
- Consolidation of efforts
- Cybering is hard
- The threat is real
- A collective Maturity Model

Program Goals (Next five years)

Improve Response

- Incident Response Plans
- Decrease Detection Time

Harden Systems

- Security Policies
- Security Controls
- Continuous Improvement

Community

- Increased awareness
- Mutual Cyber Assistance
- Strengthen external relationships

Education

- Training
- Apprenticeships
- Certifications
- Conferences

NRECA
America's Electric Cooperatives

Strategic Partnerships & Outreach

Strategic Federal Partnerships

- E-ISAC (MOU)
- NSA (MOU)
- DOE
- DOD
- DHS

Strategic Academic Partnerships

- CyberUp
- EnergySec
- KU Innovation Park
- New Mexico State University
- University of Illinois Urbana-Champaign
- Many more….

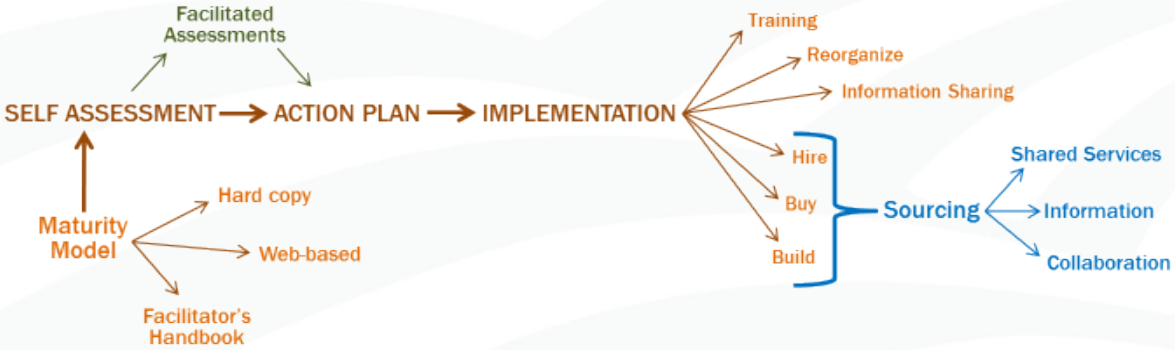
NRECA
America's Electric Cooperatives

NRECA National Threat Analysis Center (TAC)

1. Collective defense through distributed analysis
2. Coordinate with Federal entities
3. Asset management
4. Incident response
5. On-call SME support
6. Anonymized information sharing

RC3 Program

Rural Cooperative Cybersecurity Capabilities (RC3) Program



RC3 Cybersecurity Self-Assessment

Hard copy & Online Versions

Used by 533 cooperatives

RC3 Cybersecurity Summit Series

291 co-ops & 389 co-op staff

1,262 visits to RC3 Summit webpages

NRECA
America's Electric Cooperatives

This material is based upon work supported by the Department of Energy National Energy Technology Laboratory under Award Number DE-OE0000807.

RC3

Improve Training, Information Coordination & Access

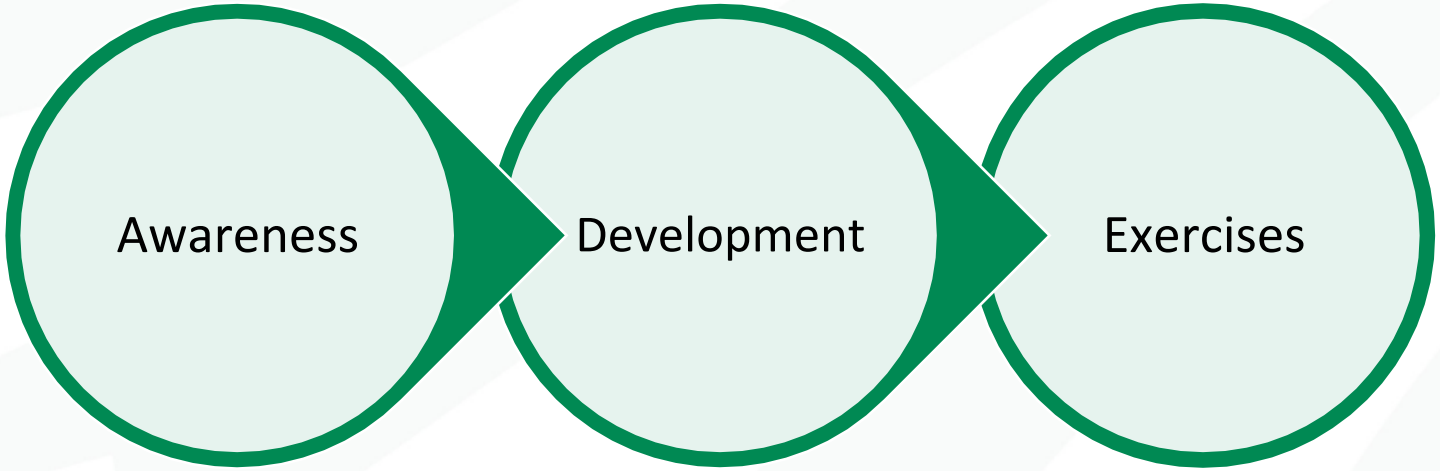
1. *Self Assessment & Axio* partnership (licensing model)
2. RC3 Guidebooks - CIRP just came out
3. “Information Sharing” publications & Cyber security podcasts
4. Summits and Tabletops (TTX)
5. Remediations + Reports + Continual Monitoring
6. Operation Cooperative
7. Incident Response
8. Cyber Champions
9. Asset Management

Improving Incident Response

- **Challenges**:
  - Staffing: No IT, contractor IT, dedicated (overcommitted) IT staff
  - Awareness: None, little, or some cyber security knowledge
  - Funding: Unfunded, partially funded, fully funded
  - Time: Competing priorities

Approach:

- Seminars to raise **awareness** of existing resources (NIST)
- Workshops to help co-ops **develop** their own incident response plans
- **Exercises** to increase familiarity and continually improve plans



NRECA
America's Electric Cooperatives

Cyber Champions - Conceptual

RECAP approach and ownership

One or more cyber champions

- per state
- Statewide
- per region
- G&T family

Boots on the ground advisor-Trusted and heard

Multi-directional communication

How:

- We start with Identifying the who
- Work with the members to figure out what this looks like
- Develop what your state's Cyber program will look like with the Cyber Champion
- Opportunities related to the new Threat Analysis Center

Good Jobs Challenge

EDA's American Rescue Plan Good Jobs Challenge aims to get Americans back to work by building and strengthening systems and partnerships that bring together employers who have hiring needs with other key entities to train workers with in-demand skills that lead to good-paying jobs.

Problem

- 600,000 vacant jobs
- Underserved areas and communities

NRECA

- NRECA is Backbone Org
- 11 Sectoral Partners
- 3-year program

Status

- $500 mil
- 509 applicants
- 25-50 awards

Outcome

- July awards
- Qualified & trained Cyber personnel
- Co-op specific training

NRECA
America's Electric Cooperatives

Questions

What is NRECA Doing

Strategic Partnerships & Outreach

TAC

RC3 Program

Improving Incident Response

Cyber Champions

Good Jobs Challenge

NRECA
America's Electric Cooperatives

(423) 490-7772

SevenStatesPower.com

PO Box 11128
Chattanooga, TN 37401

@7StatesPower

@Seven States Power Corporation