RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: TECH-W12

Making Security Automation Real

Jessica Fitzgerald-McKay
Security Automation Lead
National Security Agency

David Waltermire
Security Automation Lead/Architect
National Institute of Standards and Technology

What will we talk about today?

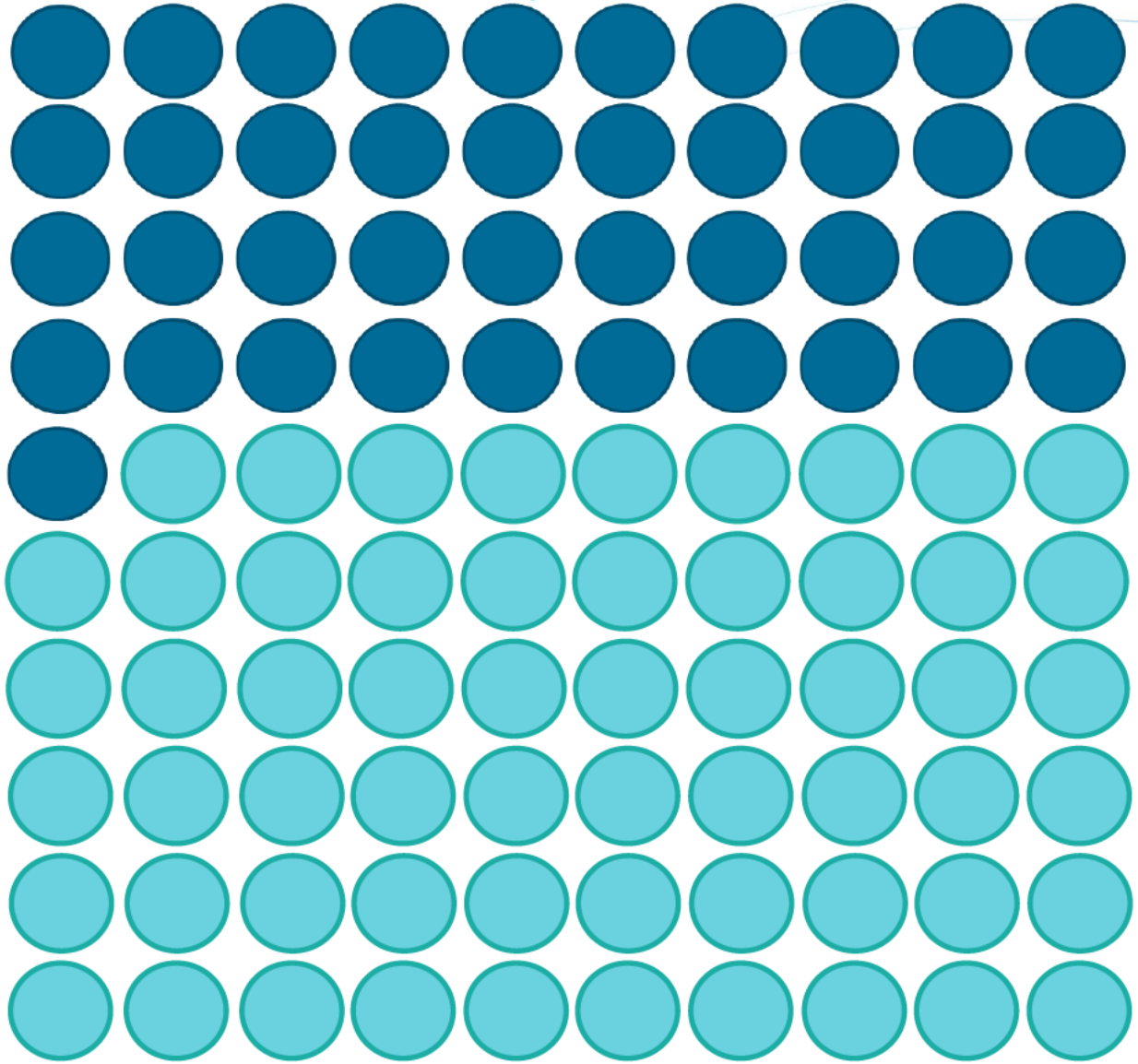
- How currently available network security solutions have failed to scale to protect complex multi-vendor networks
- How we propose to automate security:
  - For all endpoint types
  - For all enterprise networks
  - In support of network analytics and continuous monitoring

RSAConference2019

Why does security automation matter?

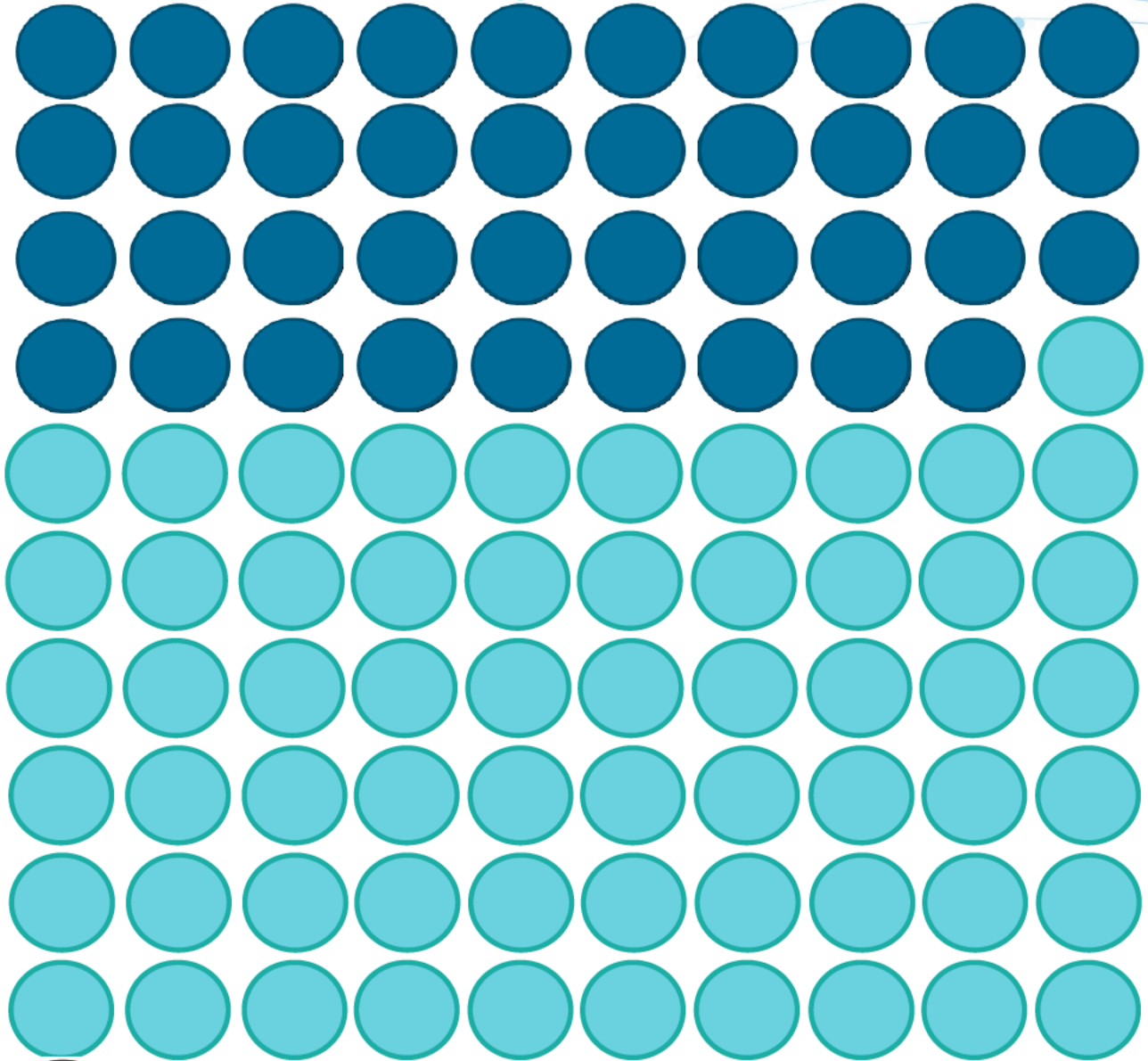
These attacks were made possible by:

- Known vulnerabilities left unremediated and
- Poor network monitoring



41% Cannot Locate Key Network Assets

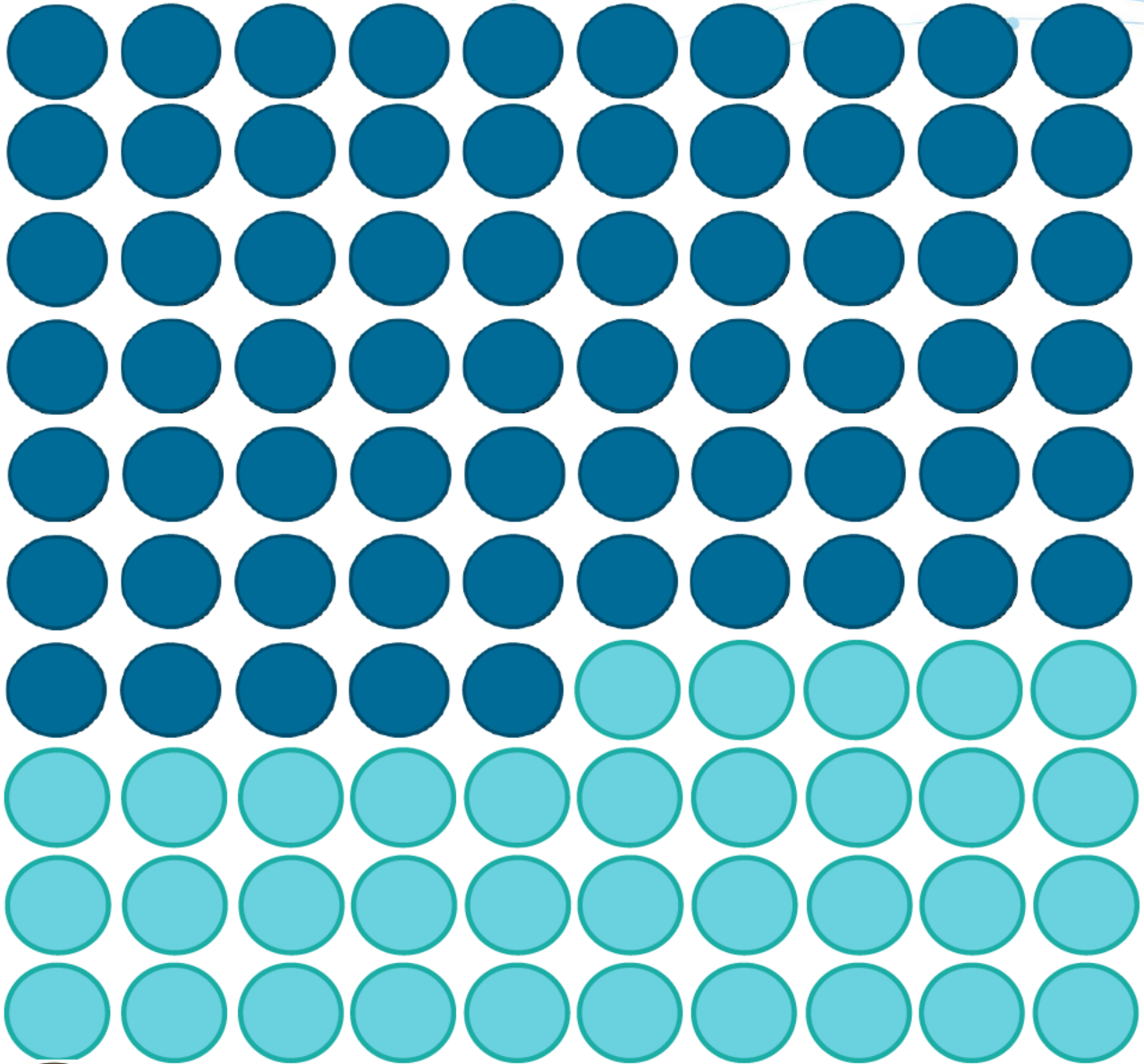
"The State of Cybersecurity from the Federal Government Perspective", (ISC)[2]



39% Don't Know What Their Key Assets Are

"The State of Cybersecurity from the Federal Government Perspective", (ISC)²

NIST National Institute of Standards and Technology U.S. Department of Commerce

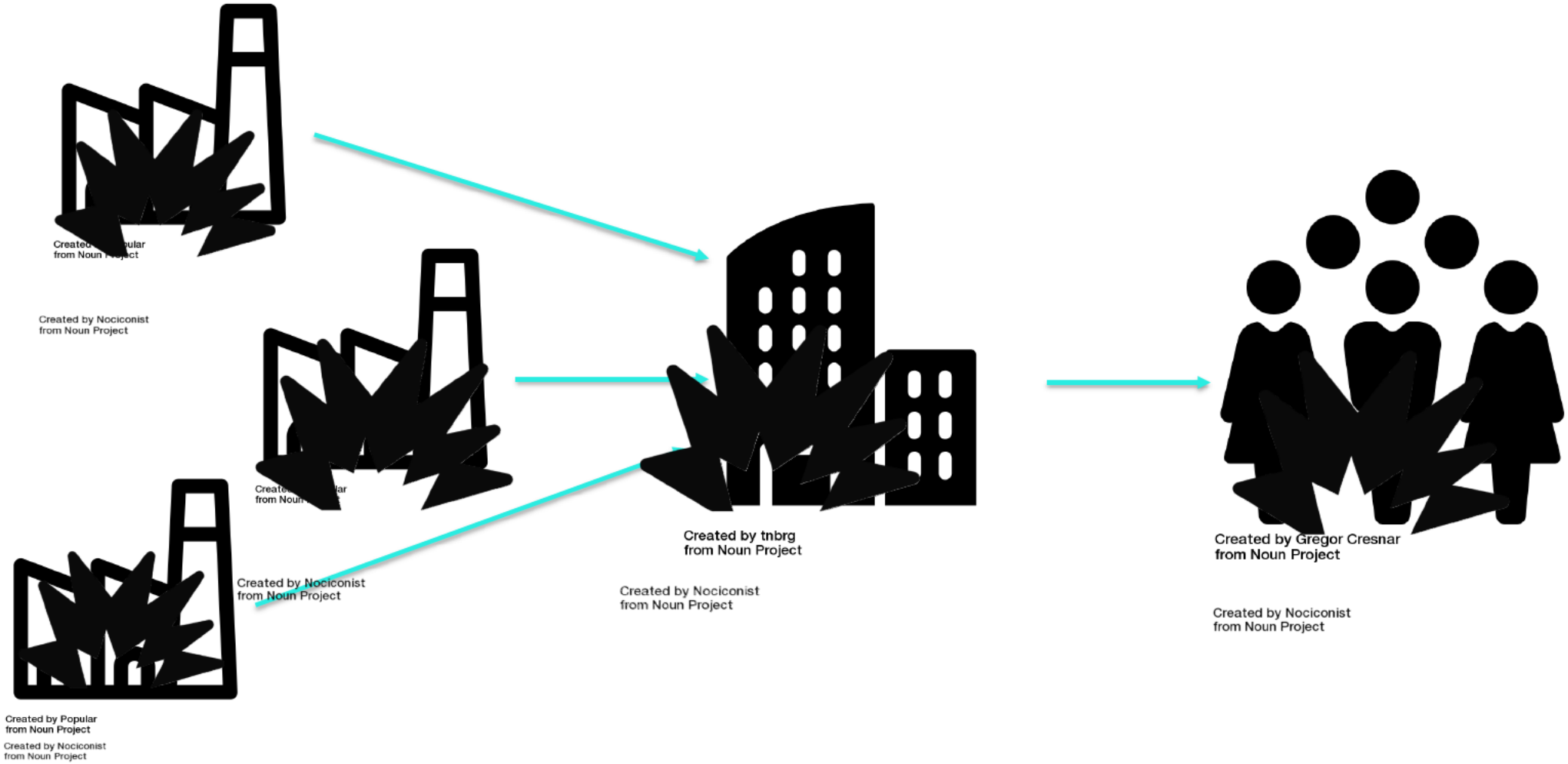


65% Said Federal Gov't Can't Respond Effectively to Attacks

"The State of Cybersecurity from the Federal Government Perspective", (ISC)²

NIST National Institute of Standards and Technology U.S. Department of Commerce

Attacks Cause Collateral Damage



RSAConference2019

How is security automated?

CIS Top 20

1- Device Inventory

2- Software Inventory

3- Secure Configurations (Mobile, Workstations)

4- Vulnerability Assessment

5- Admin Privileges

6- Audit Logs

7- Email/Browser Protections

8- Malware Defense

9- Port Control

10- Data Recovery

11- Secure Configurations (Network Devices)

12- Boundary Defenses

13- Data Protection

14- Controlled Access

15- Wireless Access

16- Account Monitoring

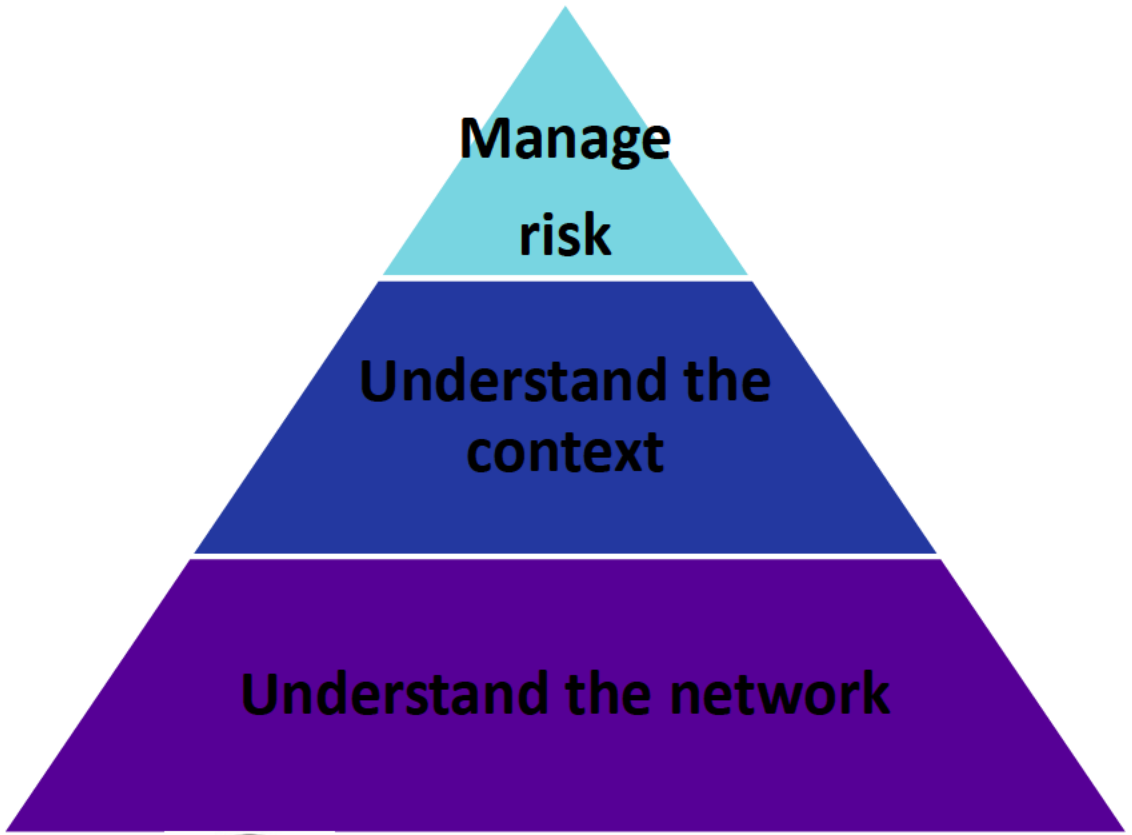
17- Security Skills Assessment

18- Application Software Security

19- Incident Response

20- Penetration Testing

Security Automation in Three Simple Steps



- Step 3: Understand how to manage risk
  - Knowing what to patch, uninstall, harden
- Step 2: Understand the context
  - Understand what vulnerabilities apply to assets
- Step 1: Understand the network
  - Focus on hardware and software asset management

NIST National Institute of Standards and Technology U.S. Department of Commerce

How can we perform these steps?

Action Items

- Things you can do right now
- Improve security automation capabilities
- Can be integrated with security automation solutions you have right now

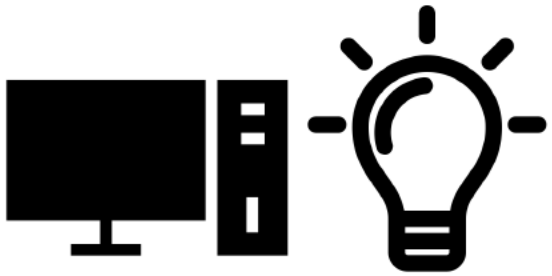
Proposals

- Currently available, but not yet widespread
- Standards-based, open-source implementations
- Represent the next generation of security automation technologies

RSAConference2019

Step 1: Understand the Network

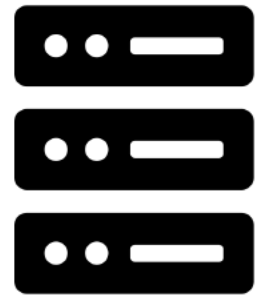
What is an Endpoint?



Created by Dinosoft Labs
from Noun Project

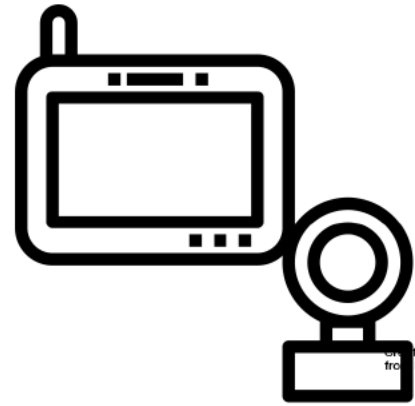
Created by Numero Uno
from Noun Project

Created by Philipp Koerner
from Noun Project

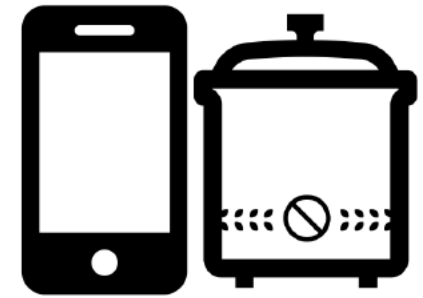


Created by Adrien Coquet
from Noun Project

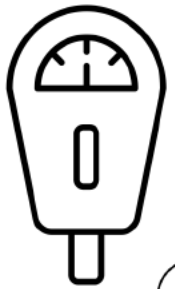
Created by Ralf Schmitzer
from Noun Project

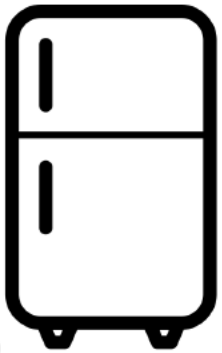


Created by VINZENCE STUDIO
from Noun Project



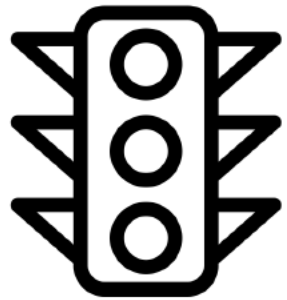
Created by Rose Alice Design
from Noun Project





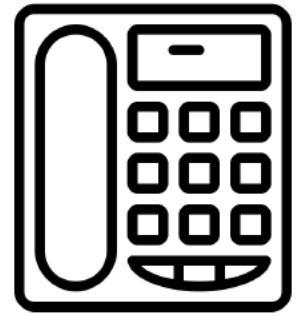
Created by Sergey Novosyolov
from Noun Project

Created by Sergey Demushkin
from Noun Project



Created by Paisley
from Noun Project

Created by Dan Jenkins
from Noun Project



Created by Creaticca Creative Agency
from Noun Project

Created by Daniel Luft
from Noun Project

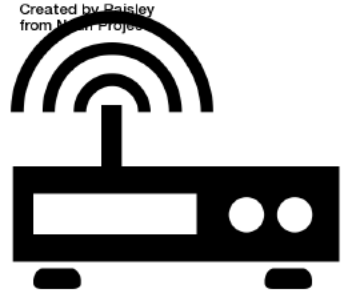
Created by Jae Deasigner
from Noun Project

Created by Deemak Daksina
from Noun Project

Created by b farias
from Noun Project

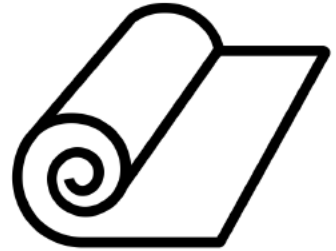
Created by Pedrovisc
from Noun Project

Created by Mohamad Arif Prasetyo
from Noun Project

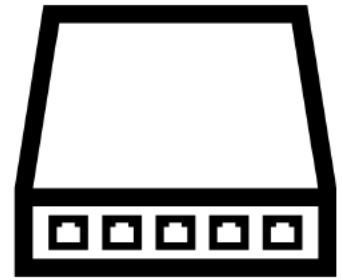


Created by Mister Pixel
from Noun Project

Created by Dmitry Mirolyubov
from Noun Project



Created by Moonyoon
from Noun Project



Created by Georgiana Ionescu
from Noun Project

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Addressing management of a diverse set of assets

Attacks are shifting beyond classical IT assets to supply chain partners and operational technology (OT) environments

- Asset diversity makes a single solution impossible
- Standardized methods are needed that enable a best-fit approach

There are some existing, concrete approaches that can help address this problem.

Action Item #1- Use SWID Tags to Identify Software Assets

- International standard defined in ISO/IEC 19770-2
- Two key aspects:
  - Structured format for software description and metadata
    - Simple structure with minimum required fields
    - Can support a wide range of metadata: publisher, file manifest, etc.
  - Lifecycle process to align presence of a tag with presence of a software product on an endpoint
    - Add tag when software installed; revise tag when software updated; delete tag when software uninstalled
    - Discovery of endpoint tags is a simple way to develop a rough software inventory

Action Item #2: Correlate Device Identities

Devices have many identifiers. . .

- Easily changed and/or Mutable Identifiers
  - MAC Address
  - IP Address
- Semi-mutable Identifiers
  - FQDN
  - Software certificates
  - Agent-based identifiers
- Permanent Identifiers
  - Identifiers secured by cryptographic hardware modules
  - Serial numbers

That are used differently for various services. . .

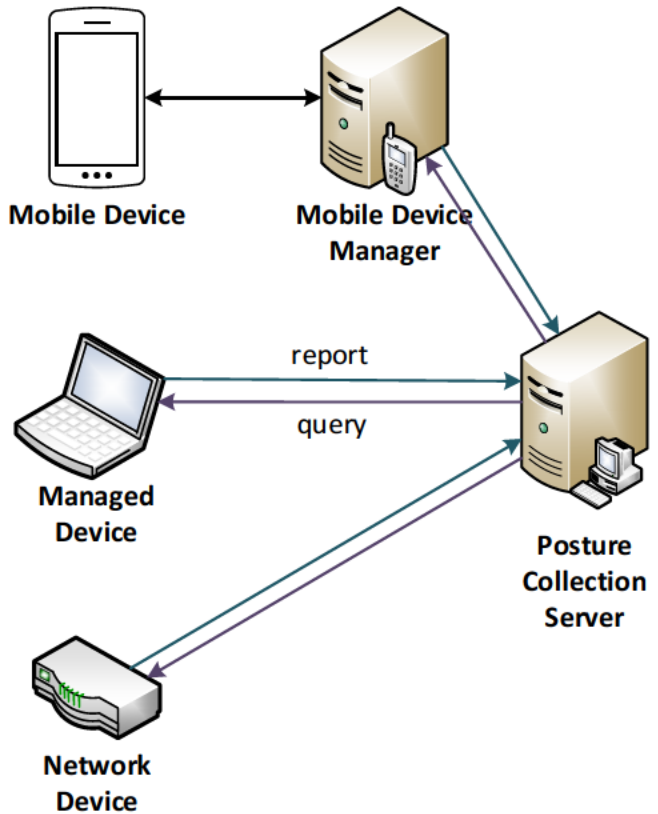
- Behavior Monitoring
- Compliance testing
- Provisioning
- User Services

Proposal #1: Collect Event-Driven Posture Information from All Endpoint Types

Methods of Posture Collection

- Collect software load from all types of devices
- Report posture changes as they occur
- Leverage other posture managers (e.g., MDM)
- Query additional information on an as-needed basis

Proposed Architecture for Posture Collection



Proposal #2- Use SWIMA to Maintain Situational Awareness

- Software Inventory Message and Attributes (SWIMA) for PA-TNC (RFC 8412)
  - An extension of the Network Endpoint Assessment (NEA, RFC 5209 et al.)
- Supports collection of software inventory information from endpoints to a central server
- Key features
  - Supports both server queries and event-based reporting by endpoints
  - Flexible and extensible support for inventory reporting formats
  - Can report full inventory or change events relative to a point in time
- Result in a way to collect and efficiently maintain timely information about endpoint software inventories that is easily added to any NEA implementation
- Open source implementation in strongSwan

RSAConference2019

Step 2: Understand the context

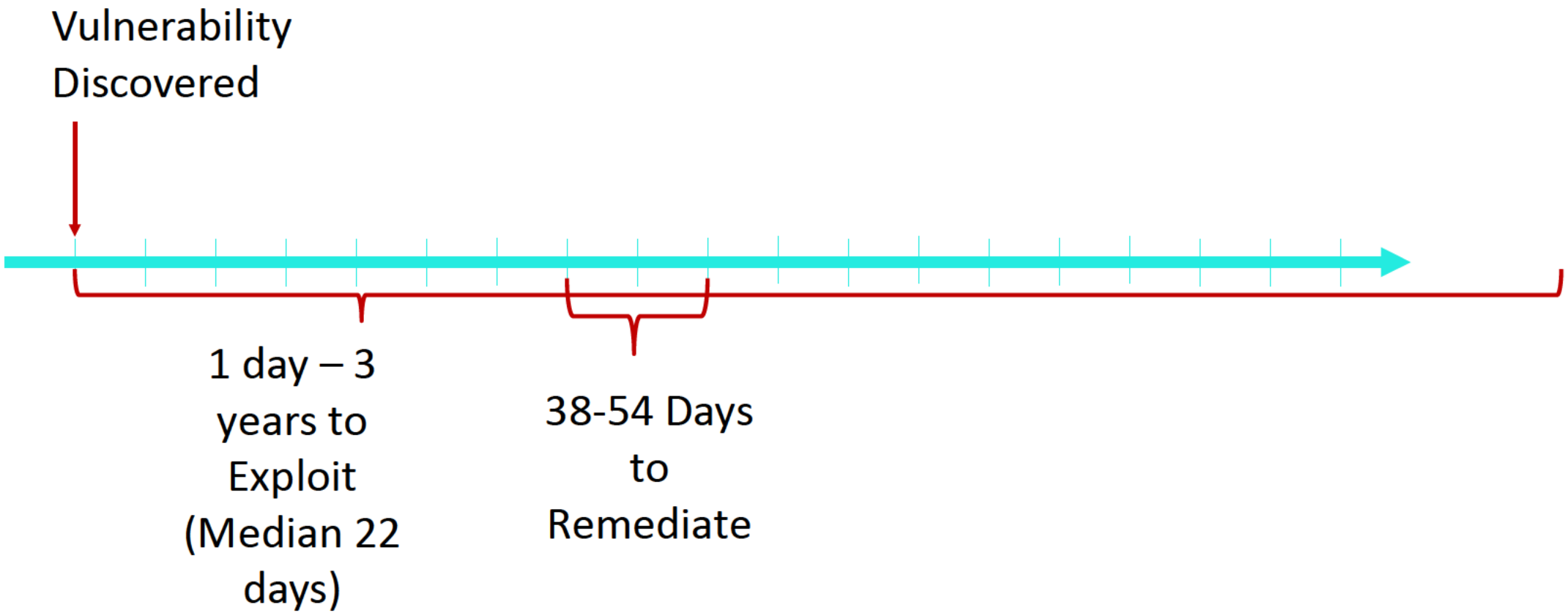
57% of breach victims were breached due to an unpatched known vulnerability

"Today's State of Vulnerability Response: Patch Work Demands Attention", Ponemon Institute for ServiceNow,

34% knew they were vulnerable before they were breached

"Today's State of Vulnerability Response: Patch Work Demands Attention", Ponemon Institute for ServiceNow,

Vulnerability Discovery, Exploitation and Remediation

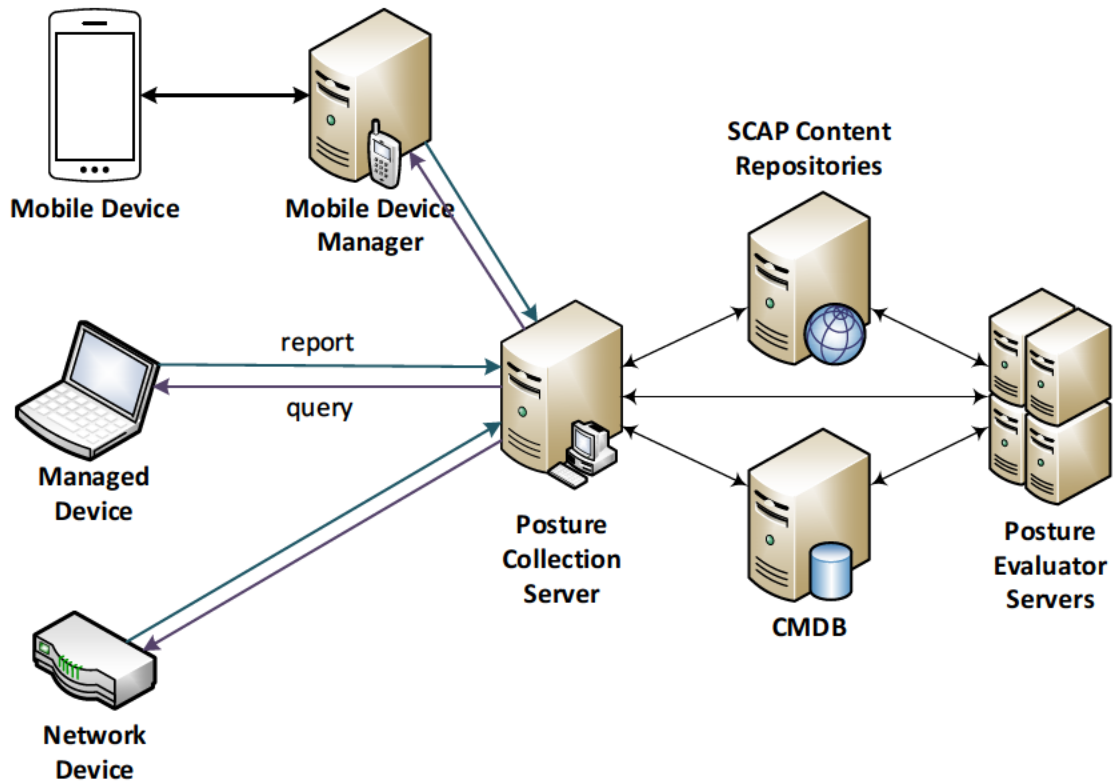


Proposal #3: Share Network Posture Information Across Analytics and Use Cases

Supported Use Cases

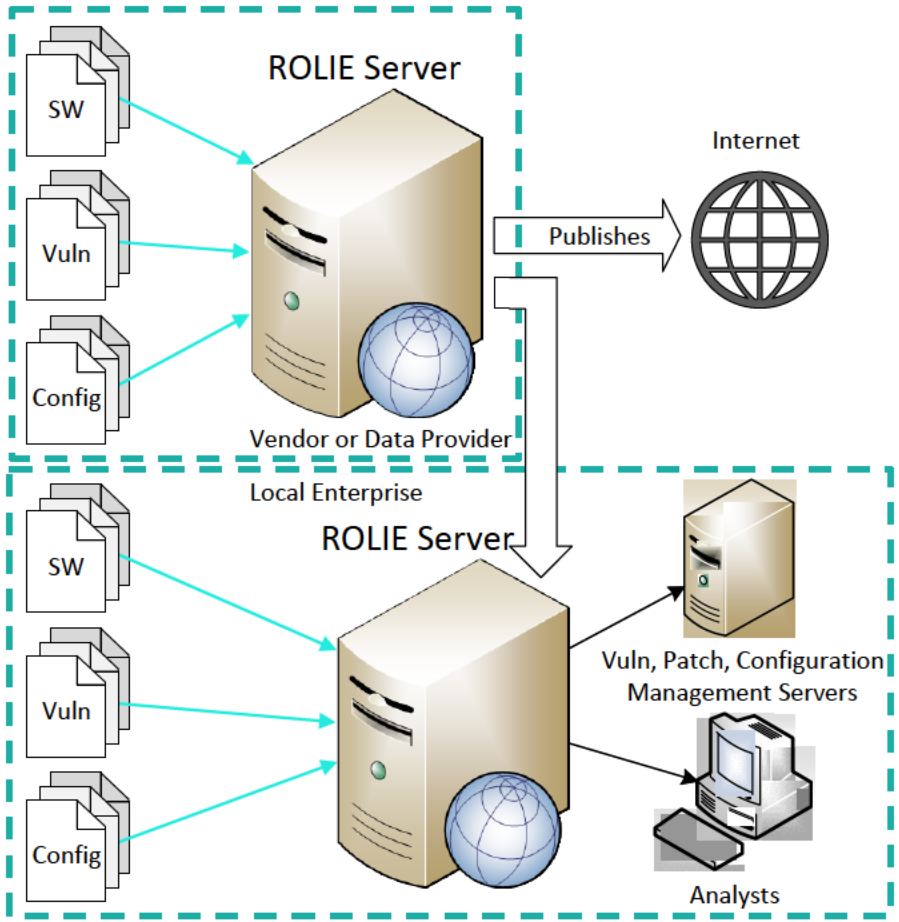
- Configuration Manager
- Vulnerability Manager
- Behavior Monitor
- License Manager
- Comply-to-Connect
- Information Sharing
- Automated Courses of Action

A Security Automation Architecture



ROLIE and its Use Cases

- Resource-Oriented Lightweight Information Exchange (ROLIE) (RFC 8322) provides a data format and transport protocol for publishing, organizing, and sharing computer security information
- ROLIE allows published data to be accessed by 3rd parties, using optional authentication, supporting information sharing
- ROLIE can serve information supporting a number of use cases at the same time, including:
  - Software metadata (e.g., SWID Tags)
  - Vulnerability Information (e.g., CVE)
  - Configuration Setting Checklists (e.g., SCAP)
- ROLIE Servers discover each other and publish/receive information between them, accelerating information sharing between parties
- Allows organizations to maintain their own information collections
- Analysts and tooling use this information to automate security and management of devices



Proposal #4- Leverage ROLIE to Provide Context to Network Posture Information

- Standardized data format and protocol for storing, retrieving, receiving and sending security automation information
  - Provides tagging and categorization metadata that facilitates searching
- Allows software product maintainers to publish their own security automation information, including:
  - SWID Tags
  - CVE-based vulnerability data
  - SCAP-based configuration setting checklists
- Being implemented in the National Vulnerability Database to publish CVE-based vulnerability data and configuration setting checklists

RSAConference2019

Step 3: Understand managing risk

Action Item #3: Leverage vulnerability information

Development

Identify and manage vulnerable components / libraries

Acquisition

Understand risks in the supply chain and from service providers

Deployment

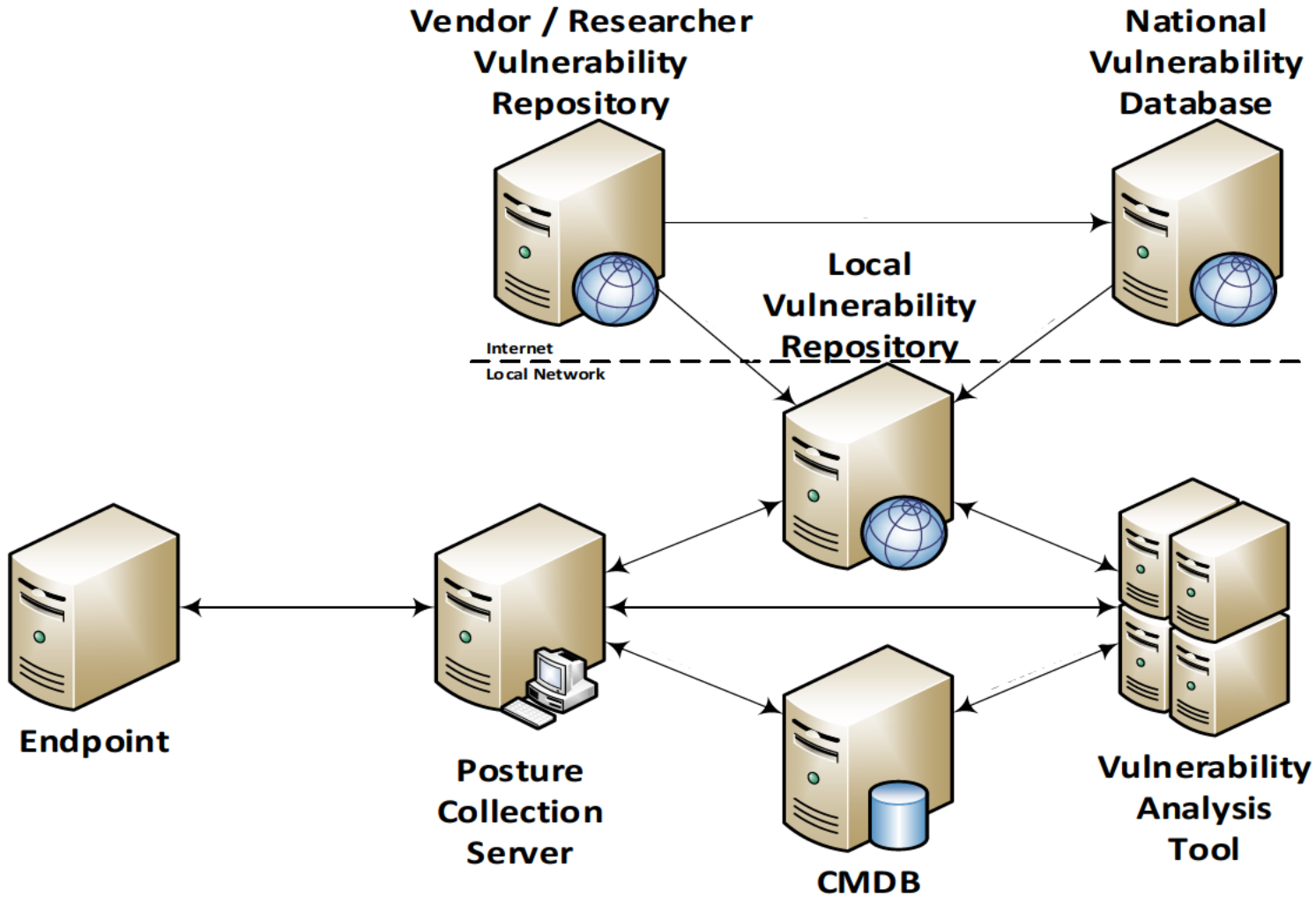
Assess vulnerabilities on the network

Managing Vulnerabilities During Software Development and Maintenance

- Reuse of software accelerates software development
- Open source software is used in 96% of commercial applications
- DevOpsSec vs SecDevOps - Vulnerable dependencies introduce risks that need to be managed during development
- SWID Tags provide information on software dependencies (e.g., identifiers, versions, hashes)

Vulnerability Information and Supply Chain Risk Management

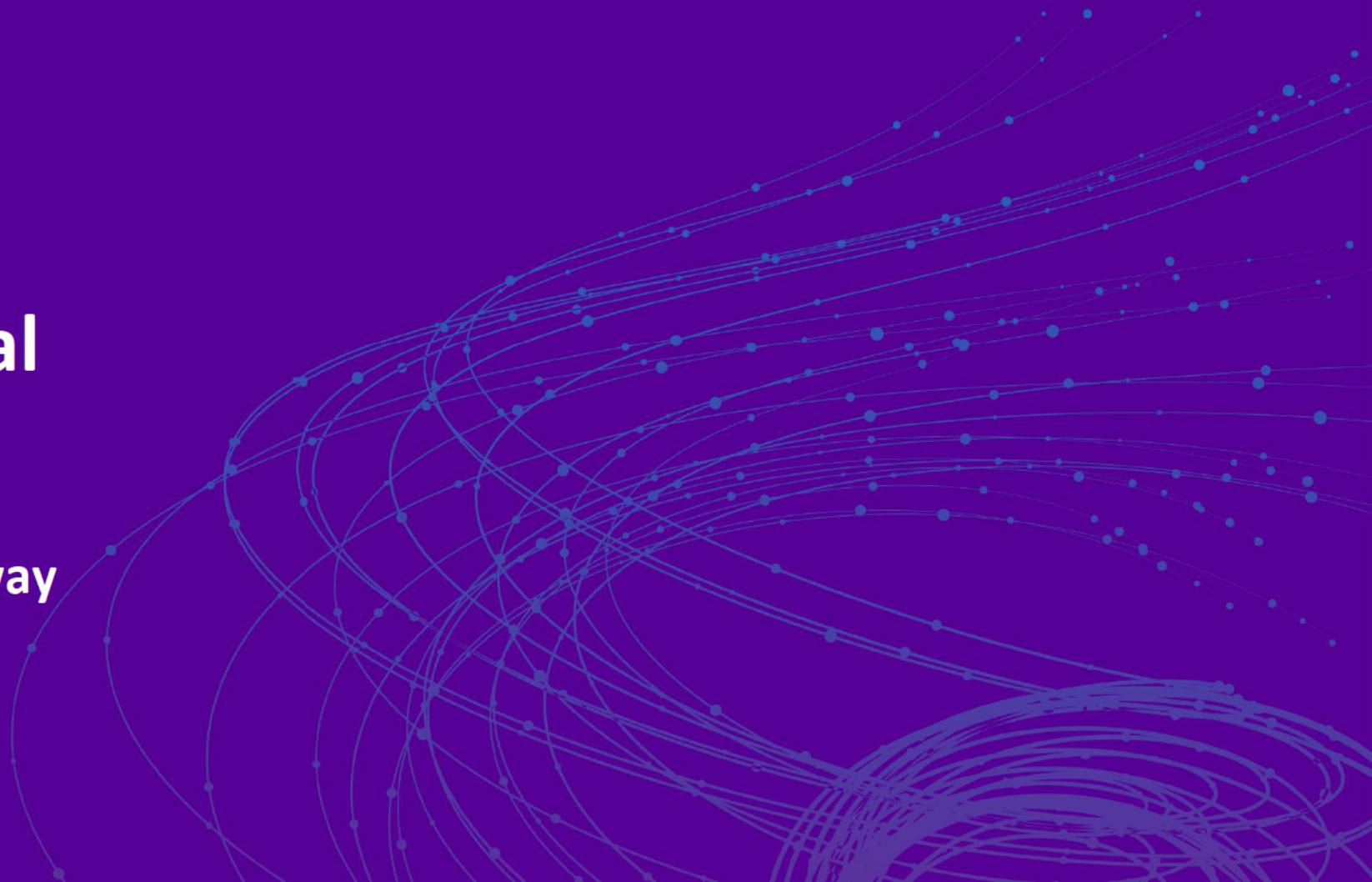
Vulnerability Management on the Network



RSAConference2019

Making it real

Or keeping it that way



Standardized Security Automation

- For all endpoint types
- For all enterprise networks
- In support of network analytics and continuous monitoring

Putting Software Asset Management Standards into Practice

- For users:
  - Use the SWID tags that you already have
  - Ask your software providers for SWID tags
- For Software Creators:
  - Provide SWID tags with your software
  - Use SWID tags as a part of your SecDevOps process
- For tool developers
  - Implement SWIMA for software inventory
  - Make use of SWID tag information in analytics

Security Content Automation Protocol (SCAP) 2.0 Update

- Incorporates standardized transport protocols
- Incorporates standardized schema, beginning with Software Identification (SWID) tags
- Makes this data available to network analytics to automate security functions

Join us at https://scap.nist.gov/community.html

RSAConference2019

Applying what you have learned

Apply What You Have Learned Today

- Next week you should:
  - Identify gaps in your software inventory
- In the first three months following this presentation you should:
  - Talk to your software providers about providing SWID tags
  - Use SWID Tags to address software asset management requirements and for vulnerability management
  - Collaborate with us on the further development of SCAP v2
- Within six months you should:
  - Provide SWID tags for software your organization produces as a part of SecDevOps and Supply Chain Risk Management practices

Security Content Automation Protocol (SCAP) 2.0 Update

Join us at https://scap.nist.gov/community.html

Resources

Consensus Standards Groups

- Managed Client Data Model and Protocols
  - Internet Engineering Task Force (IETF) Network Endpoint Assessment (NEA) https://datatracker.ietf.org/wg/nea
  - IETF Security Automation and Continuous Monitoring (SACM) http://datatracker.ietf.org/wg/sacm
- Unmanaged Clients Data Model and Protocols
  - Trusted Computing Group (TCG) www.trustedcomputinggroup.org
- Sharing Context
  - IETF Managed Incident Lightweight Exchange (MILE) https://datatracker.ietf.org/wg/mile

Whitepapers and Specifications

- SCAP v2 Whitepaper https://doi.org/10.6028/NIST.CSWP.09102018
- Guidelines for the Creation of Interoperable Software Identification (SWID) Tags https://doi.org/10.6028/NIST.IR.8060
- Resource Oriented Lightweight Information Exchange (ROLIE) Protocol https://doi.org/10.17487/RFC8322
- Software Inventory Message and Attributes (SWIMA) for PA-TNC https://doi.org/10.17487/RFC8412