

The CDM Learning Community Event (LCE)

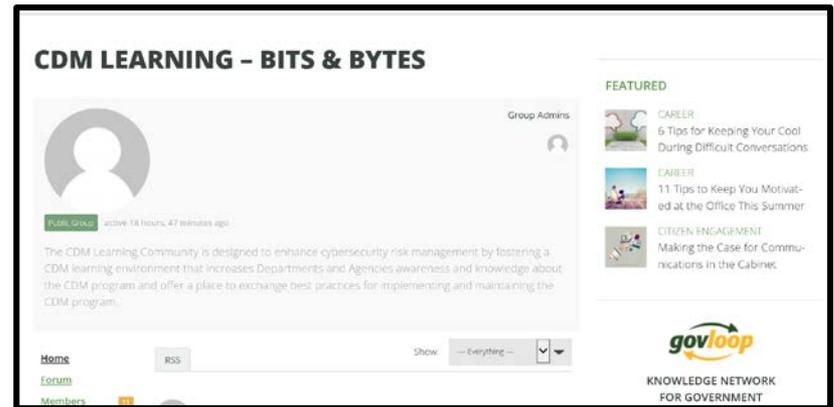
We will begin at 1:00PM EST

Welcome to the CDM LCE – Automating Hardware Asset Management: Notes From the Field

While you wait, check out:



Our CDM Homepage



Our CDM Bits and Bytes Blog

Have a topic suggestion for a future webinar or LCE? Please send it to cdmlearning@hq.dhs.gov





Homeland Security

Automating Hardware Asset Management: Notes from the Field

May 26, 2016

1:00 pm – 3:00 pm

A CDM Learning
Community Event



Event Goal

The goal is to discuss the automation of hardware asset management, including sharing best practices and lessons learned through experiences from the field.



Event Objectives

Hardware Asset Management

- Automation of inventory (end points, mobile devices, network devices, other)
- Automation of unauthorized devices
- “Architecture” for categorizing devices
- Device attributes
- Change Management
- Overcoming the obstacles



Ask questions!



Share experiences!



Discuss challenges and solutions!



Today's Agenda

- Welcome and overview
- Panel introductions, opening remarks
- Open discussion
- Panel closing comments
- Final remarks



Today's Speakers

- Kevin Yasuda, DOJ
- Dwayne King, OPM
- Timothy Jones, ForeScout



Cybersecurity Architect Department of Justice

- Defines, communicates, and implements the DOJ enterprise cybersecurity strategy
- At DOJ, has supported Insider Threat Prevention and Detection Program, Security Operations, Vulnerability Assessment and Penetration Testing, and IBM BigFix implementation





DOJ Cybersecurity Hardware Asset Management

OCIO, Cyber Security Staff

5/26/2016



Kevin Yasuda – Kevin.H.Yasuda@usdoj.gov

- Previously served as
 - Engineer on the DOJ Enterprise endpoint management system deployment
 - Involved in the scoring and dash boarding efforts at DOJ
 - Lead for the DOJ Vulnerability Assessment and Penetration Test Team
 - Engineer Lead for the Justice Security Operations Center
- Currently, Cybersecurity Architect and Program Manager for the DOJ Insider Threat and Prevention Program



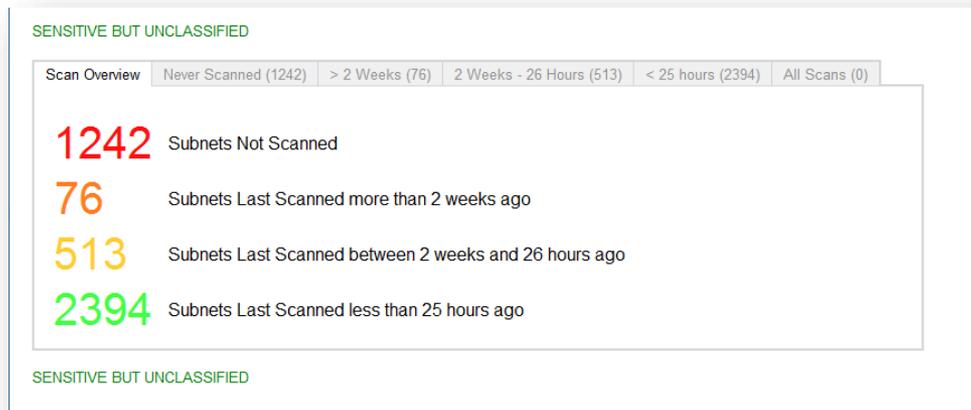
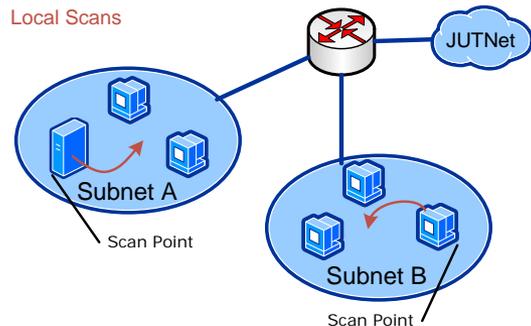
Enterprise Hardware Asset Visibility

- Implemented an enterprise endpoint management system based on an agent based technology
 - Desktops, laptops, servers
 - Developed MSI to customize agent install with unique file per administrative domain
 - Used as an identifier for Asset inventory
 - Logon GPO used for client install to capture new managed systems



Asset Discovery – Distributed Scans

- Centrally managed distributed Nmap scans with consolidated results
 - Goals: low-effort, low network impact
 - Automated scans every 25 hours
 - Identify the assets that are not “managed”





Asset Discovery

- Good to have a source of network space
 - How do you know you've looked everywhere possible for assets?
 - Current approach uses advertised route information from WAN routers
- Develop asset aging approach
 - When do you remove discovered assets, or managed devices that stop reporting
 - Current approach is 60 days
- Remember scanning considerations
 - MAC addresses are only available to scans on the same broadcast domain
 - DNS resolution requires PTR records for devices
 - Considerations for Firewalls, NATs, Proxies, IPv6 networks, etc.



Hosted System Model

- Owner:
 - The GSS, System, Site, or Accreditation Boundary that is responsible for the maintenance and management of the hardware asset
- Consumer:
 - The GSS, System, Site, or Accreditation Boundary that makes use of the hardware asset
- One to many relationship
- An asset can have one owner but multiple consumers



Asset Management

- Developed a way to automate a manual process incorporating sensor data
 - “Tag” authorized assets to system boundaries in our SA&A tool and have the functionality align with the security professionals.

Asset Management

Select Hardware Assets to map to this system

Search Parameters to filter results

Filter By:

Hostname: HW-6*

Hardware Asset Type: -All-

Operating System: -All-

Operating System Type: -All-

IP Address with Wildcard:

MAC Address with Wildcard:

Active Directory Path:

BigFix Group: DEA

Ownership: -All-

Search

Message from webpage

This rule will tag all HW assets that meet the search criteria to this system. Click OK to continue.

OK Cancel

Existing Rules

Save as Rule

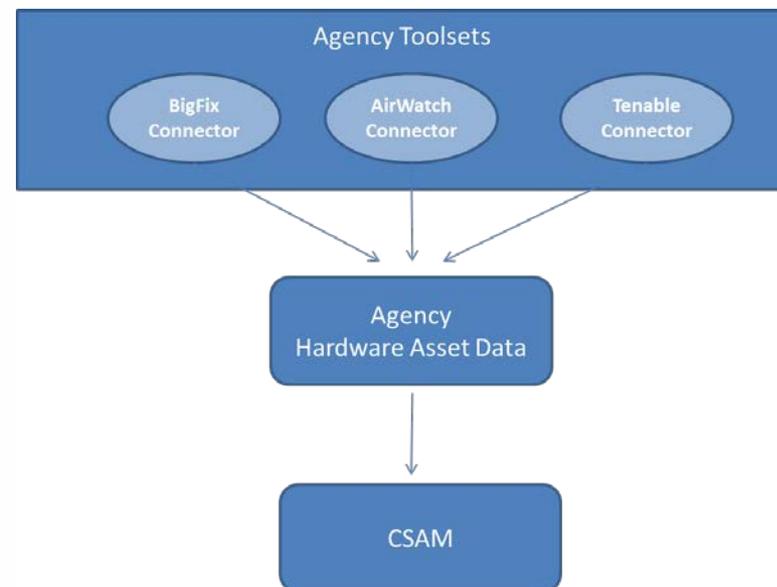
Name: HW-6* for DEA Big Fix Group

Save Cancel

Zone	Org	Hostname	Hardware Type	OS	cpu	Active Directory Path	MAC Address	IP Address	Has an Owner	
<input type="checkbox"/>	BIGFIX_DOJ	CDO	HW-60	Desktop	Win7 6.1.7601	3100 MHz Core i5-2400	cne=HW-60,ou=CDO,ou=doj,ou=gov	35-39-32-3f-71-f9	1.1.100.212	False
<input type="checkbox"/>	BIGFIX_DOJ	CDO	HW-62	Desktop	Win7 6.1.7601	3000 MHz Core 2 Duo	cne=HW-62,ou=CDO,ou=doj,ou=gov	00-0f-f3-0f-93-09	1.1.100.34	False
<input type="checkbox"/>	BIGFIX_DOJ	CDO	HW-61	Desktop	Win7 6.1.7601	3100 MHz Core i5-2400	cne=HW-61,ou=CDO,ou=doj,ou=gov	37-39-32-3a-30-29	1.1.100.220	False
<input type="checkbox"/>	BIGFIX_DOJ	CDO	HW-64	Desktop	Win7 6.1.7601	3100 MHz Core i5-2400	cne=HW-64,ou=CDO,ou=doj,ou=gov	04-03-4f-10-10-14	1.1.100.135	False

Page size: 10

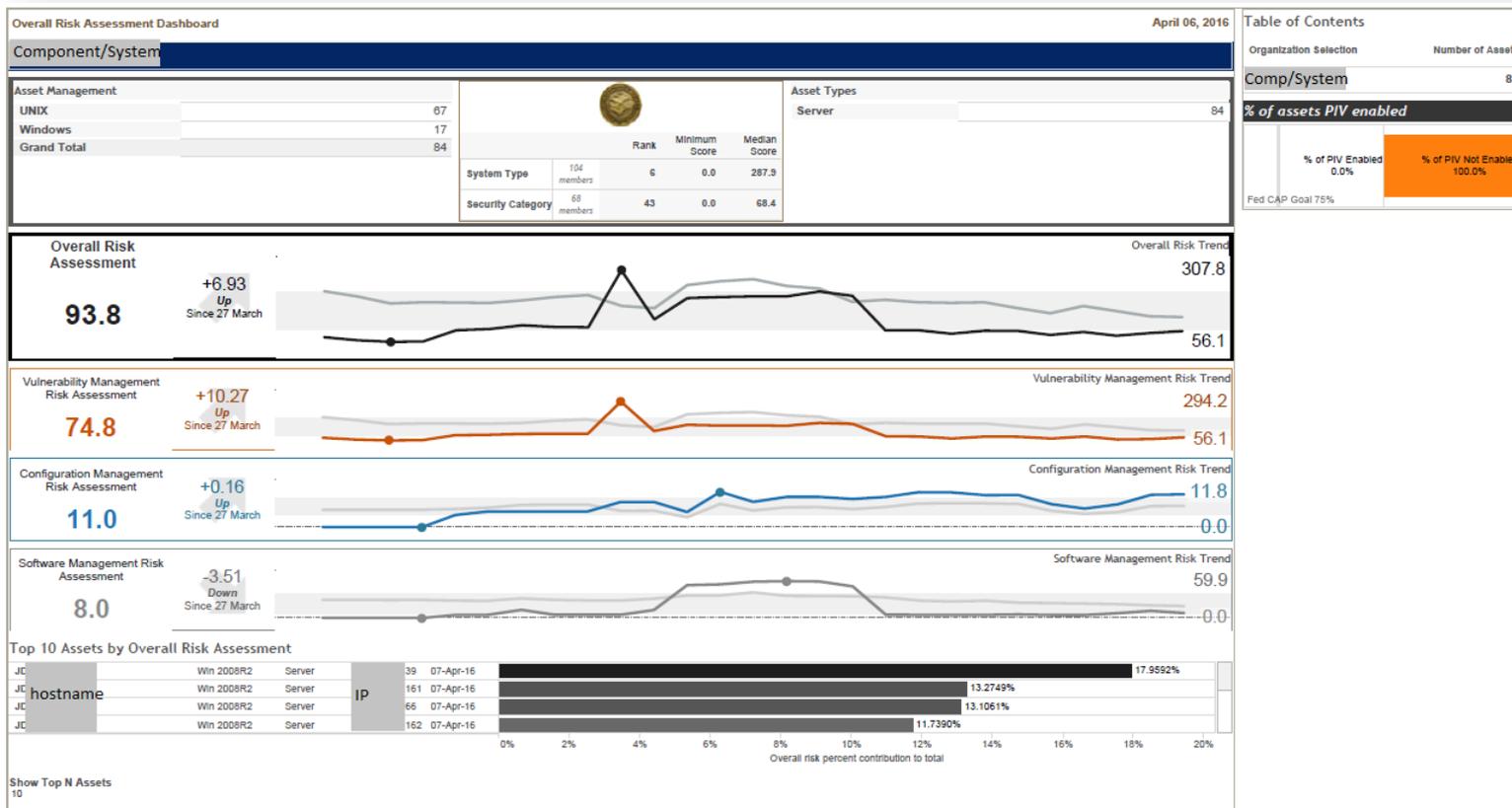
Add Selected Hardware Assets Add All Available Assets Cancel





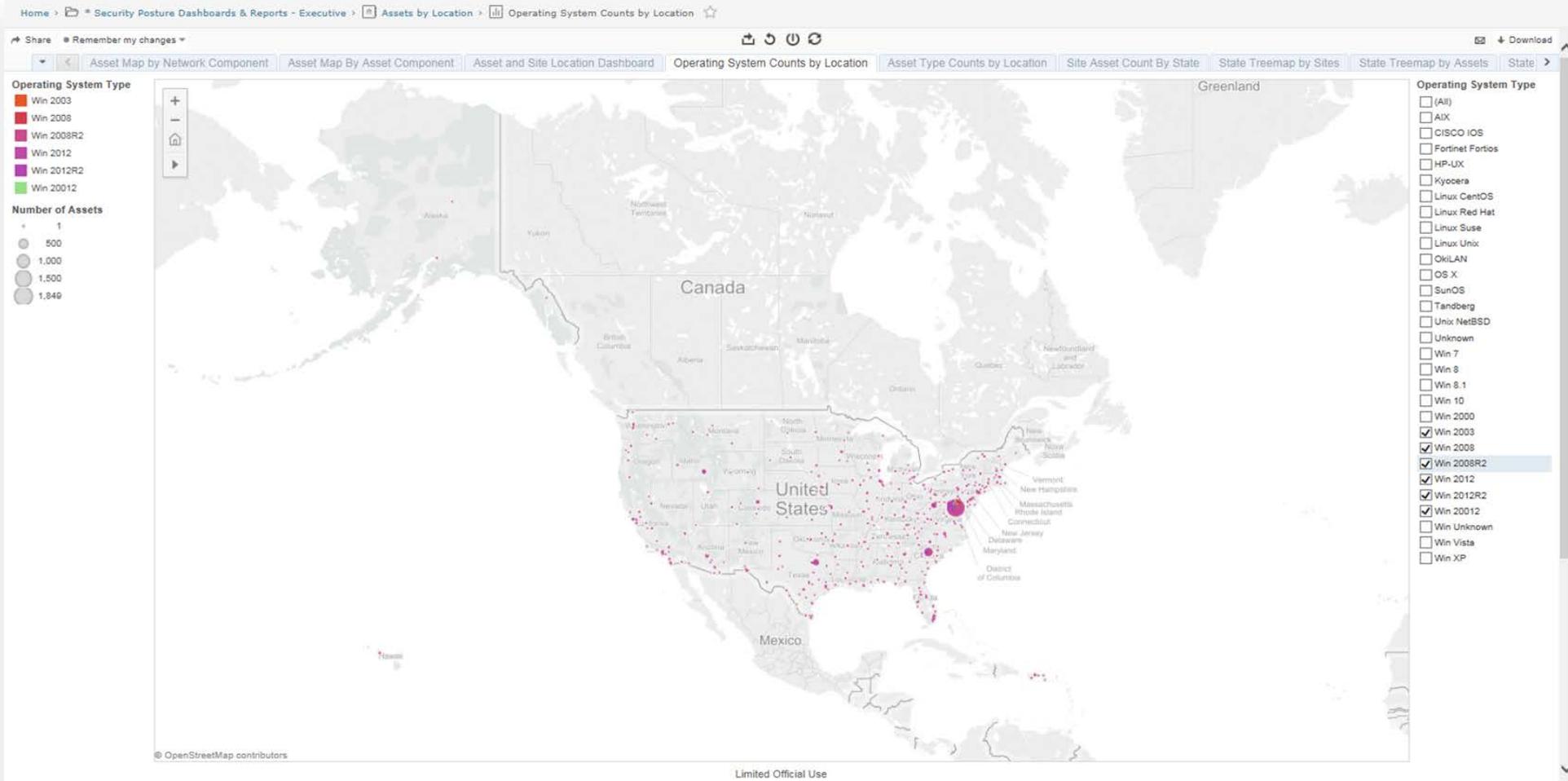
Provide Security “Scoring” against assets

- Looking at assign a score associated to “untagged” assets that resides at an organization level





Visualizing Endpoint and WAN data



Dwayne King

Senior IT Specialist Office of Personnel Management

- Implementation of CIO's CM strategy
- Project Manager of OPM's CDM program
- Previously Acting Chief for CFO's Policy and internal Controls
- Previous assignments at DHS, DOJ, and State



Dwayne King

- **Introduction to OPM environment**
- **Hardware inventory management**
 - Previous and current Conditions/Methods
 - Challenges
- **Asset Discovery**
 - CDM Planning stage
 - Policy development
 - What we discovered
 - Establishing the baseline
- **Methodology**
 - Implementation at OPM



Dwayne King

- **Challenges**

- Technical
- Administrative

- **Lessons Learned**

- Suggestions for preparation
- Background investigations
- Points of contact
- Stakeholder engagement
- Acquisitions, forms and more forms
- Configuration Management Process
- Administrator account



Timothy Jones

Enterprise Cyber Security Lead Engineer, ForeScout Technologies, Inc.

- Tim is a Lead Systems Engineer with ForeScout
- Public Sector focused on Federal Civilian Accounts
- Enterprise Cyber Security Background
- Focused on Network Security Analytical & Enterprise Architecture
- IT Security Industry for several years, and is very aware of both the DHS CDM Requirements & Phases and the technical deployment being conducted in the Federal Government today

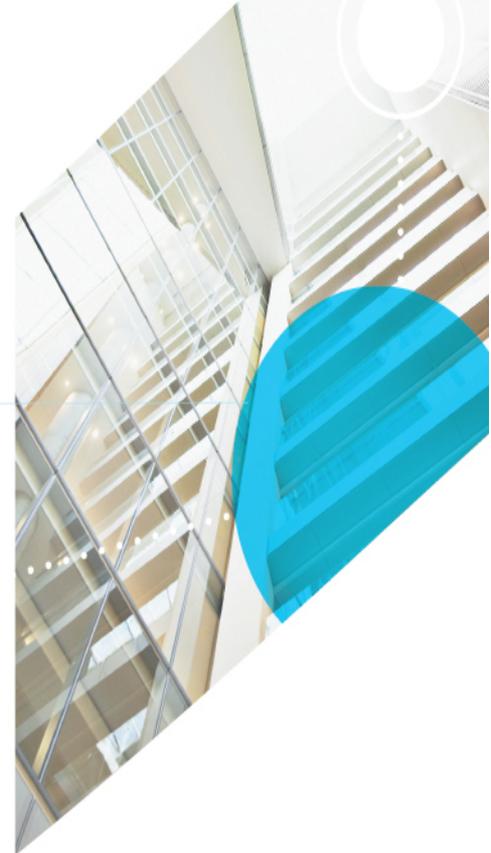




ForeScout™

The Next Step in Cyber Defense and Response

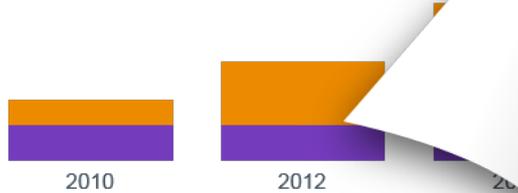
Tim Jones CISSP, CISM, CCSK, FSCA
Lead Systems Engineer
ForeScout Technologies, Inc.



The Challenging Threat Landscape



Less than 10% of new devices connecting to the corporate environment will be manageable through traditional methods

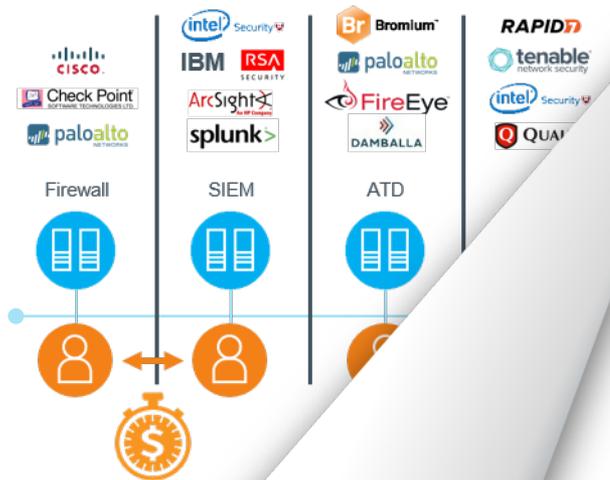


Source: Gartner, BI Intelligence, Verizon, ForeScout

Number of unmanaged devices is exploding

Dec 2014: “Within two years, 90% of all IT networks will have an IoT-based security breach”





Human beings

SecOps

Fragmented security lets attackers in

“70 to 90 percent of all malicious incidents could have been prevented or found sooner if existing logs and alerts had been monitored”

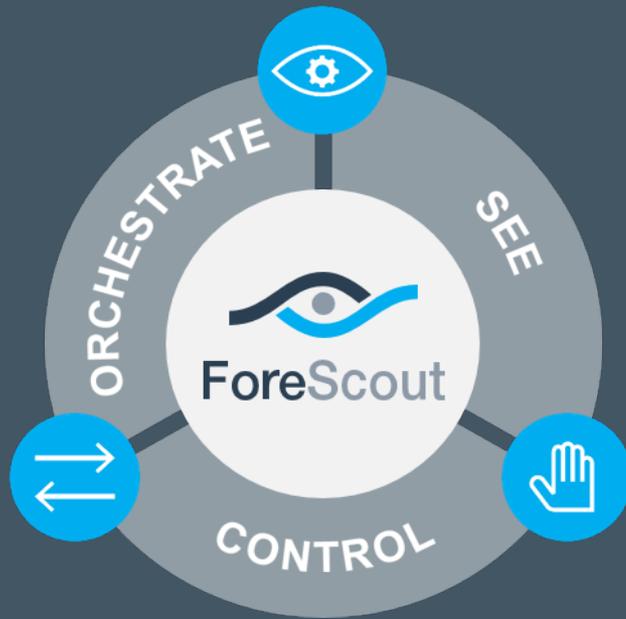
Verizon Data Breach Investigations Report

“Average time to contain a cyber attack is 31 days”

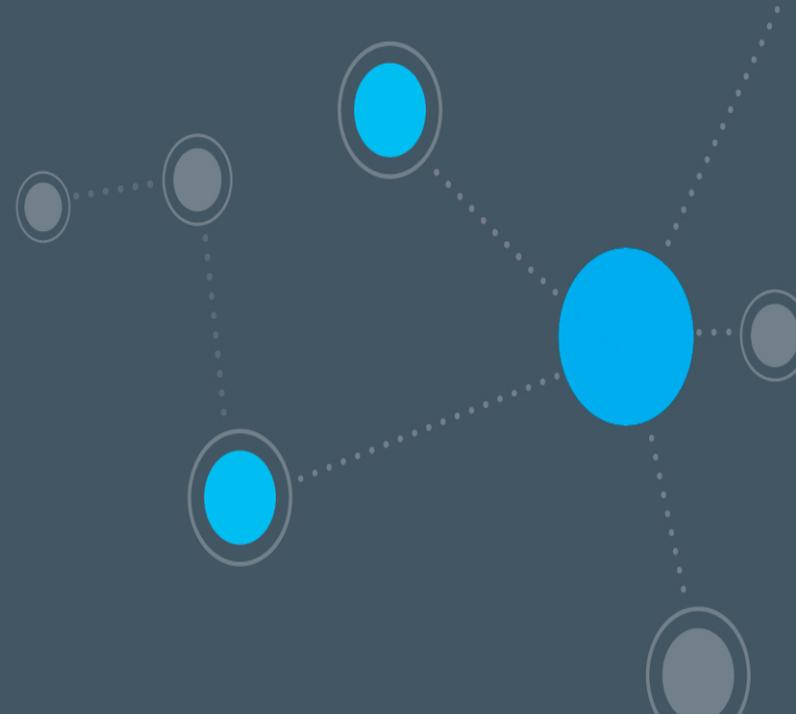
Ponemon Institute “2014 Global Report on the Cost of Cyber Crime”

5 Key CDM Gaps...

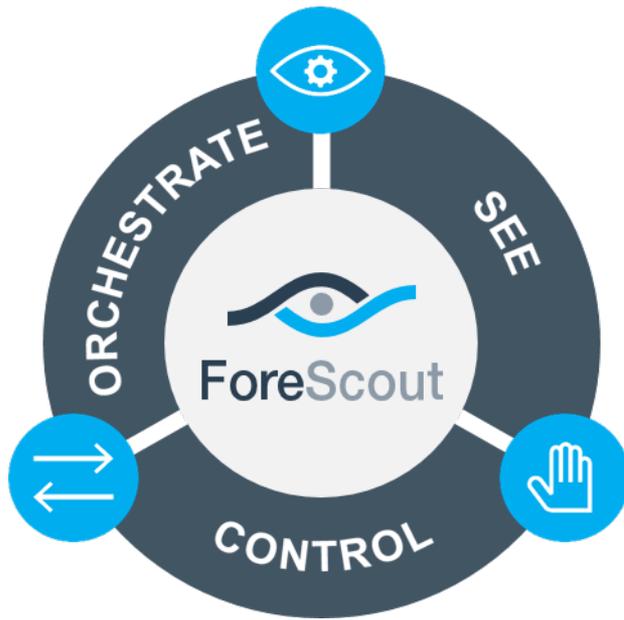
- **GAP 1:** Difficulties persist in detecting every device connecting to classified and unclassified networks
- **GAP 2:** Difficulties with automated classification of non-traditional IP-enabled devices connecting to networks
- **GAP 3:** Significant difficulties in identifying non-manageable devices connecting to the network
- **GAP 4:** Significant difficulties still persist in removing unauthorized or non-compliant devices from networks
- **GAP 5:** Difficulties in ensuring that all required software components are persistently present and operational on all devices



ForeScout Solution



ForeScout Benefits



Real-time visibility

- No gaps
- No agents

Broad range of responses

- User
- Network
- Endpoint
- Existing IT systems

Information sharing and automation

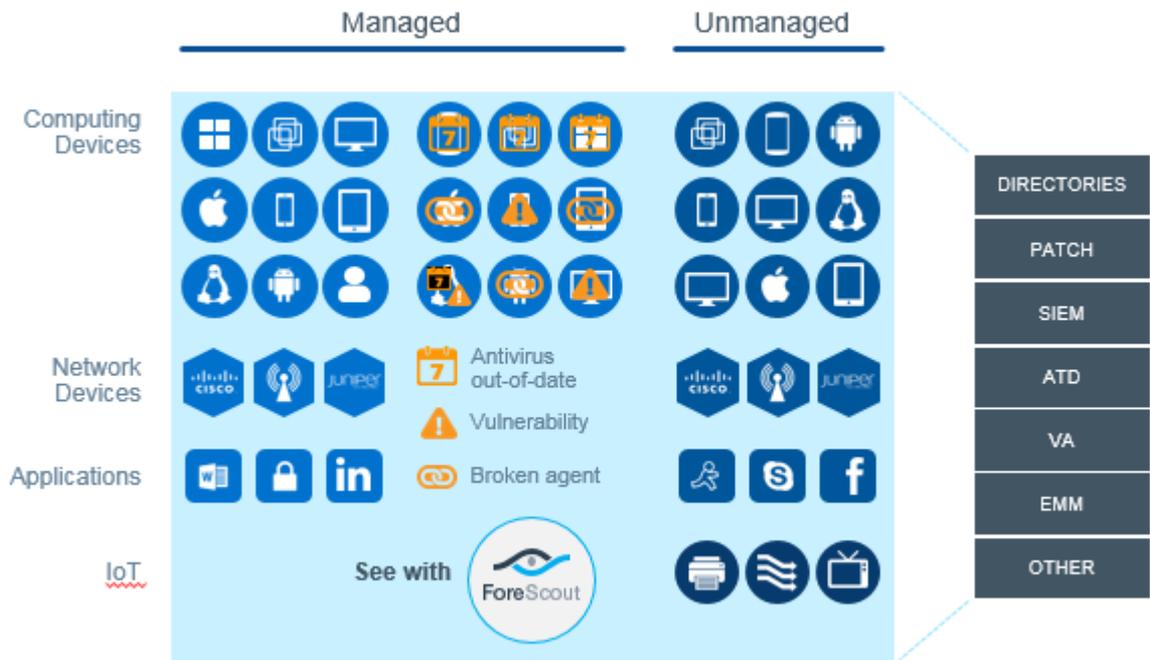
- Reduce security fragmentation
- Speed incident response

See



AGENTLESS

CONTINUOUS



Answers to Your Questions...



Who are you?

- Employee
- Partner
- Contractor
- Guest



Who owns your device?

- Corporate
- BYOD
- Rogue



What type of device?

- Windows, Mac
- iOS, Android
- VM
- Non-user devices, IoT



Where/how are you connecting?

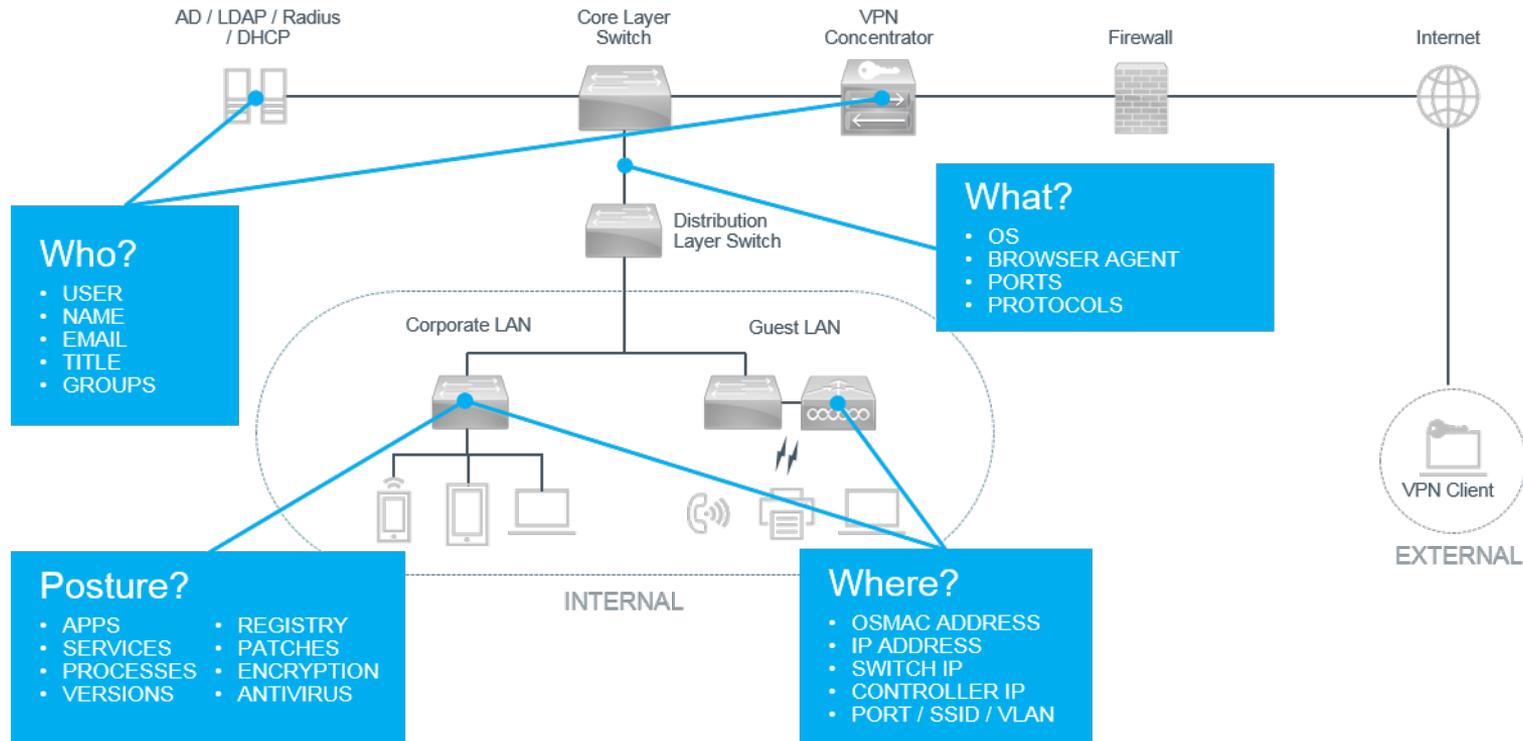
- Switch/Port/PoE
- Wireless/Controller
- VPN
- IP, MAC
- VLAN



What is the device hygiene?

- Configuration
- Software
- Services
- Patches
- Security Agent

How WE Detects and Inspects Devices



See Levels

CLASSIFY - CLARIFY - ASSESS



- Device Type
 - Windows, Macintosh, Linux, Mobile, Network device, IoT, Printer, VOIP, etc.
 - OS Type
 - Hardware properties such as NIC vendor (MAC address)
 - Switch information
- Corporate Managed/Unmanaged
 - Manageable (Domain/Local/Secure Connector)
 - User information
 - Directory information
 - Device ownership
 - Connection Type (LAN, WAN, Wireless, VPN)
 - IP Assignment (DHCP, Static)
 - Geographic Location
- Compliance Policies
 - Authorized applications installed/running
 - Rogue applications installed/running
 - Anti-virus agents status (installed/running) and database versions
 - Patch management agent status (installed/running)
 - P2P/IM clients installed/running
 - Number of devices on any port
 - Member of Corporate domain
 - Network adapter (DeviceID, name, adapter type and speed)
 - Firewall status (installed/running)
 - Registry and configuration
 - Patch level

Type of Information WE Need to Learn



Device
Type of device
NIC vendor
Location
Connection type
Hardware info
MAC and IP address
Certificates



User
Name
Authentication Status
Workgroup
Email and phone number



Operating System
OS Type
Version number
Patch level
Services and processes installed or running
Registry
File names, dates, sizes



Applications
Installed
Running
Version number
Registry settings
File sizes



Security Agents
Anti-Malware/Virus/DLP agents
Patch management agents
Encryption agents
Firewall status
Configuration



Network
Malicious traffic
Rogue devices



Peripherals
Type of device
Manufacturer
Connection type

Open Discussion

What is the impact of ...??

What about??

How did the stakeholders adjust to??

What would you do differently about??

What should I do about??

What would you recommend for??

How much time did it take to??

How are you maintaining 95% compliance with HWAM CAP....??

How did you handle ... (latency, centralization, control issues, etc.) ??



Event Conclusion

Thank you for attending today's CDM Learning Community Event!

- A certificate of attendance will be available to download on the CDM Learning Program website at www.us-cert.gov/cdm/training, within one week of today's event
- Visit our website to learn more about the CDM Learning Program and upcoming events at www.us-cert.gov/cdm
- For any questions, comments, or suggestions for future topics, please email us at cdmlearning@hq.dhs.gov



The CDM Learning Program

CDM Learning Program – What’s in it for you:

- Monthly Learning Community Event (CDM-LCE)
 - CDM leaders and implementers discuss relevant CDM topics in-depth, either in a live face-to-face session or using a virtual platform such as AvayaLive!
- Monthly Webinars
 - CDM experts deep-dive into specific CDM topics and participants are able to ask relevant questions using a text-chat function
- Weekly CDM Bits & Bytes
 - Short email awareness tips that link to additional content posted to the CDM Learning forum on GovLoop
- Online Vignettes
 - Short video vignettes which allow the learner to develop foundational knowledge around key CDM concepts and topics

Resources Available: <https://www.us-cert.gov/cdm>



Homeland
Security

Federal Network Resilience

Sign up for our blog!

<https://www.govloop.com/groups/cdm-learning-bits-bytes/>

CDM LEARNING – BITS & BYTES



Group Admins



Public Group active 18 hours, 47 minutes ago

The CDM Learning Community is designed to enhance cybersecurity risk management by fostering a CDM learning environment that increases Departments and Agencies awareness and knowledge about the CDM program and offer a place to exchange best practices for implementing and maintaining the CDM program.

[Home](#)

[RSS](#)

Show:

— Everything —



[Forum](#)

[Members](#)

11

FEATURED



CAREER

6 Tips for Keeping Your Cool During Difficult Conversations



CAREER

11 Tips to Keep You Motivated at the Office This Summer



CITIZEN ENGAGEMENT

Making the Case for Communications in the Cabinet



KNOWLEDGE NETWORK
FOR GOVERNMENT



Homeland
Security

Federal Network Resilience