THREAT HUNTING:

A PROACTIVE TECHNIQUE FOR FINDING SOPHISTICATED CYBER THREATS

September 27, 2017
Morgan Reynolds
Chris Horvath
U.S. Department of the Interior Office of Inspector General

OFFICE OF
INSPECTOR GENERAL
U.S. DEPARTMENT OF THE INTERIOR

Today's cyber attacks are increasingly dangerous and targeted, designed by advanced actors to damage or disrupt critical U.S. infrastructure that deliver vital services*

*The President's National Infrastructure Advisory Council August 2017 Report, "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure"

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

U.S. Power Grid Hacked!

- Security firm Symantec reported that a series of recent hacker attacks known as the Dragonfly 2.0 campaign, not only compromised energy companies in the United States and Europe but also resulted in the intruders gaining hands-on access to power grid operations that could have been used to cause blackouts in the United States.
- Symantec traces attacks back to at least December of 2015, but found that they ramped up significantly in the first half of 2017, particularly in the US, Turkey, and Switzerland.
- Analysis found that they began with spear phishing emails that tricked energy sector victims into opening a malicious attachment that was a fake invitation to a New Year's Eve Party in order to steal the victims credentials and access their computers.
- Attackers also used watering hole attacks by compromising websites commonly used by the energy sector to steal credentials

*Symantec Security Response- "Dragonfly: Western energy sector targeted by sophisticated attack group," September 6, 2017 https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

December 2016 and December 2015 Ukraine Power Grid Attacks

- In two separate attacks, industrial control systems operated by Ukrainian electric power distribution companies were infected with sophisticated malware.

- Once infected, the remote attackers caused Ukraine power companies' industrial control systems to malfunction, which resulted in power outages affecting hundreds of thousands of customers.

December 2016 and December 2015 Ukraine Power Grid Attacks

- Remote attackers put malware on the industrial control systems by sending emails with malicious payloads to employees that operated the industrial control systems.

- When the employee accessed the email and downloaded a file or clicked a link in the email, the employee's computer was infected giving the remote attacker a foothold on the organization's computer network.

- These cyber threats bypassed firewalls and went undetected by the organization's intrusion detection system and antivirus software. The use of group accounts (accounts shared by multiple individual users) on these systems made it harder to detect inappropriate logons and activity.

December 2016 and December 2015 Ukraine Power Grid Attacks

Malware analysis performed by DHS in conjunction with US private sector IT security firms determined that **the affected entities were breached about nine months prior to the outages!**

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

December 23, 2015 – Western Ukraine Electric Utility Provider Hacked - Video

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Source: YouTube (C&M News) https://www.youtube.com/watch?v=8ThgK1WXUgk

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Cyberattack on New York Dam by Iranian Hacktivists

- An Iranian hacktivist group claimed responsibility for a cyberattack that gave it access to the Bowman Avenue Dam in Rye Brook, New York
- Did not control or harm the dam, but this compromise is just the tip of the iceberg

Targeted Malware

Malware Name	Description
STUXNET	• First confirmed example of ICS tailored malware • Designed to sabotage the Iranian nuclear project and was used to attack Iran's centrifuges in 2009 and 2010.
Dragonfly/HAVEX	• Dragonfly campaign was an espionage effort that targeted over 2,000 ICS locations and leveraged the HAVEX malware • HAVEX used to map out the industrial equipment on the ICS network

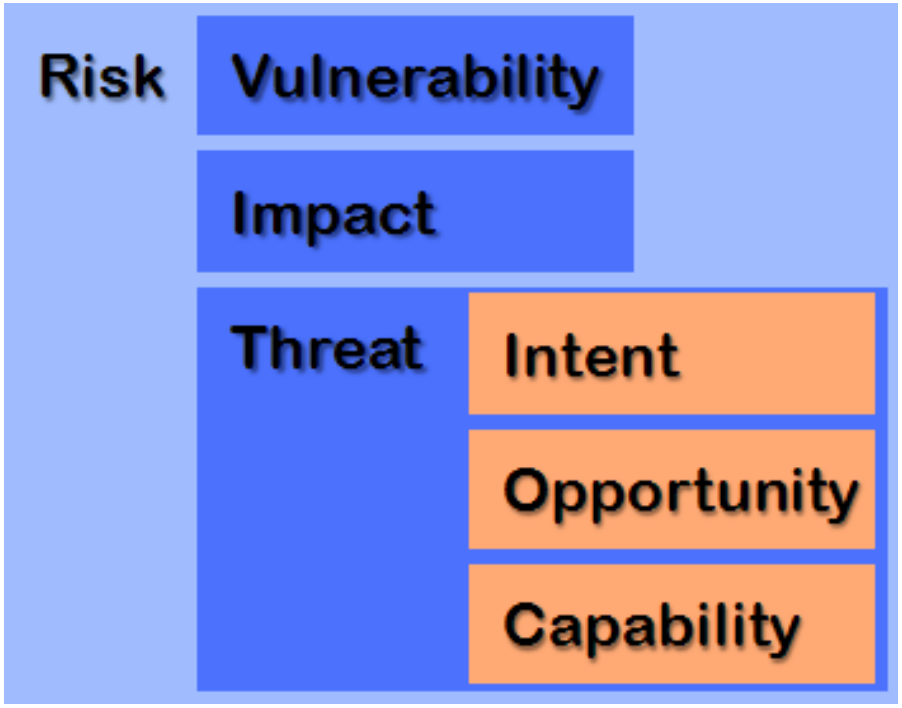
*Source- DRAGOS, INC. "Analysis of the Threat to Electric Grid Operations" https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Targeted Malware

Malware Name	Description
BLACKENERGY	• Designed to conduct DDoS, cyber espionage and information destruction attacks. Used to attack ICS and energy markets around the world in 2014. • Ukraine Cyber Attack 2015- BLACKENERGY3 used by adversaries to gain access to the corporate networks of power companies and then pivot to the SCADA networks
CRASHOVERRIDE	• Ukraine Cyber Attack 2016- employed on the Ukraine transmission substation which impacted the operations of the electric grid operations • First ever malware framework designed and deployed to attack electric grids

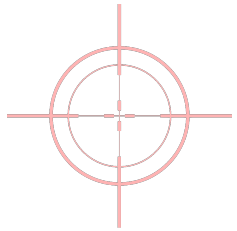
*Source- DRAGOS, INC. "Analysis of the Threat to Electric Grid Operations" https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

A Proactive Approach to IT Audit



Source- Mike Cloppert, "Security Intelligence: Introduction (pt 2)," SANS Institute Digital Forensics and Incident Response Blog, July 23, 2009
https://digital-forensics.sans.org/blog/2009/07/23/security-intelligence-introduction-pt-2/

- Traditionally, IT Audits have been focused on helping to identify vulnerabilities
- Threat hunting is focused on identifying and communicating active threats to incident responders



Overview

1. What is threat hunting?

2. Why is threat hunting is necessary?

3. Overview of the "hunt"

4. Threat hunting in action at the U.S. Department of the Interior

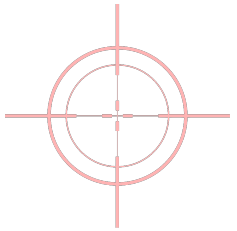
5. How do we integrate threat hunting in to the IT audit function?

What is Threat Hunting?

- **Combating nation-state cyber threats requires acknowledging that traditional cyber defenses** such as firewalls, intrusion detection systems, and antivirus software, **often fail to deter or detect sophisticated malware**.

- Thus, the organization **should assume its computer networks and systems are already compromised** and search them for hidden malware.

- This proactive approach is referred to as "**threat hunting**" and includes but is not limited to analyzing computer network traffic for malicious content and dissecting computer memory to find malware.



What is Threat Hunting?

Network Traffic Analysis	Memory Forensics
• Computers infected with malware **often produce network traffic matching a known pattern or signature which can be detected by capturing the traffic** and analyzing it with a software tool.	• Operations performed on a computing device by both legitimate users and adversaries **modify the device's memory (RAM), leaving evidence of their actions on the device.**
• Malware infections may also be detected by analyzing network traffic **to determine whether a computer on the organization's network is communicating with a known malware command and control site.**	• Memory forensics is an integral part of threat hunting and **involves acquiring RAM off network devices and analyzing its contents to identify artifacts that may indicate compromise, malicious code and processes, and abnormal network connections,** and assess the impact of the compromise on the network.

Why is Threat Hunting Necessary?

- **Rapid increase in targeted and sophisticated threats from nation-states such as Russia, China, and Iran.**

- **Adversaries** research and perform reconnaissance so that they can get into networks and compromise systems **without detection**.

- Threat hunting searches **for these adversaries who are already within the organization's networks and systems or were present in the past**

Why is Threat Hunting Necessary?

- Industrial controls systems (ICS) are the IT systems used to control electrical, mechanical, hydraulic, or pneumatic components to achieve a physical outcome.

- ICS play a key role in the operation of the Nation's critical infrastructure including power plants and dams as well as energy production, distribution, and transportation systems.

- For example, industrial control systems operate circuits that transmit electricity from a dam to a substation and open and close valves to control flow in an oil pipeline.

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

DHS's Industrial Control Systems Cyber Emergency Response Team reported 290 cyber-attacks on critical infrastructure control systems in fiscal year 2016*

*The President's National Infrastructure Advisory Council August 2017 Report, "Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure"

Why is Threat Hunting Necessary?

- Since 2009, DHS has issued alerts and advisories about suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure monitored and controlled by industrial control systems.

- **ICS are increasingly vulnerable to targeted malware** which enables an attacker to cause an infected ICS to malfunction.

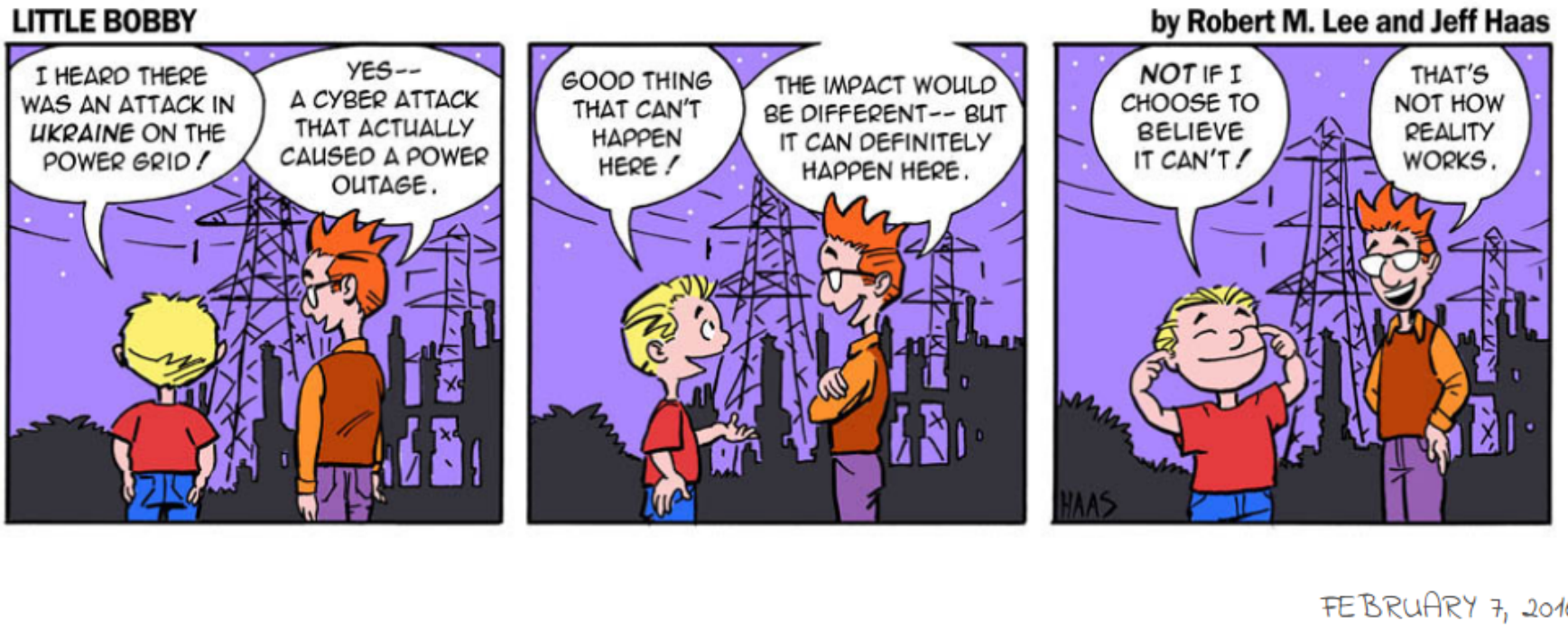
    - For example, the attacker may prevent valves on an oil pipeline from opening or closing as needed or **cause turbines in a hydropower generator to spin at dangerously high speeds.**

Why is Threat Hunting Necessary?

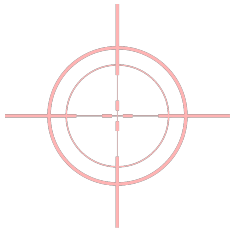
- Historically, ICS networks were physically isolated from an organization's traditional IT systems as well as from the internet and thus could be protected from unauthorized access using physical security measures like guards, fences, and locks.

- Over time, to promote connectivity, efficiency, and remote access capabilities, ICS have become interconnected with an organization's traditional IT systems rendering physical measures alone to secure these networks inadequate.

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR



Source: http://www.littlebobbycomic.com/projects/week-54/



Overview of "The Hunt"

1. **Where and how to start:**

    - What are my organization's mission operations and what IT systems support them?
    - What sensitive data does my organization maintain?
    - Where are my organization's mission critical IT systems and sensitive data located?
    - Who are the adversaries that would want to disrupt our mission operations and steal our data?

2. **Determine what and how data / artifacts will be acquired** (network packets captures, RAM captures, etc.)

3. **Ensure rules of engagement in place when directly interfacing with systems**

Overview of "The Hunt"

4. **Acquire data / artifacts** (using network packet capturing appliance, RAM acquisition tools, etc.)

5. **Analyze data / artifacts** (using network/protocol analyzers, RAM forensics tools, etc.)

6. **Validate findings**

7. **Provide recommendations for remediation**

Control Deficiencies IT Auditors Can Identify as a Byproduct of Threat Hunting

- Is the network isolated from the internet and business networks?
  - **All of our example ICS compromises occurred because the ICS was not isolated from the organization's business network**
- Unauthorized devices on the network
- Failure to implement least privilege and least functionality
- Weak passwords
- Unauthorized network services (e.g. Telnet)


Threat Hunting at the
U.S. Department of the Interior

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Threat Hunting In Action: U.S. Department of the Interior

DOI **spends about $1 billion annually on its information technology asset portfolio**, which includes computer systems that support a range of bureau programs that—

- protect and manage our Nation's natural resources and cultural heritage;
- provide scientific and other information to stakeholders interested in those resources; and
- help meet responsibilities to American Indians, Alaska Natives, and affiliated Island communities.

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Threat Hunting In Action: U.S. Department of the Interior

- **U.S. Bureau of Reclamation is the nation's second largest producer of hydroelectric power** accounting for 15 percent of U.S. annual hydropower output.

- Annually, USBR hydroelectric plants generate over **40 billion kilowatt hours of electricity meeting the residential needs of over 3.5 million homes.** The electricity is primarily **produced at 53 hydroelectric power plants** operated by USBR.

- Hydroelectric dams **are classified by the Department of Homeland Security as critical infrastructure.**

- **USBR relies on industrial control systems to operate its hydropower dams.**

U.S. DEPARTMENT OF THE INTERIOR
BUREAU OF RECLAMATION

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

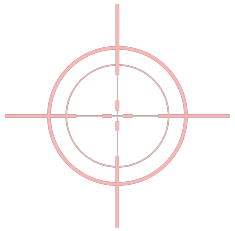
Threat Hunting In Action:
Background / Scope / Methodology

Background: Assess the Department's practices for protecting USBR Dams categorized as Critical Infrastructure from emerging cyber threats.

Scope: Bureau and Department staff, business systems, industrial control systems, and contractors that oversee, operate, manage and support the USBR dams categorized as Critical Infrastructure.

Methodology:

- Interviews with DOI / USBR
- Review of network diagrams and security documentation
- Federal and Department policies and procedures and industry best practices for protecting critical infrastructure against cyber threats
- Site visits and walkthroughs
- Network packet and RAM captures on ICS and business systems
- Technical testing and analysis
- Consultation with leading industry experts (SANS: Alan Paller, Mike Assante, Robert Lee)
- Benchmarking USBR security practices with U.S. Army Corp of Engineers and Tennessee Valley Authority



Threat Hunting In Action:
Network Packet Captures and Memory Forensics

For our evaluation of cyber security practices for systems operating USBR major hydropower dams we performed the following:

Network Packet Capture Analysis:

- Captured close to 2TB worth of data (30 million TCP/IP packets!)
- Replayed 30 million captured packets through signature (Suricata) and anomaly-based (BRO) IDS to detect indicators of compromise
- Confirmed the ICS was isolated from business systems and the internet.
- Confirmed accuracy of USBR provided hardware asset inventory using packet/protocol analyzer (CyberLens)
- Utilized the following tools: BRO Intrusion Detection System (IDS), Suricata IDS, CyberLens GRASSMARLIN, TCPDump, Wireshark, Network Miner

Memory Forensics:

- Analyzed memory (RAM) captures from key computer servers and workstations on the ICS and business system networks to identify indicators of compromise such as malicious code, unusual ports/protocols, and suspicious network connections
- Utilized tools such as Volatility, DumpIt

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Threat Hunting: Enhancing Testing of Security Controls

Malicious Code Protection (SI-3)

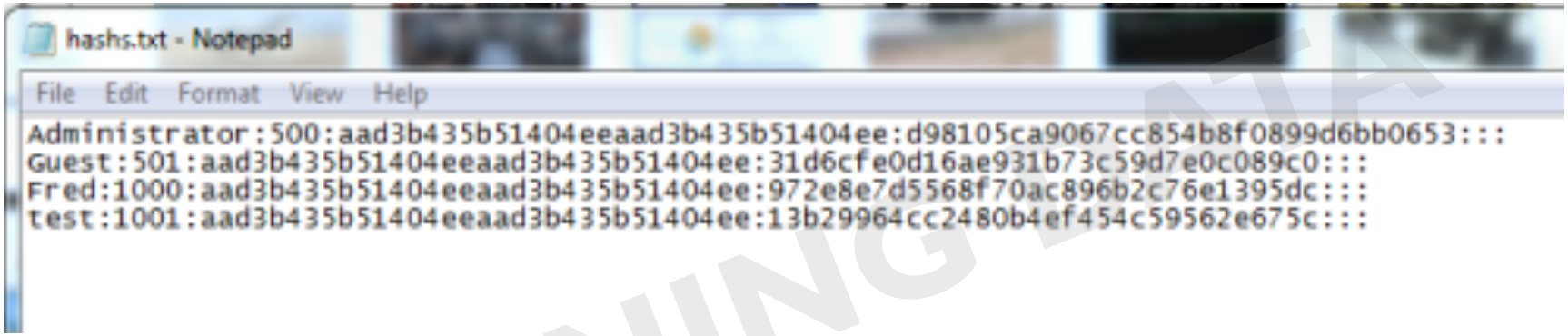
Memory forensics and network packet captures allow for identification of active and dormant malware.

Malware can hide, but it must run ~SANS Institute

Threat Hunting: Enhancing Testing of Security Controls

Account Management (AC-2)

Memory forensics can support the identification of credentials used on that asset to authenticate to the network.



OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Threat Hunting: Enhancing Testing of Security Controls

Media Use (MP-7)

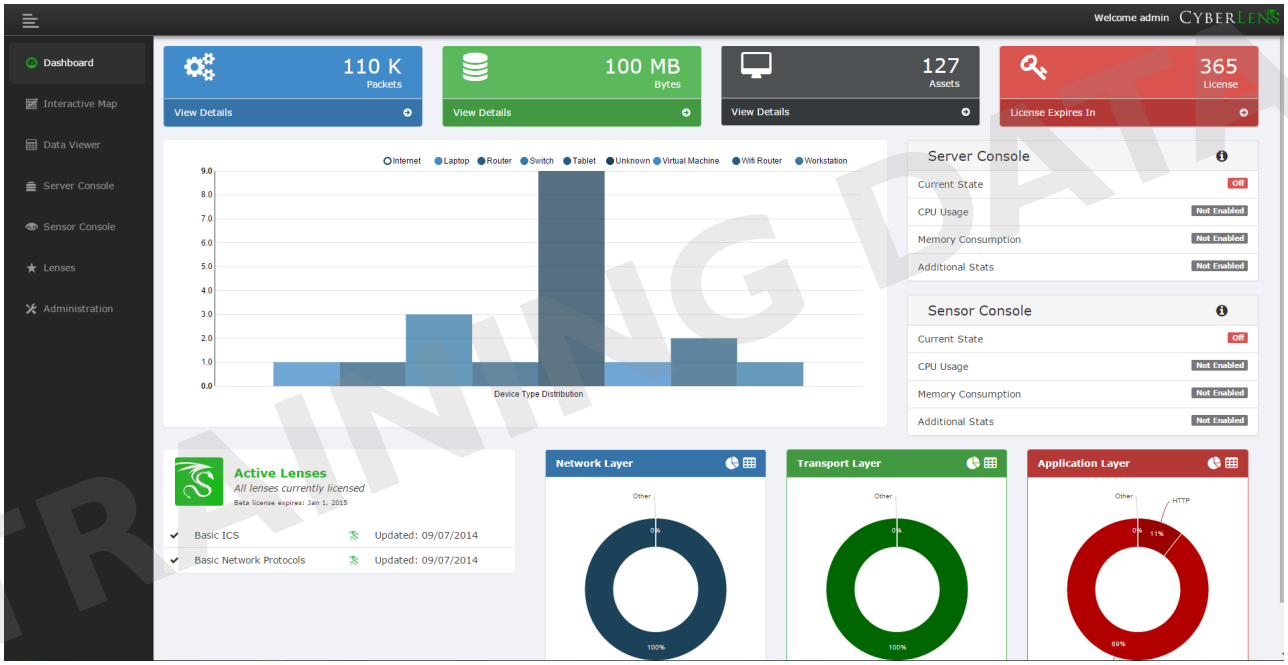
- Memory forensics can support the validation of mechanisms in place to limit media usage (e.g. USB drives, etc)
- Can look for physical port blocking devices

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Threat Hunting: Enhanced Testing of Security Controls

Least Functionality (CM-7)

Network packet captures support the validation of which ports, services and protocols are being used across the network and if they are approved or not.

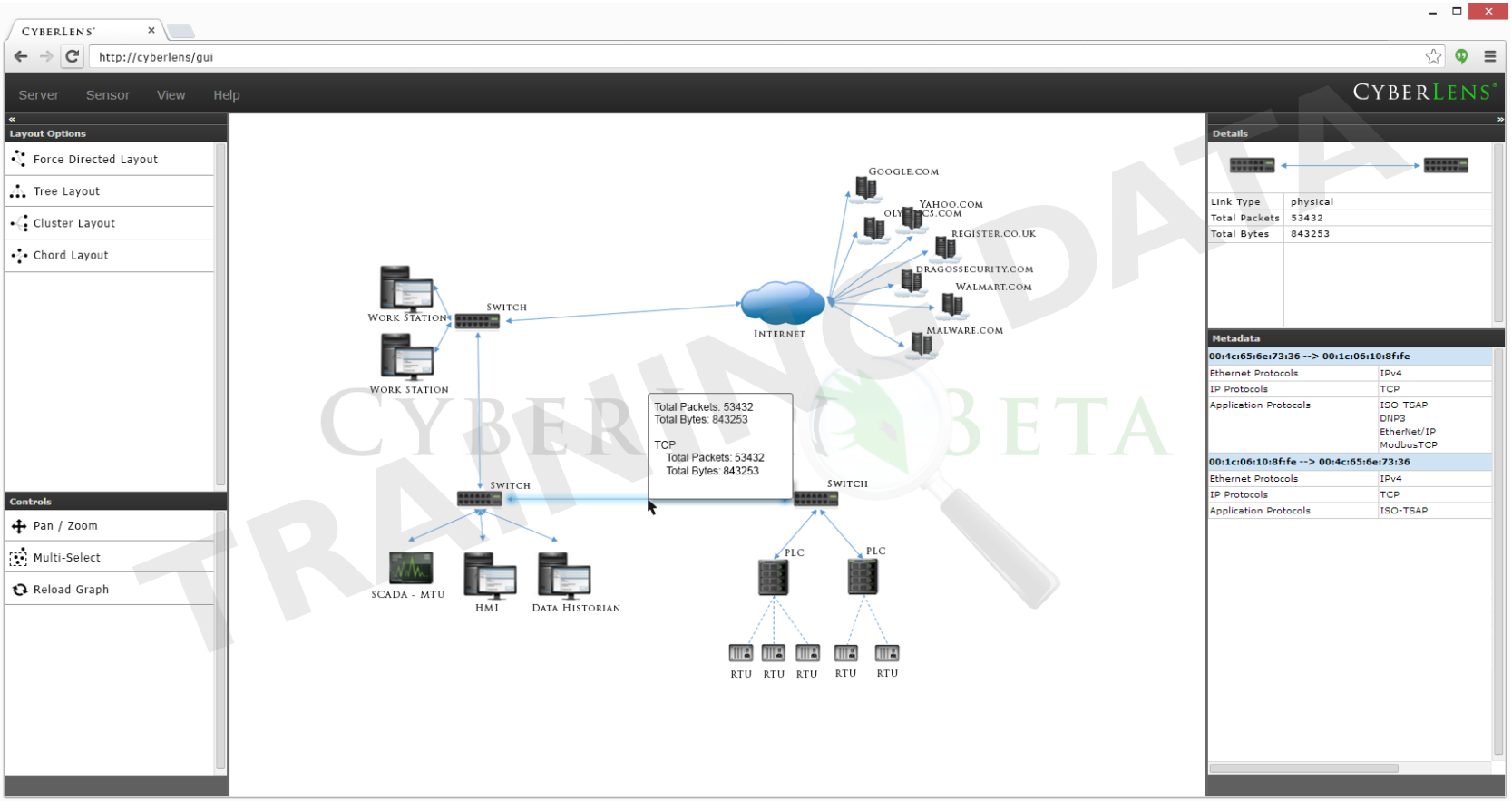


OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Threat Hunting: Enhanced Testing of Security Controls

Information System Component Inventory (CM-8)

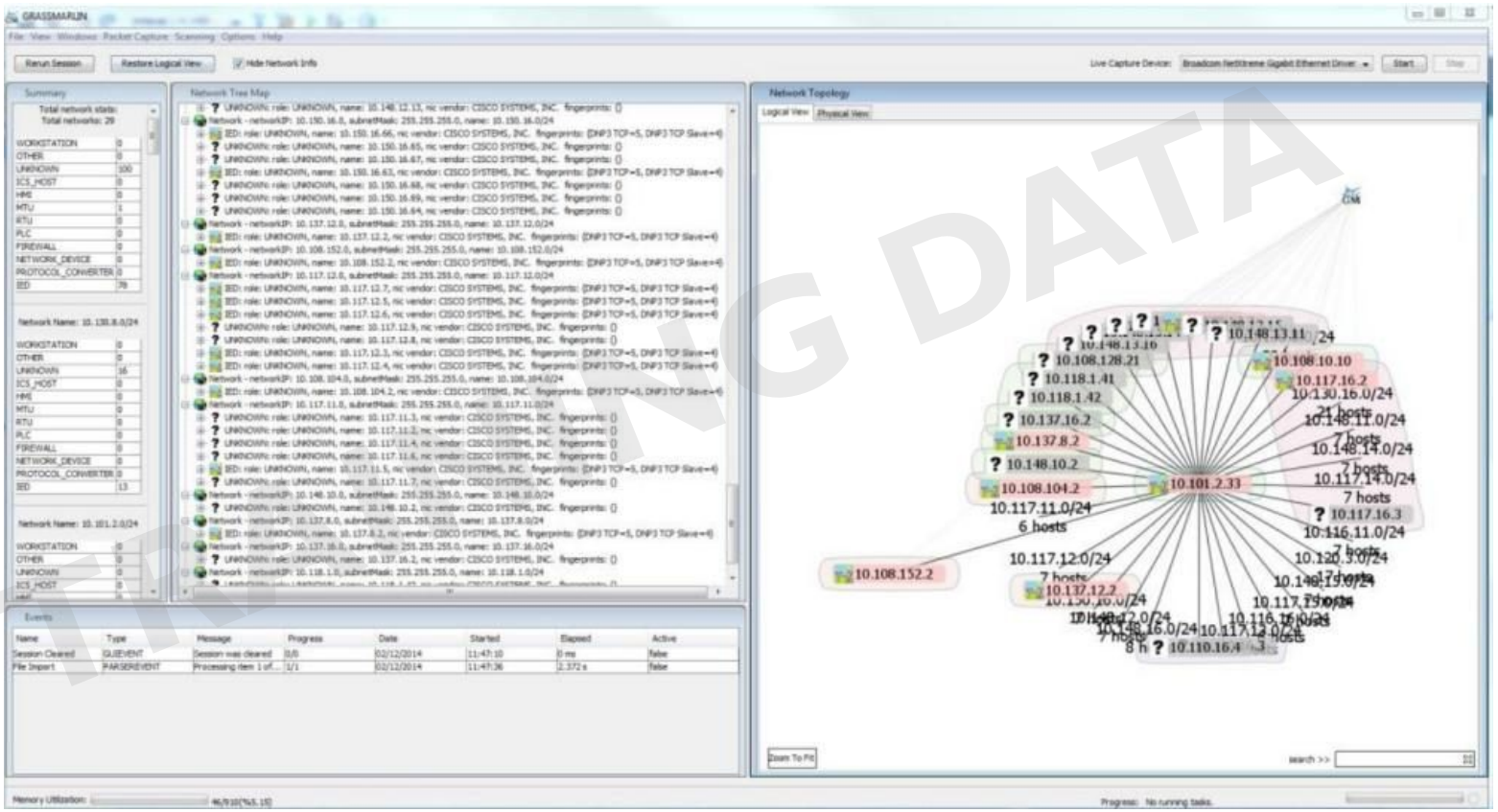
Network packet captures allow for a mapping of all assets on the network.



Threat Hunting: Enhanced Testing of Security Controls

Information System Component Inventory (CM-8)

Network packet captures allow for a mapping of all assets on network.

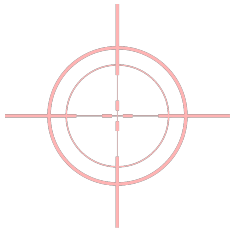



How do we integrate threat hunting into the IT audit function?

Threat Hunting Within the IT Audit Function - Benefits

Incorporating proactive threat hunting techniques in to the IT Audit function:

- Enables teams to **assess risks and test security controls**
- Provides **tangible evidence to add impact** to findings
- Provides **access to "bigger picture"** beyond internal controls
- **Enhances testing of controls**, requirements and standards (e.g. NIST)
- Allows IT auditors **to be in the trenches**
- Provides **new methods for obtaining artifacts** for testing



Threat Hunting- Where to Begin

- Identify potential projects suitable for threat hunting
- Get buy-in from Senior IG and Agency leadership
- Participate in relevant technical trainings (ex. ICS-CERT, SANS, Volatility)
- Create a lab environment to practice threat hunting techniques, learn, and analyze data
- Build relationships with industry experts (SANS, USACE, TVA)
- Acquire appropriate software (CyberLens, Volatility, GRASSMARLIN, etc.)
- Build or buy network packet capture devices with high capacity encrypted storage
- Utilize high-powered workstations for honing skills and analyzing data
    - Encrypted external drives (Two 8TB drives)
    - 64 GB RAM, 1TB SSD HD
    - Xeon CPU E3-150M @ 2.8GHz (Quad core)

Network Packet Capture Device

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

Questions?

Morgan Reynolds, IT Auditor
morgan_reynolds@doioig.gov

Christopher Horvath, IT Auditor
christopher_horvath@doioig.gov

Jefferson Gilkeson, DOI OIG Director, IT Audits
jefferson_gilkeson@doioig.gov