Threat Hunting Does Not Have to be Hard

Don C. Weber - @cutaway

Principal Consultant, Founder

Cutaway Security, LLC / Don C. Weber

- Masters Degree in Information Assurance
- IACS Security Program Maturity
- IACS Security Assessments
- Penetration Testing
- Cybersecurity Research

Agenda

- Understanding Threat Hunting
- Threat Hunting Methodology
- Threat Hunt Examples
- Summary
- Questions (possibly afterwards)

Image Source: AI generated on MidJourney on March 21, 2024

Understanding Threat Hunting

What I learned Helping a Mid-Western Generation / Transmission Team

Buckle Up, we have a LOT to cover….

What this Presentation “Is Not” and “Is”

<u>IS NOT</u>: Advanced Threat Hunting using Cyber Threat Intelligence

Joe Slowik’s “Developing an Intelligence-Driven Threat Hunting Methodology”

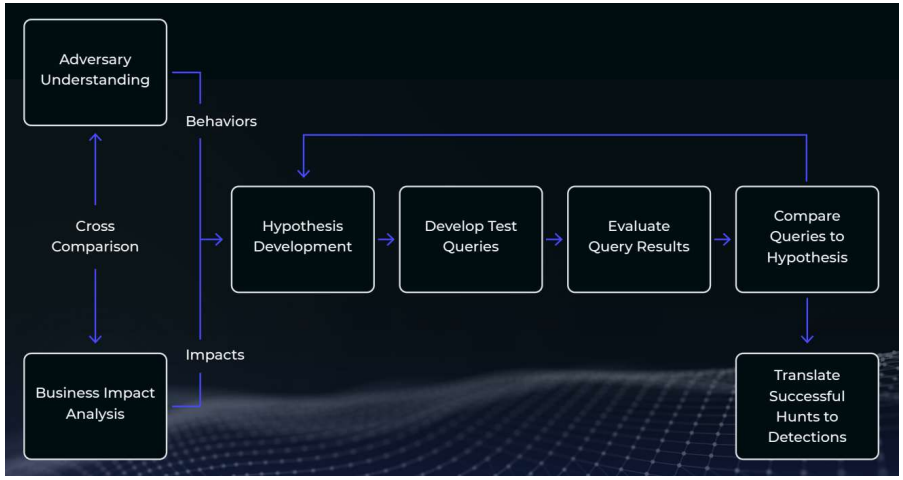


Image Source: https://www.gigamon.com/content/dam/resource-library/english/white-paper/wp-intelligence-driven-threat-hunting-methodology.pdf

<u>IS</u>: A starting point for small teams

Image Source: AI generated on MidJourney on April 23, 2024

What is Threat Hunting?

- A systematic and organized review of network data and system events generated by users, applications, and threat actors within the corporate and operational environment.

- Hunt activities vary by time, scope, and goals.

Image Source: AI generated on MidJourney on March 19, 2024

Threat Hunting Blockers

Image Source: AI generated on MidJourney on April 5, 2024

- Not Collecting Information
  - Network Artifacts
  - System Artifacts
  - Countermeasure Artifacts <- YOU BOUGHT IT!!
- Leadership Attitude
  - MSSP / SOC alerts are good enough
  - IT / Infosec / OT have better things to do
- Team Knowledge
  - Team thinks hunts require special training they do not have
  - Team knows they have better things to do

What does Threat Hunting Accomplish?

Image Source: AI generated on MidJourney on March 20, 2024

- Primary
  - Identify and address configuration issues
  - Identify and address implementation consequences
  - Familiarize team with normal network and system baselines
- Secondary
  - Tune countermeasures
  - Identify gaps in countermeasure deployments and parsing
- Tertiary
  - Find Exploited Evil

Realized Benefits of Threat Hunting?

- Identification of misconfigurations for systems and applications
- Improved server efficiency and availability
- Reduction of superfluous network traffic
- Reduction of cybersecurity alerts
- Improved network and data flow documentation for zones and conduits
- ***Things are going to get fixed***

- Countermeasure tuning will improve
- Network traffic and system events data feeds will improve
- OS and application configurations will improve
- Attack surface will decrease
- Identification of rogue hardware and software asset inventory
- ***Things are going to get fixed***
- DFIR playbook generation and updates
- Hunt types can be automated

Image Sources: AI generated on MidJourney on March 20, 2024

Team is How You Start

Image Source: AI generated on MidJourney on March 20, 2024

- Team members that are invested, understand the environment, and HATE unanswered questions
- Champion that understands the mission, can authorize tasking others, and empowers the hunt team

SOC Analyst VS Threat Hunting Team

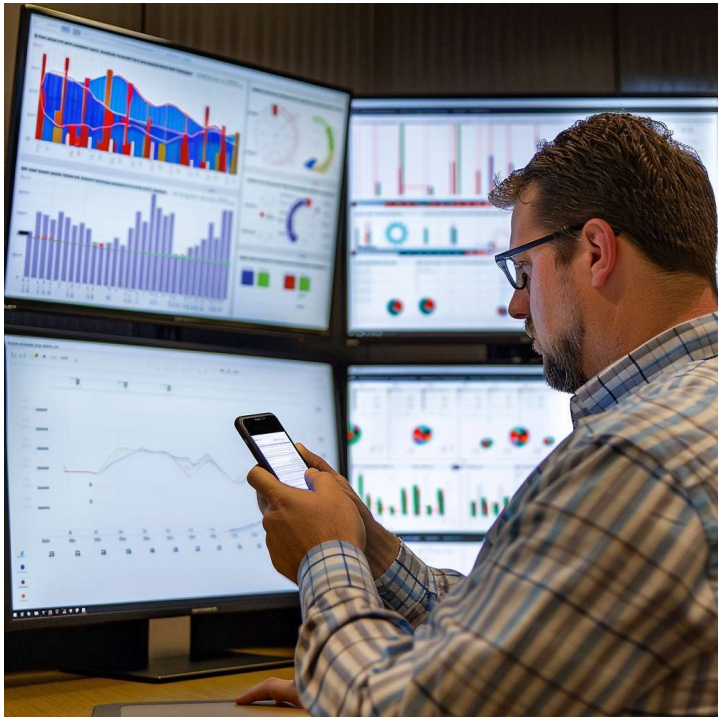


Image Source: AI generated on MidJourney on March 20, 2024

- SOC analysis provides continual monitoring for known TTPs against previous baselines
  - Feed is typically tuned alerts
  - Reactions are based on playbooks

- Hunt Operations consider raw data:
  - Dynamic conditions on OT and process networks
  - Consider unique conditions or areas with no known baselines
  - Evaluate updated or currently exploited threat actor TTPs
  - Prevent biased countermeasure tuning and hypotheses
  - Deliver actionable intelligence during incident response efforts
  - Identify gaps in countermeasure logging and parsing

Cybersecurity Incident Response

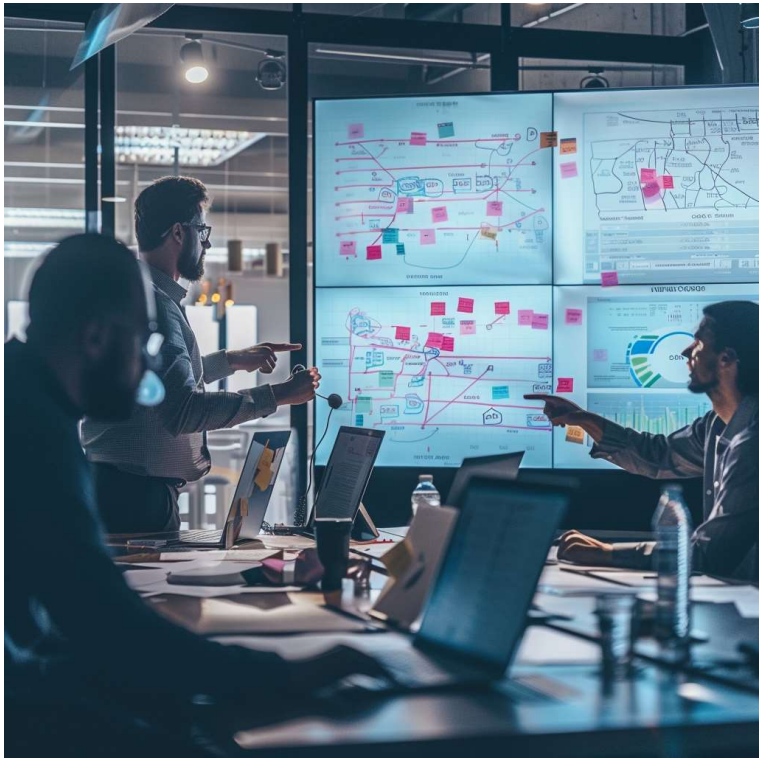


Image Source: AI generated on MidJourney on March 20, 2024

- DFIR investigations require unique analysis
- Team members should be experienced in
  - Known system and network activities
  - Data feeds
  - Collecting data from unique sources
- Administrators should be experienced in
  - Reacting to data requests
  - Managing change requests
- Leaders should be experienced in
  - Accepting input from the team
  - Using data to make decisions and manage actions

Threat Hunting Methodology

Plan for Success and you will Succeed!!!

Types of Threat Hunts

- Known Industry Activity Hunts
- Improve Operations and Cybersecurity Feeds Hunts
- Incident Response

Image Source: AI generated on MidJourney on March 20, 2024

Known Industry Activity Hunts

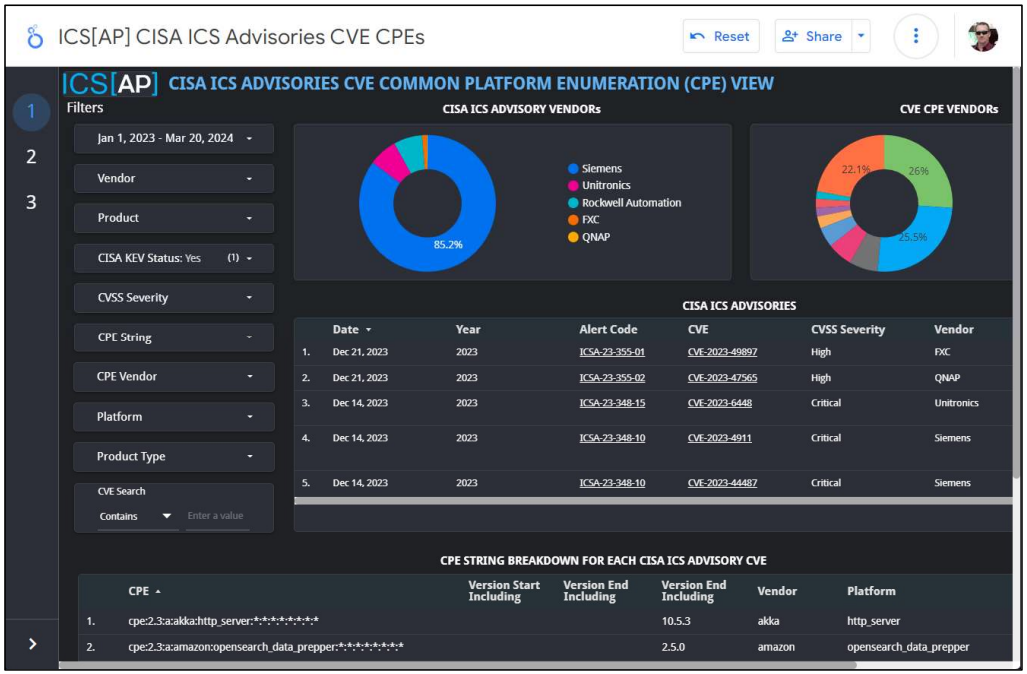
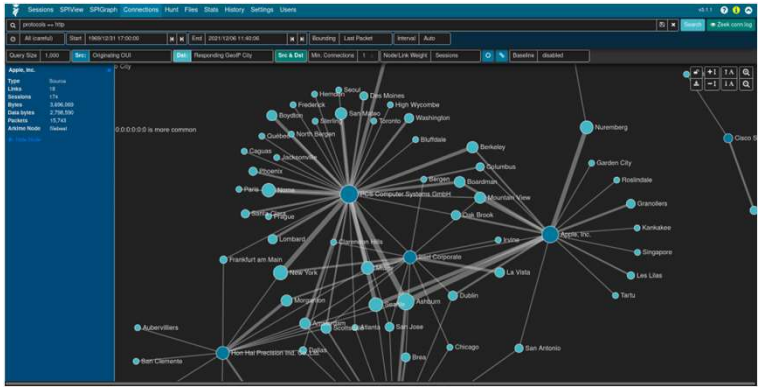


Image Source: ICS Advisory Project https://www.icsadvisoryproject.com/

- CISA Cybersecurity Alerts and Advisories
- CISA Known Exploited Vulnerabilities
- Information Sharing and Analysis Center (ISAC) Briefs
- Vendor Produced Cybersecurity Threat Intelligence

Improve Operations and Cybersecurity Feeds Hunts

- Understanding Events and Alerts
  - Remote Authentications
  - OT Management Interface Authentications
  - Wireless Authentications and Activities
  - Beacons and Sessions
  - LOLBIN Events
  - Control Network Communications
  - USB / Removable Media Events



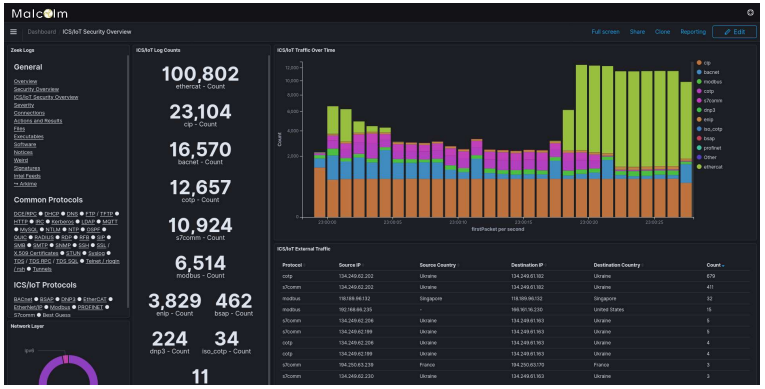


Image Source: Arkime and Malcolm https://malcolm.fyi/

Cybersecurity Incident Response Hunt

Image Source: AI generated on MidJourney on March 21, 2024

- Provide Subject Matter Expertise for
  - Data gathering
  - Data analysis
  - Known TTPs detection
  - Actionable intelligence for administrators and operations personnel
  - Recommendations to Incident Response Commanders

Responsibilities

Image Source: AI generated on MidJourney on March 20, 2024

- Hunt Champion
- Team

Hunt Champion Responsibilities

- **<u>Care / Investment</u>**
- Visualize Hunt
  - Goal / purpose of hunt
  - Scope of hunt
  - Data that will feed the hunt
  - Expected results / end state
  - Start and end times of hunt
- Task Team
  - Outline purpose
  - Confirm the team understands
  - Accept their direction / inputs / recommendations
  - Provide guidance / authorizations during execution

Image Source: AI generated on MidJourney on March 20, 2024

Team Responsibilities

- Pick a team
  - HATE unanswered questions
- Plan a simple hunt by type
  - Examples to follow…
- Conduct the hunt
- Formulate conclusions and manage findings
- Lessons Learned
- Determine time for next hunt

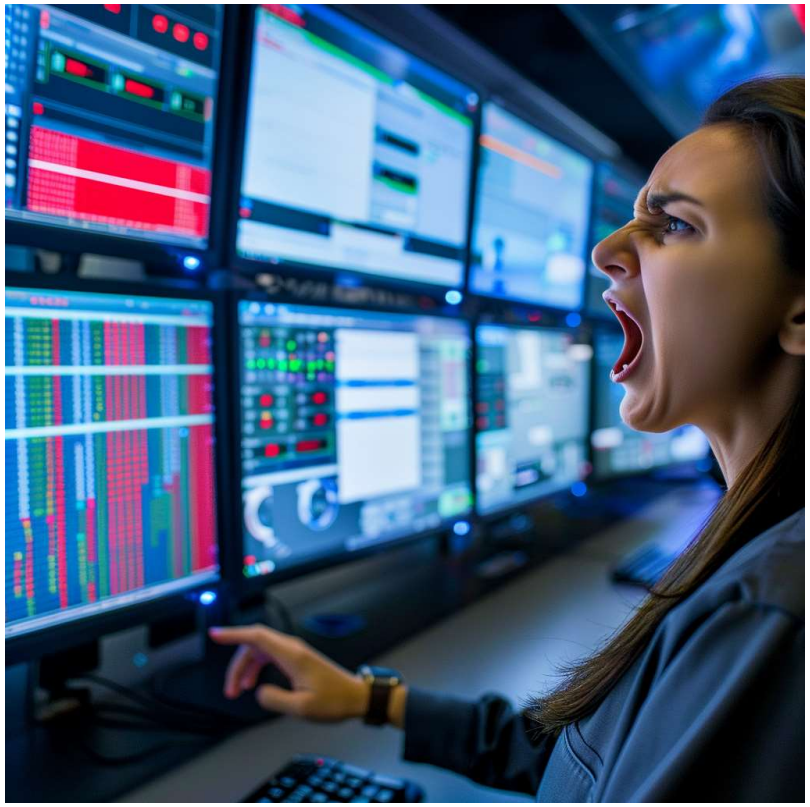


Image Source: AI generated on MidJourney on March 21, 2024

Single Team Member

- You can do this yourself
  - ***NOTE:*** Information gathering and actions on OT side ***MUST*** involve OT stakeholders

Image Source: AI generated on MidJourney on June 12, 2024

Threat Hunting Examples

Ordered, sort of….

Known Industry Activity Hunts

- CISA Cybersecurity Alerts and Advisories
- CISA Known Exploited Vulnerabilities
- Information Sharing and Analysis Center (ISAC) Briefs
- Vendor Produced Cybersecurity Threat Intelligence

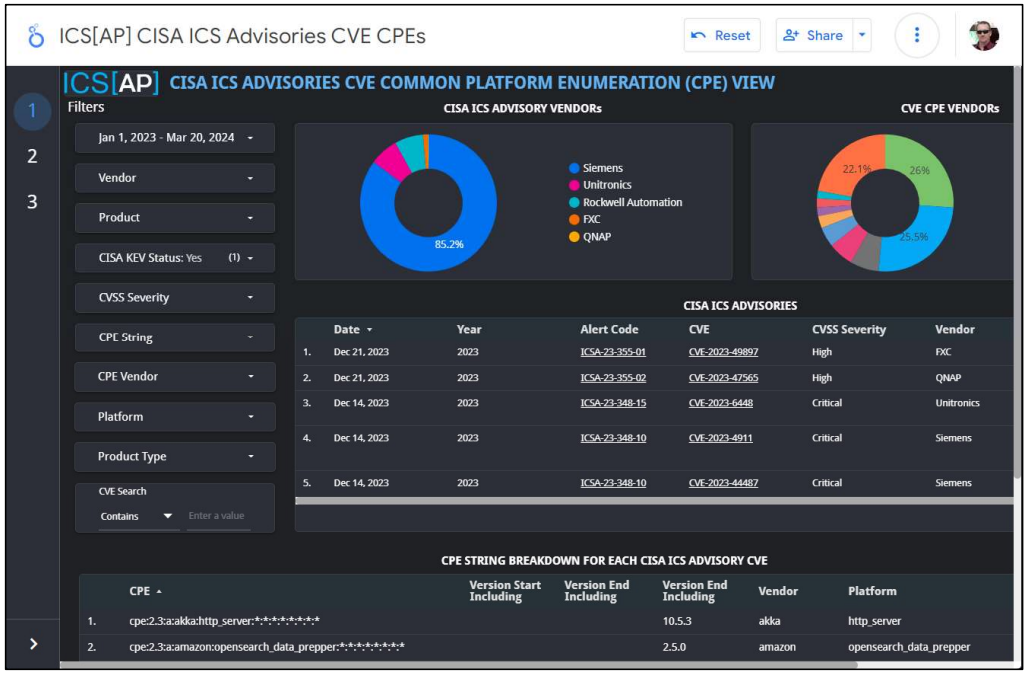


Image Source: ICS Advisory Project https://www.icsadvisoryproject.com/

Authentication Hunts

Remote Authentications

- Secure Remote Access
  - VPN
    - Active Directory and MFA - Corporate
    - Active Directory and MFA – Control
  - Remote Computer Control Software
- Questions to consider
  - How do employees authenticate?
  - How to 3rd Party (e.g. vendors, integrators, contractors) authenticate?
  - Impossible user travel?
  - Users with known breached credentials?

Application Authentications

- Windows Digest / NTLM authentications
- Application authentications to Windows event logs
- Application authentications to custom event logs
- Clear text authentications (e.g. HTTP, FTP, vendor management interfaces)

Beacons and Sessions

JA4+ Network Fingerprinting

- Network Activity Fingerprints

Application	JA4 (client)
Chrome	t13d1518h2_8daaf6152771_e5627efa2ab1 (TCP initial) t13d1518h2_8daaf6152771_9b887d9acb53 (TCP reconnect) q13d0310h3_55b375c5d22e_cd85d2d88918 (QUIC initial) q13d0311h3_55b375c5d22e_3512bcbbc9ec (QUIC reconnect)
SoftEther VPN Client	t13d880900_fcb5b95cb75a_b0d3b4ac2a14 (88 ciphers!?)
IcedID Malware	t13d201100_2b729b4bf6f3_9e7b989ebec8
Evilginx	t13d191000_9dc949149365_e7c285222651
Sliver Malware	t13d190900_9dc949149365_97f8aa674fd9 (GoLang)

Active Countermeasures / RITA

- Command and Control Beacons
- Large data transfers
- User agents
- DNS Requests
- Blacklisted/Bad Reputation Sites

Image Source: https://www.activecountermeasures.com/ac-hunter/

NOTE: Reference, not an endorsement. Understand your countermeasure gaps.

Windows Activity

Windows Stand Alone Systems*

- USB Events **
  - Compare with sheep dip solutions?
- AV / End Point Protections
- SMB Traffic
- RDP Sessions

LOLBINs

- Process Start Events
- Service Start / Modified Events
- Schedule Task Events
- Software Installed Events
- Process Memory Size

* e.g. HMIs, Servers
** e.g. mass storage, HID, license dongles

Wireless / Radio

Corporate / Control Network WiFi

- Masquerading Access Points
- Rogue Access Points
- Authentications
- Denial of Service

ICS Protocol Radio

- Cellular / SatCom / Microwave / Starlink
  - Authentications
  - Communications
- 802.15.4 Network Join Requests
  - WirelessHart
  - ISA 1100.11a
  - Zigbee
- Other?

Control Network Protocols

- ARP <- IPv4
- NDP <- IPv6
- DHCP
- DNS
- SMBv1
- CDP
- Protocol Reads and Writes

Image Source: AI generated on MidJourney on March 21, 2024

Summary

Let’s Wrap This Up….

Summary

- Hunting Doesn’t Have to be Hard
- Common Hunting Issues
- Automation
- Resources

Image Source: AI generated on MidJourney on April 2, 2024

Hunting is Hard?

Image Source: https://twobrainbusiness.com/two-brain-summit-jocko-willink/

Common Hunt Issues

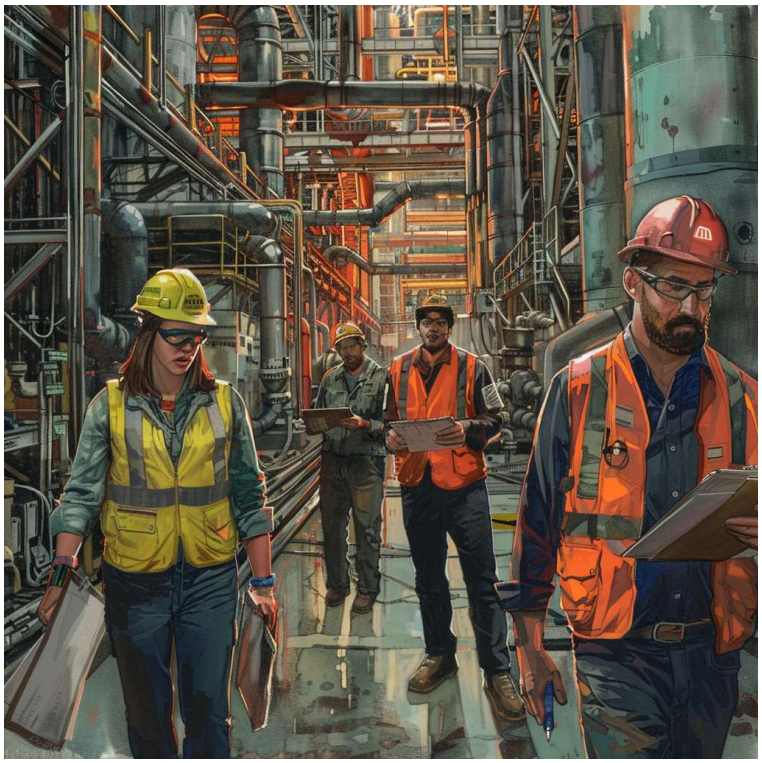


Image Source: AI generated on MidJourney on March 21, 2024

- **NOT MONITORING!!!**
- Team does not know where the data is
- Feed data is not what is expected
- Data feeds are broken
- Countermeasure tuning is inconsistent with system or network activity
- Activity is a risk but necessary for operations

Automation

- One goal is the team learns to automate as many of these hunts as possible.
- However, they also need time to review the results, tune the automation, and perform manual hunts.

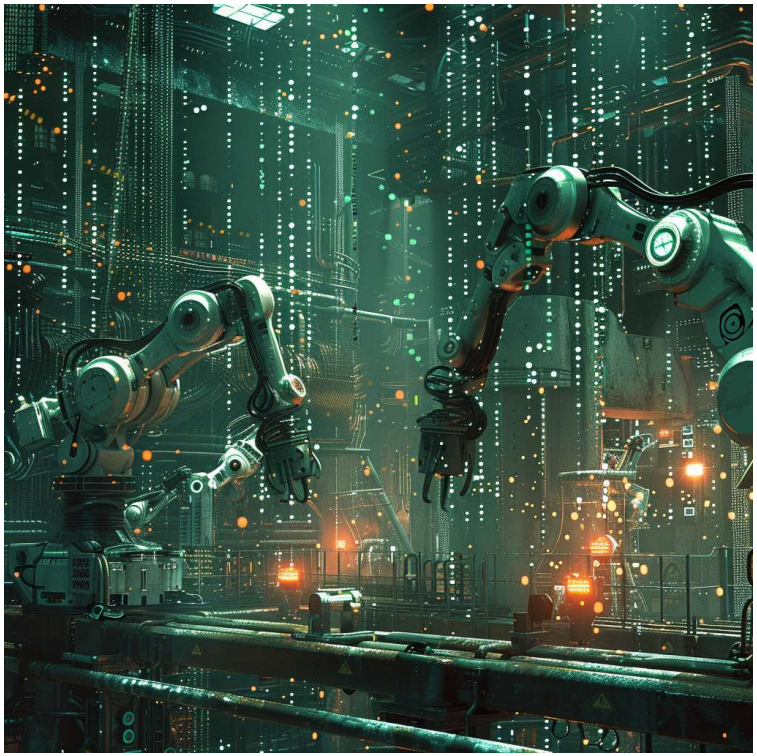


Image Source: AI generated on MidJourney on April 23, 2024

Resources

- Frameworks
  - Army Threat Hunting paper: https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1028345
  - Splunk's PEAK Threat Hunting Framework: https://www.splunk.com/en_us/blog/security/peak-threat-hunting-framework.html
  - AI Threat Hunting for System-based Artifacts: https://www.rsaconference.com/library/blog/ai-powered-threat-hunting
  - Joe Slowik's "Developing an Intelligence-Driven Threat Hunting Methodology": https://www.gigamon.com/content/dam/resource-library/english/white-paper/wp-intelligence-driven-threat-hunting-methodology.pdf
- General Links
  - Arkime: https://arkime.com/
  - FOXIO-LLC JA4+: https://github.com/FoxIO-LLC/ja4
  - Zeek: https://zeek.org/
  - RITA: https://github.com/activecm/rita
  - AC-Hunter: https://www.activecountermeasures.com/ac-hunter/
  - Sysmon: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon
  - Event ID 7045: https://learn.microsoft.com/en-us/defender-for-identity/other-alerts
  - Detecting Kerberoasting Activity: https://adsecurity.org/?p=3458
  - AI Threat Hunting Virtual Machine: http://www.ds4n6.io/tools/daisy.html
- Blogs
  - Cutaway Security Presentations 2024: https://github.com/cutaway-security/cutsec_presentations/tree/main/2024/Threat_Hunting_Does_Not_Have_To_Be_Hard
  - Joe Slowik: https://industrialcyber.co/events/first-impressions-and-lasting-insights-from-an-s4-rookie/
  - Lesley Carhart: https://www.linkedin.com/feed/update/urn:li:activity:7199738825613467648/
  - Dan Gunter: https://www.sans.org/white-papers/38710/
  - Robert M. Lee, David Bianco: https://www.sans.org/white-papers/37172/

Special Thank You To:

CutSec Discord
Beer-ISAC
Other OT/IT/Infosec Professionals

Don C. Weber - @cutaway
info@cutawaysecurity.com
https://www.cutawaysecurity.com
https://www.linkedin.com/in/cutaway/
Cutaway Security Discord