Adapting to the Latest Cyber Threats to ICS/OT

Integrating Continuous Security Testing into the Purdue Model

Advanced services and solutions
for the world’s most difficult
environments and
business problems.

Plurilock
CRITICAL SERVICES

About Today’s Speaker - Adapting to the Latest Cyber Threats to ICS/OT

Christian Scott
PLCS Practice Leader

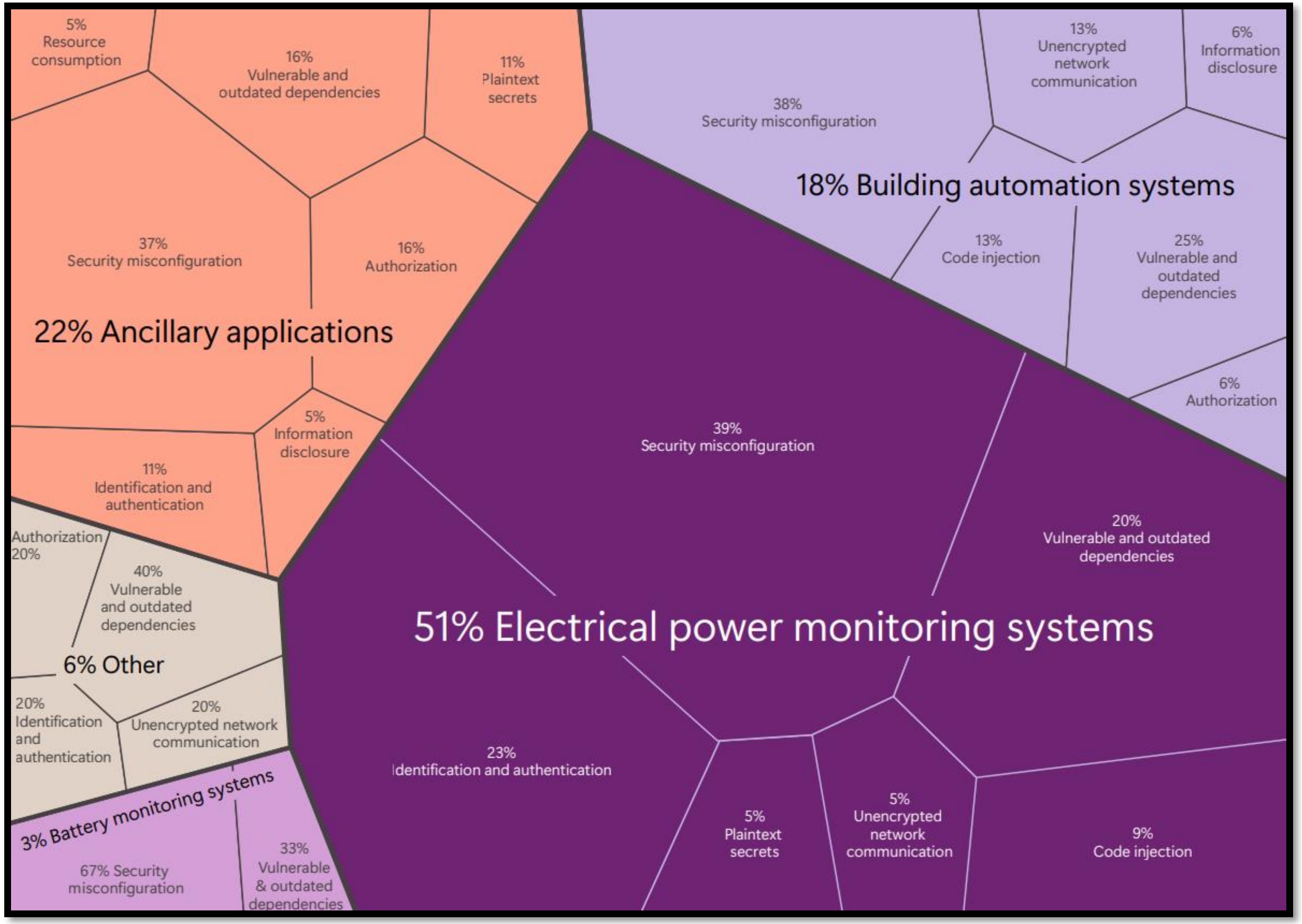
- 20+ Year of Technology & Cybersecurity Expertise
- Original background in software development, systems engineering, cybersecurity program management and offensive cybersecurity testing
- “White Hat” ethical hacker who has overseen thousands of penetration tests, social engineering tests, red teaming, purple teaming, cybersecurity risk assessments and white box security architecture reviews
- Preeminent cybersecurity researcher and educator through numerous contributions including Kali Linux featured open-source tools like Legion as well as helping hundreds break-into-cyber through his educational non-profit “Cyber Judo”

[redacted]

The Current OT Threat Landscape

- In Fortinet's recent OT security report, they found that nearly one-third of respondents had suffered six or more security intrusions, up from 11% in 2023. They also found that all types of intrusions increased in 2024 with the exception of malware which remained relatively consistent with last year.
- The amount of OT-specific malware disclosed in the last 3 years is greater than in the entire previous decade.
- The US Cybersecurity and Infrastructure Security Agency (CISA) warns that malicious actors are increasingly targeting internet-connected operational technology (OT) and industrial control system (ICS) endpoints.

Timeline of OT-Specific Malware
•**2010**: Stuxnet
•**2013**: Havex
•**2014**: BlackEnergy3
•**2016**: Industroyer/CrashOverride
•**2017**: Trisis/Triton
•**2022**: Industroyer2, Pipedream
•**2023**: CosmicEnergy
•**2024**: Fuxnet, FrostyGoop



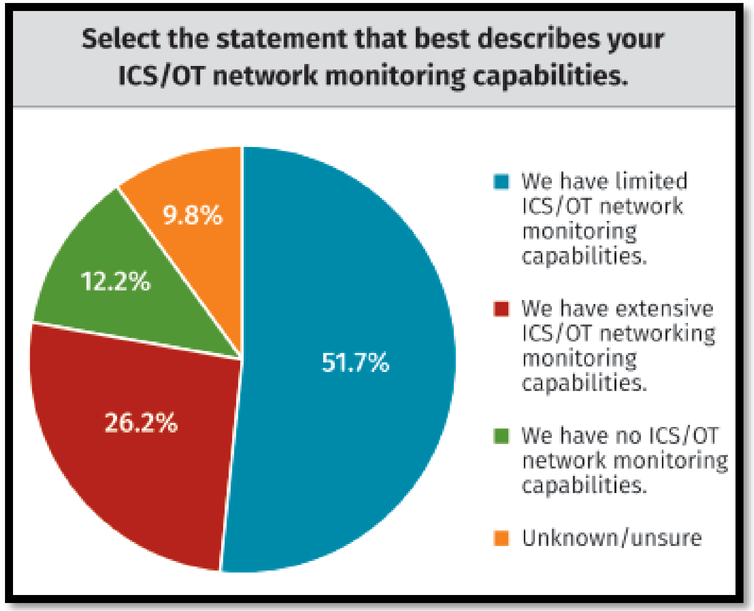
Reference(s):
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

[redacted]

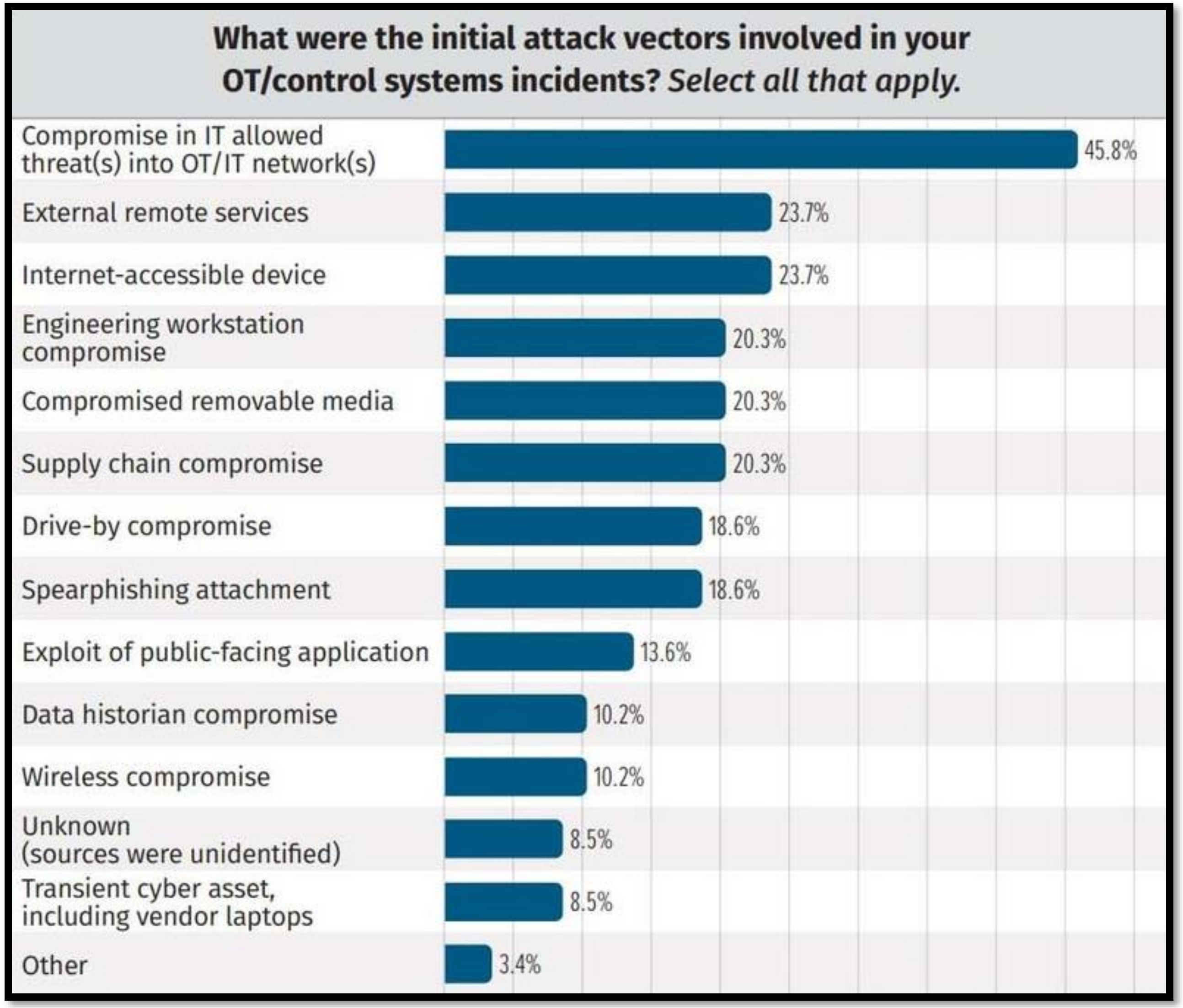
What Are The Key Drivers Behind OT Cyber Intrusions?

The *State of ICS/OT Cybersecurity 2024* report from SANS is based on responses from cybersecurity professionals in various critical infrastructure sectors.

The survey results provide insights into the key attack vectors and root causes behind those OT system intrusions.



Select the statement that best describes your ICS/OT network monitoring capabilities.



What were the initial attack vectors involved in your OT/control systems incidents? *Select all that apply.*

Reference(s):
https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/

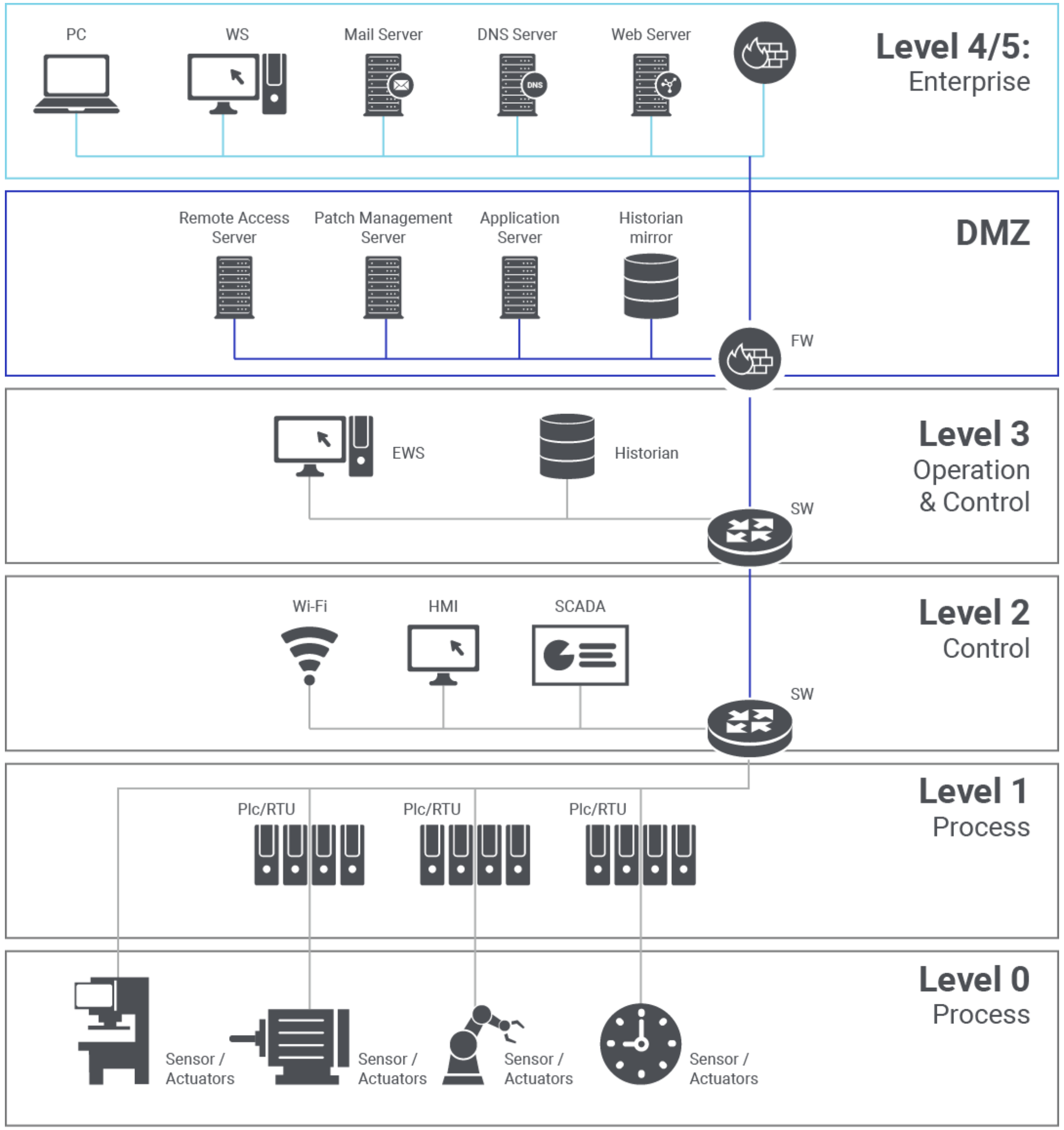
[redacted]

The Purdue Model & OT Security

- The Purdue model, part of the Purdue Enterprise Reference Architecture (PERA), defines a standardized ICS network structure that supports OT security.
- By dividing the ICS architecture into six hierarchical zones, it maintains a controlled flow of data between IT and OT layers. When implemented correctly, the model establishes an "air gap" between IT and OT systems, enabling strong access controls while preserving business continuity.

The Challenges With The Purdue Model

- The air gap doesn't really work anymore. The rise of IoT and cloud adoption across the industrial value chain has made many industrial networks so integrated that the traditional air gap simply isn't effective. This is why most OT system intrusions are via Compromised IT Networks, External Remote Services & Internet Accessible Devices.
- ICS devices were built to last—not to evolve. Many OT systems rely on older, inherently insecure protocols that lack modern security features. In some cases, the hardware is not powerful enough to run encrypted protocols. Upgrading these systems to support secure protocols can be challenging and costly.
- Malicious actors continue to increase their evasion capabilities by leveraging the same remote monitoring and management (RMM) tools that IT departments use to support IT and OT systems.



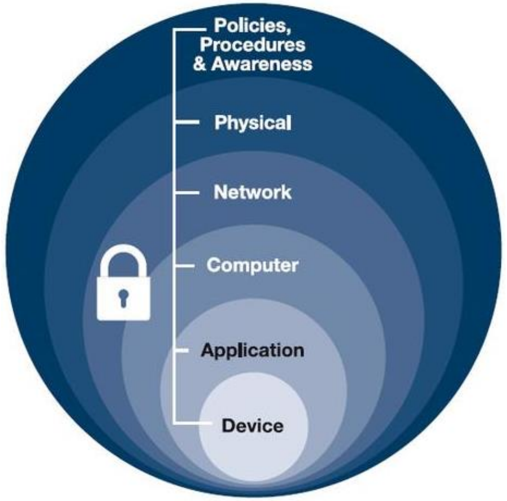
Reference(s):
https://www.sans.org/white-papers/sans-2024-state-ics-ot-cybersecurity/
https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

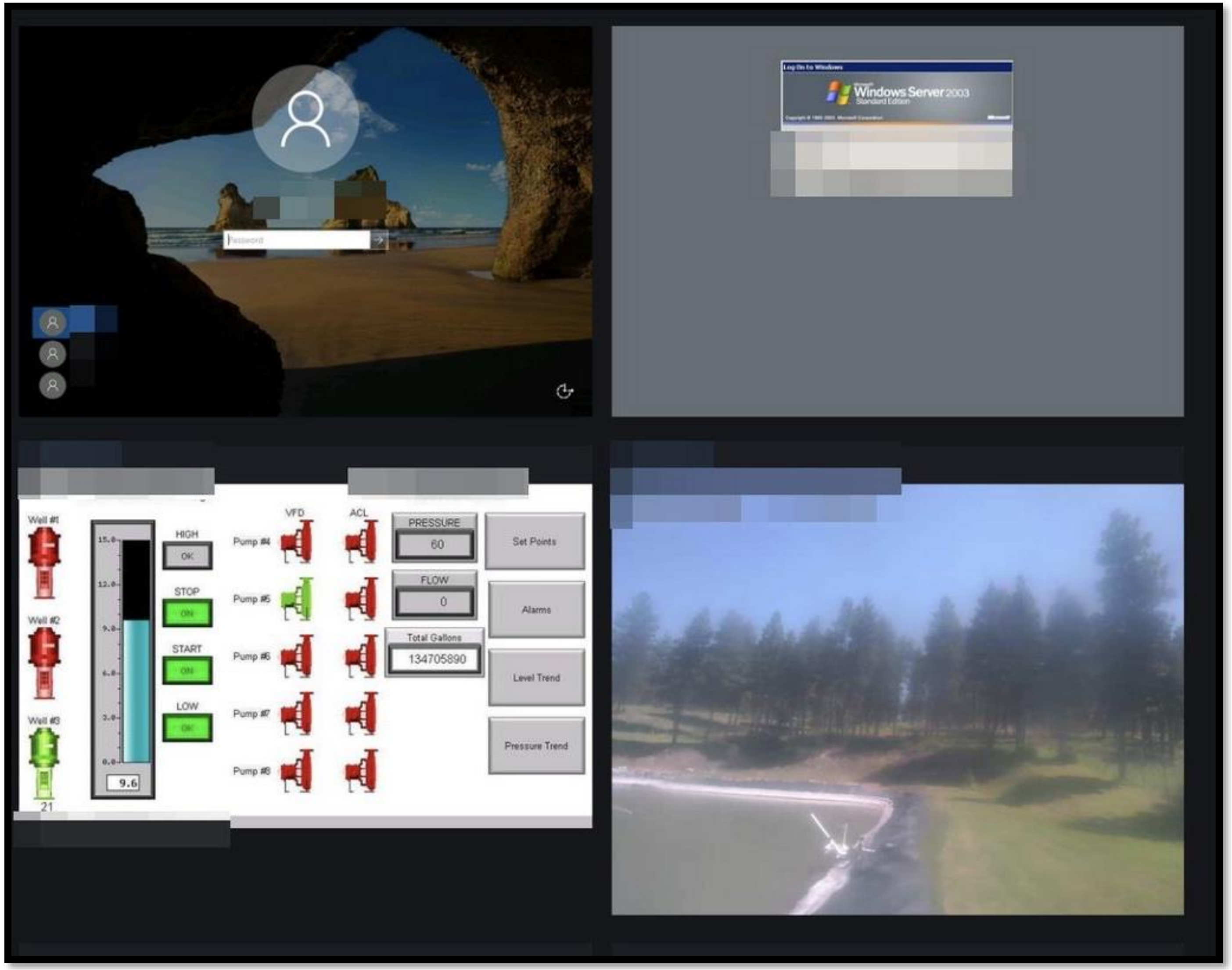
[redacted]

The Most Common Exploited OT Vulnerabilities & Weaknesses

In their *2024 Digital Defense Report*, Microsoft identified and disclosed over 300 vulnerabilities to suppliers through their OT application review initiative. The most common security vulnerabilities they identified, prioritized by risk and impact, were:

- **Outdated Authentication**
- **Insecure Communications**
- **Default Configurations & Credentials**
- **Outdated Legacy Software & Libraries**





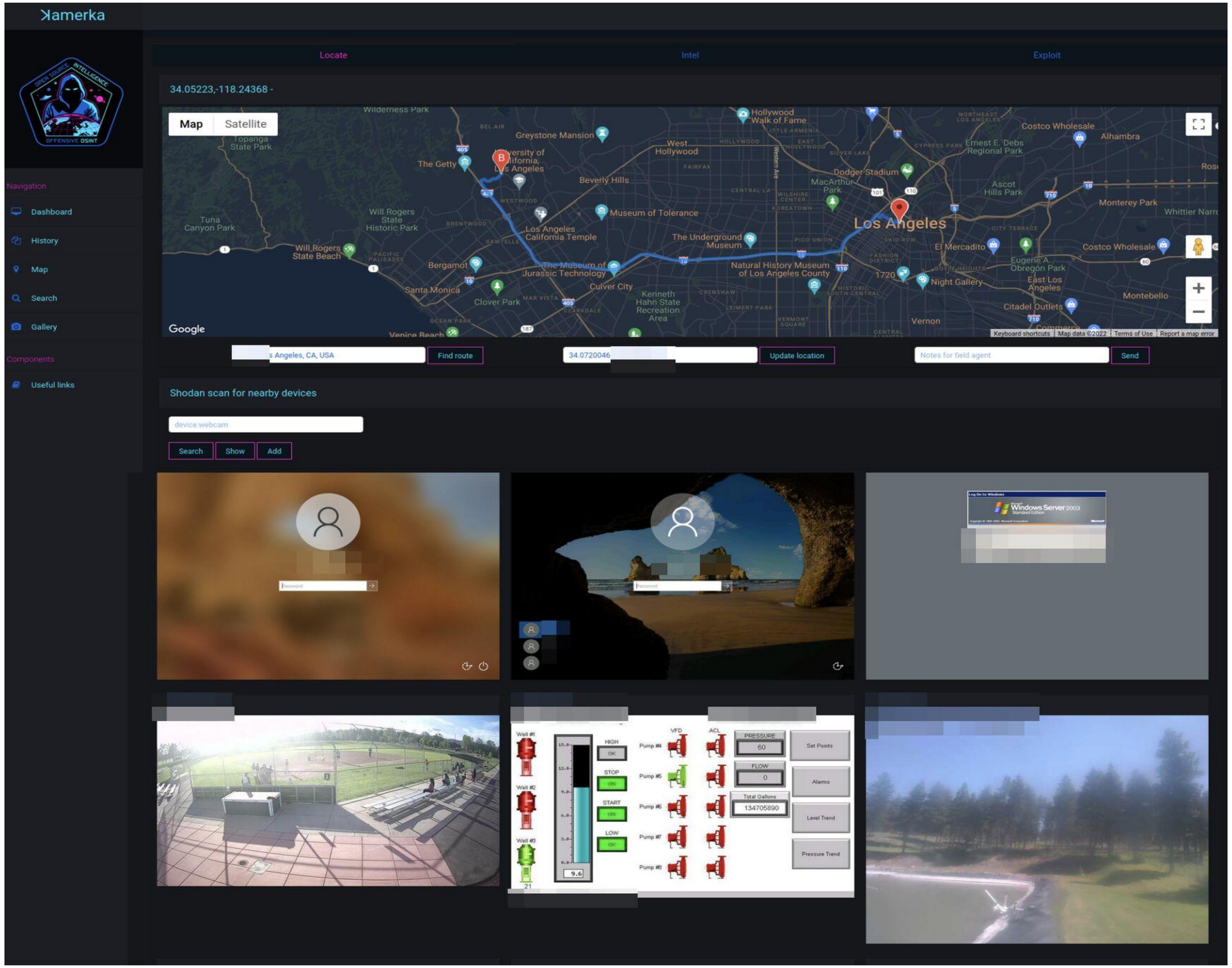
Reference(s):
https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[redacted]

Practical Defensive Tip #1:

Map Your Organization’s External Attack Surface For Vulnerable OT Systems On a Regular Basis

- To help prevent two of the top three most common OT initial intrusion vectors (compromised IT networks and Internet accessible devices) it’s important to go beyond conventional OT asset discovery and perform OSINT scanning on a continuous basis across their external attack surface.
- Kamerka GUI is a free and open-source reconnaissance tool for discovering and assessing exposed Internet of Things (IoT) and Industrial Control Systems (ICS) devices.
- Kamerka leverages Shodan with support from Binary Edge and WhoisXMLAPI to scan for internet-facing ICS and IoT devices by IP, country, or geographic coordinates.
- Kamerka can quickly provide insights into unintentionally exposed OT infrastructure and the vulnerabilities that are present across those systems.



34.05223,-118.24368 -

s Angeles, CA, USA

34.0720046

Notes for field agent

Shodan scan for nearby devices

device:webcam

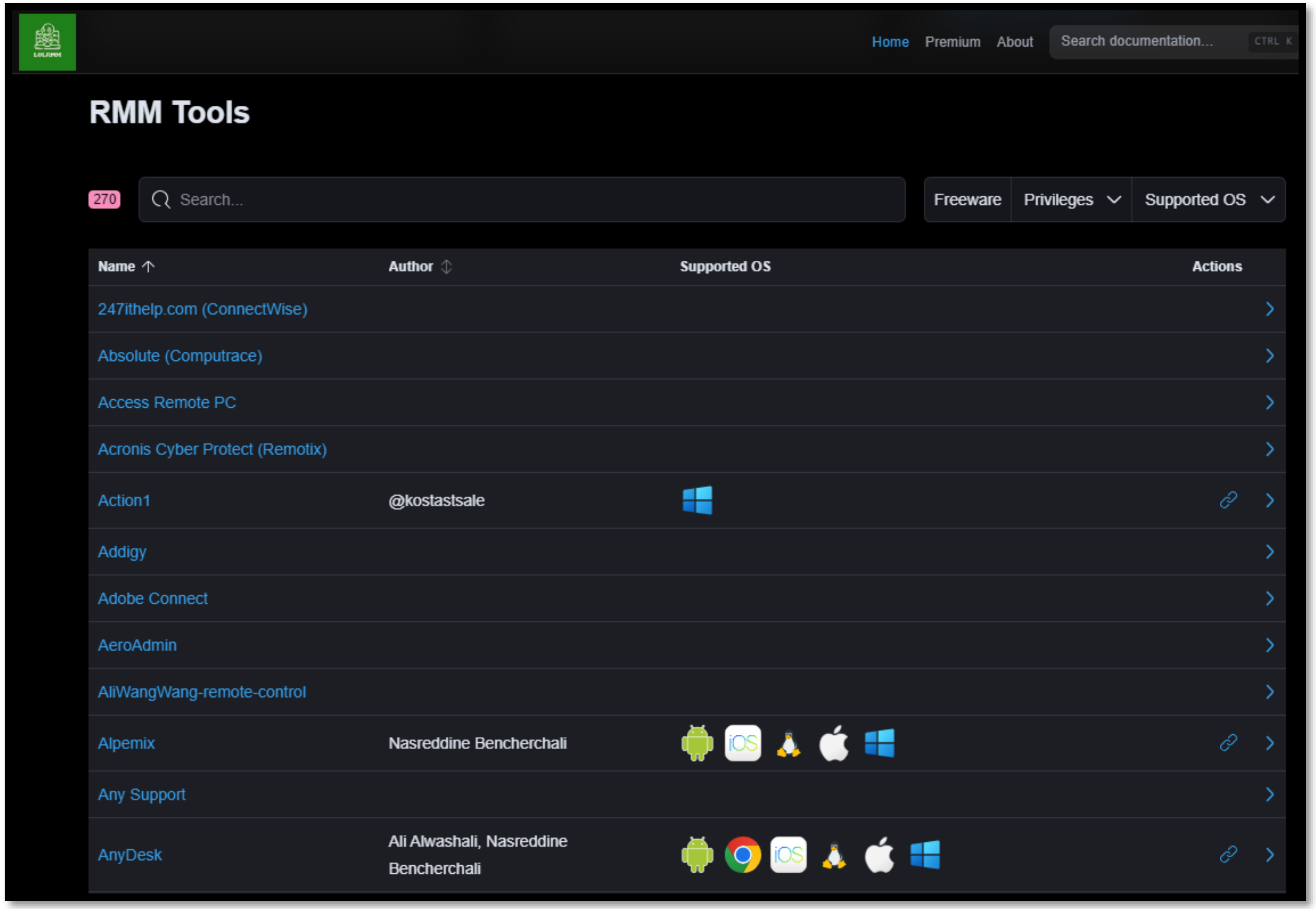
Reference(s):
https://github.com/woj-ciech/Kamerka-GUI

[redacted]

Practical Defensive Tip #2:

Configure Your Security Solutions To Block Unauthorized RMM IT Tools With The Company

- Malicious actors continue to increase their evasion capabilities by leveraging the same remote monitoring and management (RMM) tools that IT departments use to support IT and OT systems.
- This RMM-based living of the land (LOTL) attack allows malicious actors to gain a foothold into systems, laterally move about, perform privilege escalation and maintain persistence, including in OT environments.
- According to the *CrowdStrike 2024 Threat Hunting Report*, there's been a staggering 70% increase in RMM tool abuse in the last year.
- LOLRMM (Living Off the Land Remote Monitoring and Management) is a community-driven project that provides a curated list of RMM tools that can be misused by threat actors.
- Lists of unauthorized RMM tools can be imported into your organization's XDR, EDR and SIEM solutions via the LOLRMM API or using CSV, JSON and pre-built Sigma rules.



RMM Tools

Name ↑	Author	Supported OS	Actions
247ithelp.com (ConnectWise)			›
Absolute (Computrace)			›
Access Remote PC			›
Acronis Cyber Protect (Remotix)			›
Action1	@kostastsale	⊞	🔗 ›
Addigy			›
Adobe Connect			›
AeroAdmin			›
AliWangWang-remote-control			›
Alpemix	Nasreddine Bencherchali	🤖 iOS 🐧 ⊞	🔗 ›
Any Support			›
AnyDesk	Ali Alwashali, Nasreddine Bencherchali	🤖 ◎ iOS 🐧 ⊞	🔗 ›

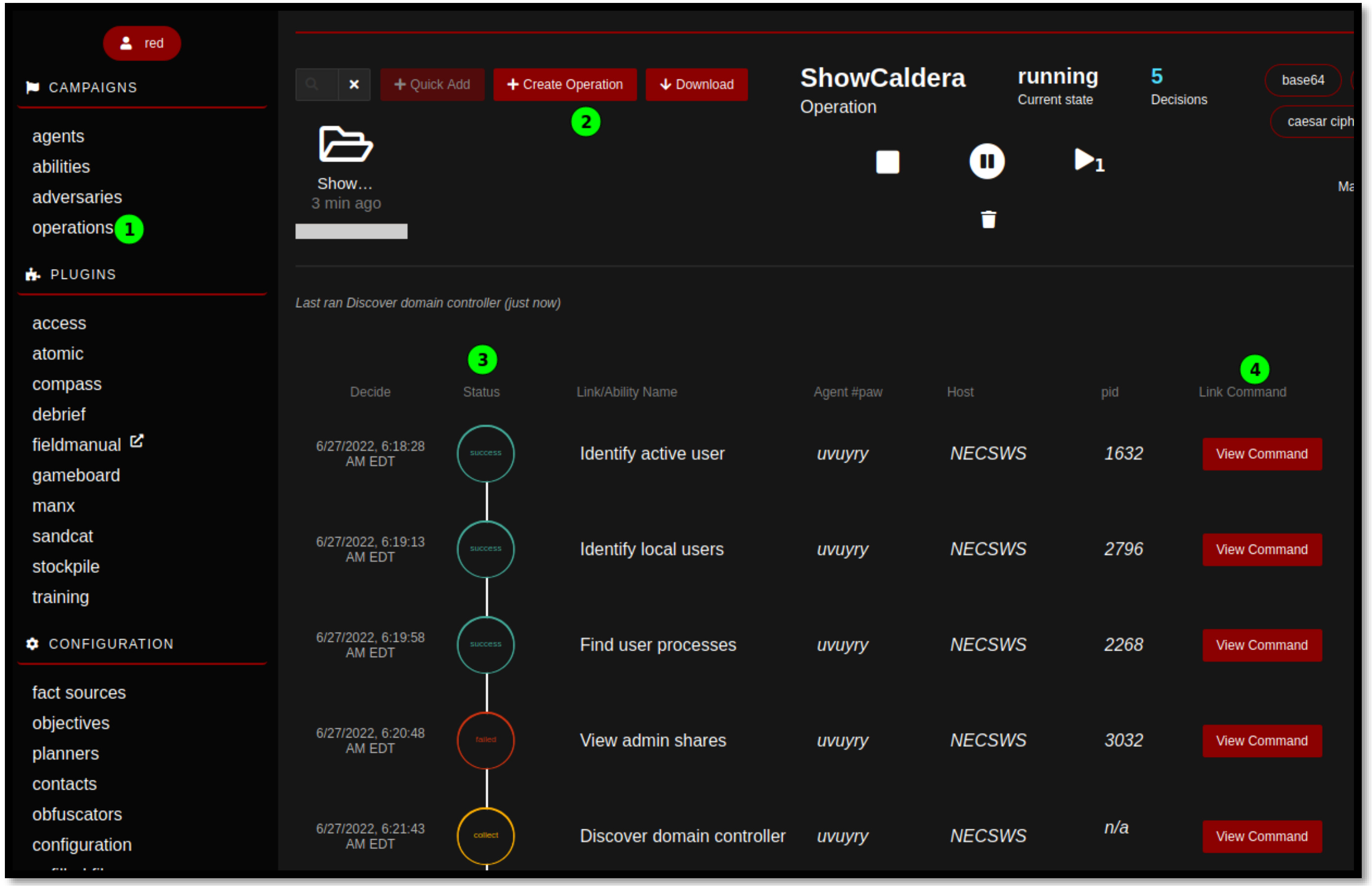
Reference(s):
https://www.crowdstrike.com/resources/reports/threat-hunting-report/
https://github.com/magicsword-io/LOLRMM

[redacted]

Practical Defensive Tip #3:

Implement OT Specific Continuous Security Testing Tools Like MITRE Caldera

- MITRE Caldera is an open-source tool for simulating adversarial tactics, techniques, and procedures (TTPs) in a controlled environment.
- It leverages the MITRE ATT&CK framework to provide automated, repeatable adversary emulation, helping organizations evaluate their defenses against real-world attack scenarios.
- With the MITRE Caldera OT Plugin, organizations can simulate adversary actions within OT systems. More specifically, this plugin provides plugins for key OT communication protocols:
  - BACnet (Building Automation Control Networks)
  - DNP3 (Distributed Network Protocol 3)
  - ModbusProfinet (Basic Discovery and Configuration Protocol)
  - IEC 61850 (Manufacturing Message Specification)



Last ran Discover domain controller (just now)

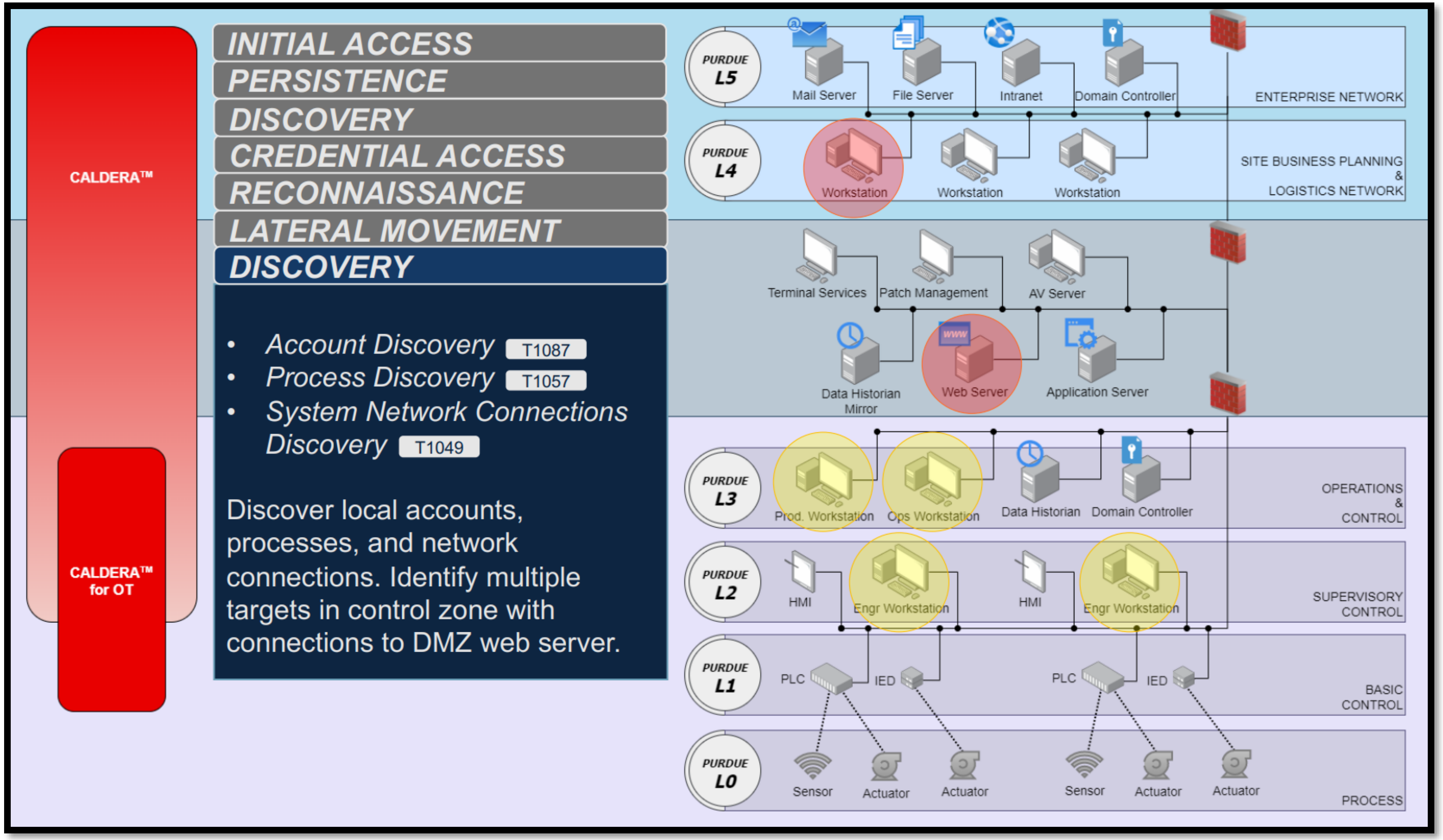
Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command
6/27/2022, 6:18:28 AM EDT	success	Identify active user	uvuyry	NECSWS	1632	View Command
6/27/2022, 6:19:13 AM EDT	success	Identify local users	uvuyry	NECSWS	2796	View Command
6/27/2022, 6:19:58 AM EDT	success	Find user processes	uvuyry	NECSWS	2268	View Command
6/27/2022, 6:20:48 AM EDT	failed	View admin shares	uvuyry	NECSWS	3032	View Command
6/27/2022, 6:21:43 AM EDT	collect	Discover domain controller	uvuyry	NECSWS	n/a	View Command

Reference(s):
https://github.com/mitre/caldera
https://github.com/mitre/caldera-ot

[redacted]

MITRE Caldera Use Case:

Simulating system intrusions from IT networks into OT systems in a way that tracks across the Purdue Model and MITRE ATT&CK Framework.



CALDERA™

CALDERA™ for OT

INITIAL ACCESS

PERSISTENCE

DISCOVERY

CREDENTIAL ACCESS

RECONNAISSANCE

LATERAL MOVEMENT

DISCOVERY

- *Account Discovery* T1087
- *Process Discovery* T1057
- *System Network Connections Discovery* T1049

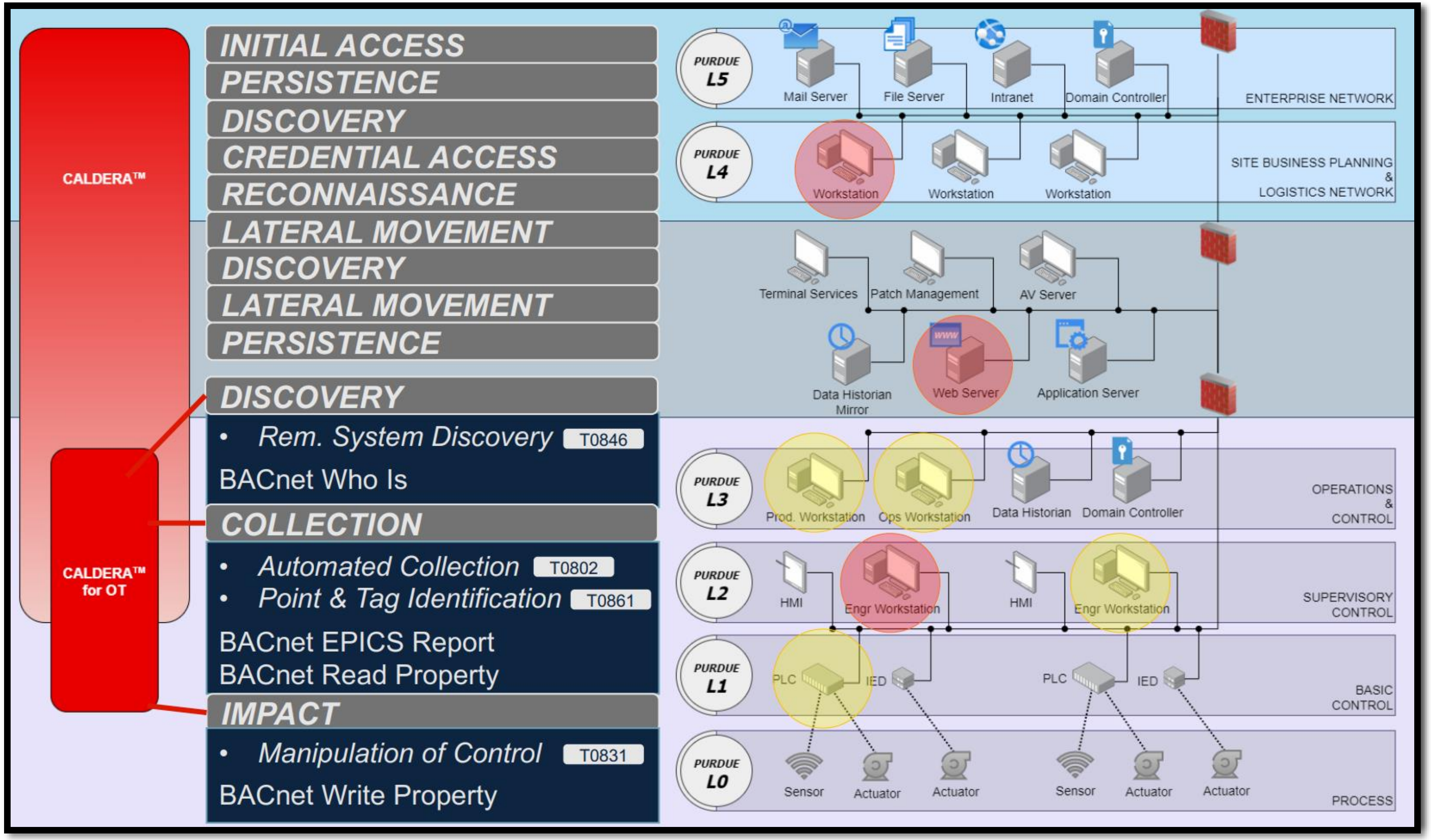
Discover local accounts, processes, and network connections. Identify multiple targets in control zone with connections to DMZ web server.

Reference(s):
https://github.com/mitre/caldera
https://github.com/mitre/caldera-ot

[redacted]

MITRE Caldera Use Case:

Simulating system intrusions from IT networks into OT systems in a way that tracks across the Purdue Model and MITRE ATT&CK Framework.



CALDERA™

INITIAL ACCESS
PERSISTENCE
DISCOVERY
CREDENTIAL ACCESS
RECONNAISSANCE
LATERAL MOVEMENT
DISCOVERY
LATERAL MOVEMENT
PERSISTENCE

CALDERA™ for OT

DISCOVERY

- *Rem. System Discovery* T0846

BACnet Who Is

COLLECTION

- *Automated Collection* T0802
- *Point & Tag Identification* T0861

BACnet EPICS Report
BACnet Read Property

IMPACT

- *Manipulation of Control* T0831

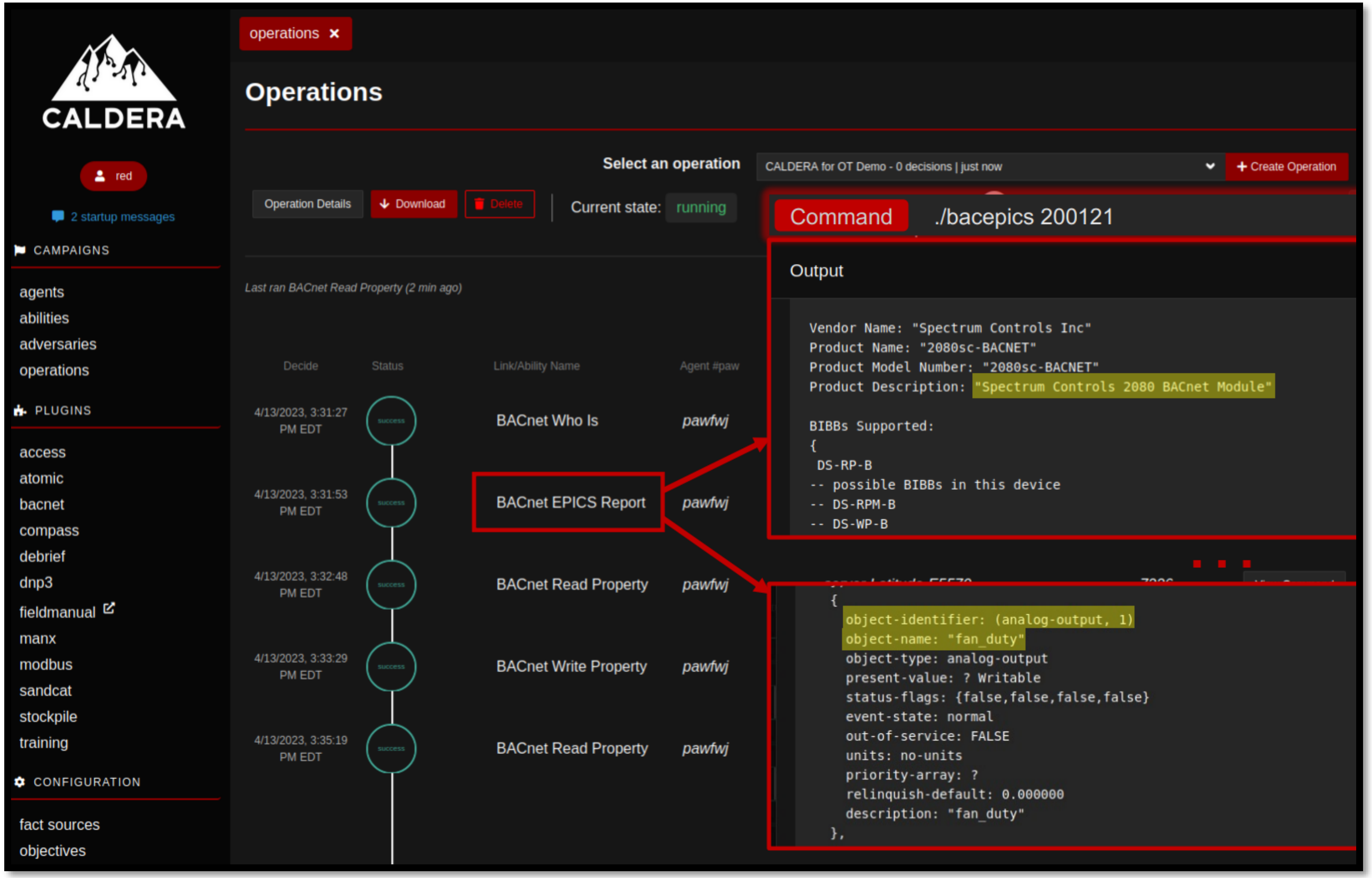
BACnet Write Property

Reference(s):
https://github.com/mitre/caldera
https://github.com/mitre/caldera-ot

[redacted]

MITRE Caldera Use Case:

Simulating system intrusions from IT networks into OT systems in a way that tracks across the Purdue Model and MITRE ATT&CK Framework.



Operations

Select an operation: CALDERA for OT Demo - 0 decisions | just now

Current state: running

Last ran BACnet Read Property (2 min ago)

Decide	Status	Link/Ability Name	Agent #paw
4/13/2023, 3:31:27 PM EDT	success	BACnet Who Is	*pawfwj*
4/13/2023, 3:31:53 PM EDT	success	BACnet EPICS Report	*pawfwj*
4/13/2023, 3:32:48 PM EDT	success	BACnet Read Property	*pawfwj*
4/13/2023, 3:33:29 PM EDT	success	BACnet Write Property	*pawfwj*
4/13/2023, 3:35:19 PM EDT	success	BACnet Read Property	*pawfwj*

Command ./bacepics 200121

Output

```
Vendor Name: "Spectrum Controls Inc"
Product Name: "2080sc-BACNET"
Product Model Number: "2080sc-BACNET"
Product Description: "Spectrum Controls 2080 BACnet Module"

BIBBs Supported:
{
 DS-RP-B
-- possible BIBBs in this device
-- DS-RPM-B
-- DS-WP-B
```

```
  {
    object-identifier: (analog-output, 1)
    object-name: "fan_duty"
    object-type: analog-output
    present-value: ? Writable
    status-flags: {false,false,false,false}
    event-state: normal
    out-of-service: FALSE
    units: no-units
    priority-array: ?
    relinquish-default: 0.000000
    description: "fan_duty"
  },
```

Reference(s):
https://github.com/mitre/caldera
https://github.com/mitre/caldera-ot

[redacted]

Thank You For Your Time!

Contact us today.

+1 (888) 282-0696 (USA West)
+1 (908) 231-7777 (USA East)
+1 (866) 657-7620 (Canada)

info@plurilock.com

Advanced cybersecurity and Zero Trust
Security assessments and consulting
IT products and solutions
Professional services
Managed services

Plurilock
CRITICAL SERVICES

Advanced Solutions for Critical Business Problems

Plurilock delivers the expertise and capabilities you need in a world of increasing risk—quickly.

Data and security breaches. Regional warfare. Natural disasters. Pandemics and social crises. Supply chain instability and opacity.

These are challenging times in cybersecurity. The rates of just about every cause of significant business risk are accelerating—along with the need to manage this risk carefully and to resolve complex, unpredictable crises as quickly as they emerge.

Plurilock Critical Services was founded to enable modern organizations to continue to safely operate—and adapt—as change happens. We offer:

- Unmatched, global, multi-domain expertise
- An extensive family of patented and proprietary cybersecurity technologies
- A comprehensive line of class-leading IT products and services

Service Catalog for a Changing World

IP Protection (IP3)

- Insider Threat Management
- Data Loss Prevention (DLP) Implementation
- Supply Chain Security Analysis
- IP Data Mapping & Risk Assessments
- Cloud Security Posture Management (CSPM)

Security Operations (SecOps)

- Threat Hunting Assessments
- SIEM/NDR/EDR/XDR Implementation
- Incident Response and Digital Forensics

Advisory (AP)

- Information Security Compliance Readiness
  - ISO27001, SOC2, CMMC, FedRAMP, FISMA, PCI-DSS, HIPAA, SEC, SOX
- Third Party Risk Analysis
- Cybersecurity Awareness & Training

Zero Trust (ZTA)

- Zero Trust Architecture Design & Implementation
  - Identity Access Management (IAM)
  - Zero Trust Network Access (ZTNA)
  - Secure Web Gateway (SWG)
  - Cloud Access Security Broker (CASB)
  - Secure Access Service Edge (SASE)
  - Micro Segmentation

Offensive Security (OffSec)

- Penetration Testing As A Service (PTaaS)
  - Including Network, Web, API, Mobile, Cloud, ICS/SCADA/IoT, AI/LLM, Social Engineering Testing and more.
- Continuous Red Teaming & Purple Teaming
- Managed Attack Surface Reduction
- White Box Security Architecture Analysis
- Cybersecurity Risk Assessments
  - Including Traditional & Cloud Systems
- Continuous Security Analysis In The SDLC
  - SCA/SAST/DAST, DevSecOps & SaC