

Emulating Adversary Actions in the Operational Environment with Caldera™ for OT

Misha Belisle, Blaine Jeffries

May 2023



MITRE

SOLVING PROBLEMS
FOR A SAFER WORLD®

Remote System Discovery (T0846)

Ability: BACnet **Who-Is**

■ I-Am

- pduSource: <Misha Belisle>
- iAmDeviceIdentifier:
Senior Applied Cybersecurity
Engineer
- vendorID: MITRE
- Adversary emulation and cyber R&D
- Interest in natural languages;
Spanish, Russian, ASL

■ I-Am

- pduSource: <Blaine Jeffries>
- iAmDeviceIdentifier:
Operational Technology Security
Engineer
- vendorID: MITRE
- Testbeds, Reverse Engineering
- Strategy card game fanatic:
MTG, Dominion, Ascension

Outline

- **What is Caldera?**
 - What can Caldera do?
- **What is Caldera for OT?**
 - What problem did we make Caldera for OT to solve?
 - What kinds of ICS protocols can we support?
 - How can you use Caldera for OT?
- **What's next?**
- **Where can I get Caldera for OT?**

What is CALDERA?

Open-Source Adversary Emulation Platform

- Automatable, repeatable emulation of realistic adversary attacks
- **Freely available on GitHub**



Portable

- Python3 app deployable to Mac/Linux server
- Frontend web interface
- Easily containerized



Accessible

- **Can run on a laptop!**
- Server Min Requirements: 8GM RAM, 2 CPU Cores
- Client: any device with a web browser



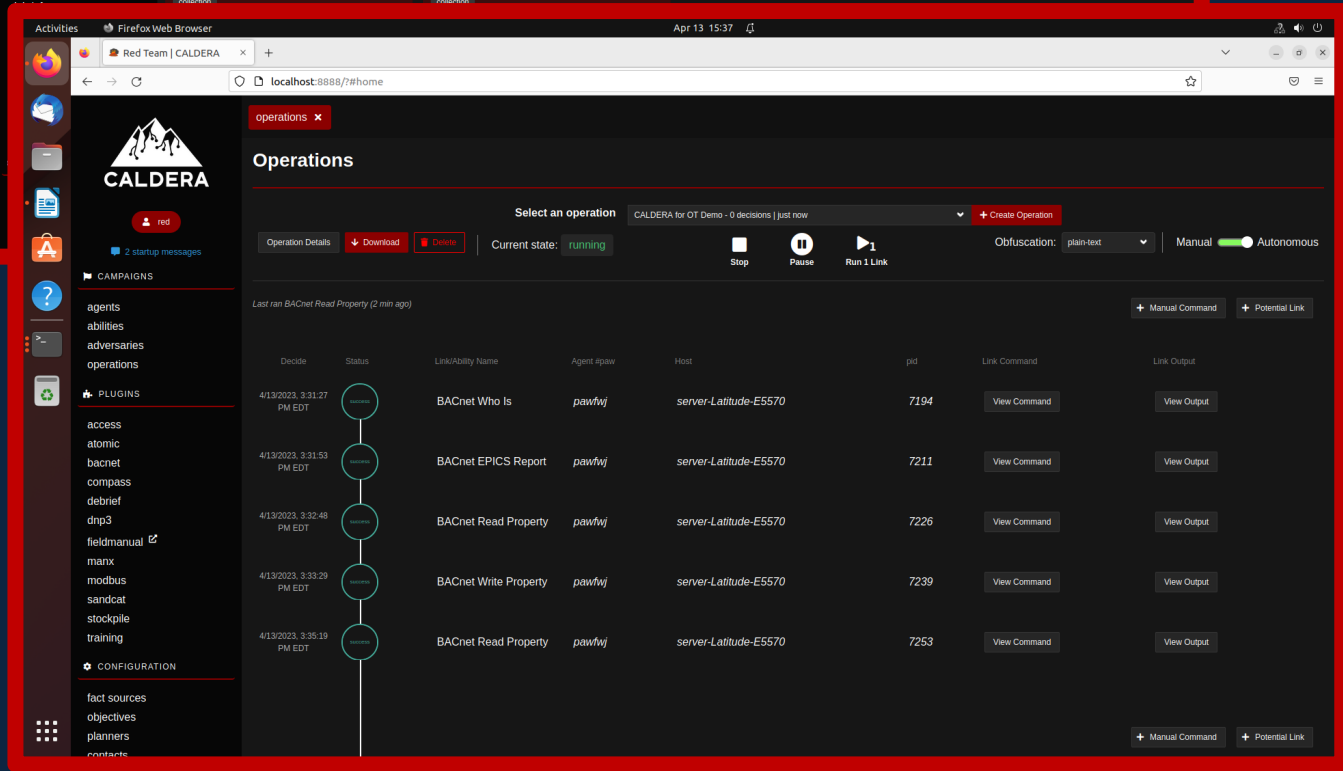
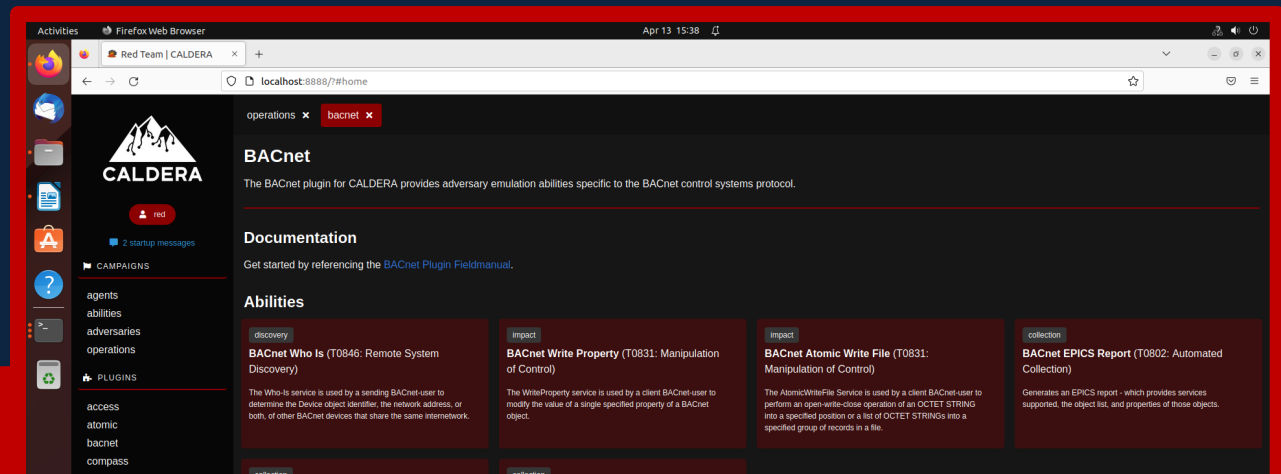
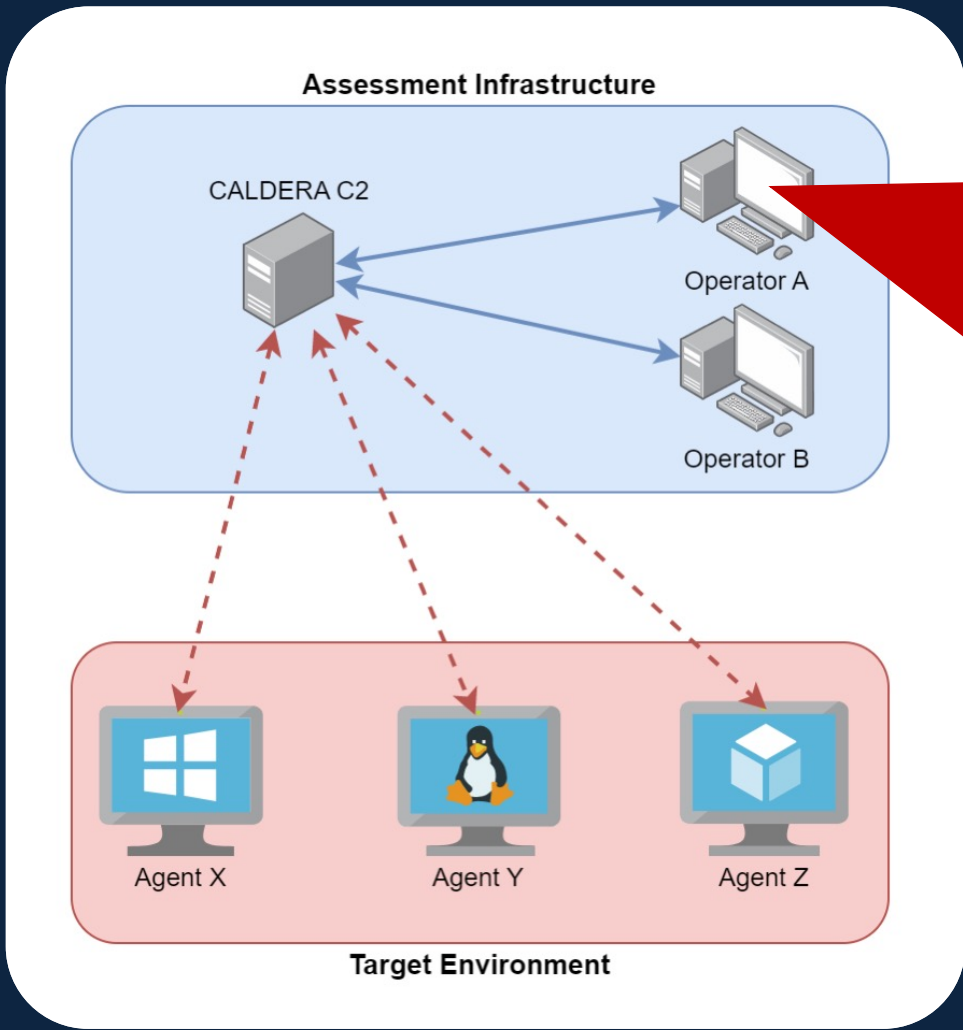
Flexible

- Agent support for: Windows, Linux, MacOS
- A dozen+ built-in plugins
- Supports custom plugin development

A Quick Note about Caldera-isms

- **Agent** – Software program that connects back to Caldera server
- **Ability** – Specific ATT&CK tactic/technique implementation; execute on an agent
- **Adversary** – Group of abilities representing the TTPs available to a threat actor
- **Operation** – Context in which abilities can be run on agent groups, based on adversary profiles. Also has the option to manually run abilities.
- **Fact** – Identifiable piece of information that may be required to execute an ability, e.g., an IP address, a hostname

Example Deployment



Why does Caldera Exist? Adversary Emulation is Hard



Exercises **cost** a lot to run



They require a significant **time** investment



Results are dependent on the capabilities of involved **personnel**



Exercises can be difficult to **repeat** unless extensively documented



Design (e.g., TTPs, scope, adversary profile, etc.) can be challenging

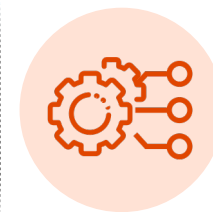
Caldera Makes Testing **Easier!**



Lowers the **cost** to run exercises



Less **time** intensive – can run and plan exercises faster



Dependent now on **attacker model**, not on personnel



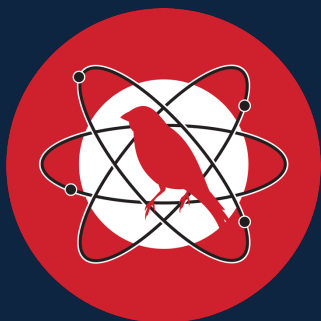
Can **repeat** tests at the push of a button



Designs can be saved, re-used, and designed with easy interfaces

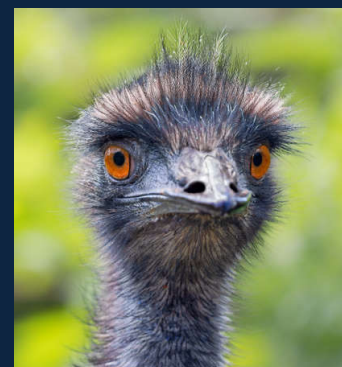
Caldera Plugins

- Core system with modular plugin architecture



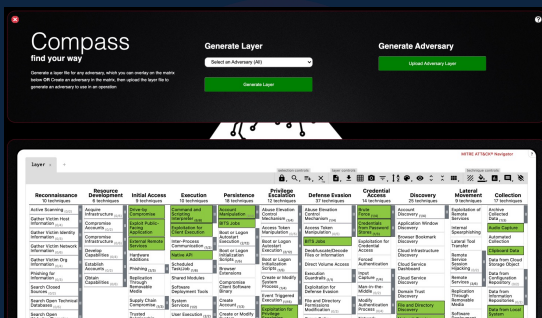
ATOMIC

Converts Atomic Red Team tests to CALDERA format



EMU

Converts Adversary Emulation Plans to CALDERA format



COMPASS

Generates Adversaries from the ATT&CK Matrix



CALDERA™ for OT

Purpose: Extend core to the OT environment

Why Caldera for OT?



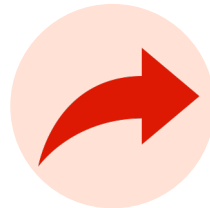
Lower the **barrier** to ICS skills



Efficient and **reliable** to repeat tests



Enable **testing** and tailoring of detections for known procedures



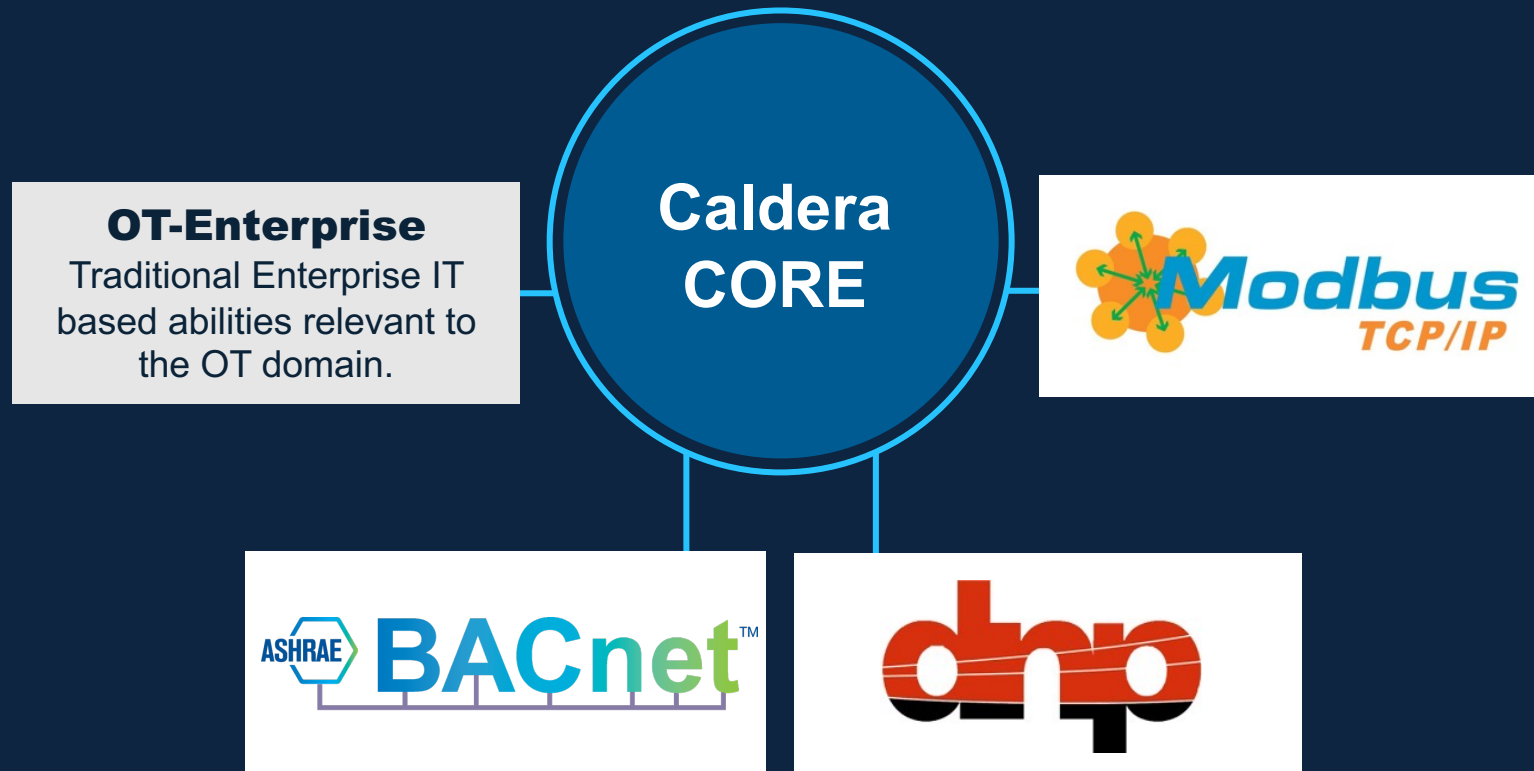
Simplify modification to execute iterative attacks to circumvent detections



Support threat emulation scenario integrators and operators **in the OT domain**

Caldera for OT Plugins

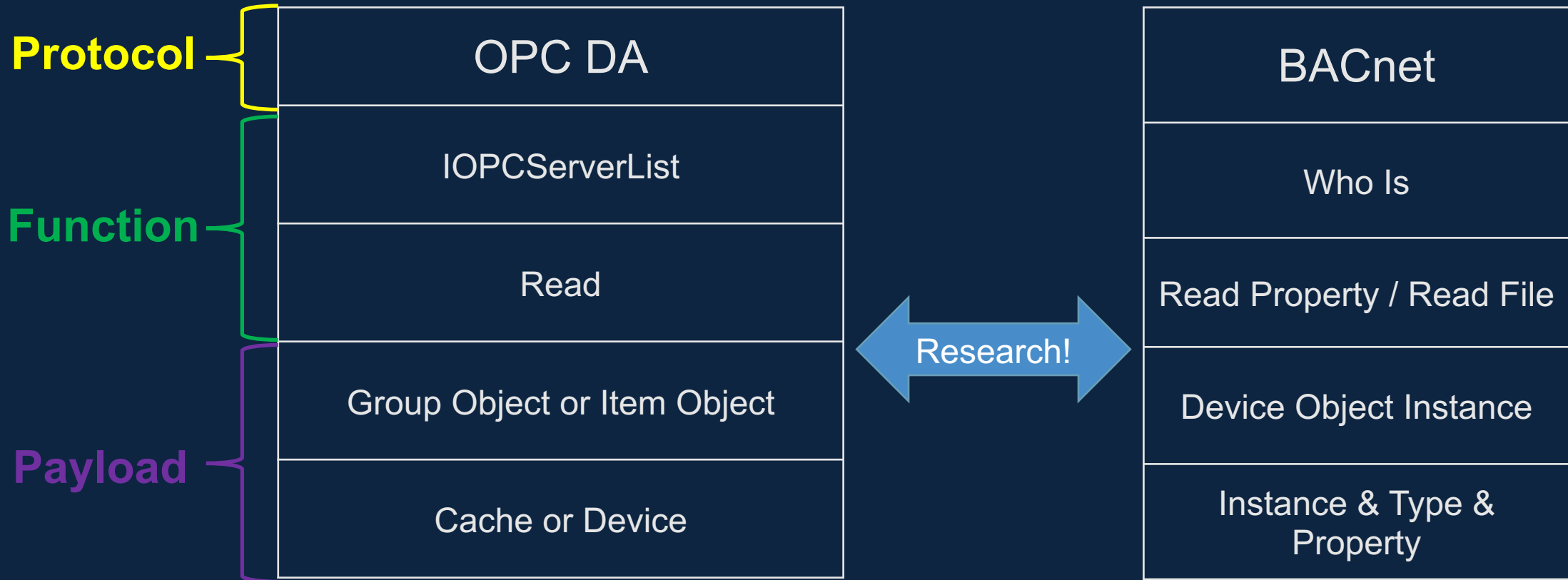
Expand operator toolkit with ATT&CK for ICS mapped OT abilities



Impact: Rapid integration & emulation in the OT environment

Expose native OT protocol functionality

Demonstrating a Technique Across Diverse Protocols



Other Use Cases



**Adversary
Emulation**



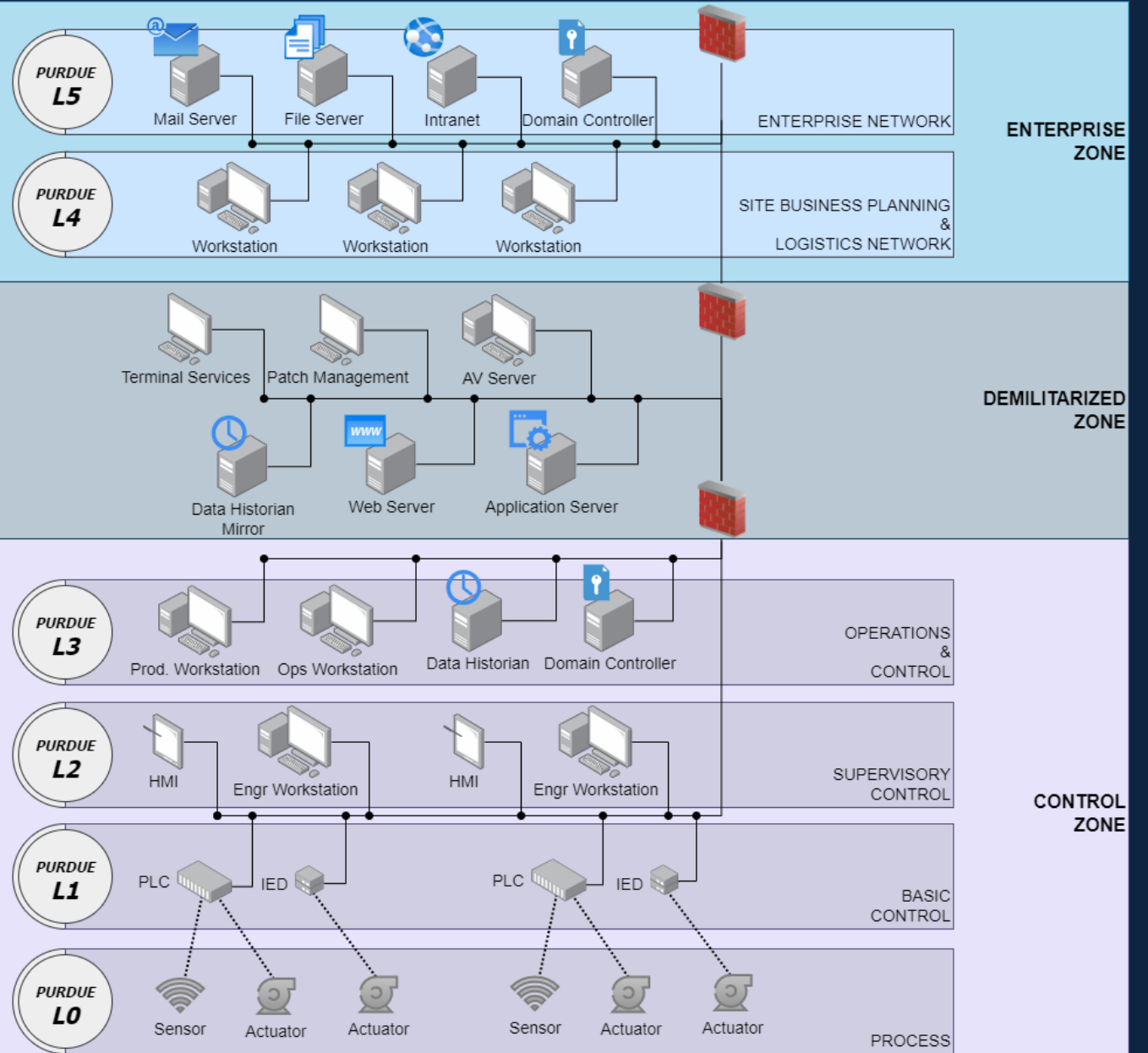
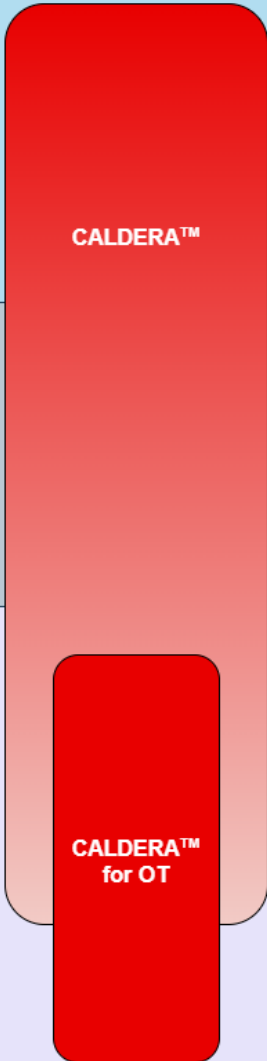
**Training &
Purple Teaming**



**FAT/SAT
Testing**

Caldera for OT Plugins provide extensible tooling for testing network security posture by coordinating the execution of real threat activity

Scenario Walkthrough



CALDERA™

CALDERA™
for OT

INITIAL ACCESS

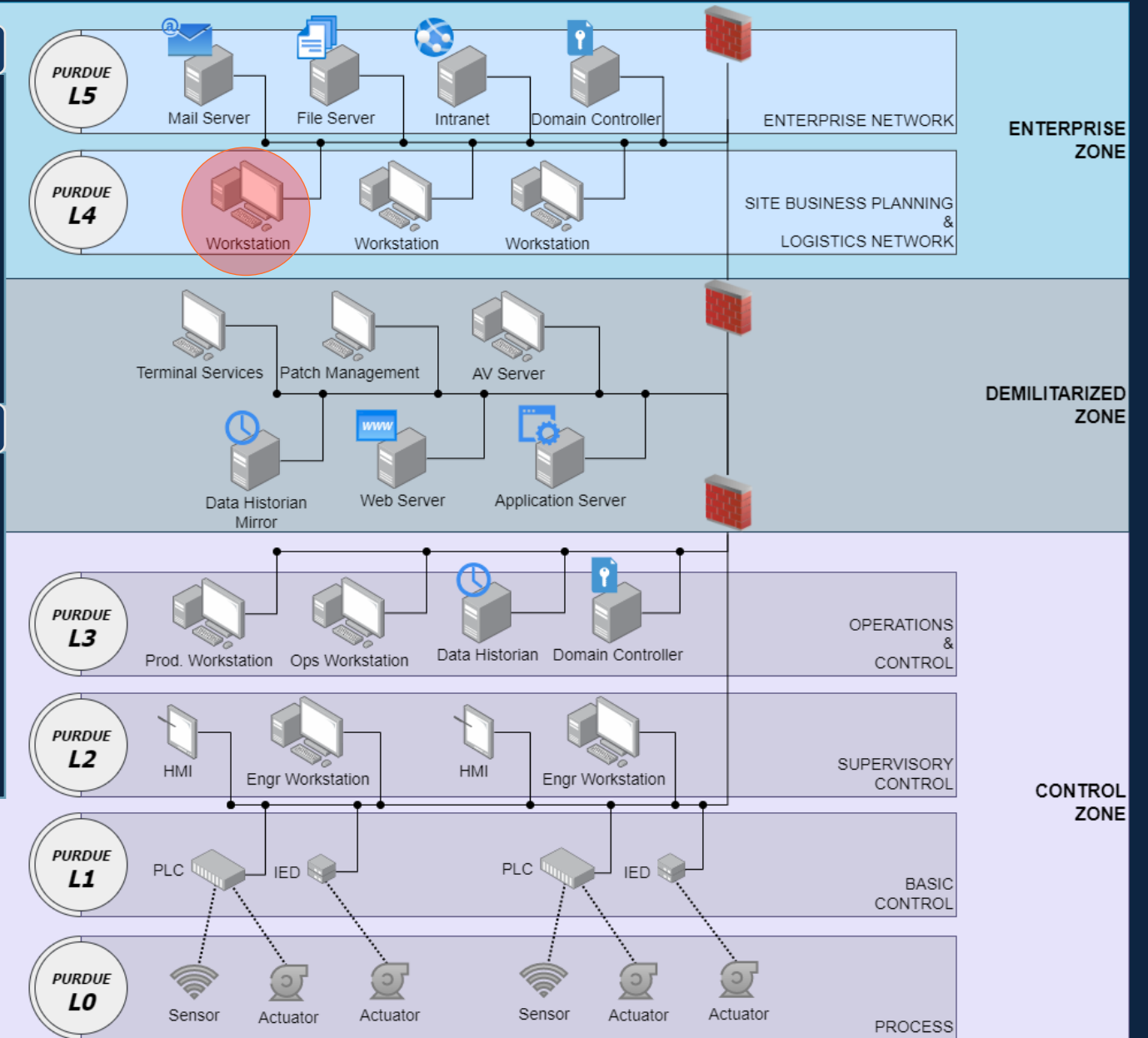
- *Phishing* T1566

User opens malicious email attachment that spawns a CALDERA agent in the Enterprise Zone.

PERSISTENCE

- *Logon / Boot Autostart Execution* T1547

Add encoded command in Windows registry to run CALDERA agent on system startup.



CALDERA™

CALDERA™
for OT

INITIAL ACCESS

PERSISTENCE

DISCOVERY

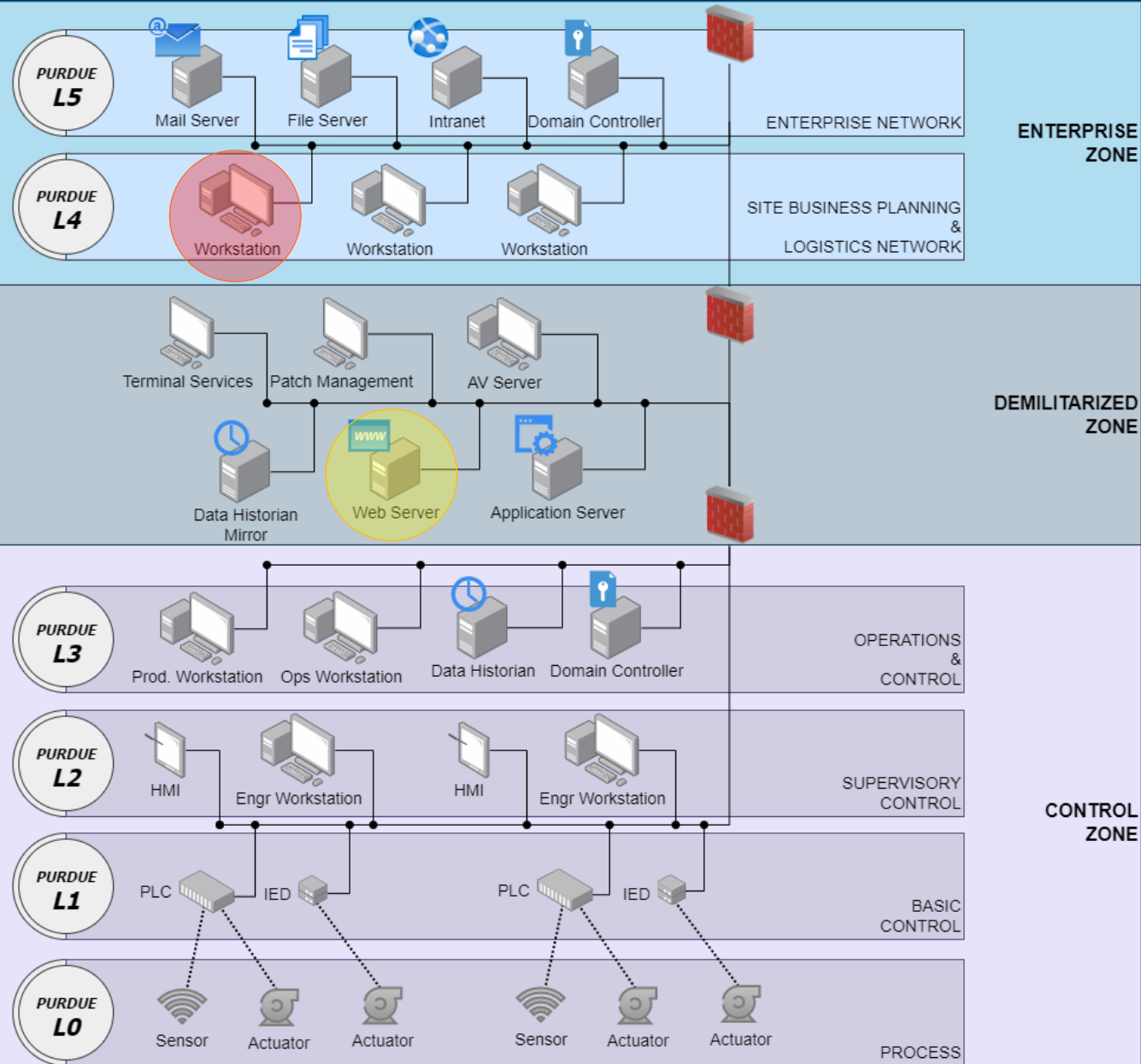
- *Account Discovery* T1087
- *Process Discovery* T1057
- *System Network Connections Discovery* T1049

Discover local accounts, processes, and network connections. An internal webserver is identified as a potential target.

CREDENTIAL ACCESS

- *OS Credential Dumping* T1003

Dump local workstation credentials using PowerSploit Invoke-Mimikatz module.



CALDERA™

CALDERA™
for OT

INITIAL ACCESS

PERSISTENCE

DISCOVERY

CREDENTIAL ACCESS

RECONNAISSANCE

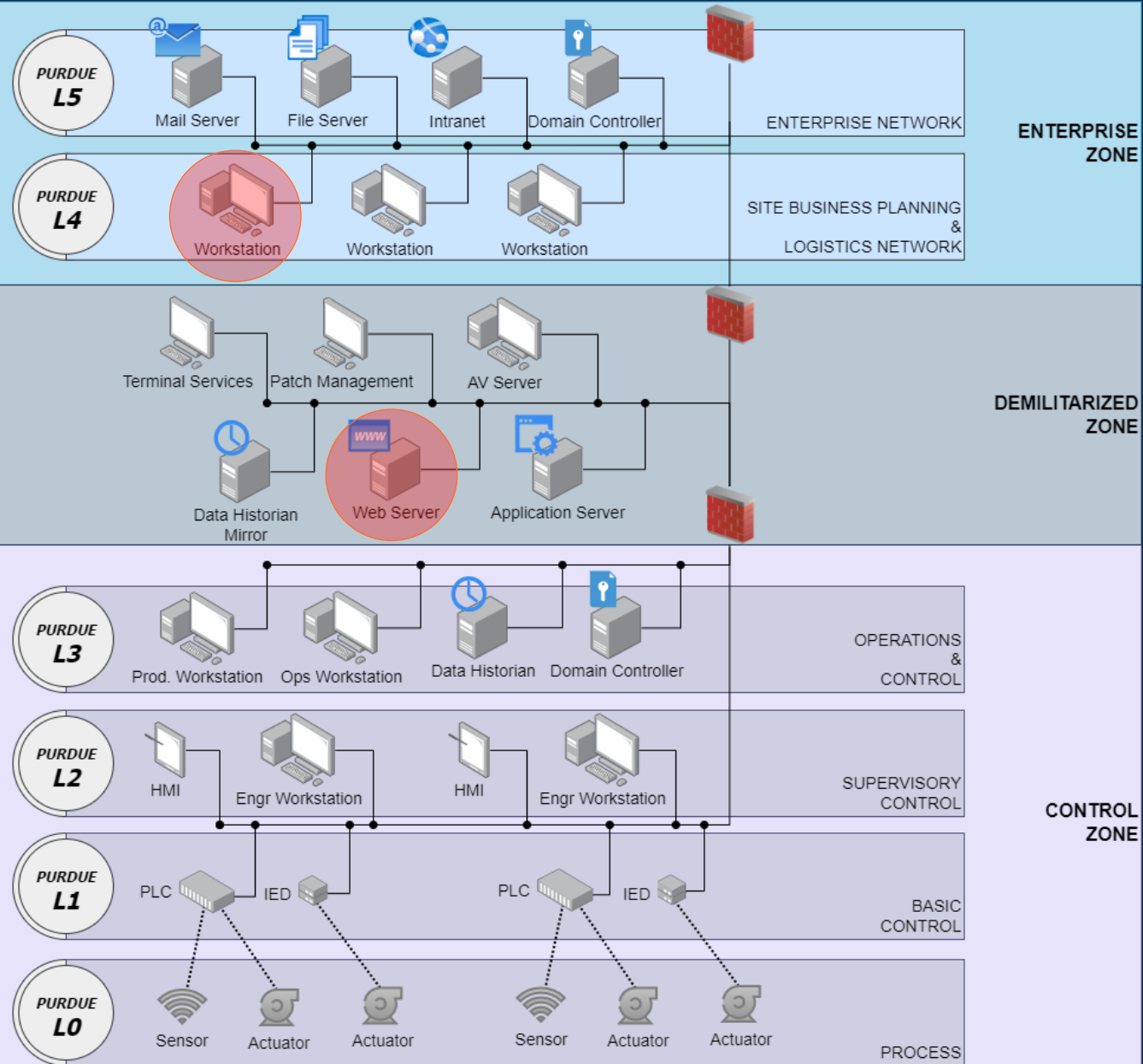
- Active Scanning T1595

Scan the identified web server for potential vulnerabilities.

LATERAL MOVEMENT

- Exploitation of Remote Services T1210

Exploit a remote-code-execution vulnerability on the web server to spawn an agent in the DMZ.



CALDERA™

CALDERA™
for OT

INITIAL ACCESS

PERSISTENCE

DISCOVERY

CREDENTIAL ACCESS

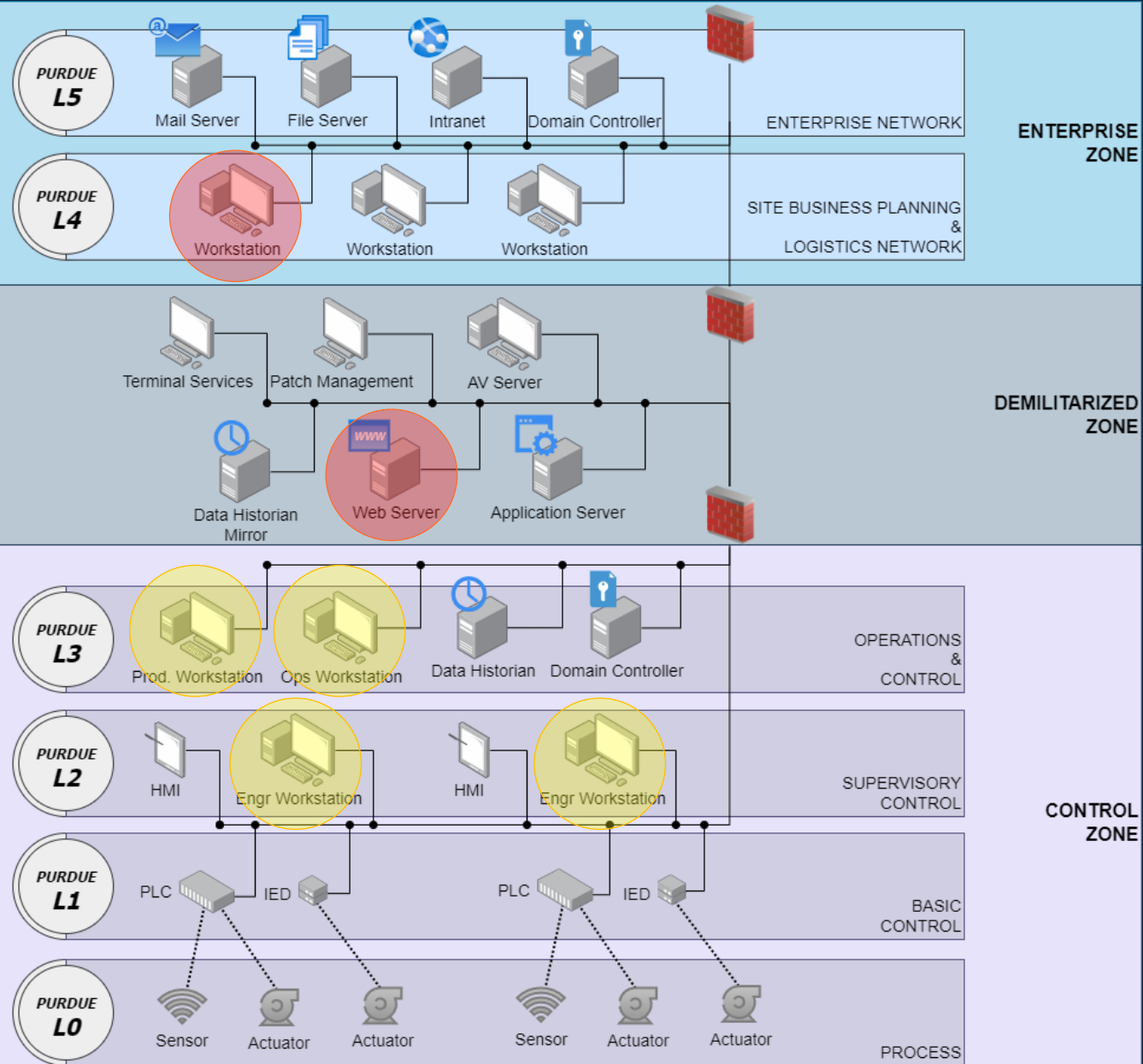
RECONNAISSANCE

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.



CALDERA™

CALDERA™
for OT

INITIAL ACCESS

PERSISTENCE

DISCOVERY

CREDENTIAL ACCESS

RECONNAISSANCE

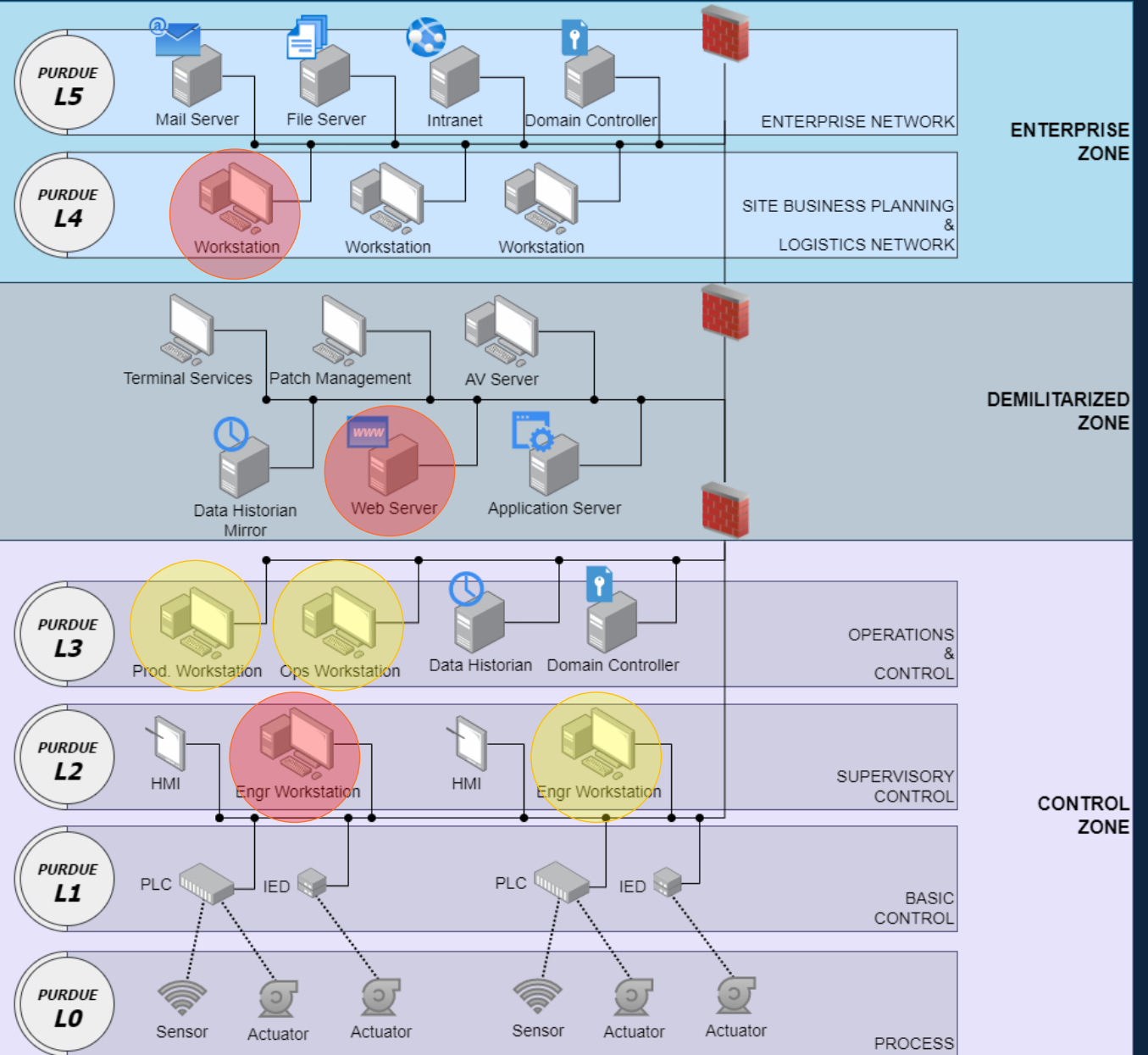
LATERAL MOVEMENT

DISCOVERY

LATERAL MOVEMENT

- Remote Services T1021
- Lateral Tool Transfer T1570

Using a valid account collected from the enterprise workstation, remotely download and execute the agent payload to gain access to a Control Zone workstation.



CALDERA™

CALDERA™
for OT

INITIAL ACCESS

PERSISTENCE

DISCOVERY

CREDENTIAL ACCESS

RECONNAISSANCE

LATERAL MOVEMENT

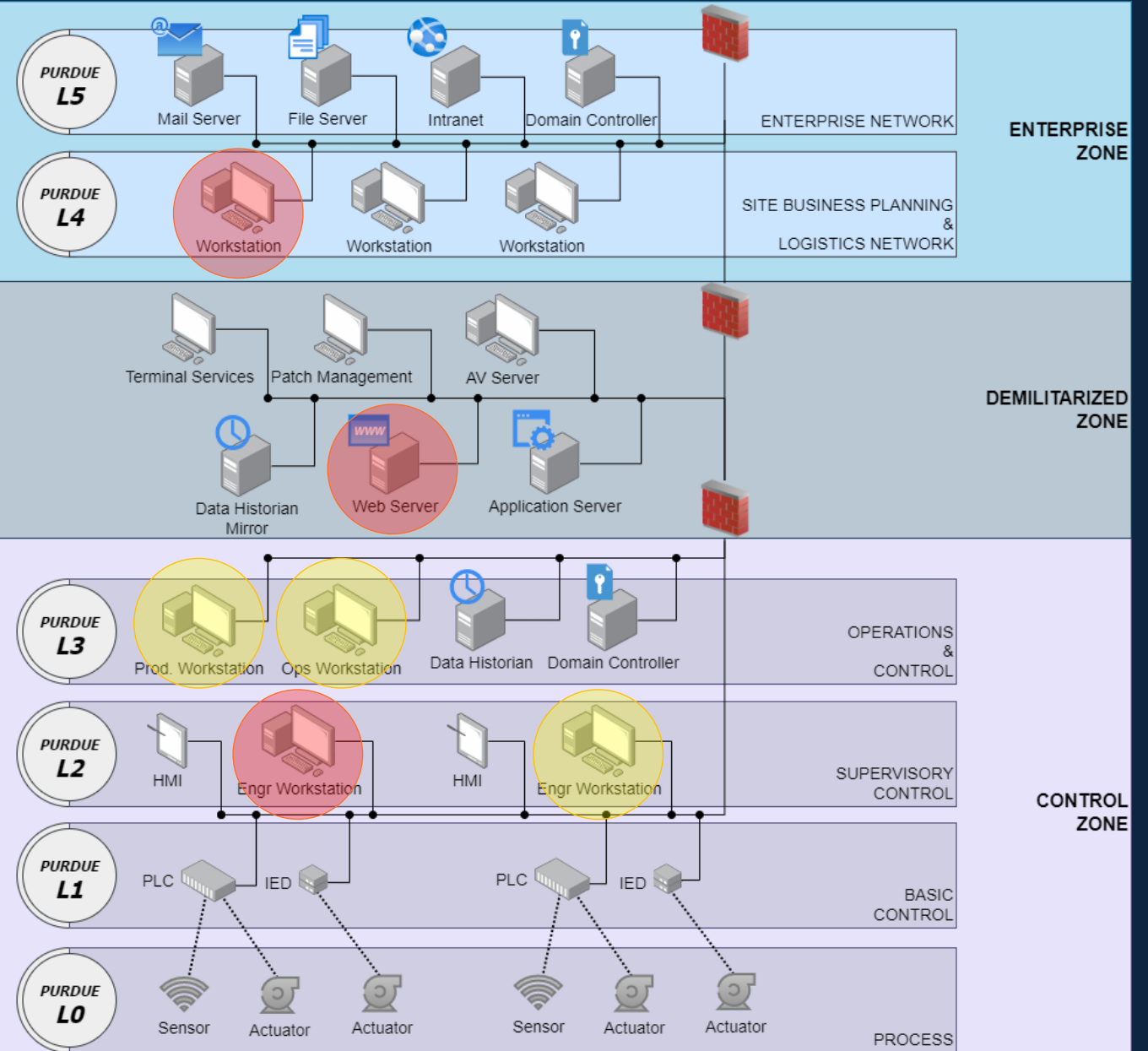
DISCOVERY

LATERAL MOVEMENT

PERSISTENCE

- Logon / Boot Autostart Execution T1547

Add encoded command in Windows registry to run CALDERA agent on system startup.



CALDERA™

INITIAL ACCESS

PERSISTENCE

DISCOVERY

CREDENTIAL ACCESS

RECONNAISSANCE

LATERAL MOVEMENT

DISCOVERY

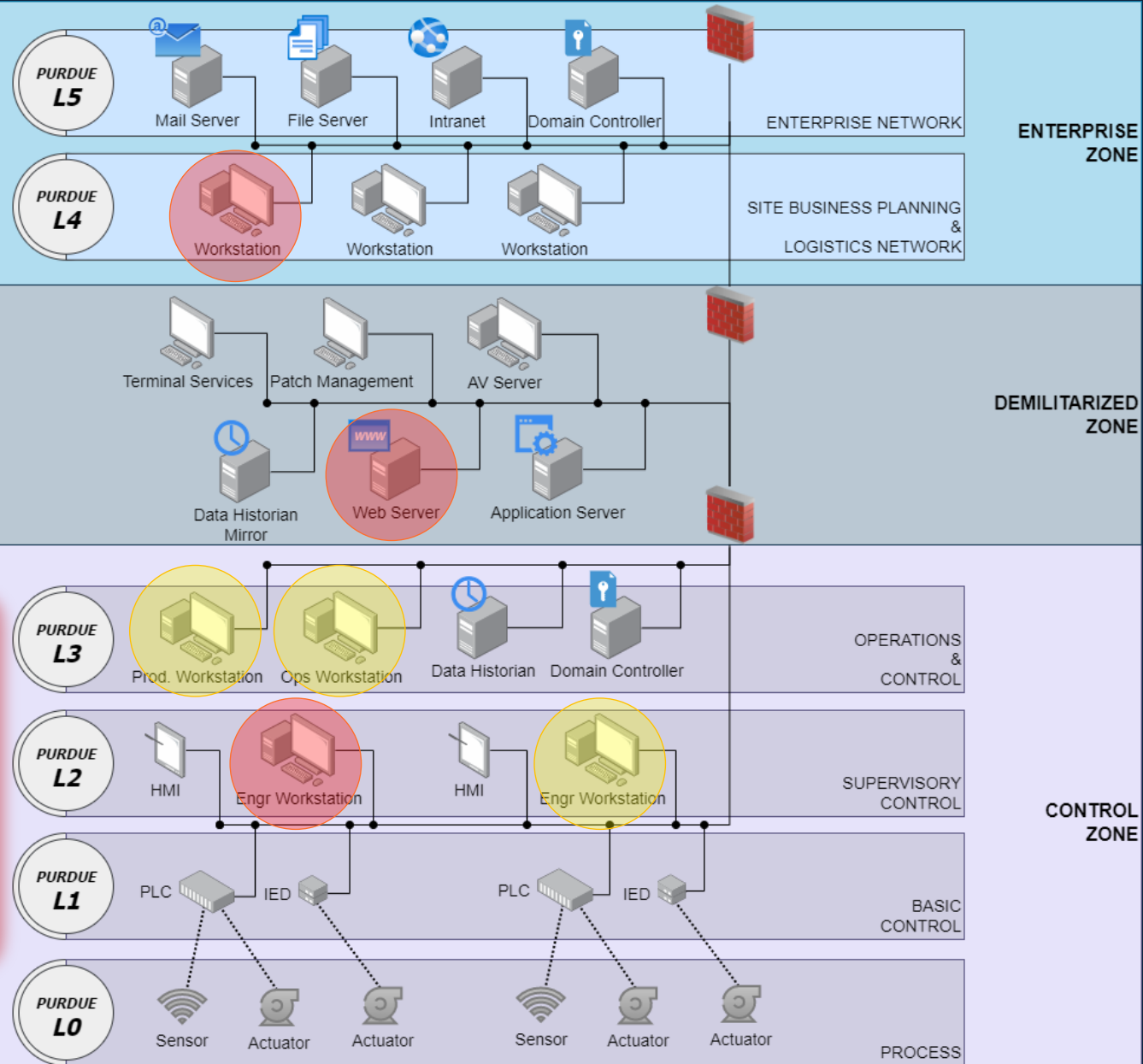
LATERAL MOVEMENT

PERSISTENCE

CALDERA™
for OT

CALDERA alone is limited in abilities applicable to Purdue L2 / L1 assets.

Enter CALDERA for OT!



BACnet Plugin Abilities

BACnet

The BACnet plugin for CALDERA provides adversary emulation abilities specific to the BACnet control systems protocol.

Documentation

Get started by referencing the [BACnet Plugin Fieldmanual](#).

Abilities

discovery

BACnet Who Is (T0846: Remote System Discovery)

The Who-Is service is used by a sending BACnet-user to determine the Device object identifier, the network address, or both, of other BACnet devices that share the same internetwork.

impact

BACnet Write Property (T0831: Manipulation of Control)

The WriteProperty service is used by a client BACnet-user to modify the value of a single specified property of a BACnet object.

impact

BACnet Atomic Write File (T0831: Manipulation of Control)

The AtomicWriteFile Service is used by a client BACnet-user to perform an open-write-close operation of an OCTET STRING into a specified position or a list of OCTET STRINGS into a specified group of records in a file.

collection

BACnet EPICS Report (T0802: Automated Collection)

Generates an EPICS report - which provides services supported, the object list, and properties of those objects.

collection

BACnet Read Property (T0861: Point & Tag Identification)

The ReadProperty service is used by a client BACnet-user to request the value of one property of one BACnet Object.

collection

BACnet Atomic Read File (T0801: Monitor Process State)

The AtomicReadFile Service is used by a client BACnet-user to perform an open-read-close operation on the contents of the specified file. The file is saved locally.



red

2 startup messages

CAMPAIGNS

- agents
- abilities
- adversaries
- operations

PLUGINS

- access
- atomic
- bacnet
- compass
- debrief
- dnp3
- fieldmanual
- manx
- modbus
- sandcat
- stockpile
- training

CONFIGURATION

- fact sources
- objectives
- planners
- contacts

operations x

Operations

Select an operation

CALDERA for OT Demo - 0 decisions | just now

+ Create Operation

Operation Details

Download

Delete

Current state: **running**

Stop

Pause

Run 1 Link

Obfuscation: plain-text

Manual Autonomous

Last ran BACnet Read Property (2 min ago)

+ Manual Command

+ Potential Link

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command	Link Output
4/13/2023, 3:31:27 PM EDT	success	BACnet Who Is	pawfwj	server-Latitude-E5570	7194	View Command	View Output
4/13/2023, 3:31:53 PM EDT	success	BACnet EPICS Report	pawfwj	server-Latitude-E5570	7211	View Command	View Output
4/13/2023, 3:32:48 PM EDT	success	BACnet Read Property	pawfwj	server-Latitude-E5570	7226	View Command	View Output
4/13/2023, 3:33:29 PM EDT	success	BACnet Write Property	pawfwj	server-Latitude-E5570	7239	View Command	View Output
4/13/2023, 3:35:19 PM EDT	success	BACnet Read Property	pawfwj	server-Latitude-E5570	7253	View Command	View Output

+ Manual Command

+ Potential Link



red

2 startup messages

CAMPAIGNS

agents
abilities
adversaries
operations

PLUGINS

access
atomic
bacnet
compass
debrief
dnp3
fieldmanual
manx
modbus
sandcat
stockpile
training

CONFIGURATION

fact sources
objectives
planners
contacts

operations x

Operations

Select an operation

CALDERA for OT Demo - 0 decisions | just now

+ Create Operation

Operation Details

Download

Delete

Current state: **running**

Stop

Pause

Run 1 Link

Obfuscation: plain-text

Manual Autonomous

Last ran BACnet Read Property (2 min ago)

+ Manual Command

+ Potential Link

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 `./bacwi`

Output

Exit Code: Nothing to show

Standard Output:

```
;Device   MAC (hex)           SNET  SADR (hex)         APDU
;-----
200121  C0:A8:00:03:BA:C0  0     00                 1476
;
; Total Devices: 1
```

Standard Error: Nothing to show

server-Latitude-E5570

7253

View Command

View Output

+ Manual Command

+ Potential Link





operations x

Operations

red

2 startup messages

CAMPAIGNS

- agents
- abilities
- adversaries
- operations

PLUGINS

- access
- atomic
- bacnet
- compass
- debrief
- dnp3
- fieldmanual
- manx
- modbus
- sandcat
- stockpile
- training

CONFIGURATION

- fact sources
- objectives
- planners
- contacts

Select an operation

CALDERA for OT Demo - 0 decisions | just now

+ Create Operation

Operation Details

Download

Delete

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"  
},
```

+ Manual Command

+ Potential Link





red

2 startup messages

CAMPAIGNS

- agents
- abilities
- adversaries
- operations

PLUGINS

- access
- atomic
- bacnet
- compass
- debrief
- dnp3
- fieldmanual
- manx
- modbus
- sandcat
- stockpile
- training

CONFIGURATION

- fact sources
- objectives
- planners
- contacts

operations x

Operations

Select an operation

CALDERA for OT Demo - 0 decisions | just now

+ Create Operation

Operation Details

Download

Delete

Current state: **running**

Stop

Pause

Run 1 Link

Obfuscation: plain-text

Manual Autonomous

Last ran BACnet Read Property (2 min ago)

+ Manual Command

+ Potential Link

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command	Link Output
4/13/2023, 3:31:27 PM EDT	success	BACnet Who Is	pawfwj			Command <code>./bacrp 200121 1 1 85 -1</code>	
4/13/2023, 3:31:53 PM EDT	success	BACnet EPICS Report	pawfwj			Output	
4/13/2023, 3:32:48 PM EDT	success	BACnet Read Property	pawfwj			Exit Code: Nothing to show Standard Output: <code>0.000000</code>	
4/13/2023, 3:33:29 PM EDT	success	BACnet Write Property	pawfwj			Standard Error: Nothing to show	
4/13/2023, 3:35:19 PM EDT	success	BACnet Read Property	pawfwj	server-Latitude-E5570	7253	View Command	View Output

+ Manual Command

+ Potential Link





red

2 startup messages

CAMPAIGNS

- agents
- abilities
- adversaries
- operations

PLUGINS

- access
- atomic
- bacnet
- compass
- debrief
- dnp3
- fieldmanual
- manx
- modbus
- sandcat
- stockpile
- training

CONFIGURATION

- fact sources
- objectives
- planners
- contacts

operations x

Operations

Select an operation

CALDERA for OT Demo - 0 decisions | just now

+ Create Operation

Operation Details

Download

Delete

Current state: **running**

Stop

Pause

Run 1 Link

Obfuscation: plain-text

Manual Autonomous

Last ran BACnet Read Property (2 min ago)

+ Manual Command

+ Potential Link

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command	Link Output
4/13/2023, 3:31:27 PM EDT	success	BACnet Who Is	pawfwj	server-Latitude-E5570	7194	View Command	View Output
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 `./bacwp 200121 1 1 85 1 -1 1 100`

Output

Exit Code: Nothing to show

Standard Output:

WriteProperty Acknowledged!

Standard Error: Nothing to show

+ Manual Command

+ Potential Link





red

2 startup messages

CAMPAIGNS

- agents
- abilities
- adversaries
- operations

PLUGINS

- access
- atomic
- bacnet
- compass
- debrief
- dnp3
- fieldmanual
- manx
- modbus
- sandcat
- stockpile
- training

CONFIGURATION

- fact sources
- objectives
- planners
- contacts

operations x

Operations

Select an operation

CALDERA for OT Demo - 0 decisions | just now

+ Create Operation

Operation Details

Download

Delete

Current state: **running**

Stop

Pause

Run 1 Link

Obfuscation: plain-text

Manual Autonomous

Last ran BACnet Read Property (2 min ago)

+ Manual Command

+ Potential Link

Decide	Status	Link/Ability Name	Agent #paw	Host	pid	Link Command	Link Output
4/13/2023, 3:31:27 PM EDT	success	BACnet Who Is	pawfwj	server-Latitude-E5570	7194	View Command	View Output
4/13/2023, 3:31:53 PM EDT	success	BACnet EPICS Report	pawfwj	server-Latitude-E5570	7211	View Command	View Output
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 `./bacrp 200121 1 1 85 -1`

Output

Exit Code: Nothing to show

Standard Output:

```
100.000000
```

Standard Error: Nothing to show

+ Manual Command

+ Potential Link

CALDERA™

INITIAL ACCESS

PERSISTENCE

DISCOVERY

CREDENTIAL ACCESS

RECONNAISSANCE

LATERAL MOVEMENT

DISCOVERY

LATERAL MOVEMENT

PERSISTENCE

DISCOVERY

- Rem. System Discovery T0846

BACnet Who Is

COLLECTION

- Automated Collection T0802

- Point & Tag Identification T0861

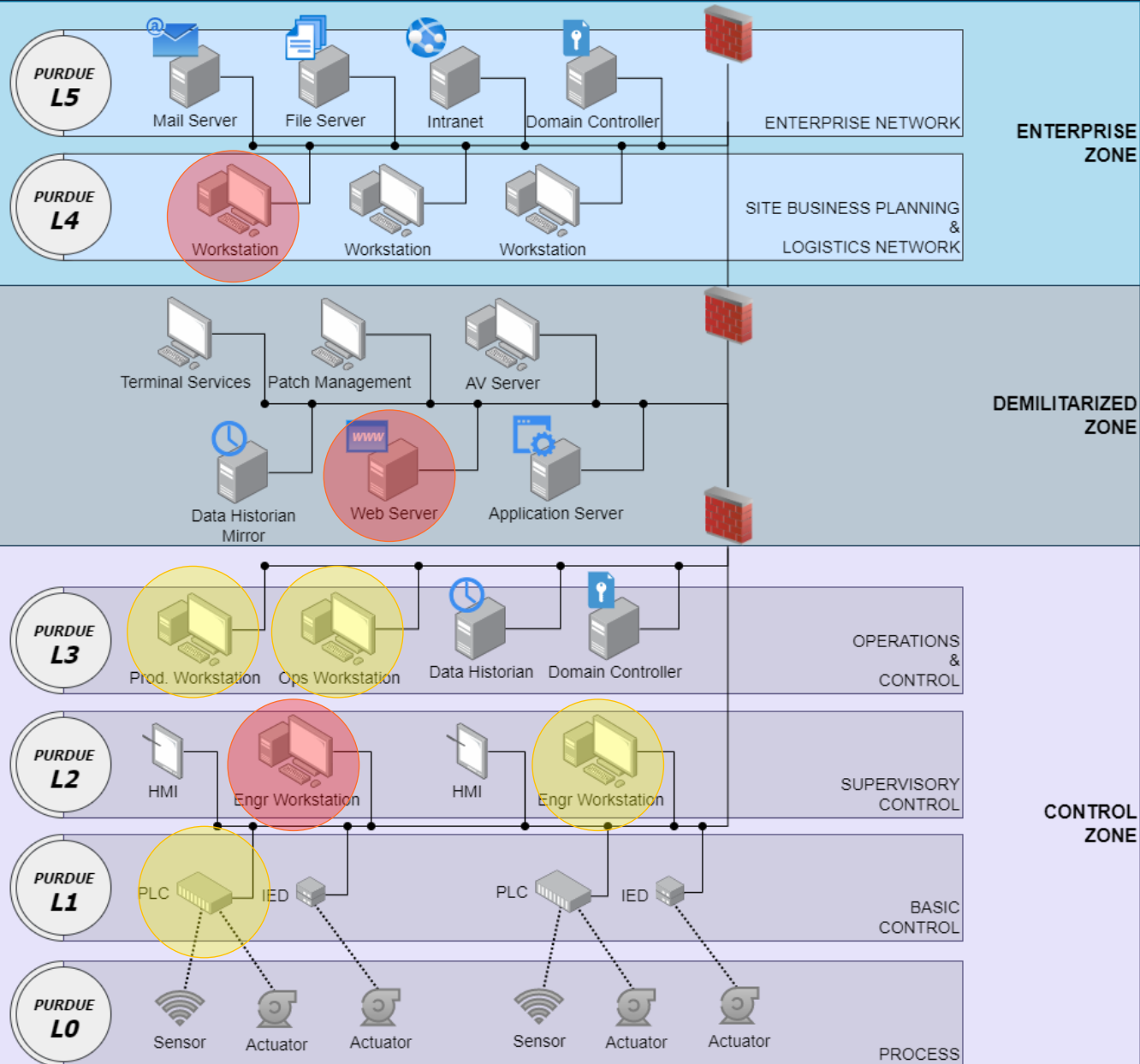
BACnet EPICS Report

BACnet Read Property

IMPACT

- Manipulation of Control T0831

BACnet Write Property



CALDERA™
for OT

Try it yourself! (visit us at Booth #8!)



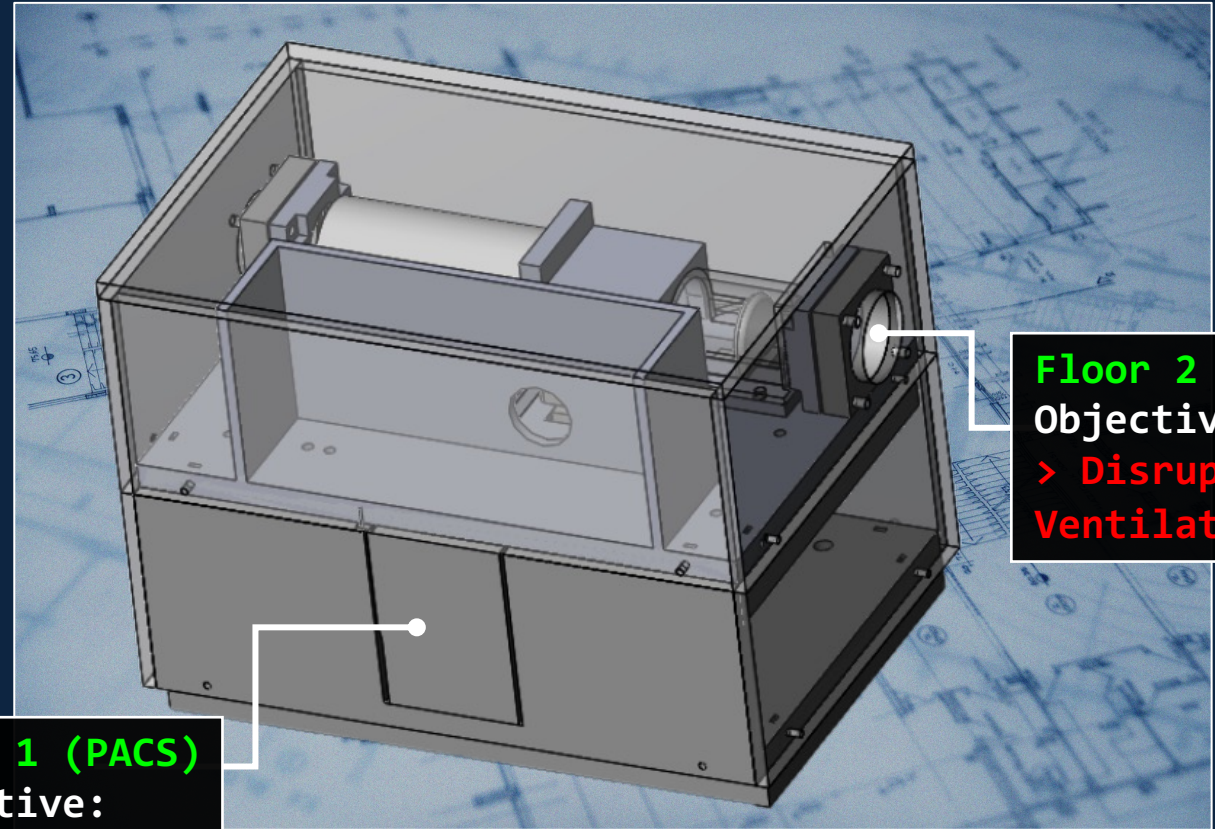
Hands-on Demo!:

- Portable “building in a box”
- Interact with Caldera for OT plugins



The Mission:

- Challenge 1: PACS
- Challenge 2: HVAC



Floor 1 (PACS)
Objective:
> **Gain Entry**

Floor 2 (HVAC)
Objective:
> **Disrupt Ventilation**

Future Direction (and how you can contribute!)



Future Releases:

- Expand ICS protocol coverage and capabilities
- Caldera for OT blog posts and learning materials



Community Engagement:

- Actively seeking feedback and collaboration opportunities
- Contribute to the open-source on GitHub!

Coming Soon:

<https://github.com/mitre/caldera-ot>

Explore Caldera:

<https://github.com/mitre/caldera>



Reach us at:

OT@mitre.org

Caldera™ for OT

Contact Information



OT@mitre.org

mbelisle@mitre.org

bjeffries@mitre.org



<https://github.com/mitre/caldera-ot>

<https://github.com/mitre/caldera>