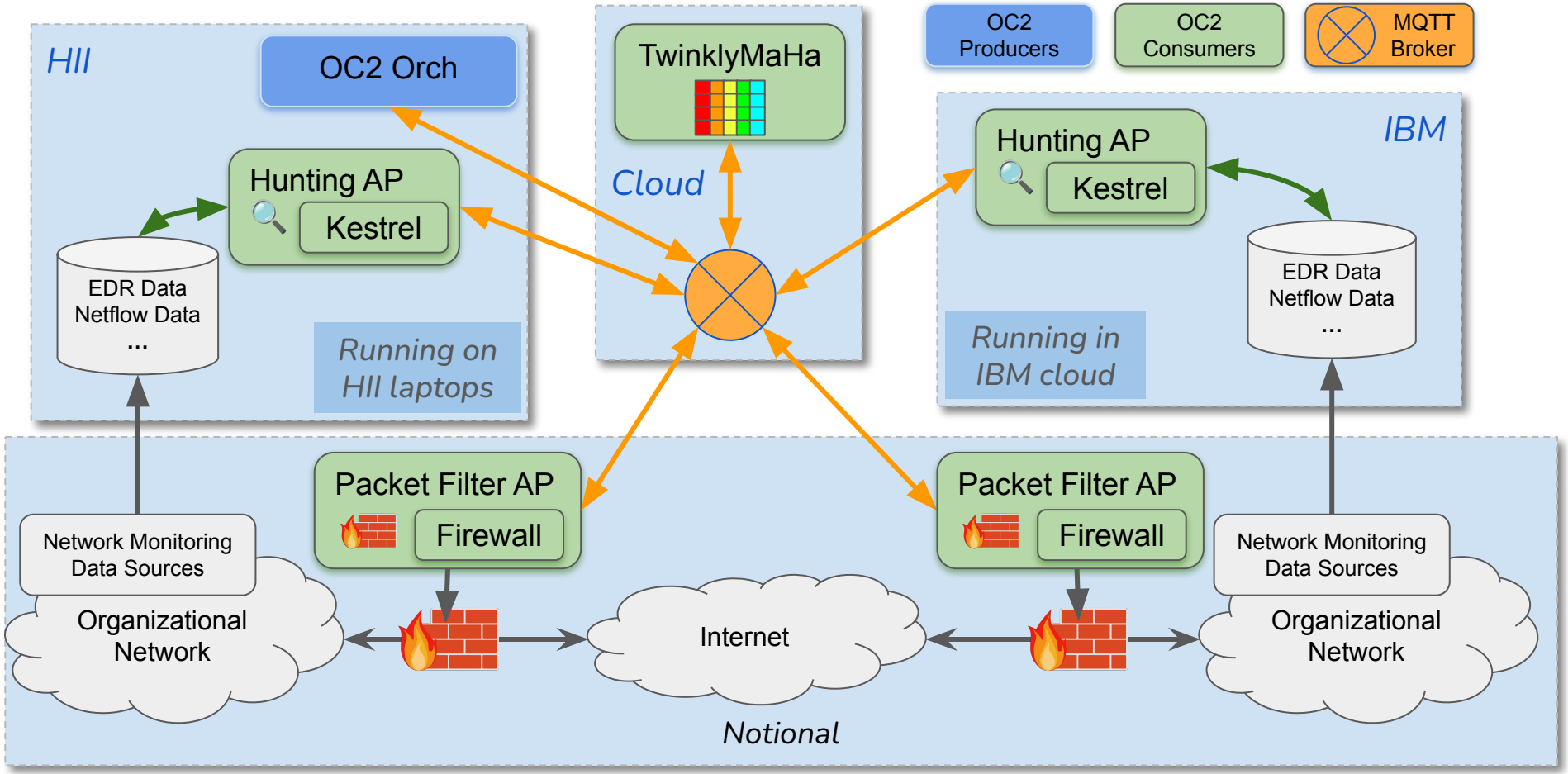
Enhancing Cybersecurity through OpenC2 and Kestrel, STIX Shifter Collaboration

Michael Le, Xiaokui Shu (IBM),
David Lemire, Kevin Cressman, Matt Roberts (HII)

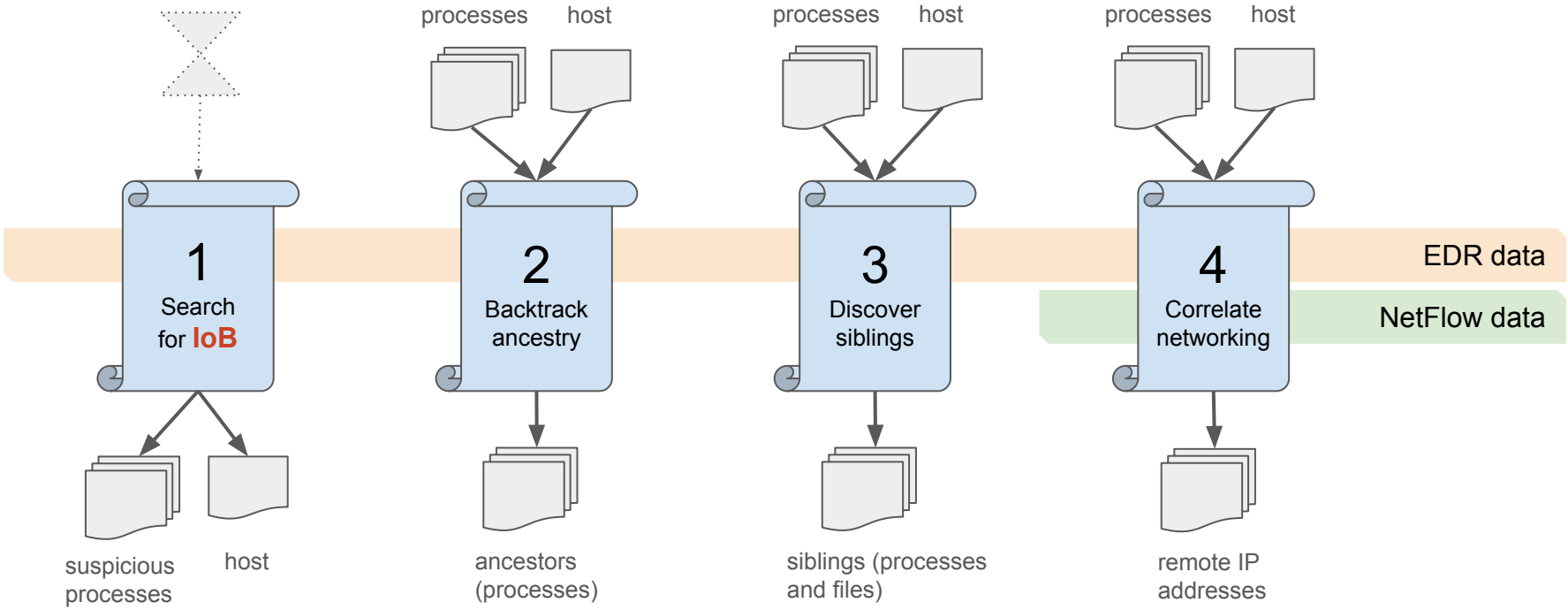
Scope (AKA, what we're demonstrating)

Demonstrating	Using
Threat Hunting Capabilities	Kestrel Threat Hunting Language
Kestrel Invocation	OpenC2 & Threat Hunting AP
Hunting for Behavior	IoB Concepts
Process Organization	CACAO Playbook
Data Formats & Transformation	STIX / STIX-Shifter
Cross-Geolocation / Organization Activity	All Demo Components
Network Block From Hunt Result Notional	*OpenC2 & Packet Filter AP*

Demonstration Network Topology

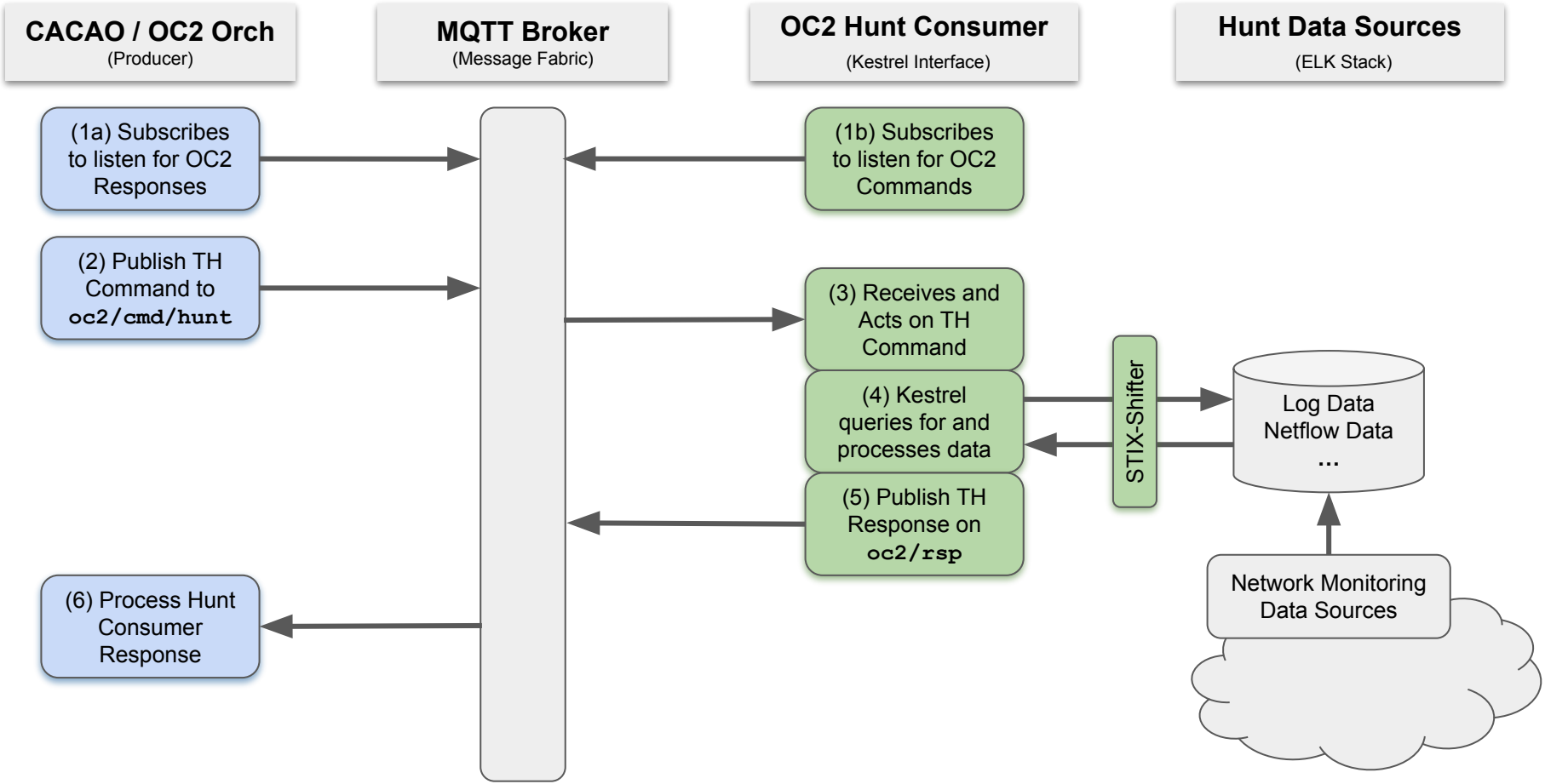


Kestrel Hunts Ready to Call



IoB provided (can be dynamically fed) for this demo: **T1562.004** Disable or Modify System Firewall

Process Flow Diagram: OpenC2 Invoking Kestrel



Demonstration

Hunting Automation with CACAO

enables

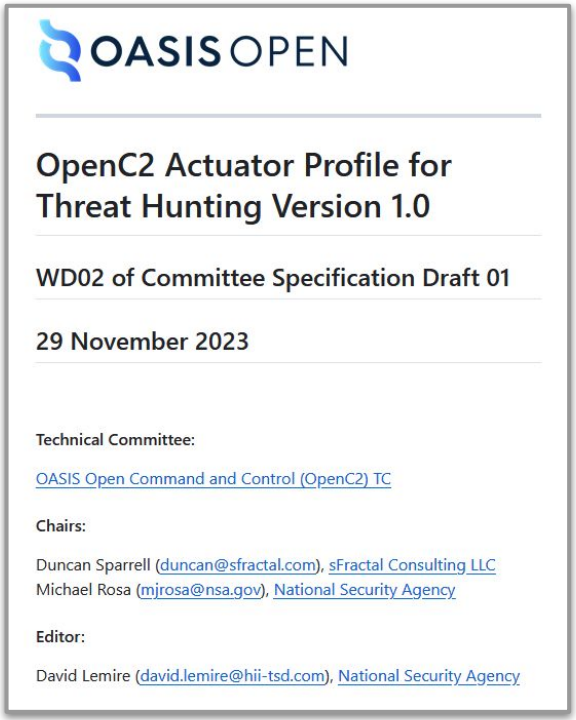
DEMO

OC2 Cross-org hunting and response

enables

OC2 Hunting AP

OIF Framework


OASIS OPEN

OpenC2 Actuator Profile for Threat Hunting Version 1.0

WD02 of Committee Specification Draft 01

29 November 2023

Technical Committee:

OASIS Open Command and Control (OpenC2) TC

Chairs:

Duncan Sparrell (duncan@sfractal.com), sFractal Consulting LLC
Michael Rosa (mjrosa@nsa.gov), National Security Agency

Editor:

David Lemire (david.lemire@hii-tsd.com), National Security Agency

Publication pending (CSD02)

The Olympic Destroyer Hunt

CASP 2024: Hunt an Entire Threat from an Indicator of Behavior

Let's start from T1562.004 *Impair Defenses: Disable or Modify System Firewall*

On the MITRE page of the TTP, there is a *Detection* section listing different ways to detect it. The first is using command execution. Let's write an IoB for this *Disable or Modify System Firewall* behavior.

Initial IoB match

```
In [1]: # IoB: T1562.004
disablefw = GET process FROM stixshifter://casp2024-edr
            WHERE (name = 'ufw' AND command_line LIKE '%disable%')
               OR (name = 'sudo' AND command_line LIKE '%ufw disable%')
               OR (name IN ('netsh', 'netsh.exe') AND command_line LIKE '%advfirewall%off%')
            LAST 30 DAYS
```

Block Executed in 4 seconds

VARIABLE	TYPE	# (ENTITIES)	# (RECORDS)	directory*	file*	ipv4-addr*
disablefw	process	1	3	3	5	3

*Number of related records cached.

Cross-source hunt

```
In [7]: # Can we find the traffic at the OPNSense/firewall to take further action, e.g., adding rule to block the IP

        # Data Issue Found
        # for some reason, the clock has 30 min diff between the host and the firewall
        # so we need to add "LAST 30 DAYS" to override Kestrel's automatic time range generation

        nt_fw = GET network-traffic FROM stixshifter://casp2024-netflow
                WHERE src_port = nt.src_port

        c2_ip = FIND ipv4-addr ACCEPTED nt_fw
        DISP c2_ip ATTR value
```

value
172.16.1.14
172.16.1.13

Block Executed in 4 seconds

VARIABLE	TYPE	# (ENTITIES)	# (RECORDS)	directory*	domain-name*	file*	ipv4-addr*	ipv6-addr*	mac-addr*	network-traffic*	process*	software*	user-account*	x-oca-asset*	x-oca-event*
nt_fw	network-traffic	3	33	0	0	0	450	0	0	147	150	0	0	0	150
c2_ip	ipv4-addr	2	157	41	7	44	477	30	30	157	194	41	30	30	180

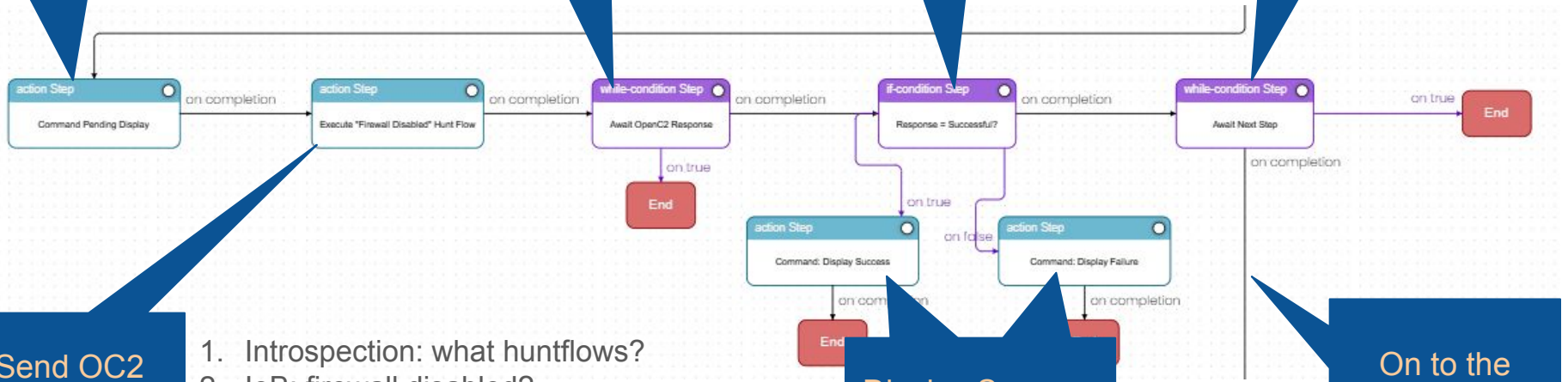
Playbook “Stages” Are Steps In The Hunting Process Demonstration

Display Action Pending Indication (Yellow) on TwinklyMaHa

Await OC2 Response(s)

Assess OC2 Response(s)

Await Direction to Proceed



Send OC2 Command to Hunt Consumer

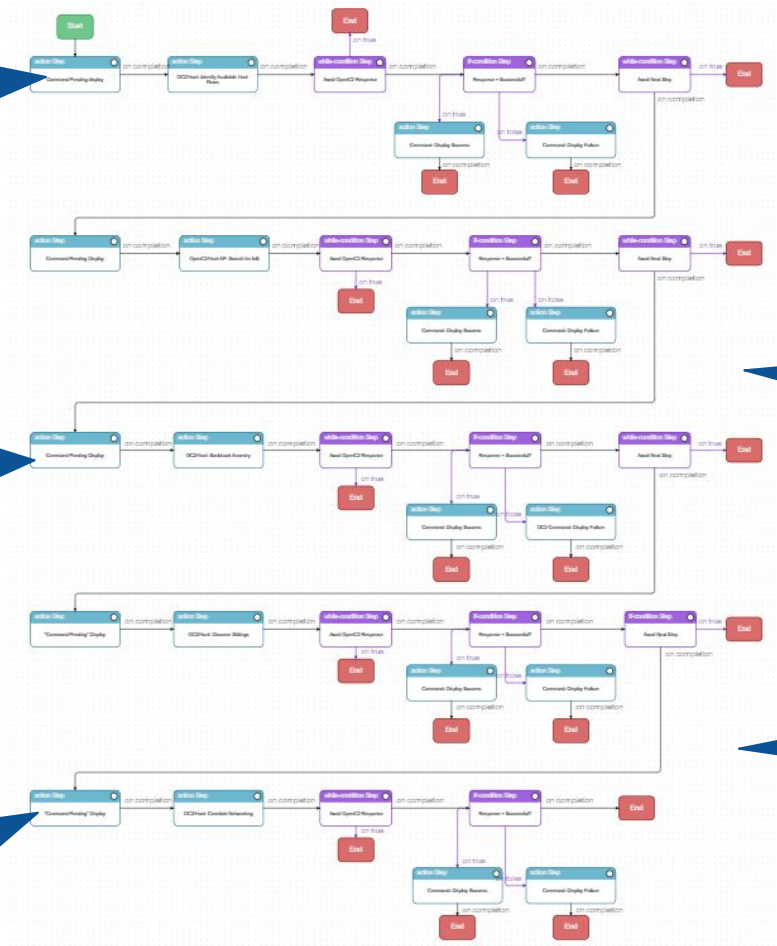
1. Introspection: what huntflows?
2. IoB: firewall disabled?
3. Hunting: parents of disabling process
4. Hunting: parents of disabling process
5. Hunting: network traffic of suspect processes

Display Success (Green) or Failure (Red) on TwinklyMaHa

On to the next stage …

CACAO Playbook Captures The Demo Hunt Process (5 “Stages”)

1. Introspection: What huntflows available?



2. Search for IoB: Was a Firewall Disabled?

3. Hunting: Backtrack Ancestry

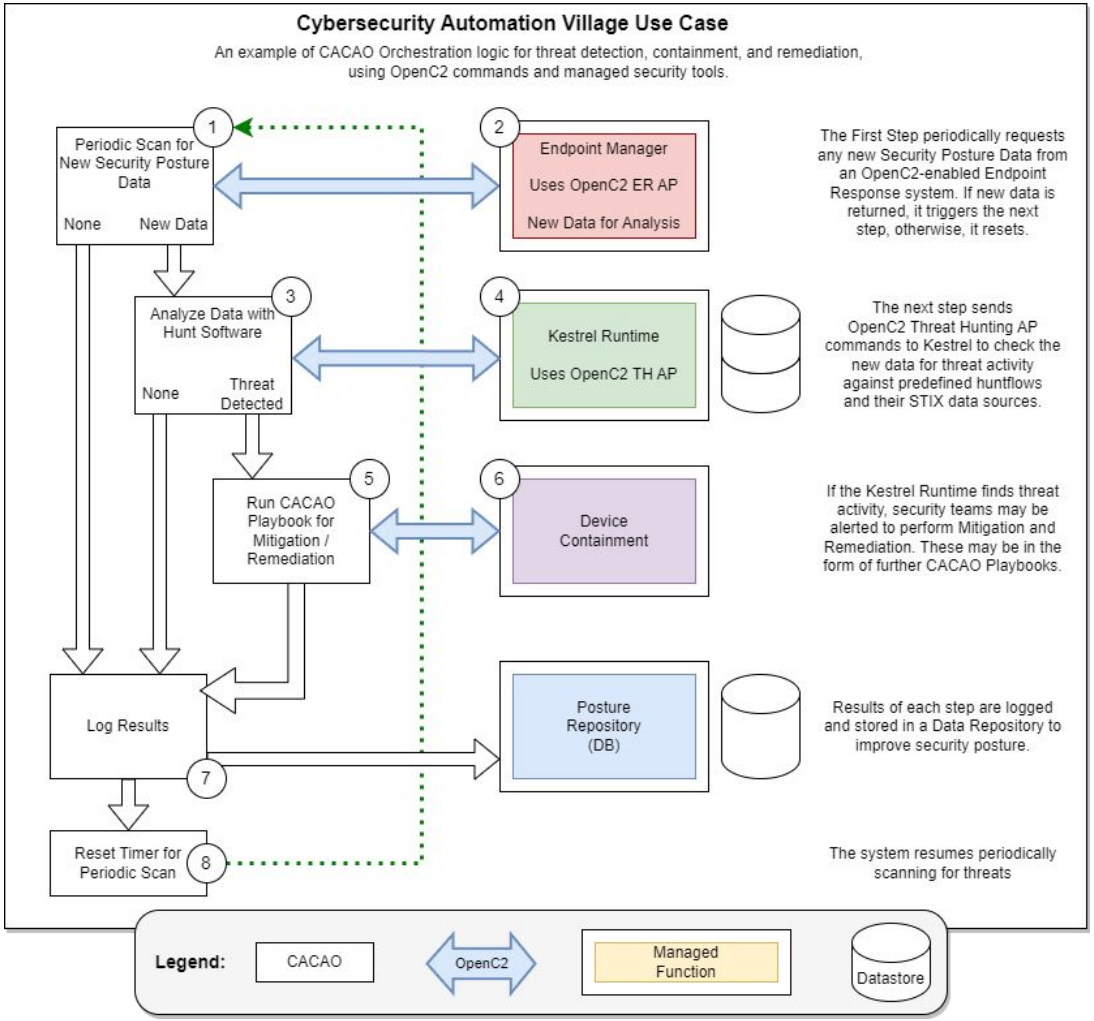
4. Hunting: Discover Siblings

5. Hunting: Correlate Networking

https://github.com/opencybersecurityalliance/casp/blob/main/Plugfests/2024-03-NorthernVirginia/SweatEquity/IBM/complete_hunt.ipynb

Orchestrated Hunt Use Case

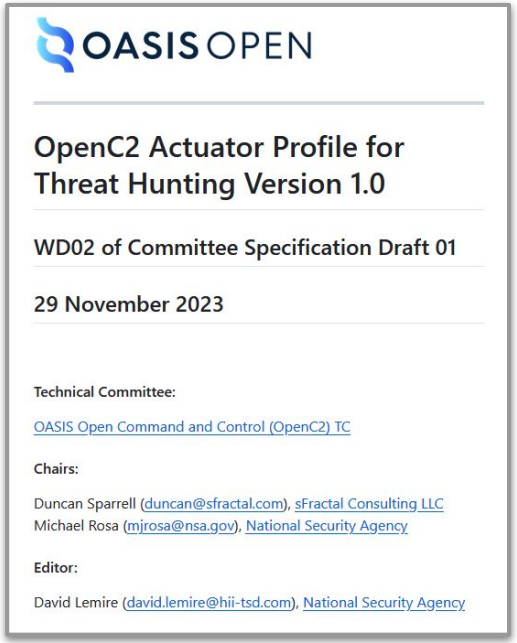
Another example of how Kestrel and OpenC2 could be integrated.



Thank You!

Takeaways

- Cross-organization development of OpenC2 Threat Hunting actuators using Kestrel
  - Based on OpenC2 Threat Hunting Actuator Profile
- Rapid development leveraging the OIF-Orchestrator/Device framework
- Cross-organization sharing of threat data and hunt playbooks
- Seed future threat hunting and remediation automation with CACAO



OASIS OPEN

OpenC2 Actuator Profile for Threat Hunting Version 1.0

WD02 of Committee Specification Draft 01

29 November 2023

Technical Committee:

OASIS Open Command and Control (OpenC2) TC

Chairs:

Duncan Sparrell (duncan@sfractal.com), sFractal Consulting LLC
Michael Rosa (mjrosa@nsa.gov), National Security Agency

Editor:

David Lemire (david.lemire@hii-tsd.com), National Security Agency

Current Status: CSD02 (publication pending)