OPEN CYBERSECURITY ALLIANCE

1. What is OCA (what, who, how, why)?
2. Why is OCA relevant to VEX community?
3. How can OCA help the VEX community?
4. How can the VEX community help OCA?

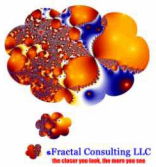
Duncan Sparrell
27-July-2023

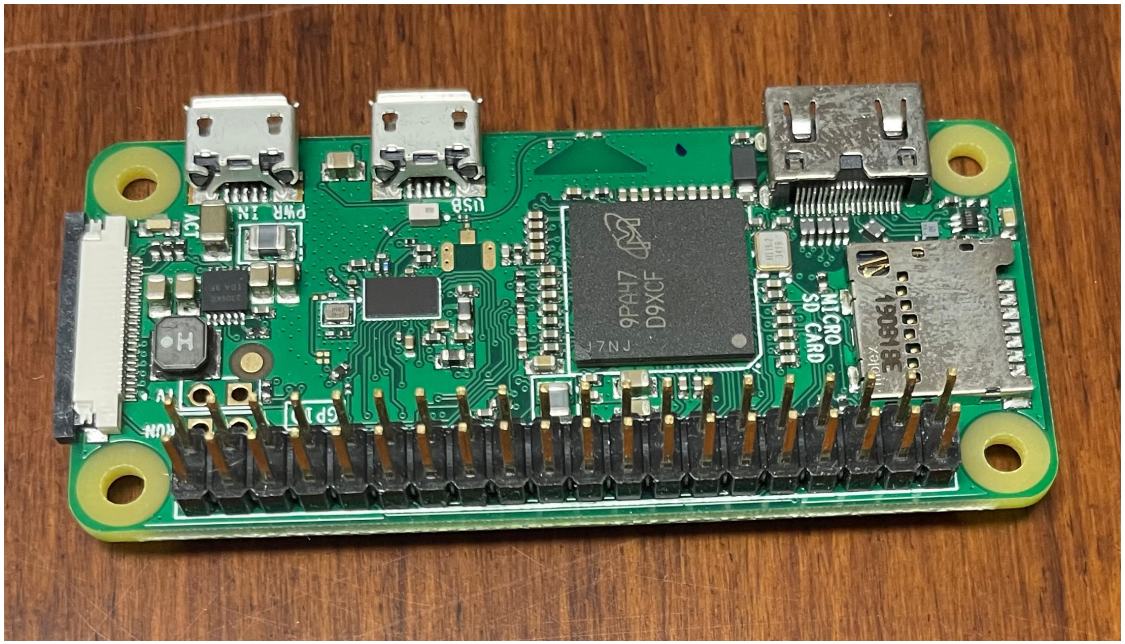
TLP Clear

Linkedin @sfractal
Twitter @dsparrell
Mastadon @sFractal:infosec.exchange

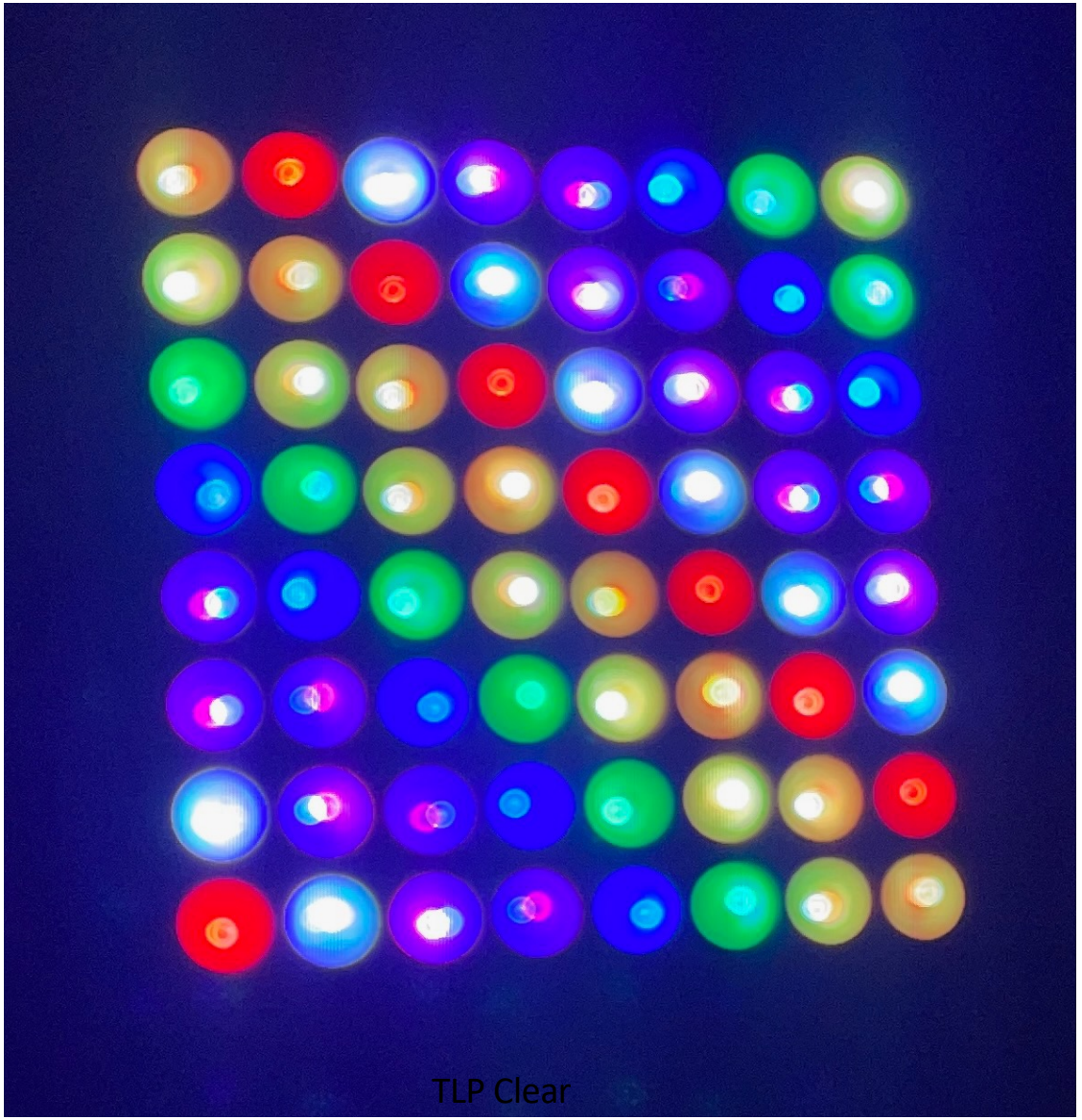
THINK EVILLY

Act Ethically





TLP Clear



TLP Clear

TLP Clear


OPEN
CYBERSECURITY
ALLIANCE
OPEN CYBERSECURITY
ALLIANCE
Cybersecurity Automation Village
Cybersecurity Automation Village

Stickers!

OPEN CYBERSECURITY ALLIANCE

Making Standards-Based, Interoperable Cybersecurity a Reality

OCA is building an open ecosystem where cybersecurity products interoperate without the need for customized integrations

https://opencybersecurityalliance.org/

TLP Clear

OASIS OPEN

Where open source and open standards thrive

2000+	6	70+	150+
PARTICIPANTS	CONTINENTS	COMMUNITIES	STANDARDS

- Nonprofit, 501(c)(6), member-driven organization
- Built on openness, inclusivity, and innovation
- ANSI-certified process
- Setting standards since 1993

AMQP Advanced Message Queuing Protocol · CSAF · CAP Common Alerting Protocol · DITA · ebXML · KMIP · MQTT · OpenC2 · OData Open Data Protocol · ODF · SAML v2.0 · PKCS Public-Key Cryptography Standards · STIX TAXII · TOSCA · UBL · XACML


OPEN
CYBERSECURITY
ALLIANCE


CIS.
Center for
Internet Security®


CYDARM


CYWARE


EclecticIQ
Intelligence
at the core


IBM Security


PROPHECY


SEKOIA.IO


Think Evilly, Act Ethically
sFractal Consulting LLC
the closer you look, the more you see


thatDot


UNB
EST. 1785
UNIVERSITY OF NEW BRUNSWICK
Canadian
Institute for
Cybersecurity


Verily IT Consulting
Integrity Acuity Results

TLP Clear

IoB

Kestrel

OCA Ontology

OXA

SpydeRisk

STIX-Shifter

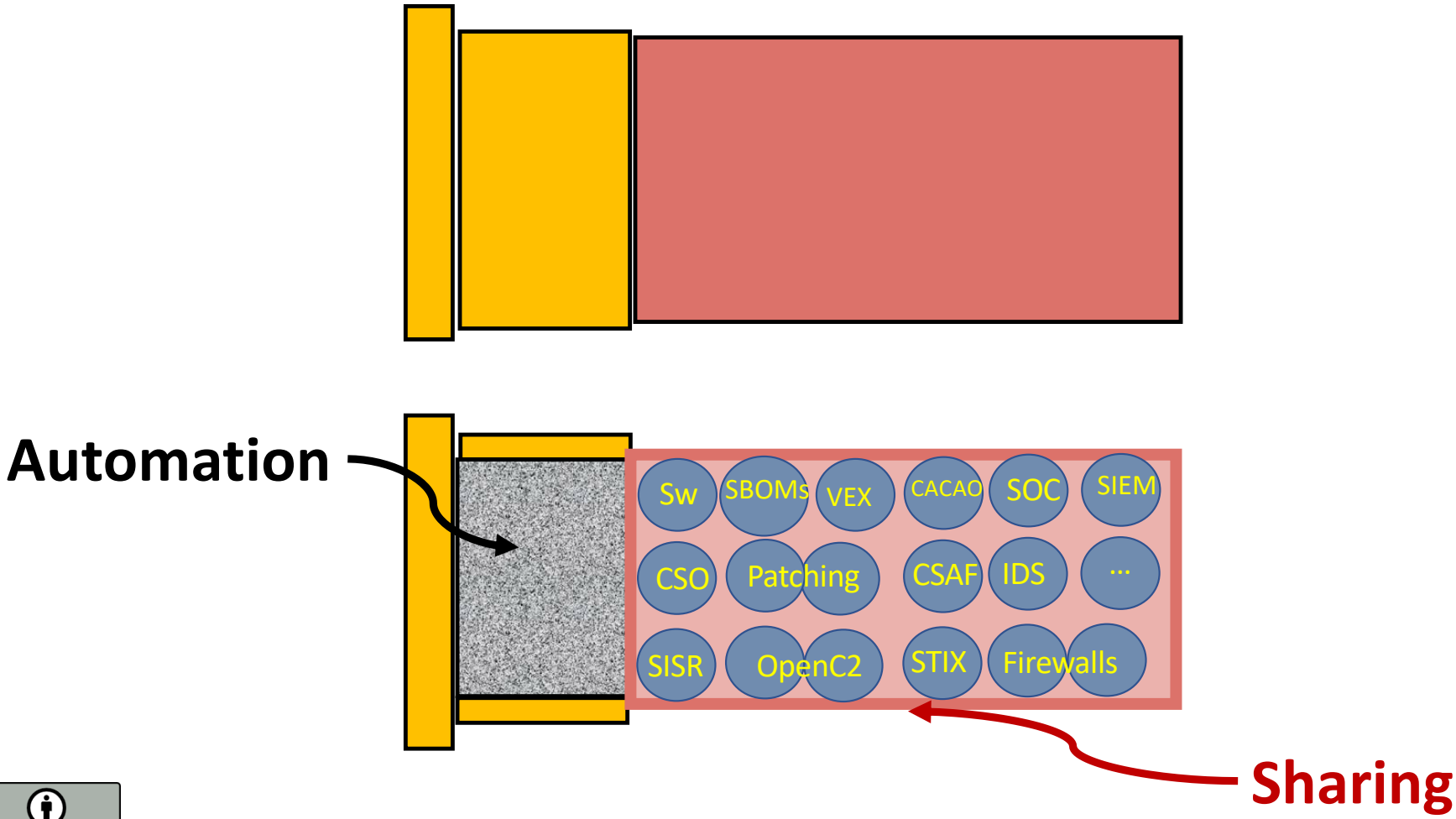
Cybersecurity
Automation
SubProject

TLP Clear

In cybersecurity, there are no silver bullets

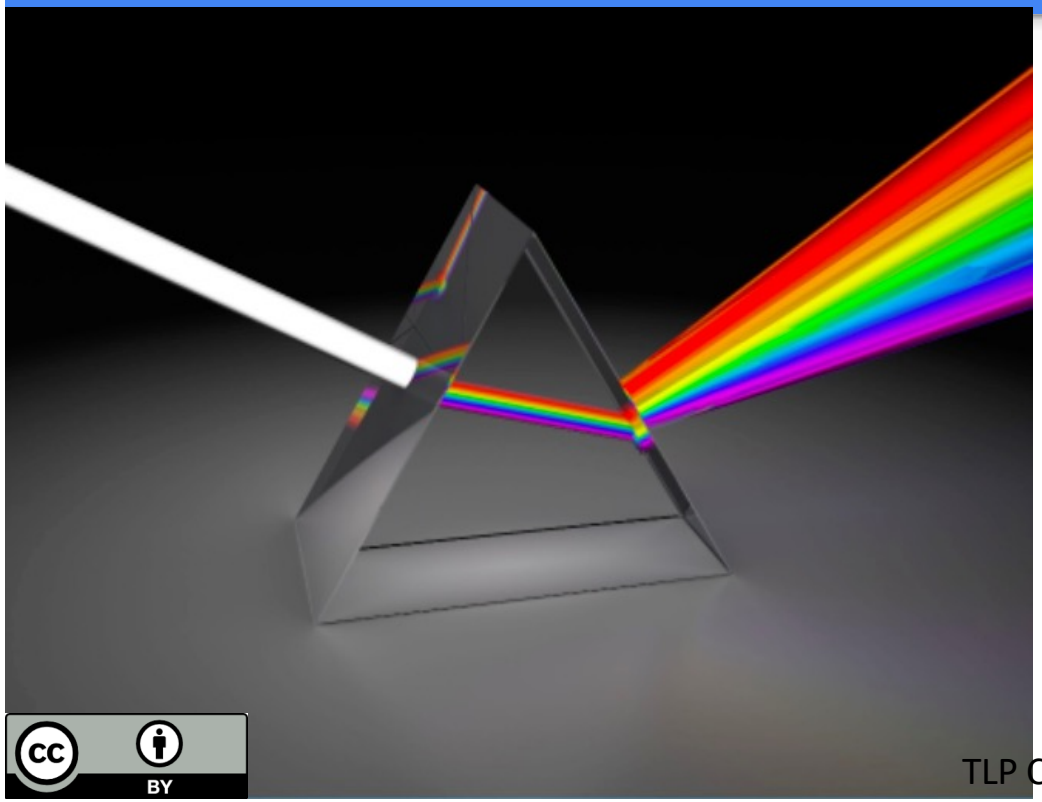
Zombie Hoard from Night of the Living Dead

Boom Stick from Ash Vs the Evil Dead

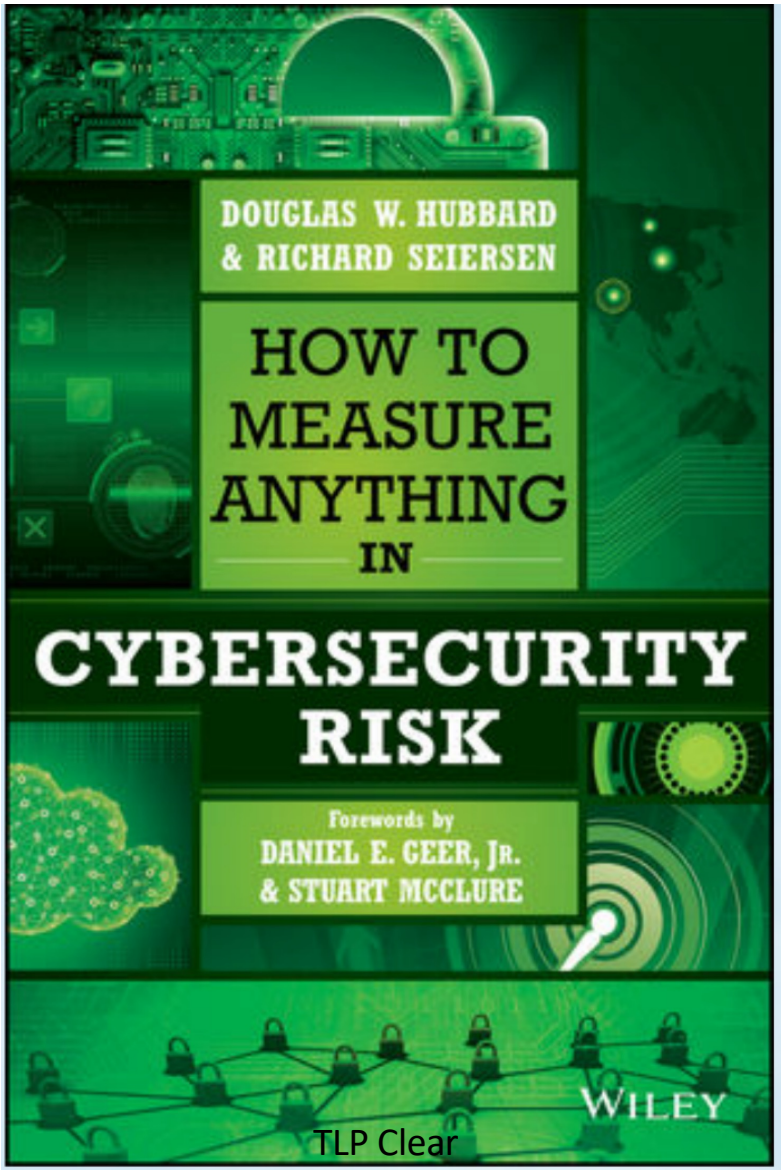


TLP Clear

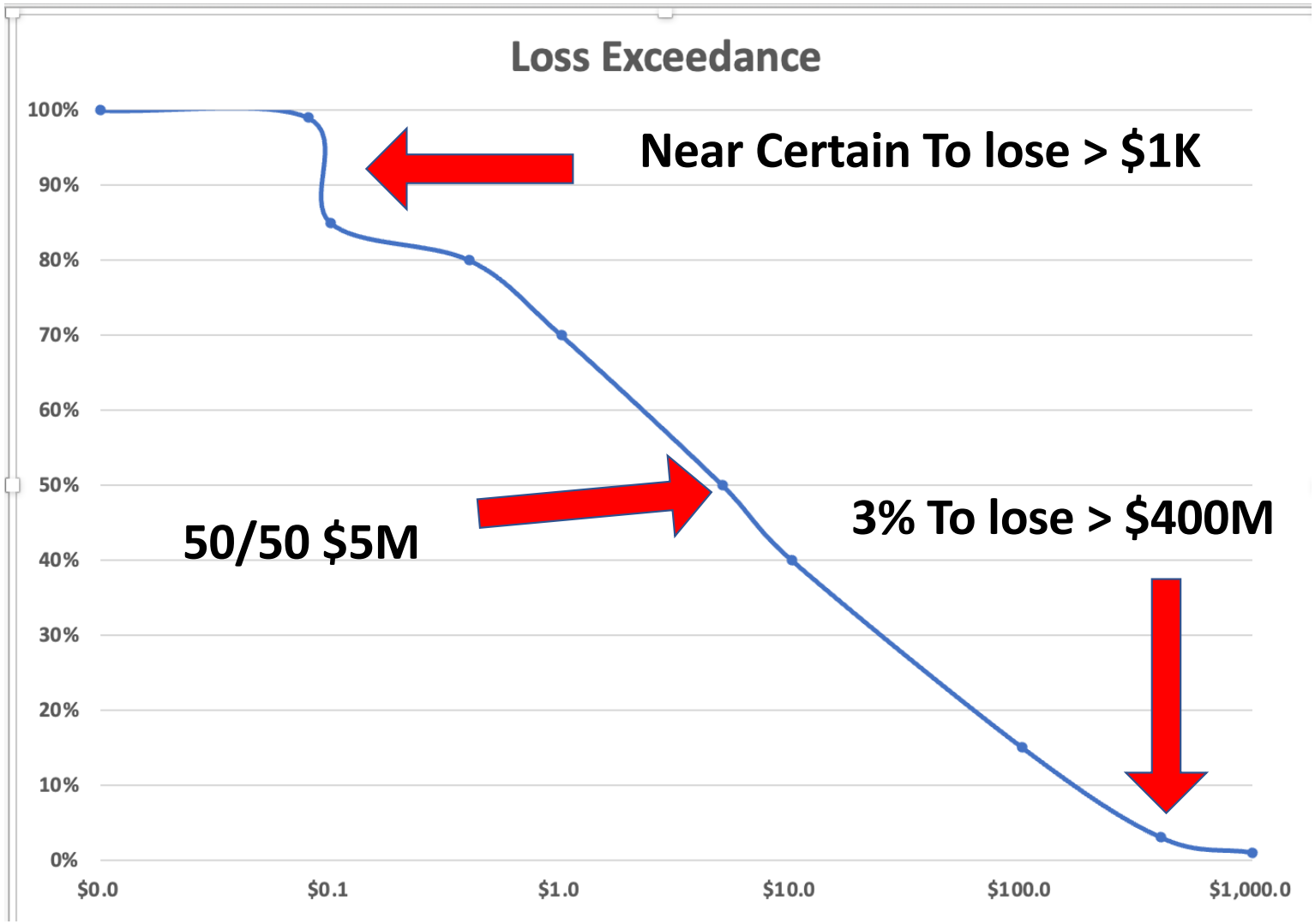
Automation



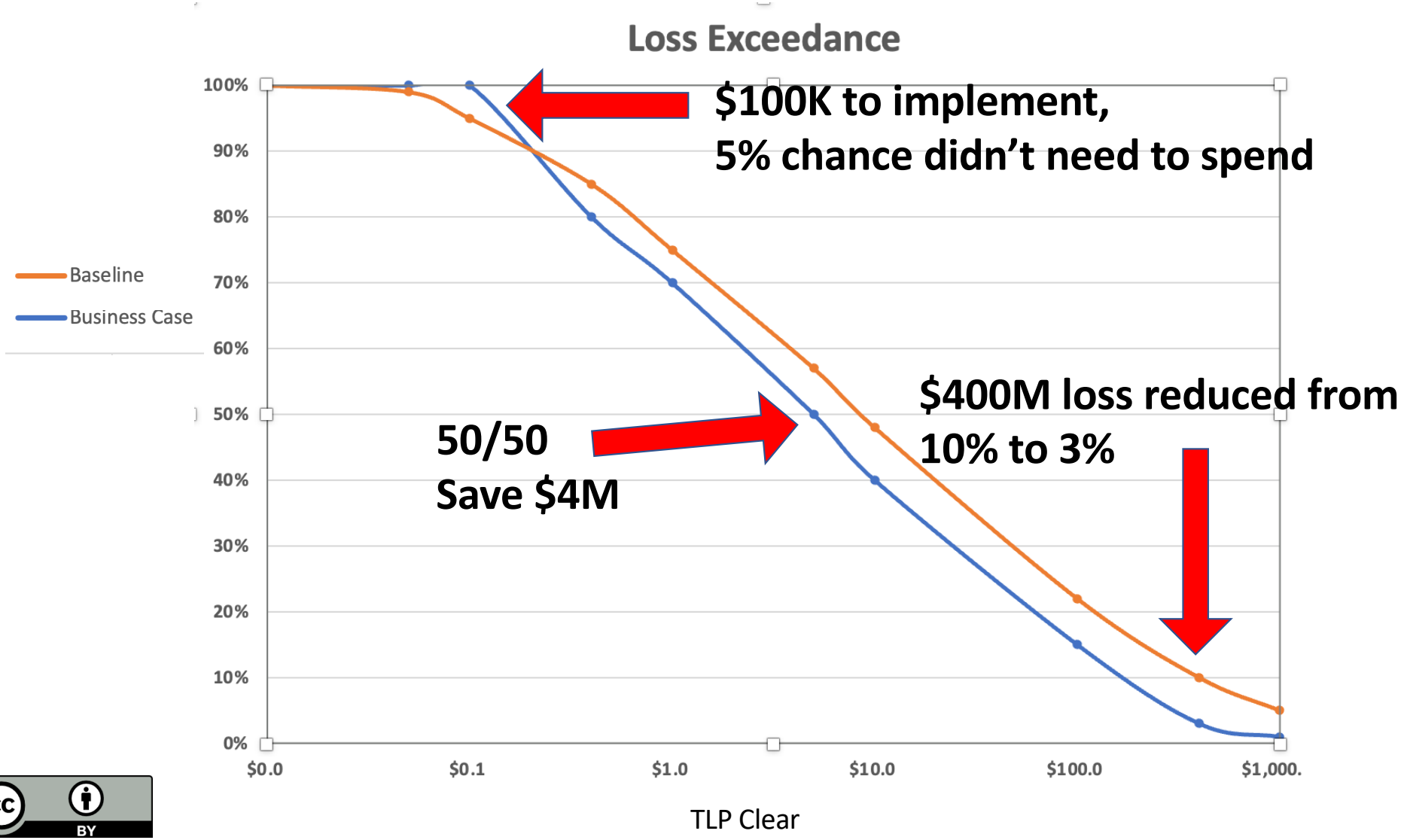
TLP Clear

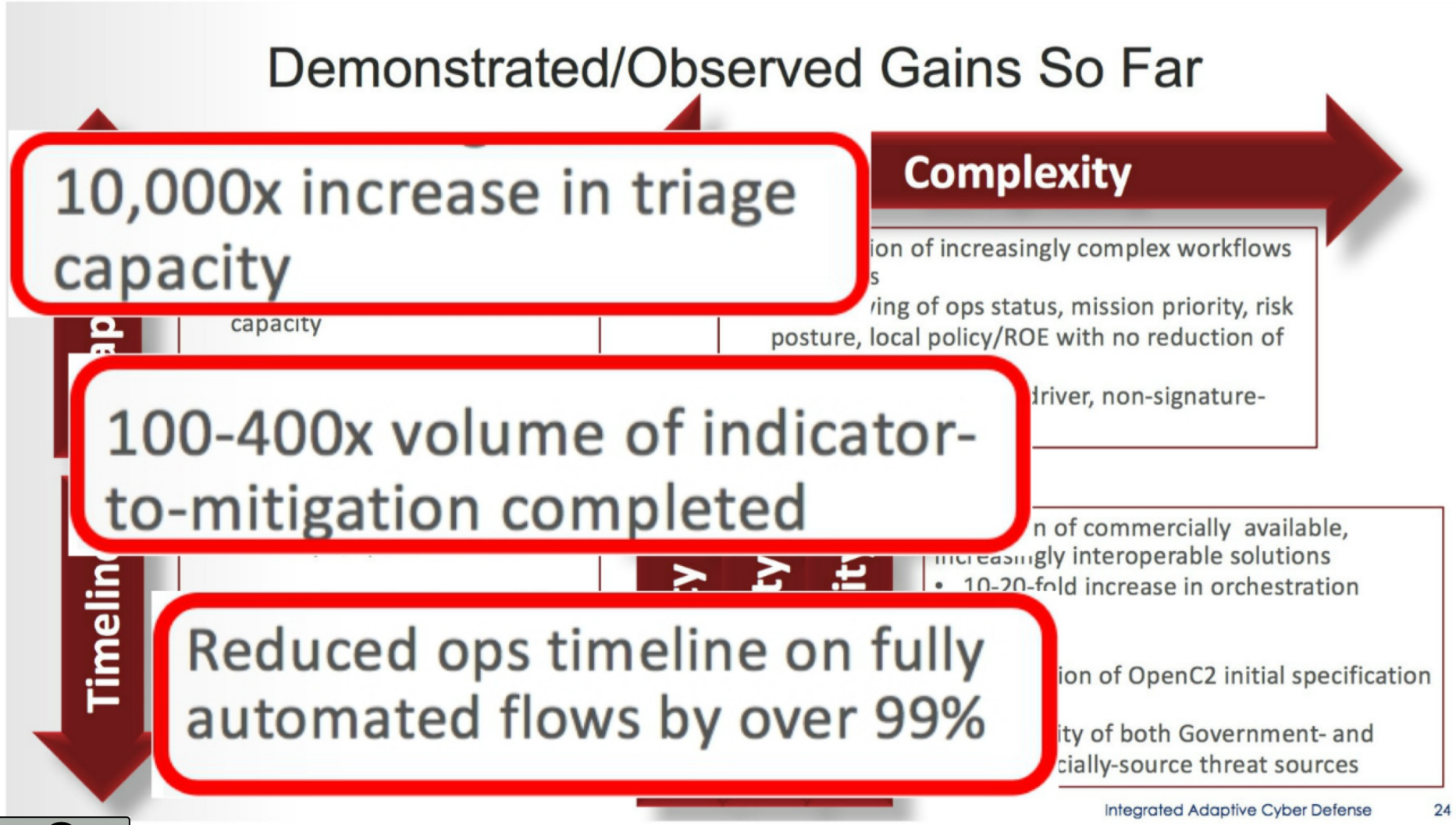


TLP Clear

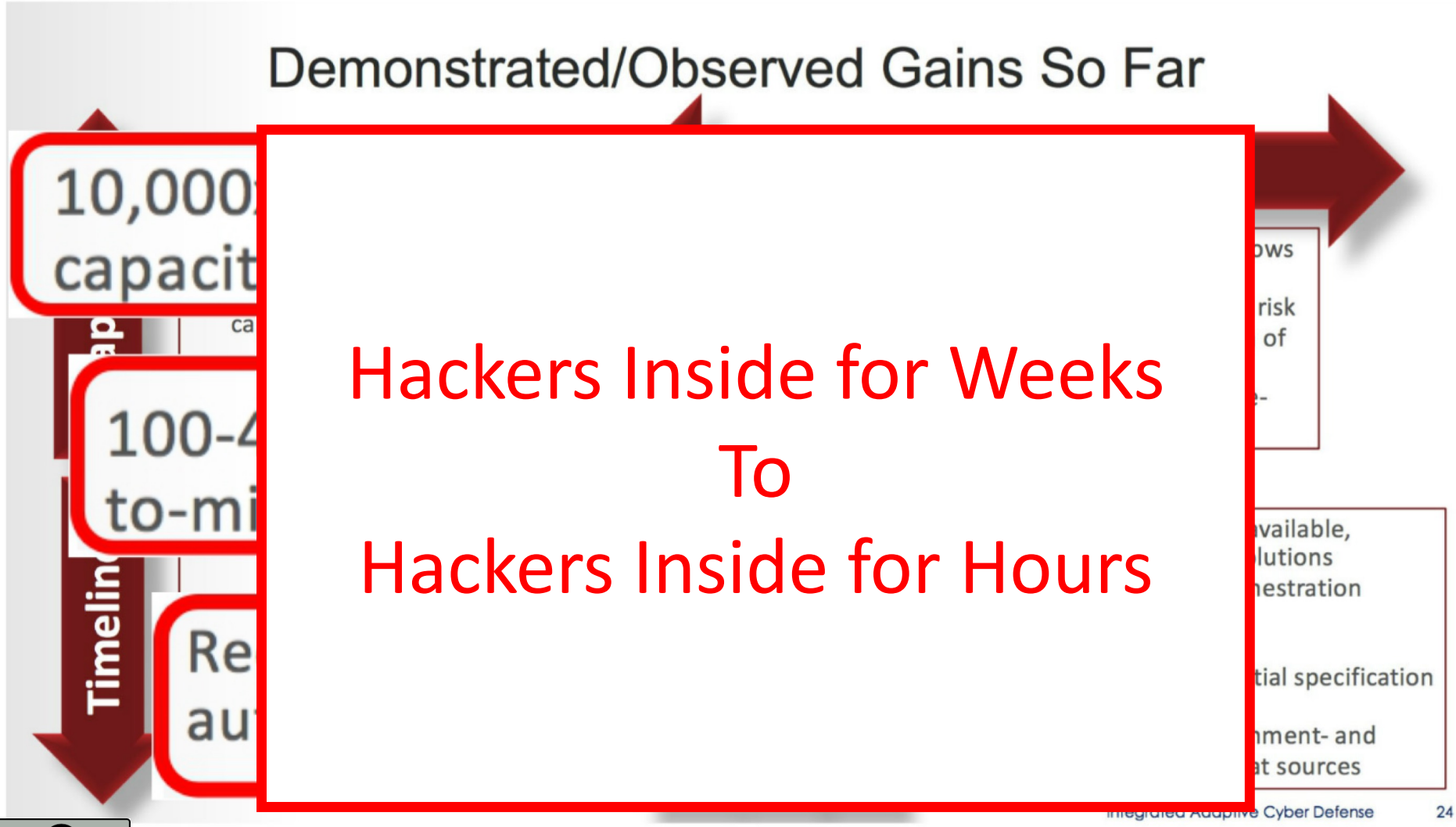


TLP Clear


Loss Exceedance
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
$0.0
$0.1
$1.0
$10.0
$100.0
$1,000.
Baseline
Business Case
$100K to implement,
5% chance didn't need to spend
50/50
Save $4M
$400M loss reduced from
10% to 3%
TLP Clear



TLP Clear



TLP Clear

- 25%-30% Efficiency Gain in SOC Analysts

TLP Clear

- 25%-30% Efficiency Gain in SOC Analysts

- 98% Savings ($1.06M) in processing phishing emails

TLP Clear

IoB

Kestrel

OCA Ontology

OXA

SpydeRisk

STIX-Shifter

Cybersecurity
Automation
SubProject

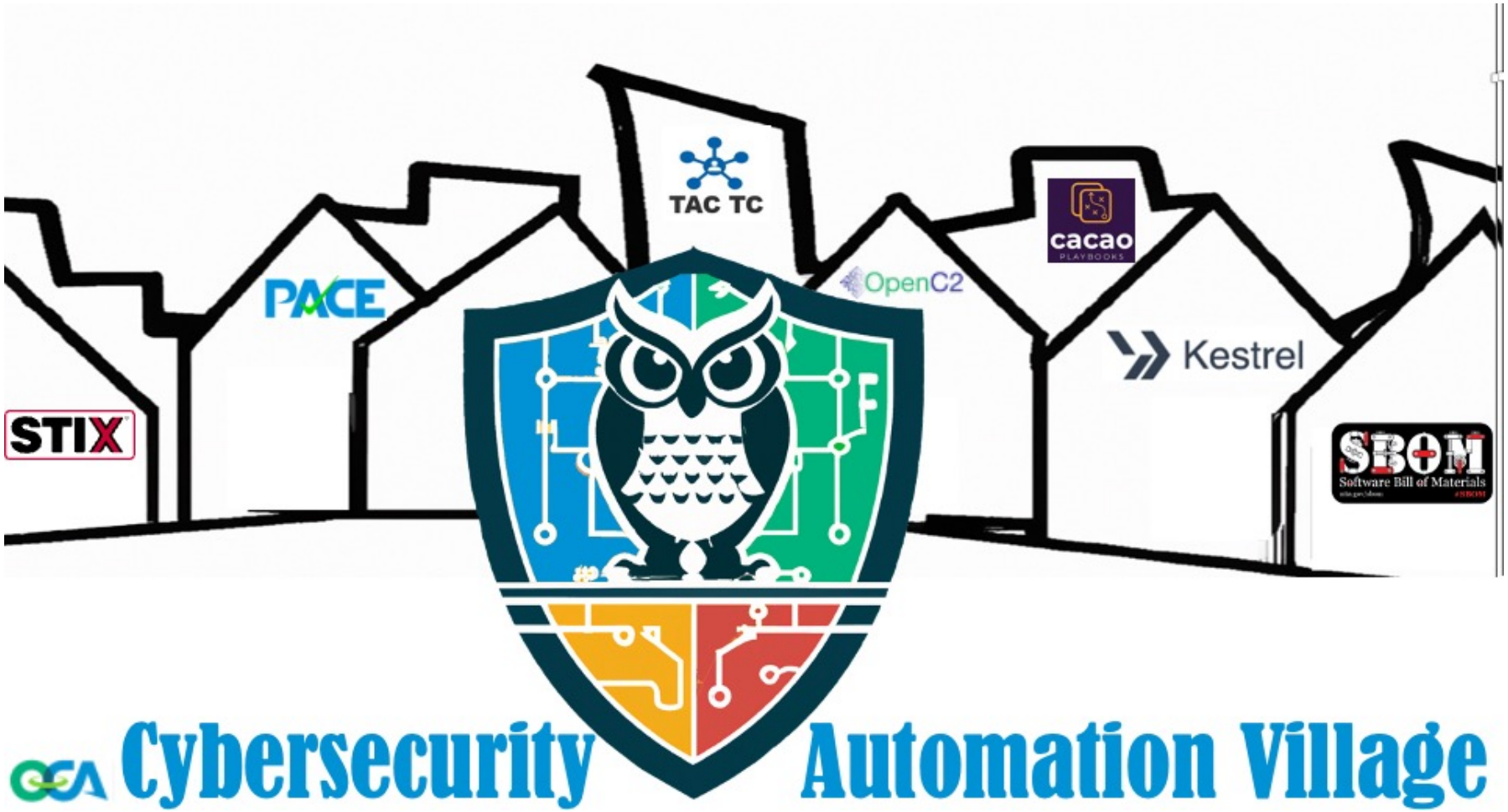
TLP Clear

OPEN
CYBERSECURITY
ALLIANCE

Cybersecurity
Automation
SubProject

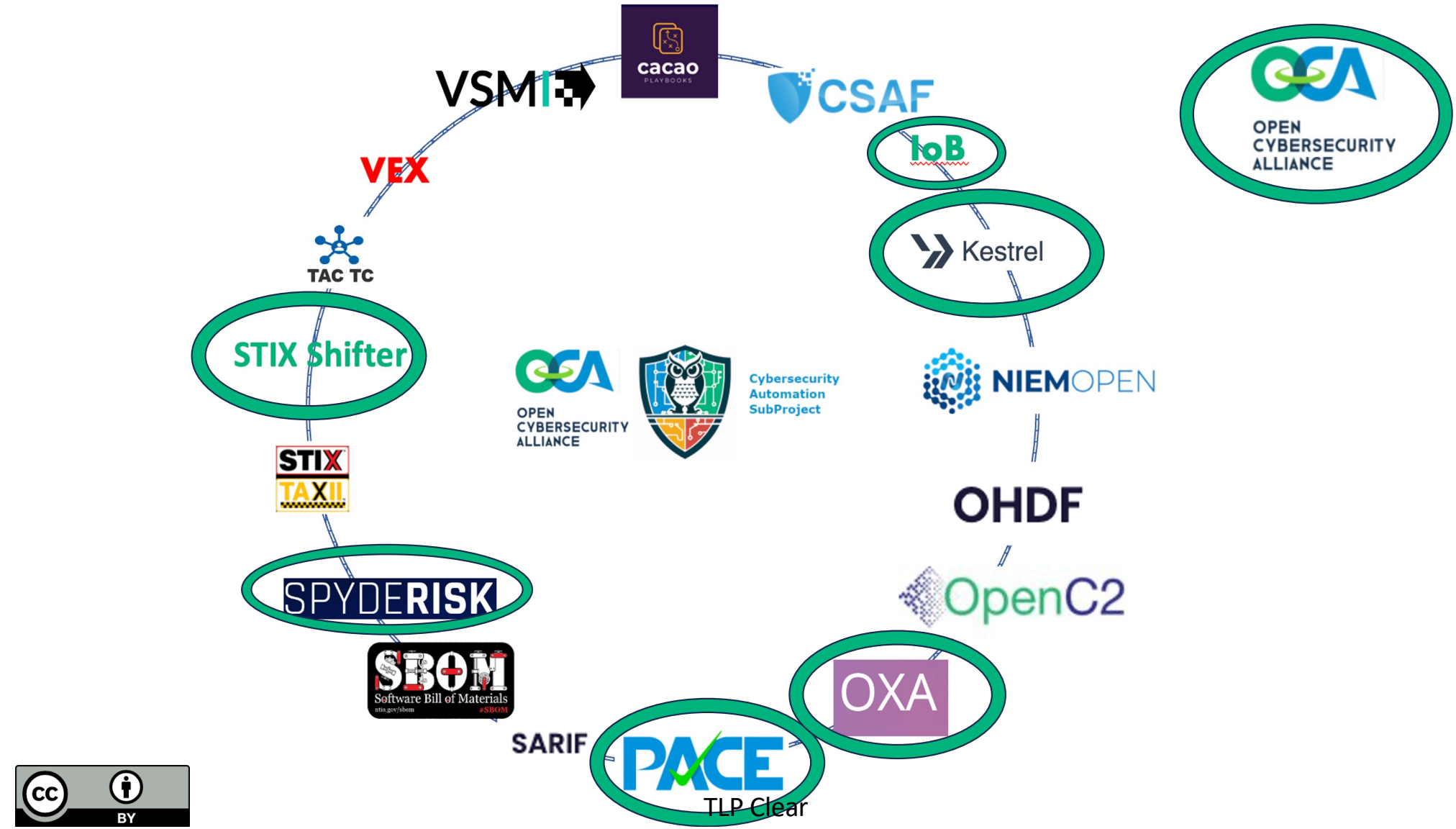
The Open Cybersecurity Alliance (OCA) Cybersecurity Automation SubProject (CASP) is comprised of global like-minded cybersecurity vendors, end users, thought leaders and individuals who are interested in cybersecurity automation.
It is a forum where products from all vendors, researchers, and software publishers can freely exchange information, insights, and reference implementations via commonly developed code and tooling, using mutually agreed upon technologies, specifications, and procedures.

TLP Clear



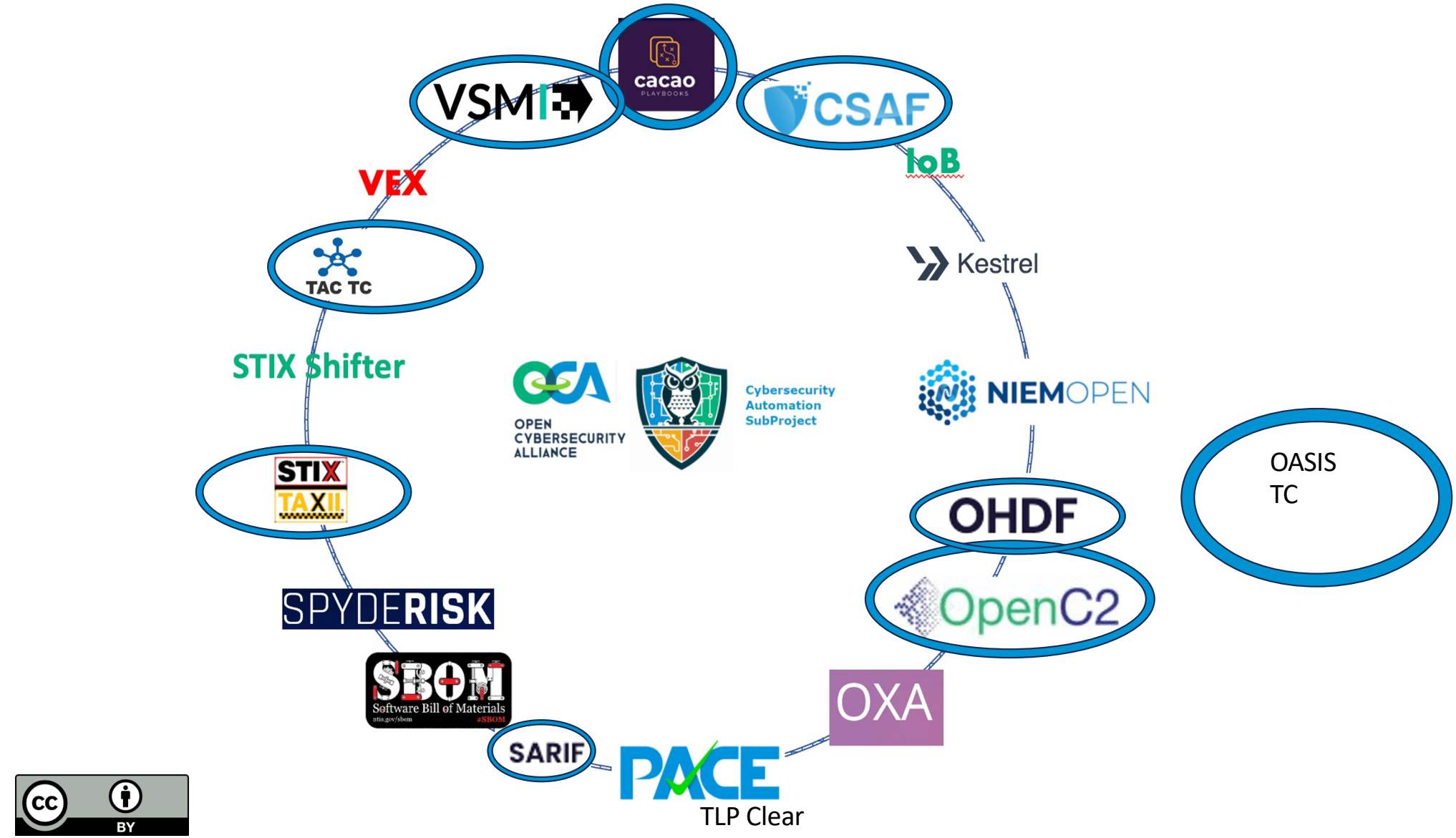
TLP Clear

TLP Clear

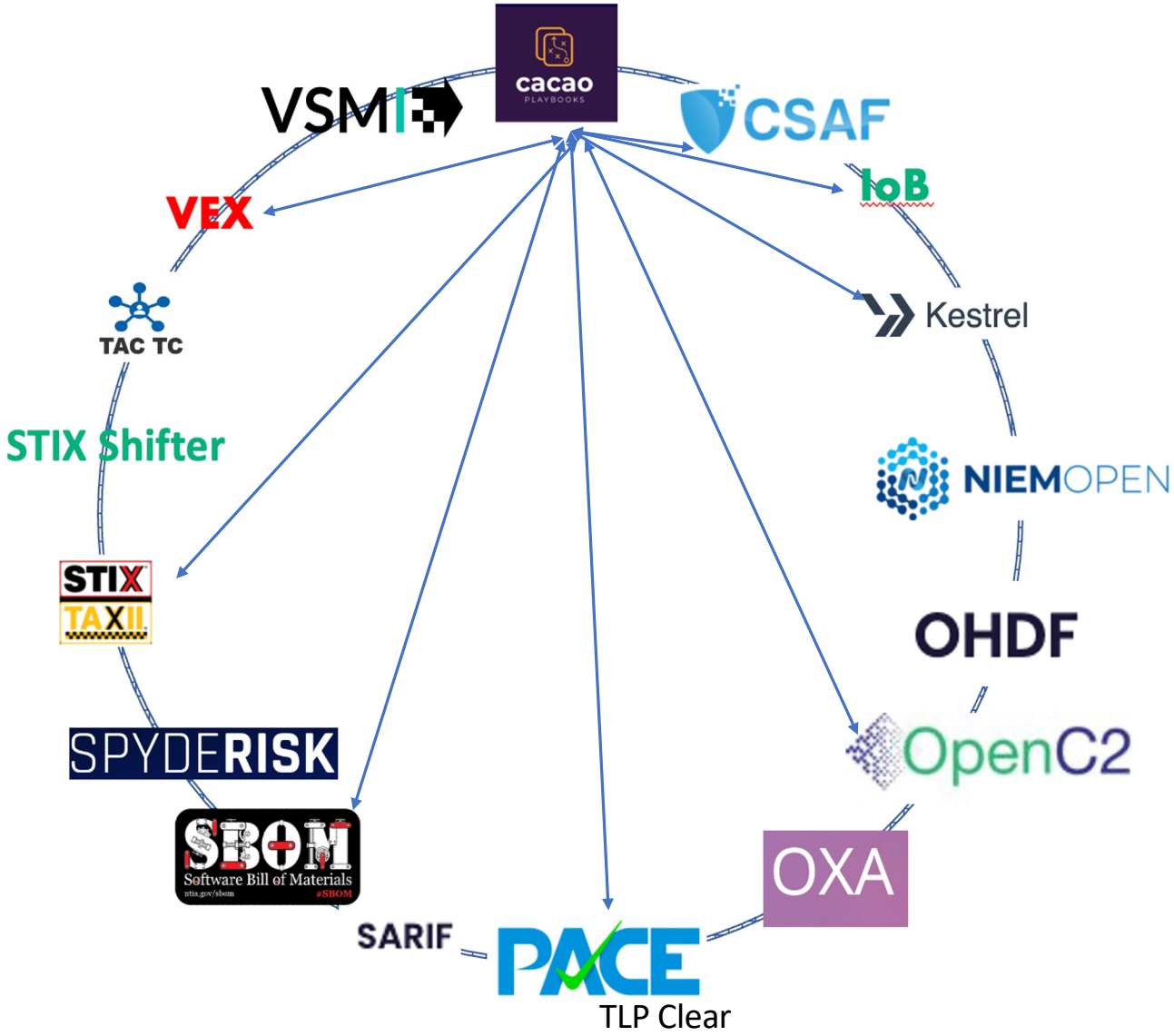


TLP Clear

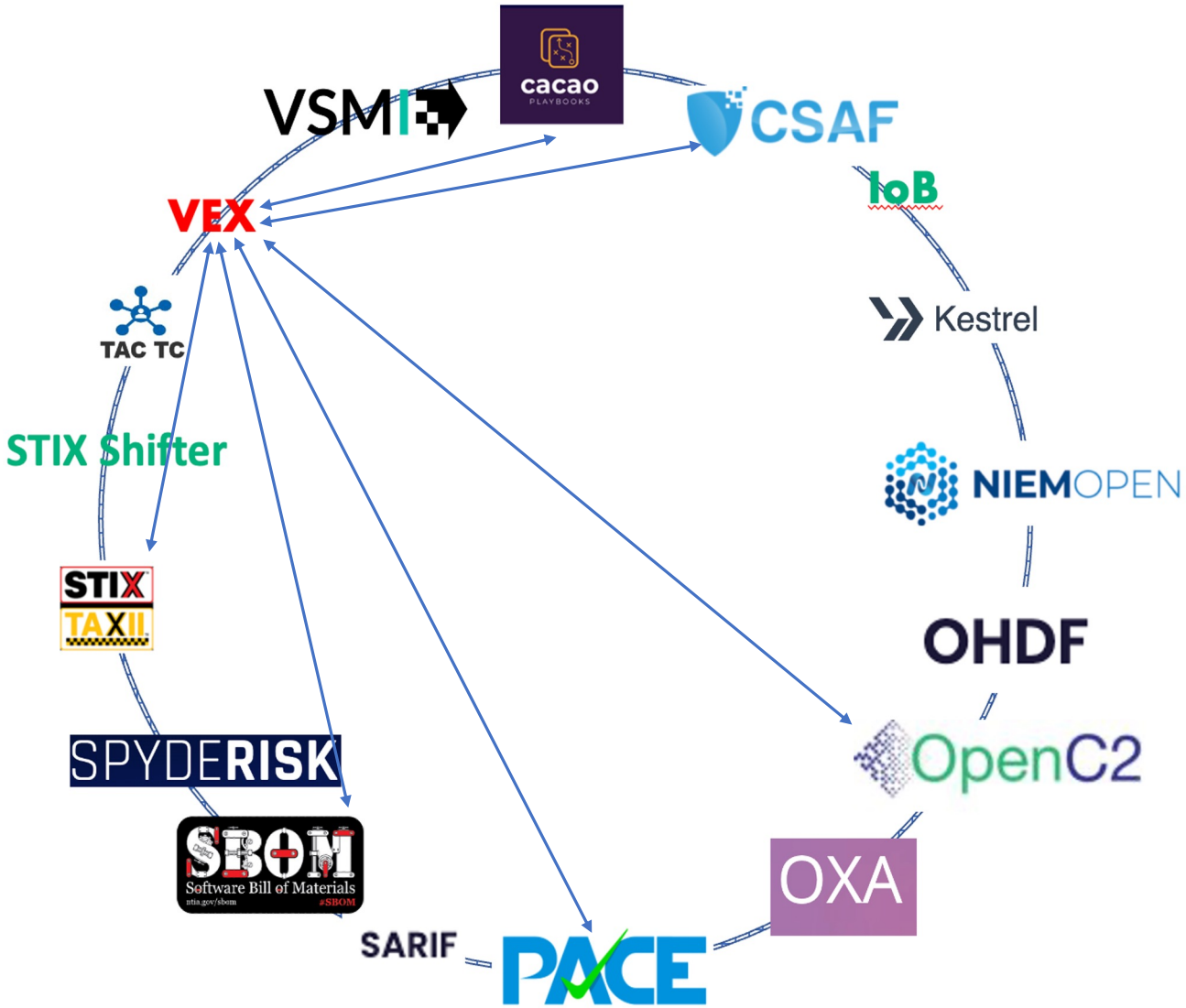

cacao
PLAYBOOKS
VSMR
CSAF
IoB
Kestrel
OASIS
Open
Project
NIEMOPEN
OHDF
OpenC2
OXA
PACE
SARIF
TLP Clear
SBOM
Software Bill of Materials
SPYDERISK
STIX
TAXII
STIX Shifter
TAC TC
VEX
OPEN
CYBERSECURITY
ALLIANCE
Cybersecurity
Automation
SubProject


VSMR
cacao
PLAYBOOKS
CSAF
VEX
IoB
TAC TC
Kestrel
STIX Shifter
OPEN CYBERSECURITY ALLIANCE
Cybersecurity Automation SubProject
NIEMOPEN
OASIS TC
STIX
TAXII
OHDF
SPYDERISK
OpenC2
SBOM
Software Bill of Materials
ntia.gov/sbom
#SBOM
OXA
SARIF
PACE
TLP Clear

TLP Clear



TLP Clear



TLP Clear

Plugfest

TLP Clear

Plugfest

Machine to Machine

CYDARM

IBM

APL JOHNS HOPKINS APPLIED PHYSICS LABORATORY

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

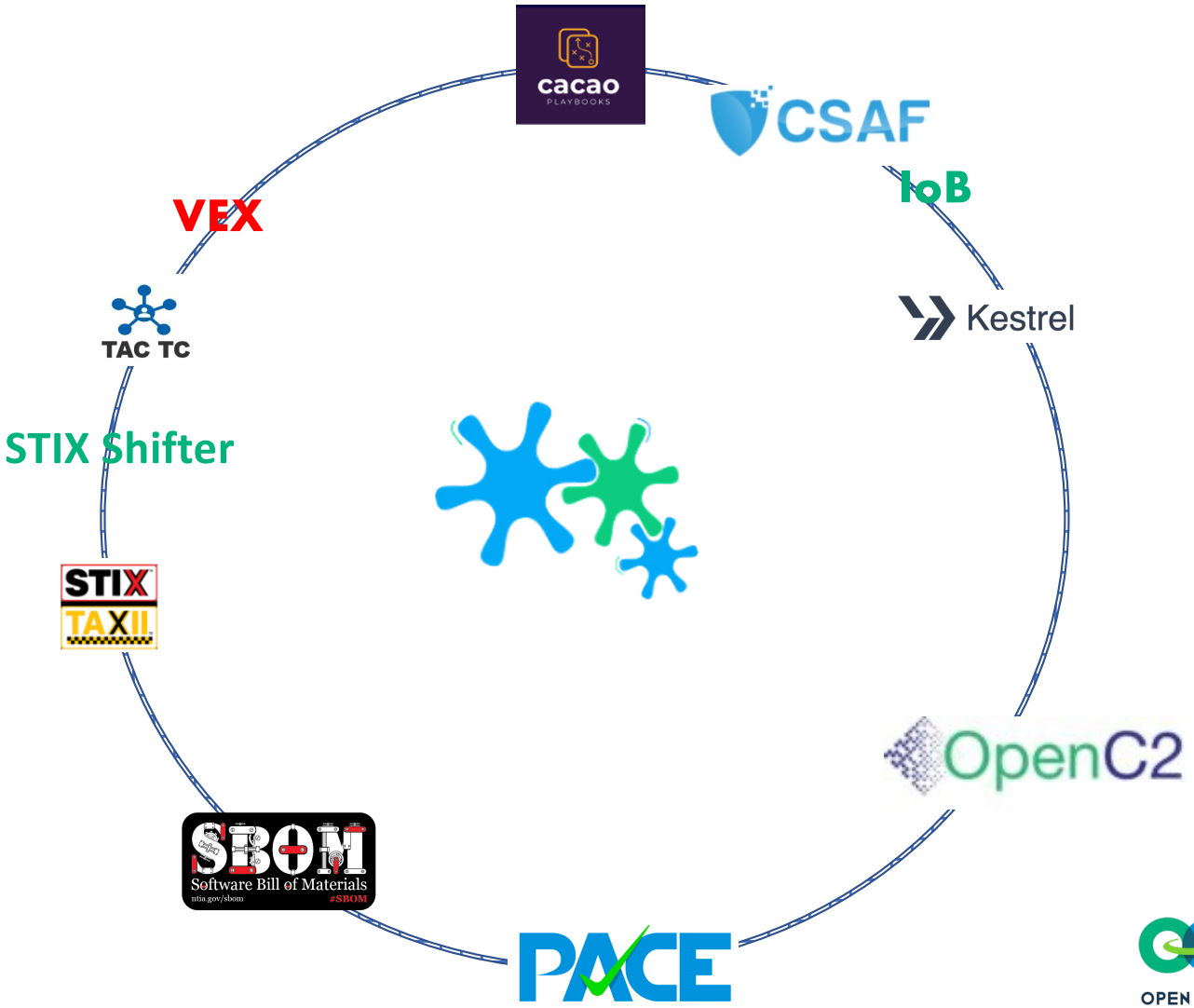
SEKOIA.IO

semantic arts

Fractal Consulting LLC

UiO University of Oslo

TLP Clear



TLP Clear

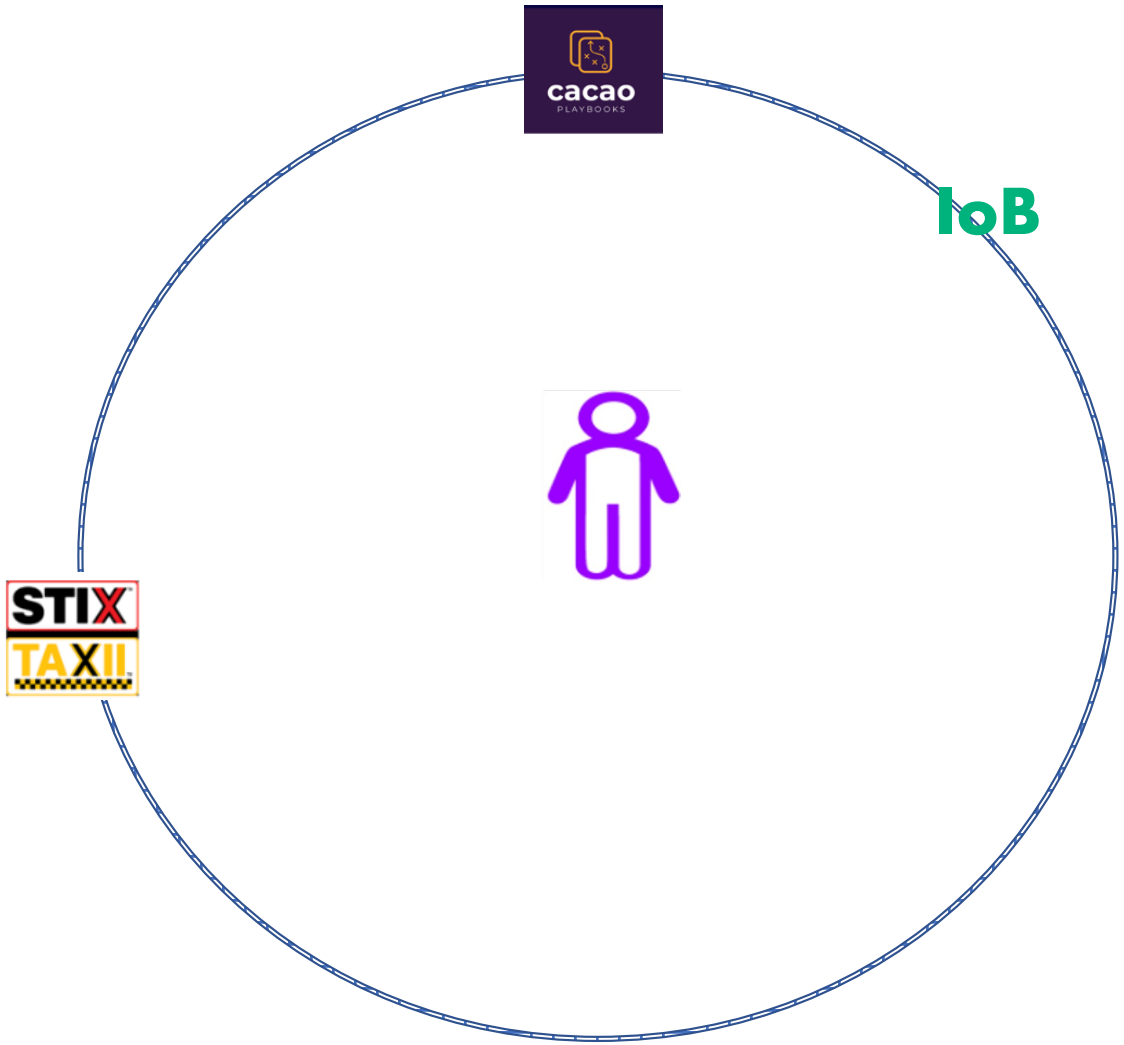
OPEN CYBERSECURITY ALLIANCE

Cybersecurity Automation SubProject

Plugfest

Machine to Machine

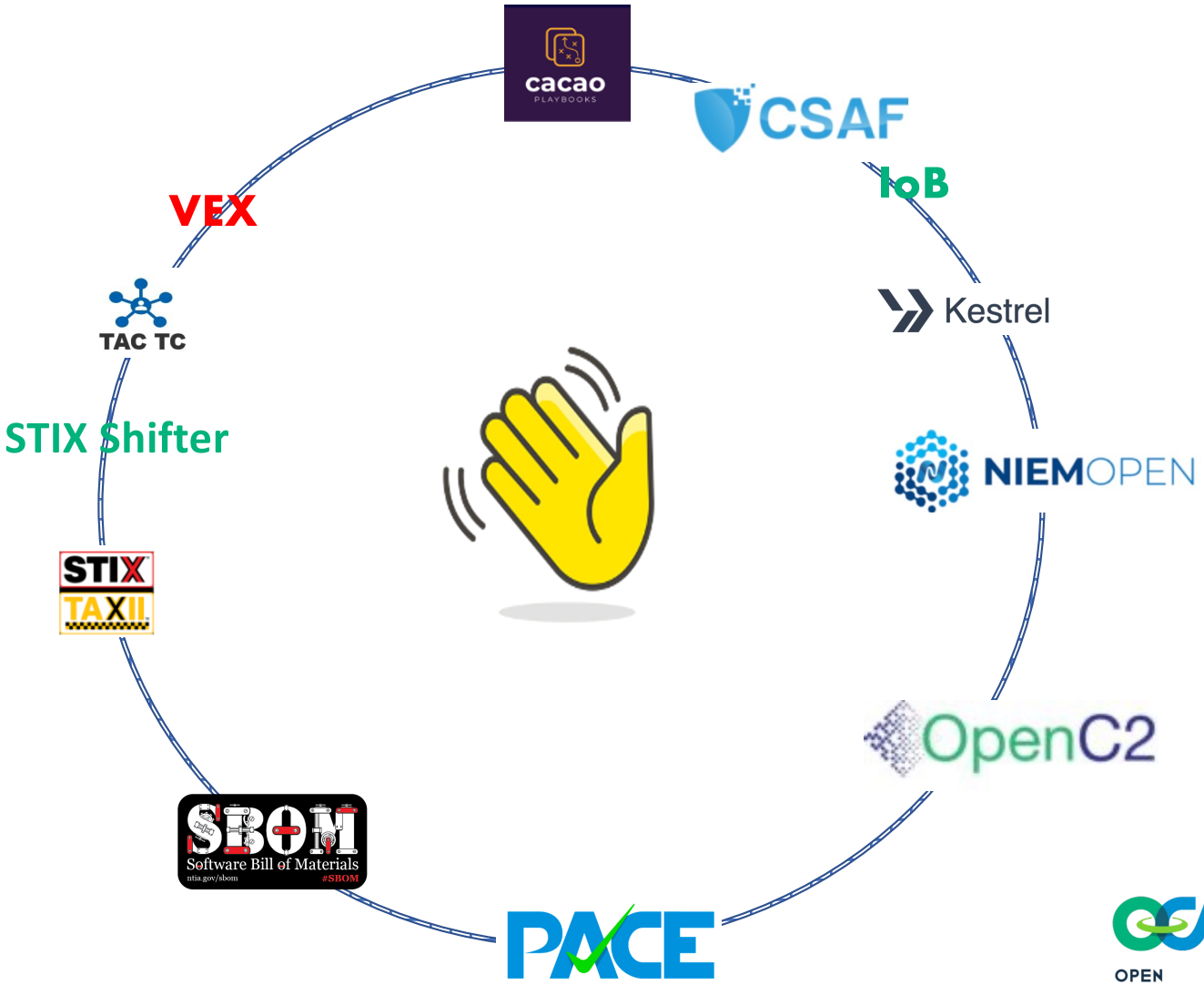
Human to Machine



TLP Clear

OPEN CYBERSECURITY ALLIANCE

Cybersecurity Automation SubProject



TLP Clear

OPEN CYBERSECURITY ALLIANCE

Cybersecurity Automation SubProject

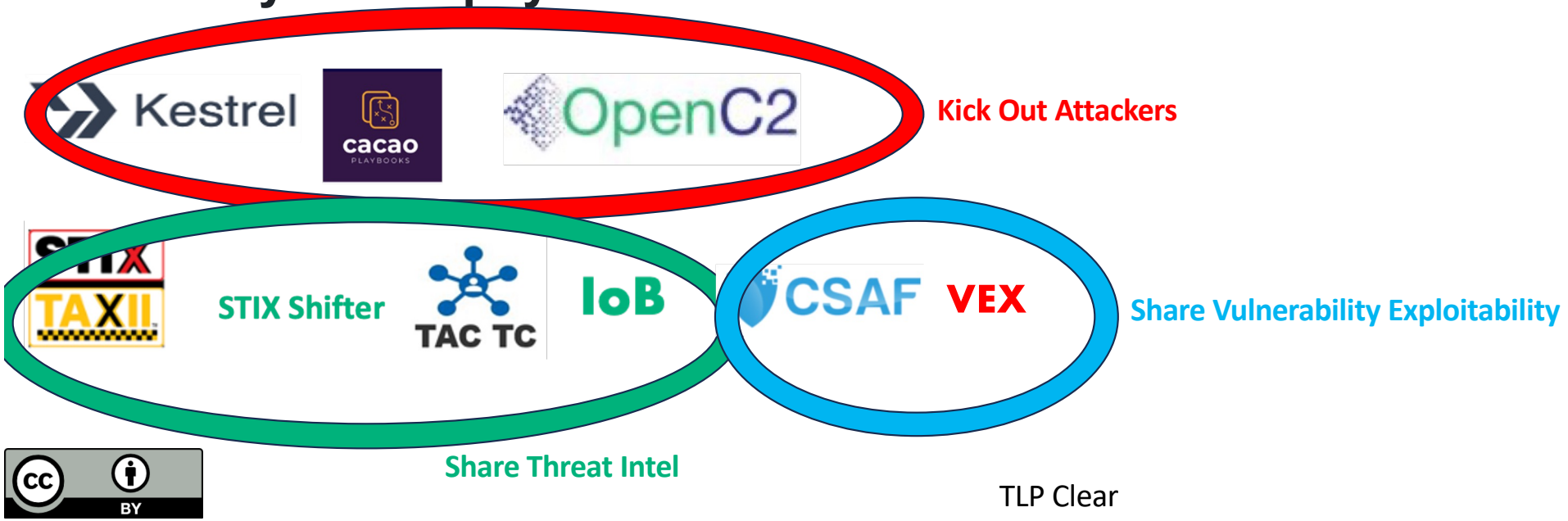
The WhitchyWashy Ransomware Use Case

https://github.com/opencybersecurityalliance/casp/blob/main/Plugfests/2023-06-13-USC/UseCases/README.md

TLP Clear

The WhitchyWashy Ransomware Use Case

- **Day 1 - Murphy's Law LLP**



TLP Clear

The WhitchyWashy Ransomware Use Case

- Day 1 - Murphy's Law LLP
- **Day 2 - On Deck Holdings**

STIX Shifter

IoB

TLP Clear

The WhitchyWashy Ransomware Use Case

- Day 1 - Murphy's Law LLP, Day 2 - On Deck Holdings
- **Day 3 - Triumvirate CleanUp Inc**



TLP Clear

The WhitchyWashy Ransomware Use Case

- Day 1 - Murphy's Law LLP, Day 2 - On Deck Holdings, Day 3 - Triumvirate CleanUp Inc
- **Day 4 – NSAANSA**

VEX




TLP Clear

The WhitchyWashy Ransomware Use Case

- Day 1 - Murphy's Law LLP, Day 2 - On Deck Holdings, Day 3 - Triumvirate CleanUp Inc
- Day 4 – NSAANSA
- **Day 5 – Law Enforcement**

TLP Clear

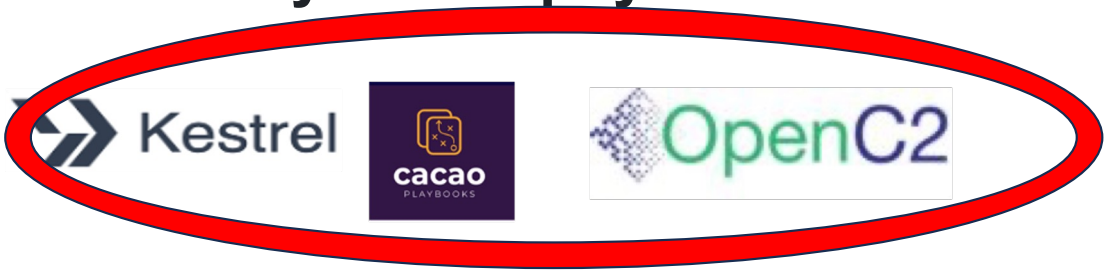
The WhitchyWashy Ransomware Use Case

- Day 1 - Murphy's Law LLP, Day 2 - On Deck Holdings, Day 3 - Triumvirate CleanUp Inc
- Day 4 – NSAANSA, Day 5 – Law Enforcement
- **Day 6 - Mil Ops**

TLP Clear

The WhitchyWashy Ransomware Use Case

- **Day 1 - Murphy's Law LLP**

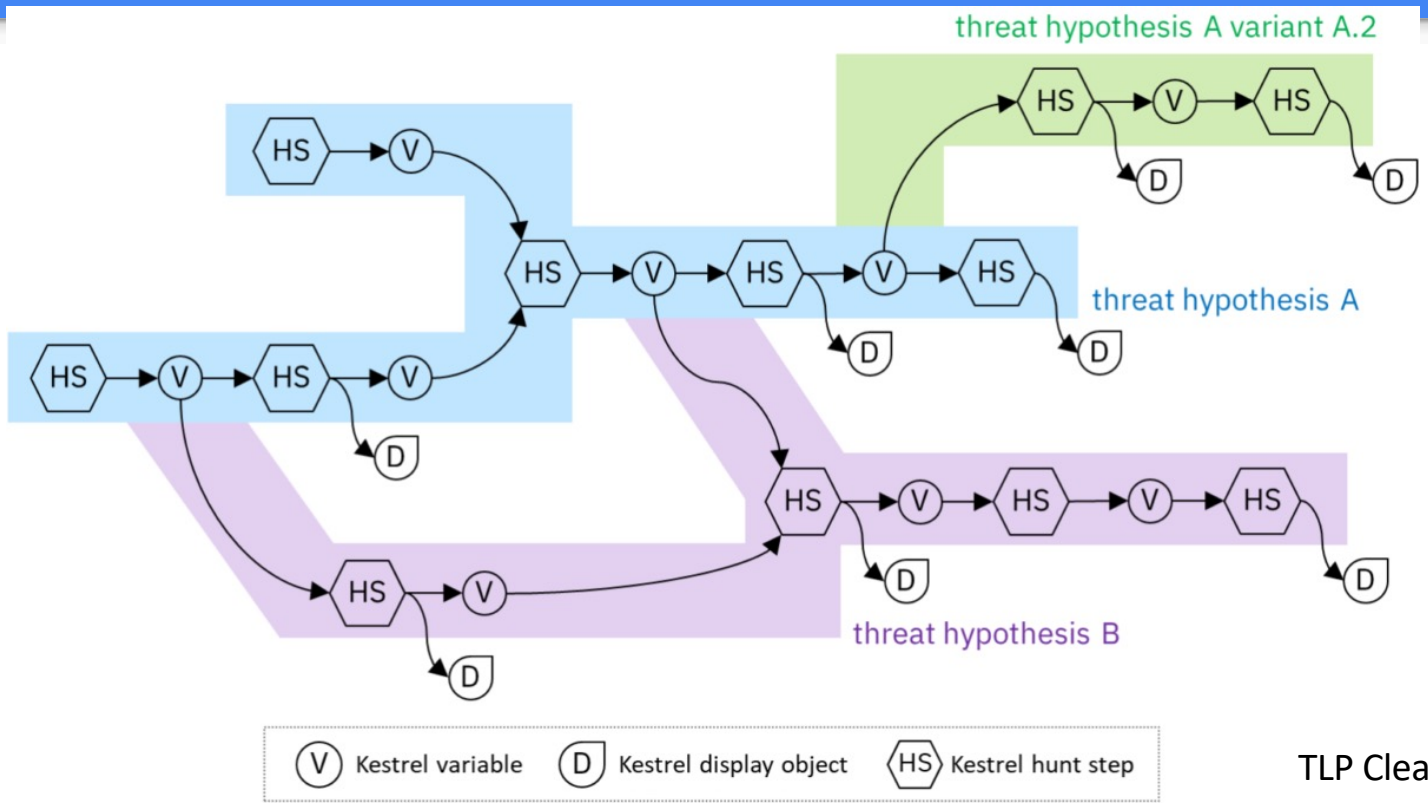


Kick Out Attackers

TLP Clear

Kestrel

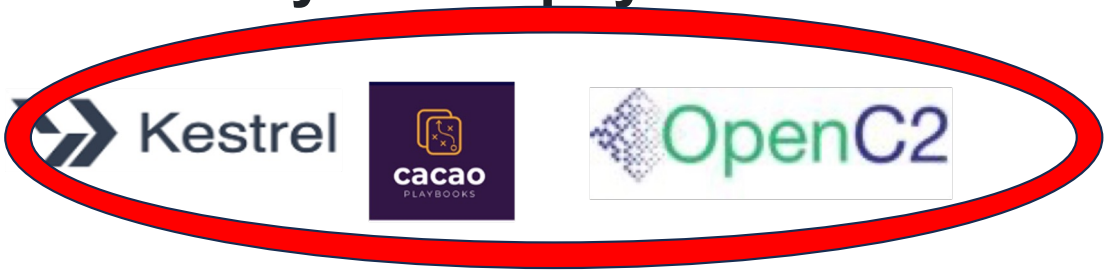
https://github.com/opencybersecurityalliance/kestrel-lang



TLP Clear

The WhitchyWashy Ransomware Use Case

- **Day 1 - Murphy's Law LLP**



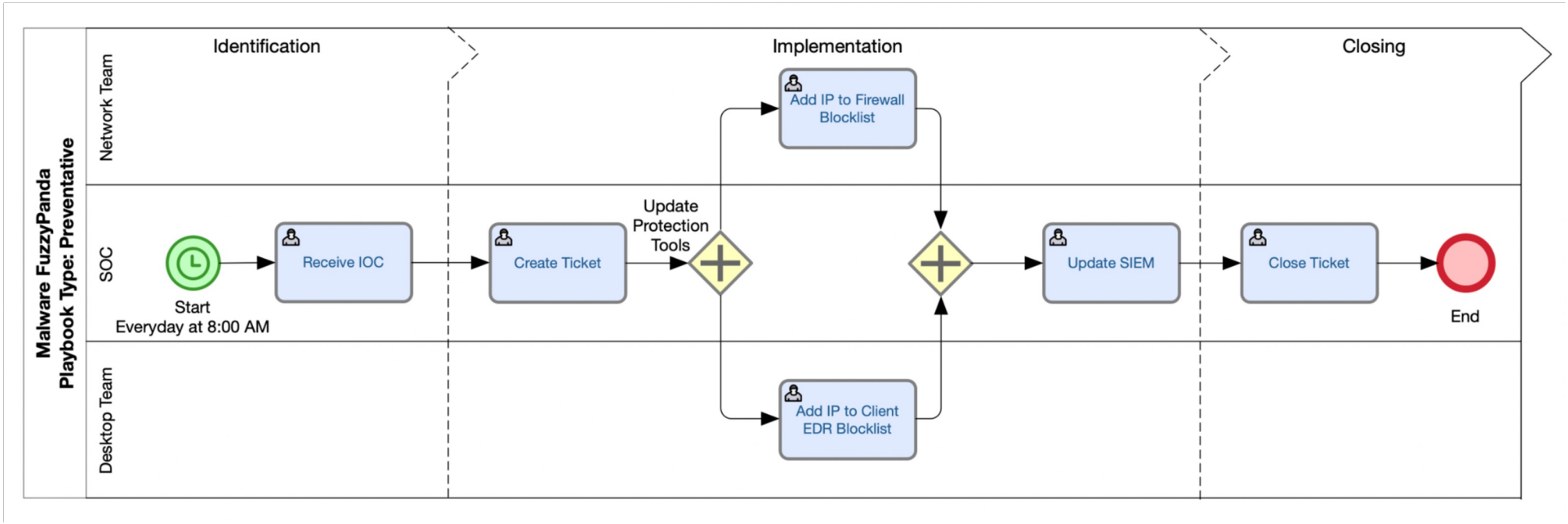
Kick Out Attackers

TLP Clear

CACAO

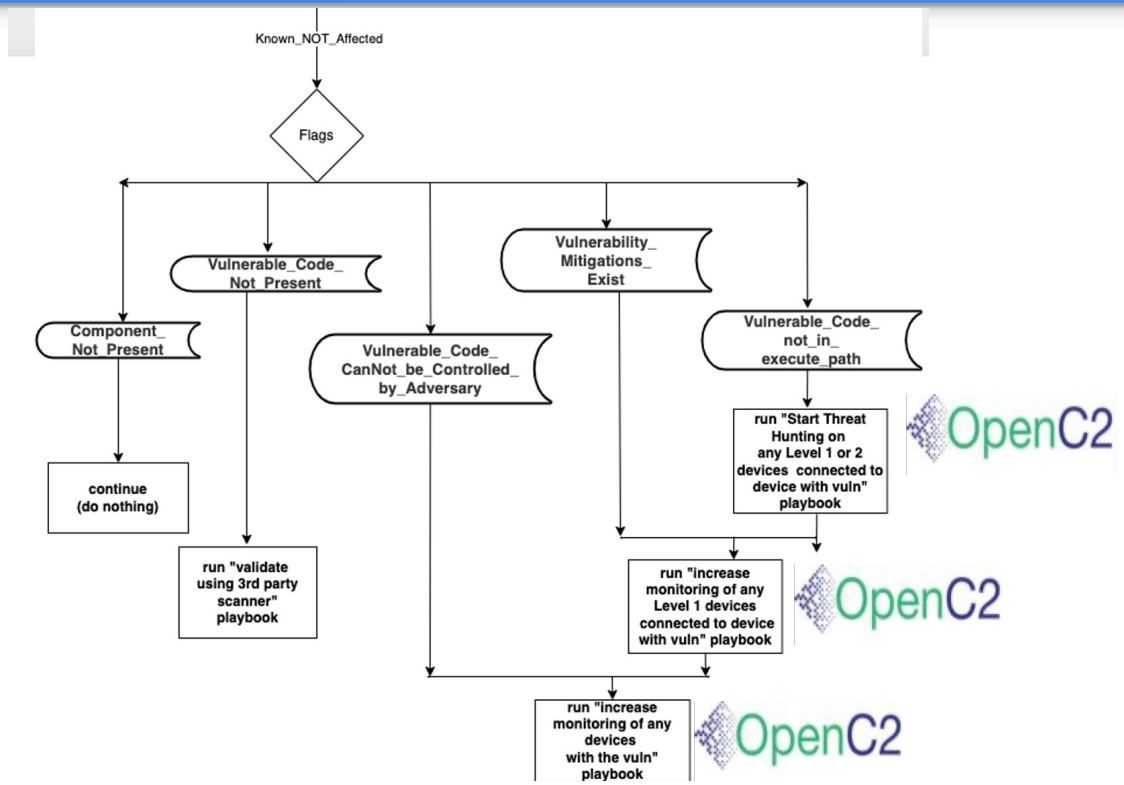
Collaborative Automated Course of Action Operations

CACAO Playbooks in Diagram Form / Similar to BPMN



- 81 existing playbooks written by CISA in BPMN
  - https://github.com/cisagov/shareable-soar-workflows
- Open Source Tool to Covert BPMN to CACAO Playbooks
  - https://github.com/cydarm/bpmn-to-cacao

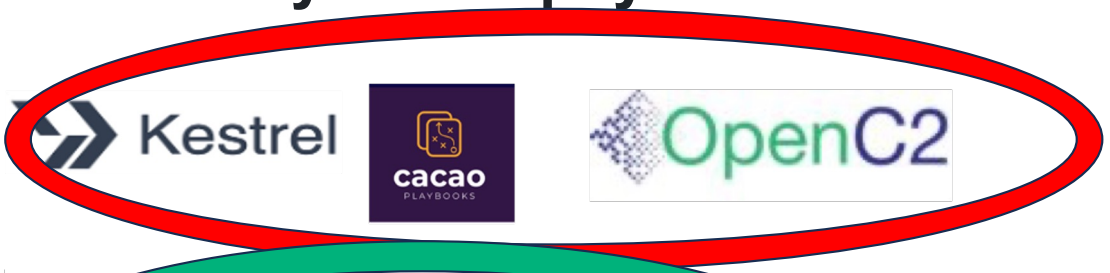
TLP Clear



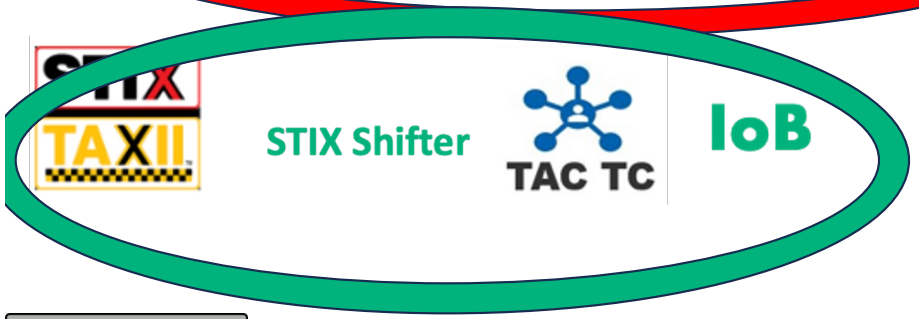
TLP Clear

The WhitchyWashy Ransomware Use Case

- **Day 1 - Murphy's Law LLP**



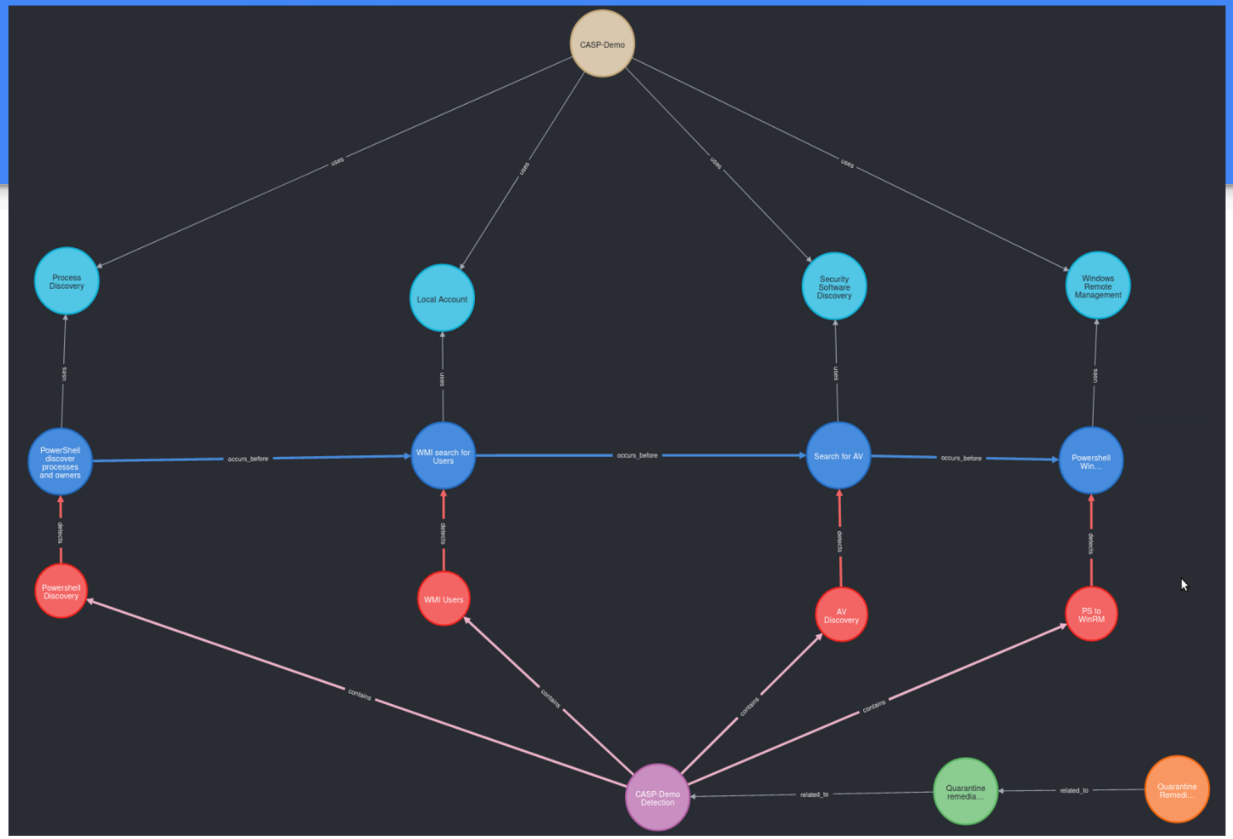
Kick Out Attackers



Share Threat Intel

TLP Clear

Converting STIX to Neo4J Visualizations

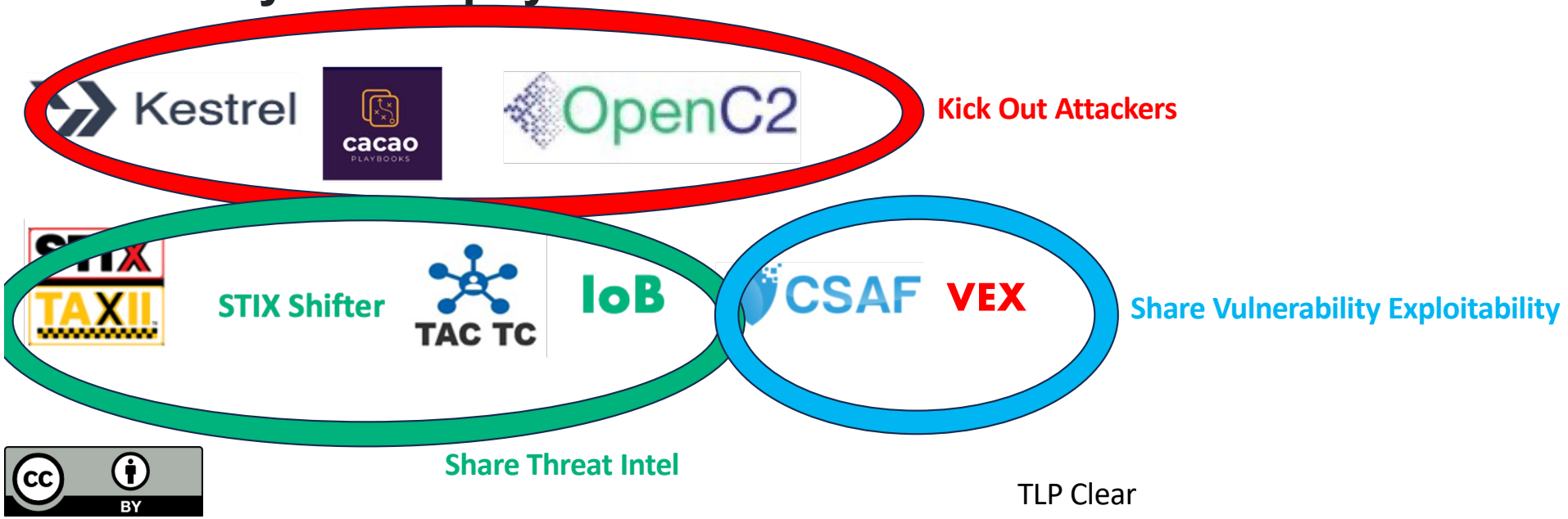


ub.com/opencybersecurityalliance/oca-iob/tree/main/STIX2NEO4J%20Converter

TLP Clear

The WhitchyWashy Ransomware Use Case

- **Day 1 - Murphy's Law LLP**

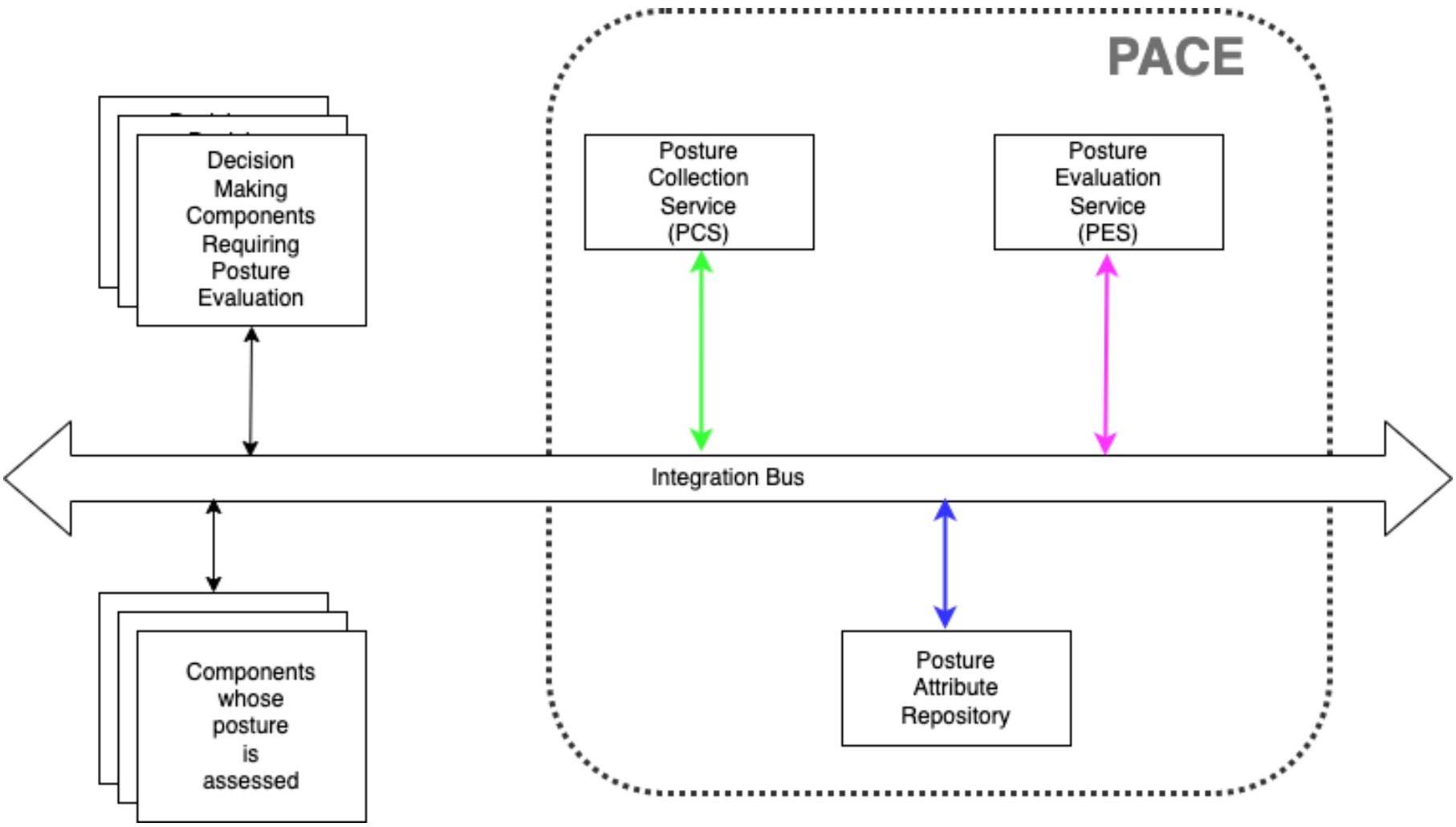


TLP Clear

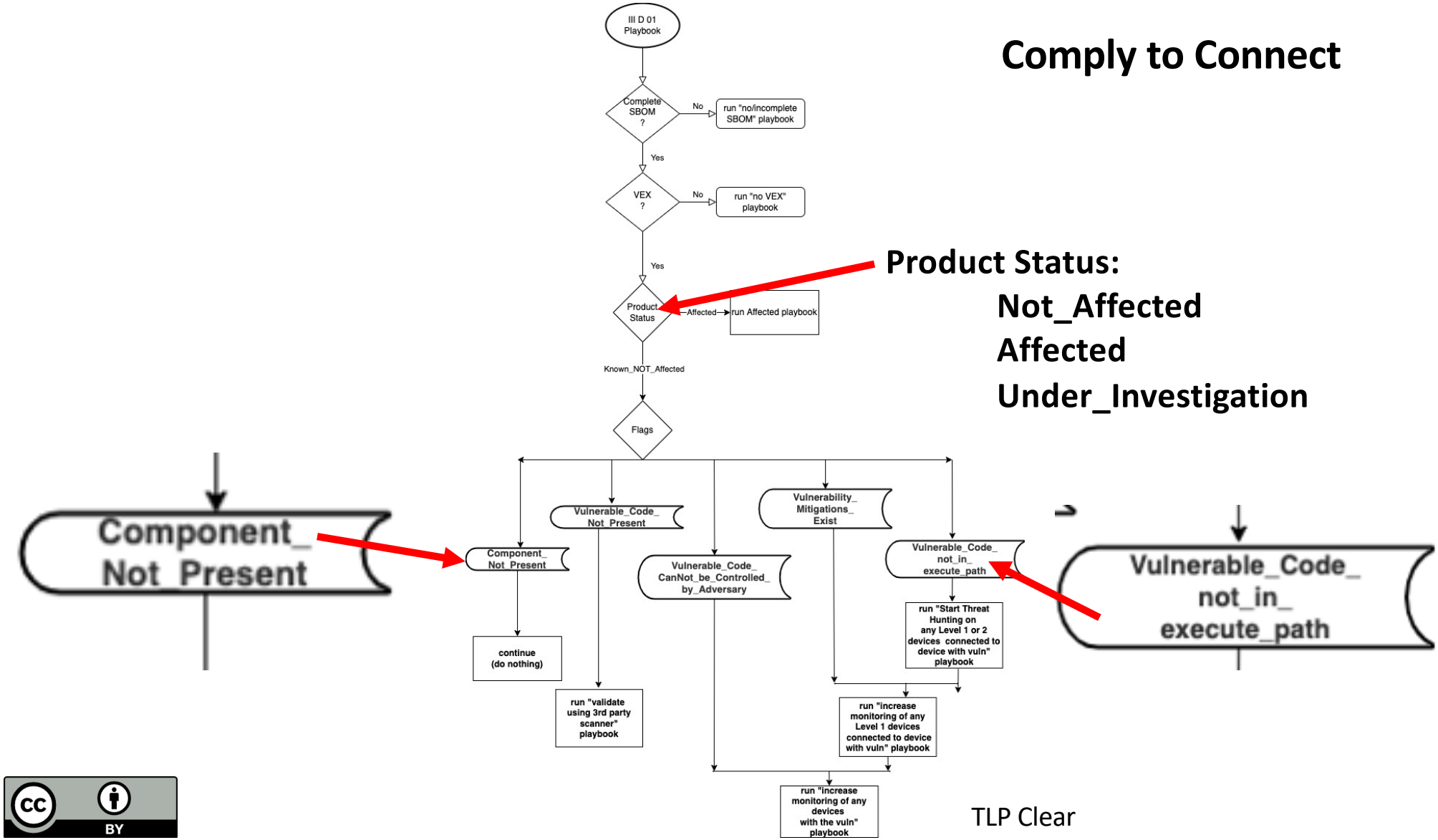
Posture Attribute Collection and Evaluation

https://github.com/opencybersecurityalliance/PACE

TLP Clear


PACE
Decision Making Components Requiring Posture Evaluation
Posture Collection Service (PCS)
Posture Evaluation Service (PES)
Integration Bus
Components whose posture is assessed
Posture Attribute Repository

Comply to Connect



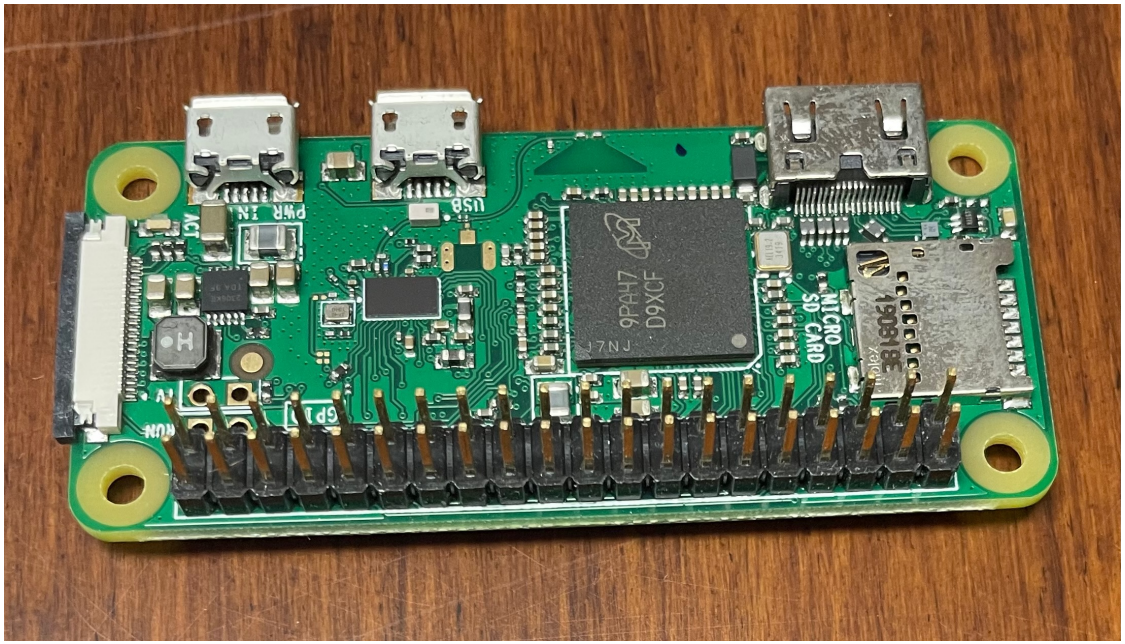
Product Status:

Not_Affected

Affected

Under_Investigation

TLP Clear



TLP Clear

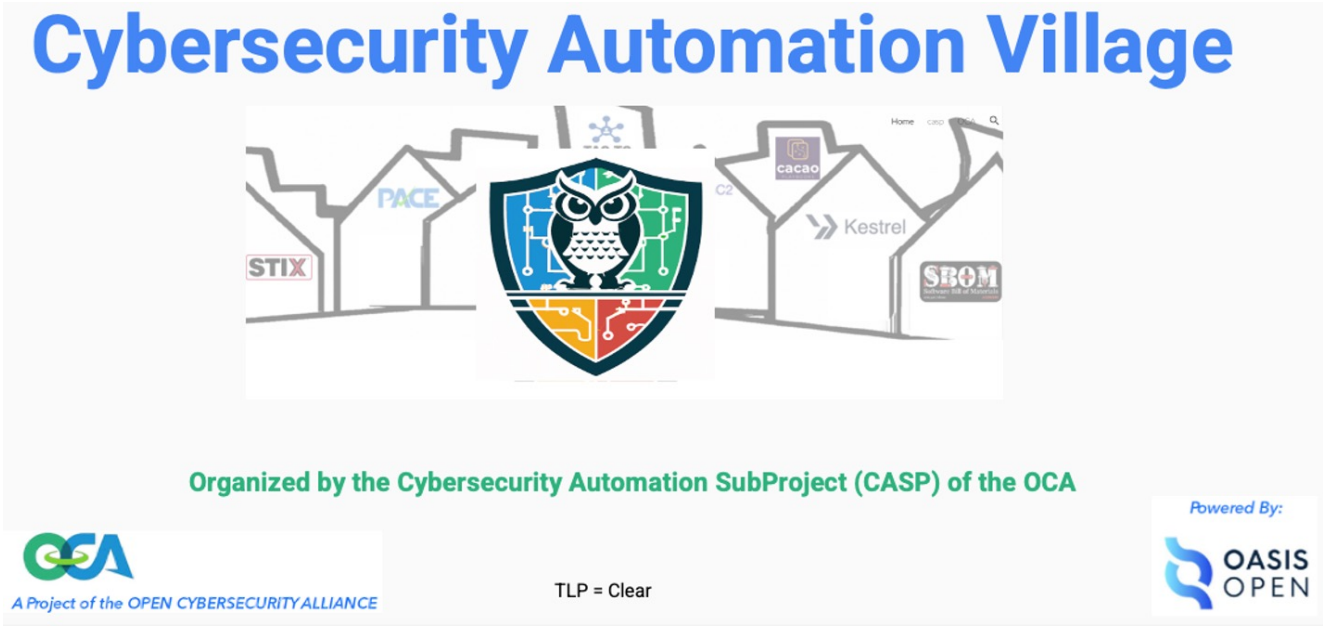
Cybersecurity Automation Village

Start	Topic	link
0:00:00	Set up, kick off	https://youtu.be/Qzv3j-HYlVU
0:00:23	Strategic Objectives	https://youtu.be/Qzv3j-HYlVU?t=23
0:06:26	Use Case Overview and Project Review	https://youtu.be/Qzv3j-HYlVU?t=386
0:47:56	Lunch	https://youtu.be/Qzv3j-HYlVU?t=2876 (s pause earlier
0:50:50	OpenC2 - JADN - Kestrel - STIX Shifter	https://youtu.be/Qzv3j-HYlVU?t=3050
1:28:03	Collaborative Automated Course of Action Operations (CACAO)	https://youtu.be/Qzv3j-HYlVU?t=5283
2:02:48	Threat Actor Context (TAC)	https://youtu.be/Qzv3j-HYlVU?t=7368
2:33:53	Break	https://youtu.be/Qzv3j-HYlVU?t=9233 a running
2:46:32	Indicators of Behavior (IoB)	https://youtu.be/Qzv3j-HYlVU?t=9992
3:11:17	PACE/SBOM	https://youtu.be/Qzv3j-HYlVU?t=11477
3:29:22	Review, Next Steps	https://youtu.be/Qzv3j-HYlVU?t=12562

hub.com/opencybersecurityalliance/casp/blob/main/Plugfests/2023-06-13-USC/Results/README.md#2-recording

TLP Clear

Next



- Still in planning stages
- 2-day event
- NJ? DC?
- March 2024

TLP Clear

OPEN CYBERSECURITY ALLIANCE

1. What is OCA (what, who, how, why)?
2. Why is OCA relevant to VEX community?
3. How can OCA help the VEX community?
4. How can the VEX community help OCA?

TLP Clear