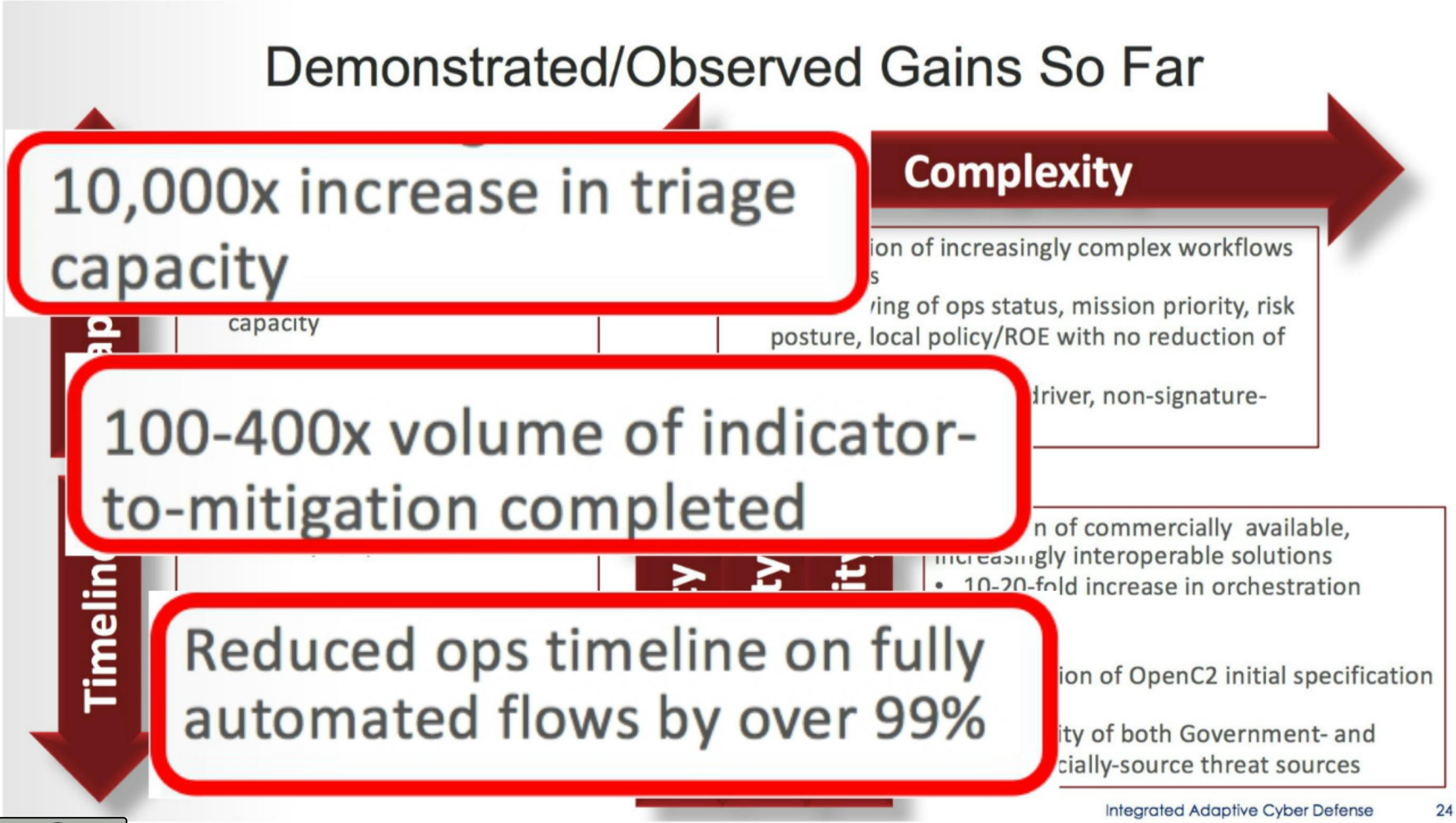
Workshop on Zero Trust and Software Supply Chain Security

Duncan Sparrell

TLP Clear



Demonstrated/Observed Gains So Far

10,000x increase in triage capacity

100-400x volume of indicator-to-mitigation completed

Reduced ops timeline on fully automated flows by over 99%

ion of increasingly complex workflows
s
ving of ops status, mission priority, risk posture, local policy/ROE with no reduction of

driver, non-signature-

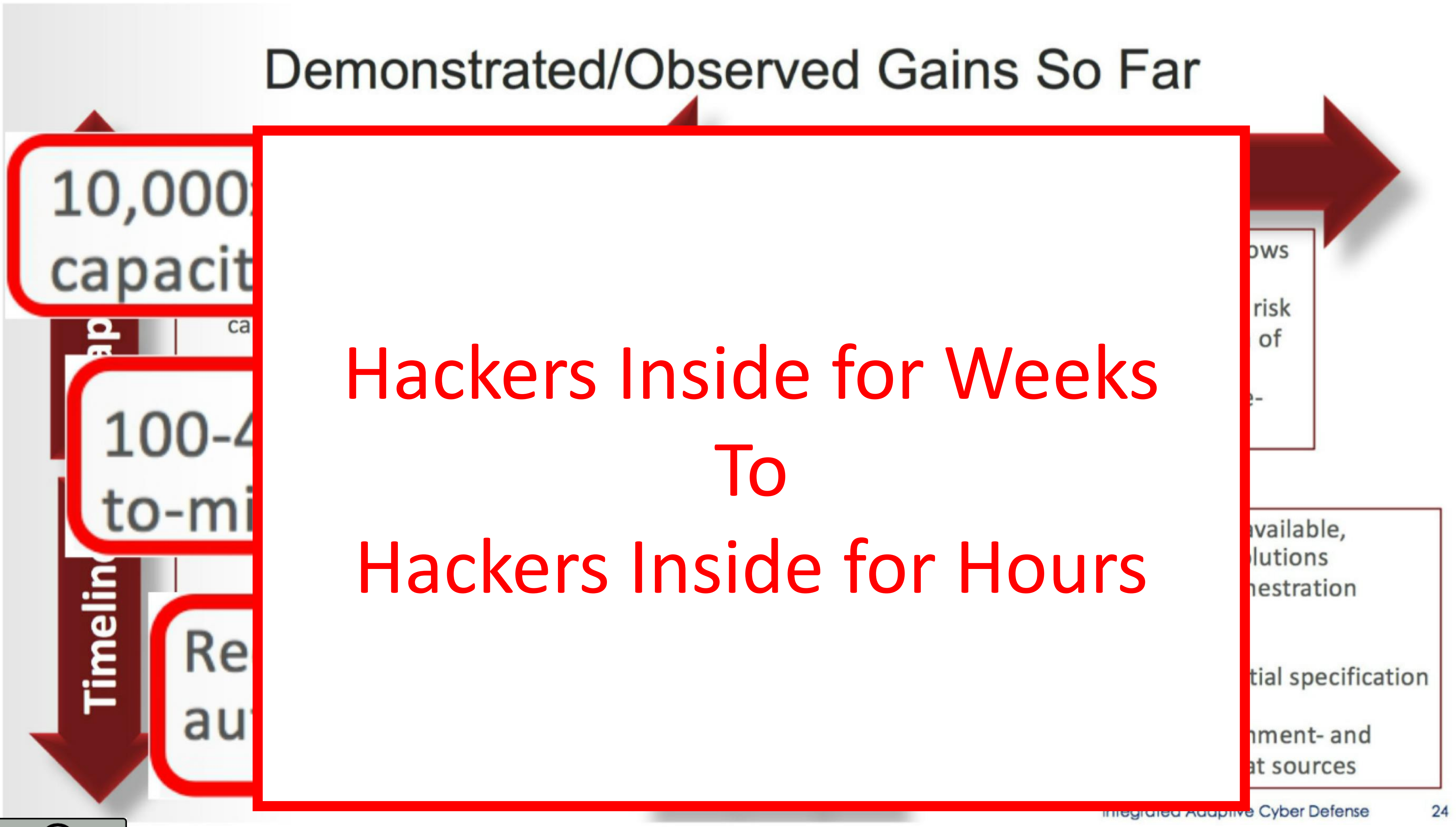
n of commercially available, increasingly interoperable solutions

- 10-20-fold increase in orchestration

ion of OpenC2 initial specification

ity of both Government- and cially-source threat sources

TLP Clear



Demonstrated/Observed Gains So Far

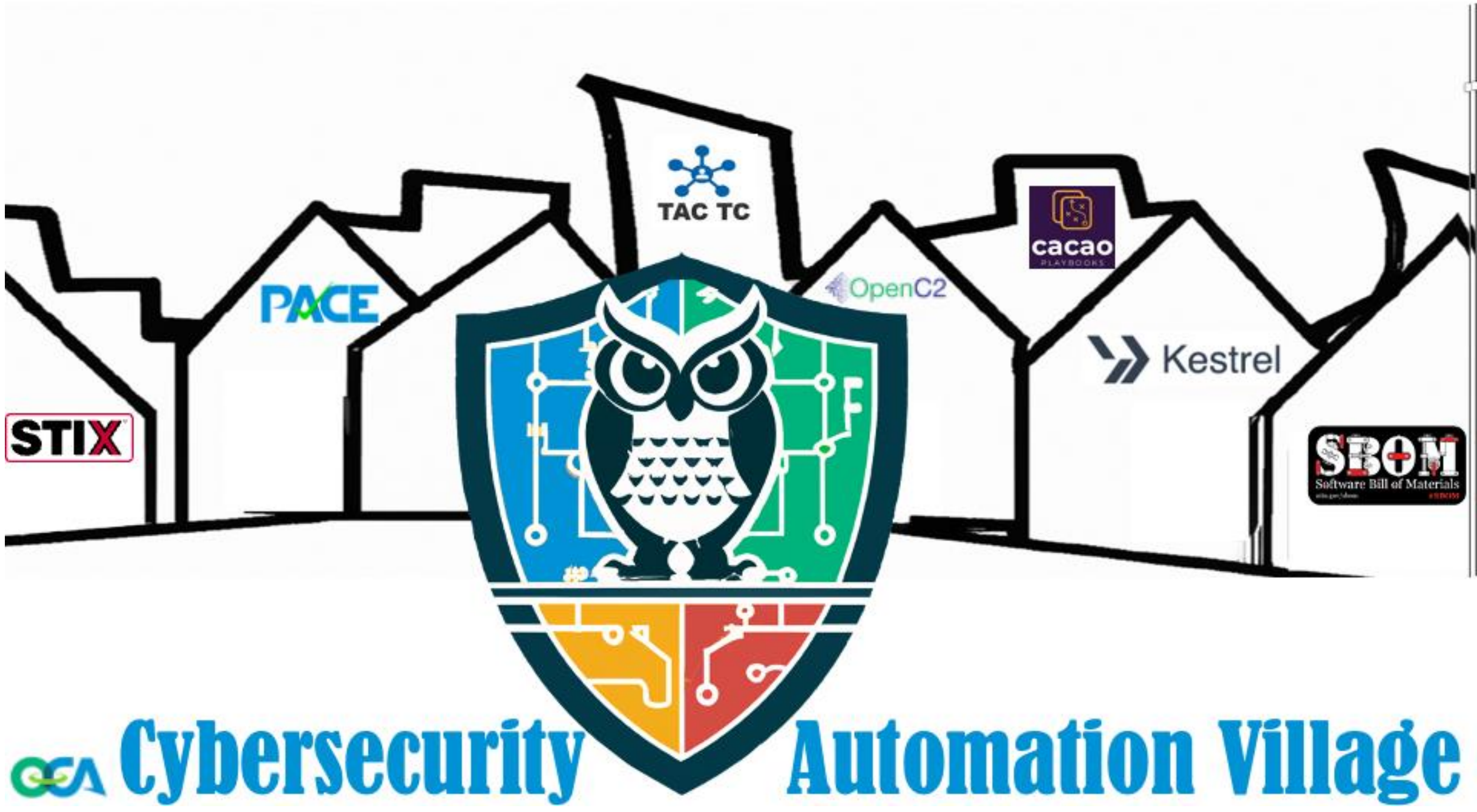
Hackers Inside for Weeks

To

Hackers Inside for Hours

TLP Clear

OPEN
CYBERSECURITY
ALLIANCE

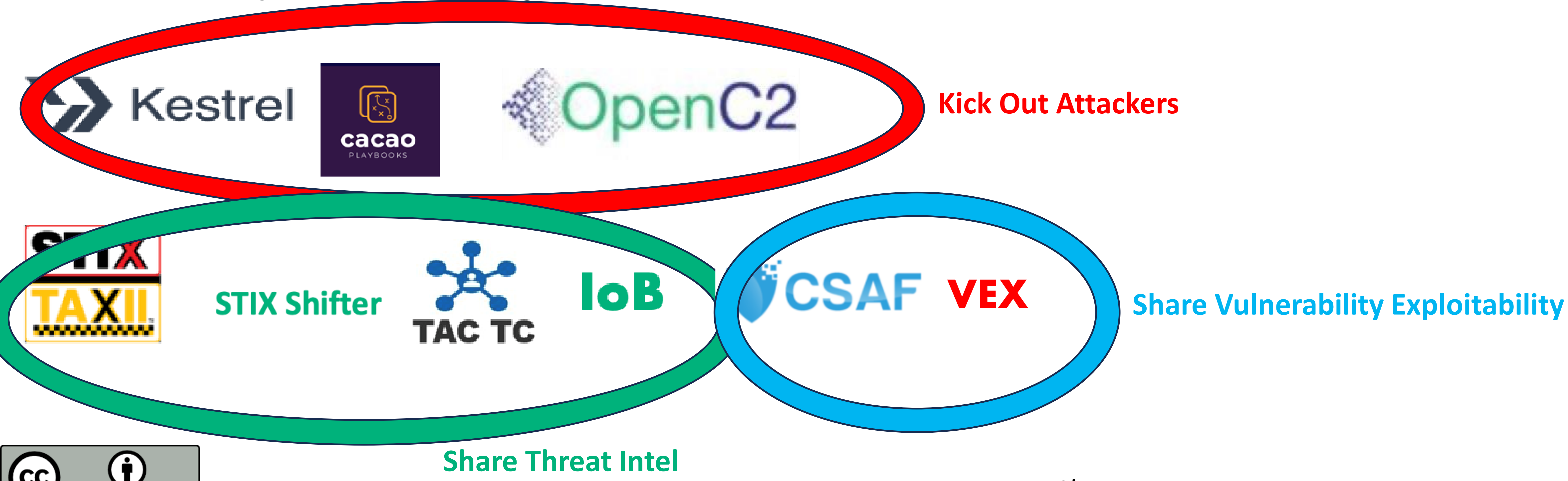


The WhitchyWashy Ransomware Use Case

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

The WhitchyWashy Ransomware Use Case

- **Day 1 - Murphy’s Law LLP**



Kick Out Attackers

Share Vulnerability Exploitability

Share Threat Intel

TLP Clear

The WhitchyWashy Ransomware Use Case

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

STIX TAXII STIX Shifter TAC TC IoB Kestrel cacao PLAYBOOKS OpenC2

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

There is never enough time.

Thank you for yours.