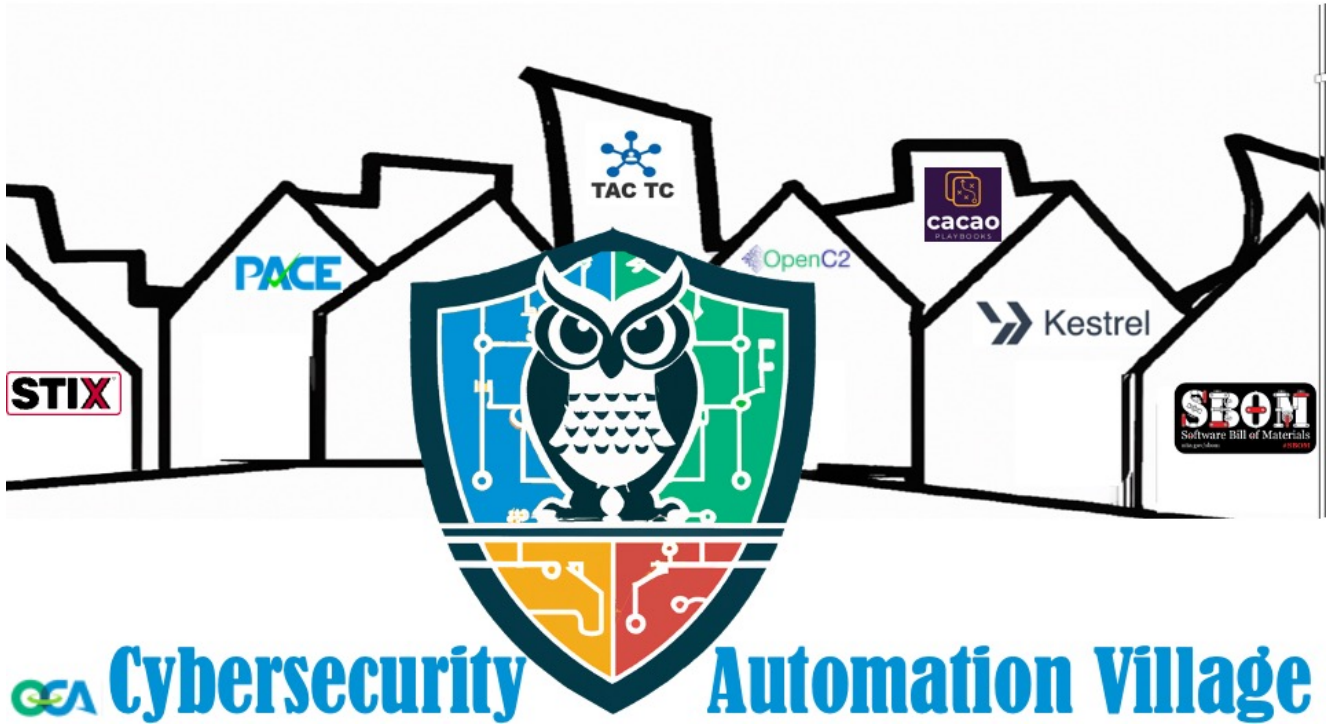
# Village
# Value Propositions, Infrastructure, Format, and Goals

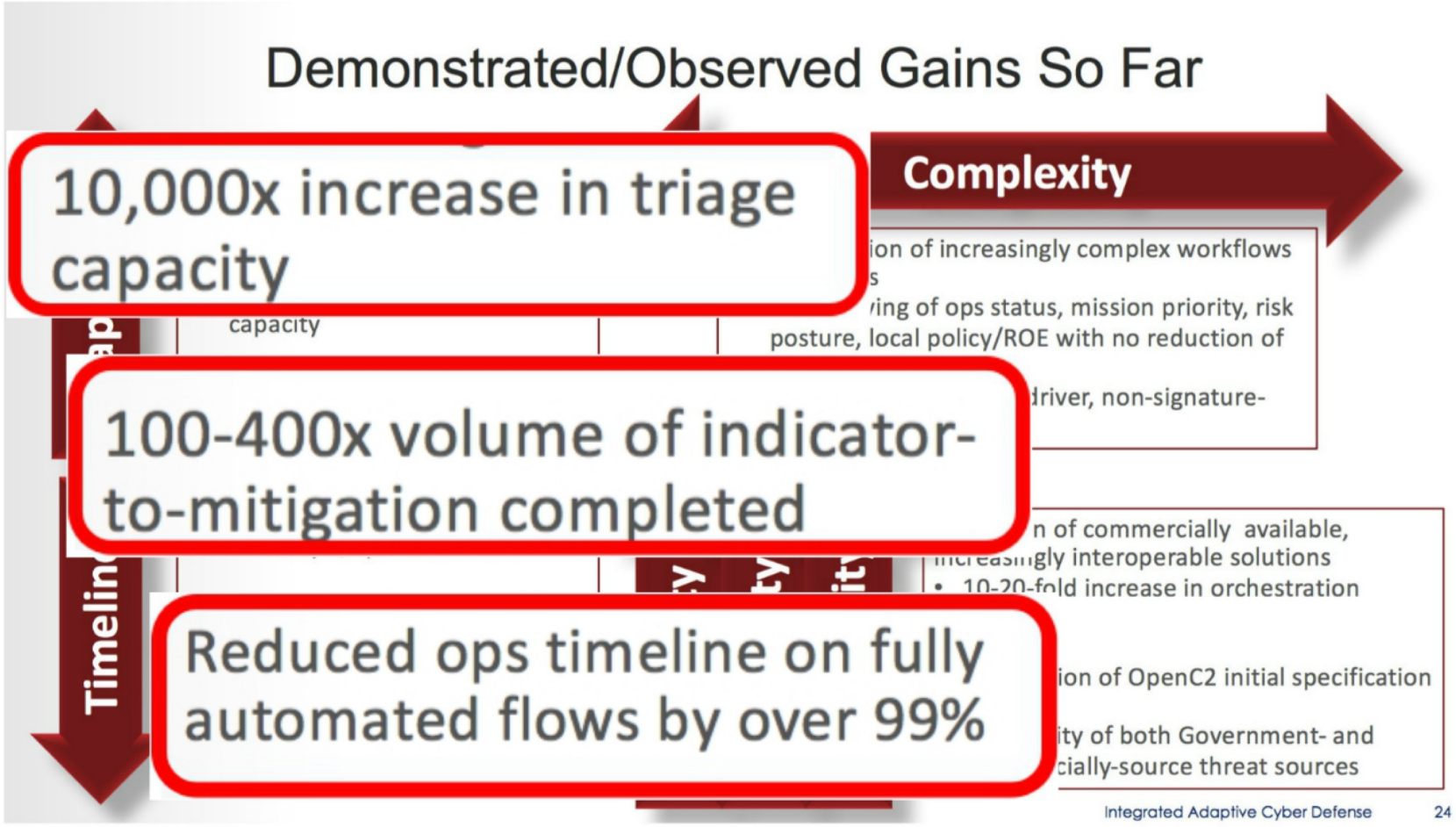



cacao
PLAYBOOKS
CACAO Roaster
CSAF
IoB
VEX
Kestrel
TAC TC
MISP
Threat Sharing
STIX Shifter
OPEN
CYBERSECURITY
ALLIANCE
Cybersecurity
Automation
SubProject
NIEMOPEN
STIX
TAXII
OPENCTI
SOARCA
OpenC2
SBOM
Software Bill of Materials
EOX
OXA
PACE
OSIM

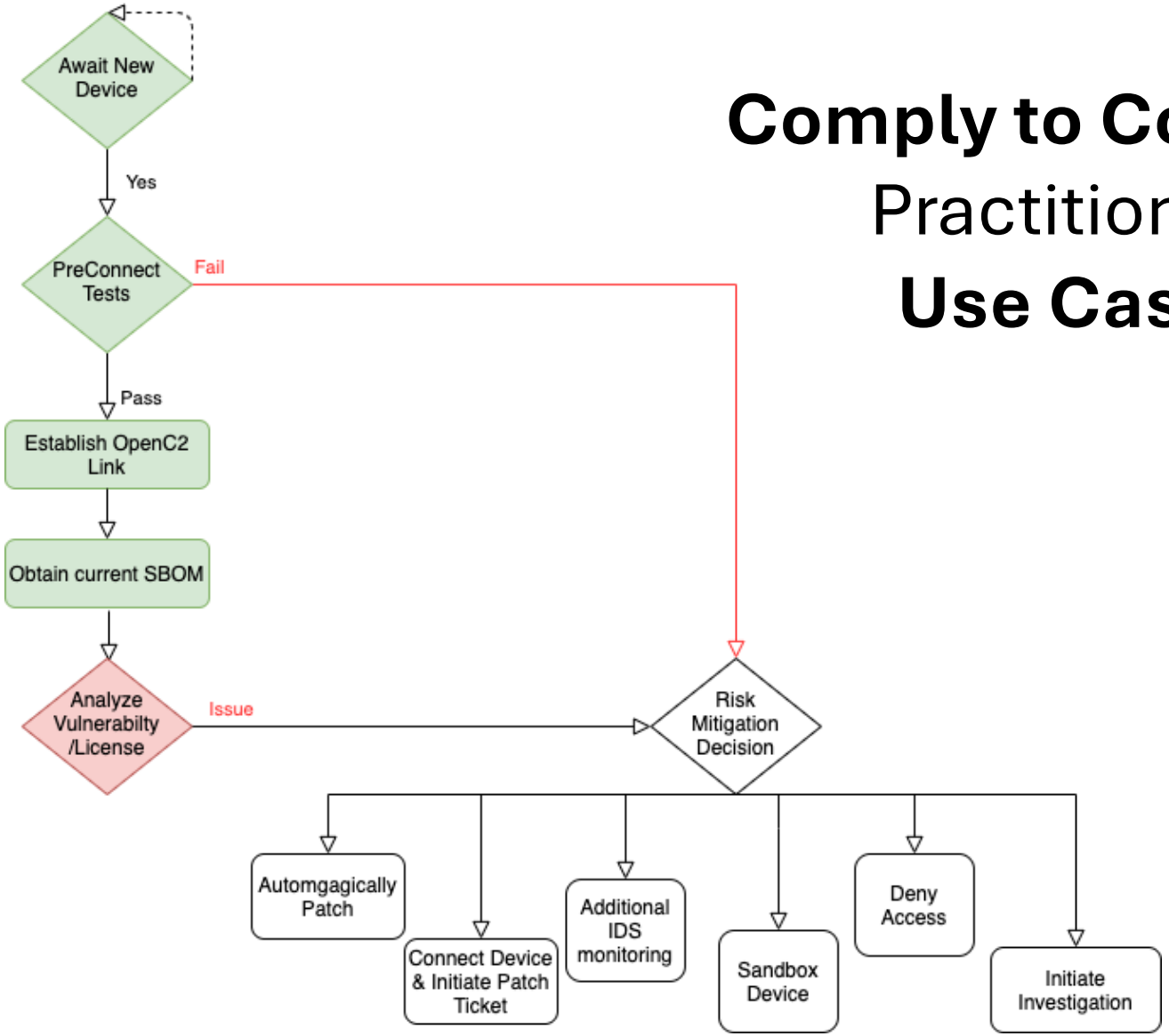

OCA
HDF
CACAO
CSAF/VEX
PACE
STIXSHIFTER
SPDX
OPENC2
NIEM
STIX/TAXII
CAW
TAC
SBOM
VSMI
KESTREL
CYCLONEDX

# Why Cybersecurity Automation?

# Why Cybersecurity Automation?



# Comply to Connect
Practitioner
# Use Case



# The WhitchyWashy Ransomware Value Proposition

- **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 - MilOps**

**Objective: As many  projects on as many days as possible**

- **Machine API's, Humans, Handwaving**

# Day 1 - Murphy’s Law LLP

During the vows at a daughter’s wedding, midway through an emergency root canal, at 8 a.m. on Christmas morning the CEO of Murphy’s Law LLP receives a most unwelcome message: a brand new exploit has made its world-wide zero-day debut in the company’s system. Fortunately, Murphy’s Law LLP had the foresight to adopt cybersecurity automation protocols. An immediate Kestrel threat hunt finds the exploited systems, and the automation kicks the attackers out of the system using CACAO playbooks with OpenC2 commands, alerts law enforcement, and analyzes the tactics and exploited vulnerabilities. Recognizing this as a zero-day, STIX bundles are prepared containing the threat information (IoCs, IoBs, TAC) and playbooks for prevention/detection/response (CACAO, OpenC2). The STIX information is shared with their ISAC for distribution to others in their industry. Because the attacks exploited previously unknown vulnerabilities in both commercial and open source software, Murphy's Law LLP submits new VEXes

# Day 2 - On Deck Holdings

Panic begins anew at On Deck Holdings as a stark uptick in server activity signals that yesterday's exploits at Murphy's Law LLP have spread to new haunts. Fortunately, On Deck Holdings previously received STIX information from their ISAC. Being similarly automated, On Deck Holdings' cybersecurity systems soon match their problem with the STIX object generated the day before, initiate the CACAO playbook, execute OpenC2 commands, and freeze out the black hat hackers that gained entry into their system.



# Day 3 - Triumvirate CleanUp Inc

As the unknown exploit becomes a known entity, the zero-day becomes an N-day.

Triumvirate CleanUp Inc, also a subscriber to their ISAC, analyzes the STIX bundle and decides to use their PACE system to analyze their environment and see if they are vulnerable to the same attack that targeted Murphy's Law and On Deck. Using their PACE system, they analyze their SBOM's and discover they do have 70 devices with components that have the CVEs reported in the STIX bundle. Further analysis with PACE shows that 30 of those potentially affected devices have VEXes from their suppliers that indicate they are not susceptible to those CVEs. Triumvirate CleanUp then initiates automated patching to harden the remaining 40 devices and avoids getting hacked.

# Day 4 - NSAANSA

The Never Say Anything and No Such Agency (NSAANSA) in the US Dept of Useless Factoids has automated cybersecurity adhering to federal guidelines including the "comply to connect" edict, which requires any new devices connecting to a network to have an acceptable security posture. NSAANSA's ISAC feed receives the STIX bundle and their systems automagically convert that informaton into new rules for calculating security posture in their PACE system. When a new device attempts to connect to the NSAANSA environment, their security posture assessment includes the PACE system examining device SBOMs and VEXes including looking for impact of the WhitchyWashy CVEs.

Although NSAANSA is not the lead agency for sharing comply-to-connect policies with the State/Local/Tribal-Terriorities (SLTT), NSAANSA creates a NIEM IEP information packet for SLTT consumption and implementation and transmits that to the lead agency, CISA,for transmission to the SLTT.

# Day 5 - Law Enforcement

Initially brought into the loop and involved throughout, law enforcement prepares multiple NIEM Message Exchange Packages (MEP) for entry in the Law Enforcement National Data Exchange (N-DEx) and for exchanges with the Royal Canadian Mounted Police (RCMP), Europol, and Interpol. A criminal takedown across 6 countries occurs and 23 miscreants are put behind bars using evidence and e-filings built from NIEM MEPs.

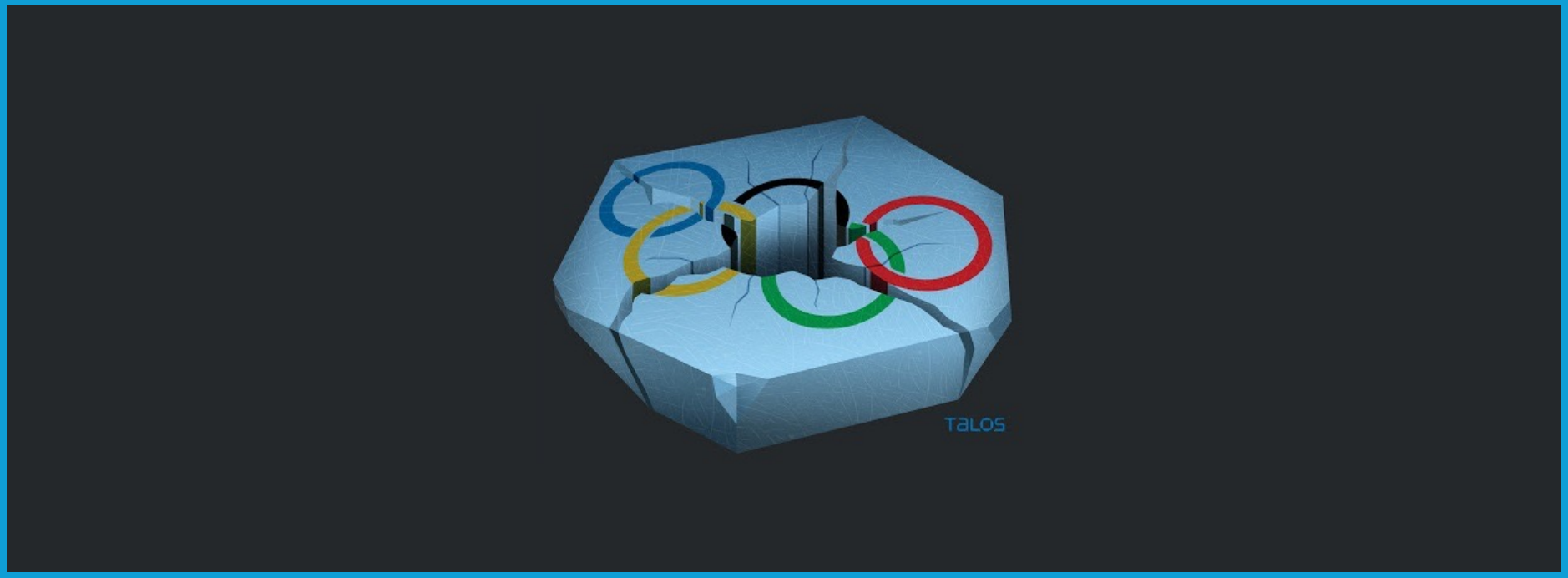


# Day 6 - MilOps

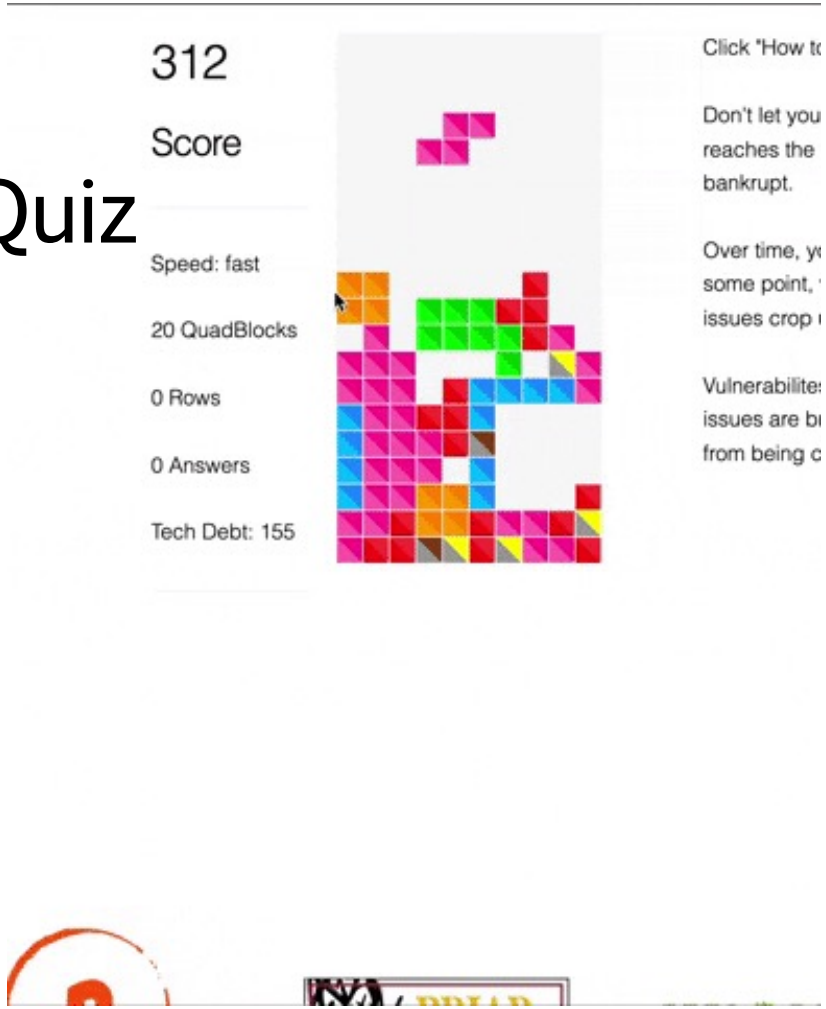
It can neither be confirmed nor denied whether rogue nation states were involved in this use case; just as it can neither be confirmed nor denied whether NIEM MilOps extensions were distributed among NATO allies and hunt forward operations bricked adversary servers behind the attack. Day 6 is out-of-scope for the Cybersecurity Automation Village.



# Olympic Destroyer



# Play QuadBlockQuiz




# Win Prizes!

amazon

BARNES&NOBLE

THE HOME DEPOT

**There is never enough time.**

**Thank you for yours.**