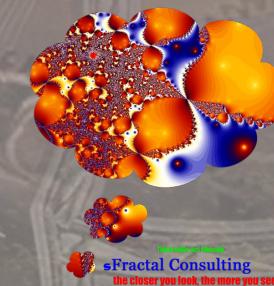
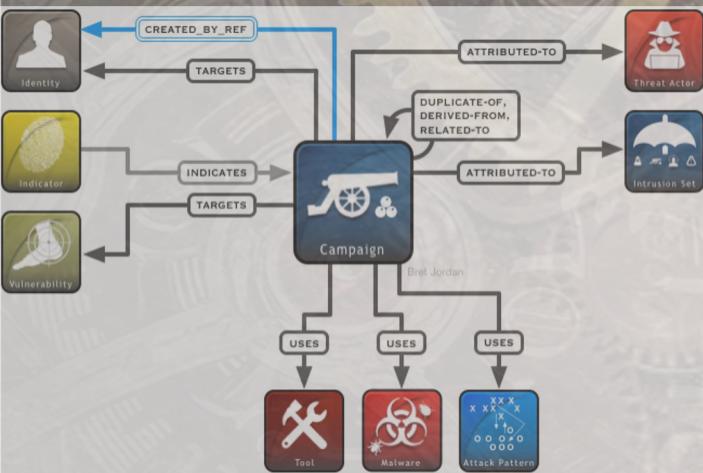


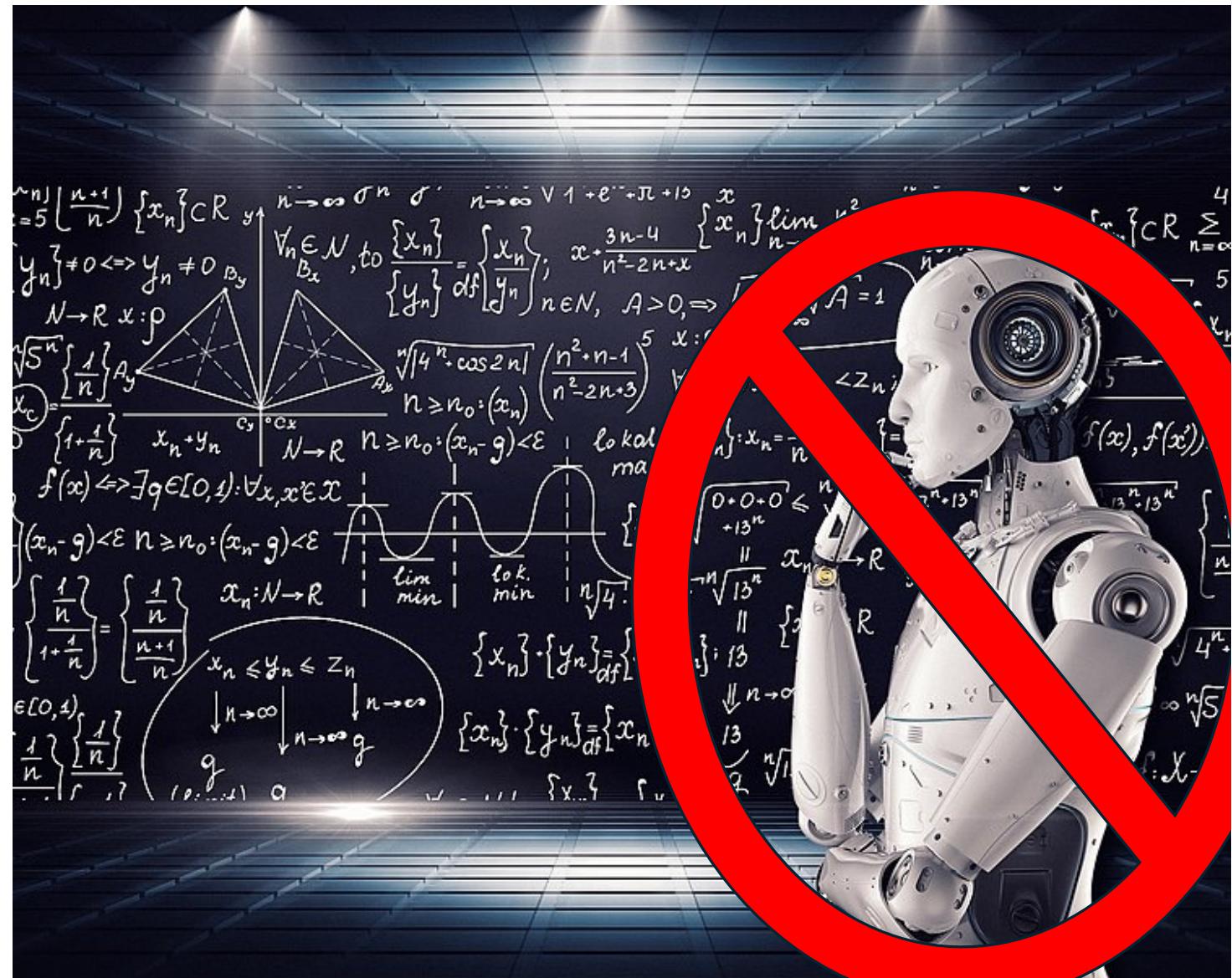
Save Time & Money Automate using Cybersecurity Standards

Duncan Sparrell



This is
NOT
an
AI Talk

CC By WikiMedia

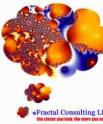




THINK EVILLY



Act Ethically

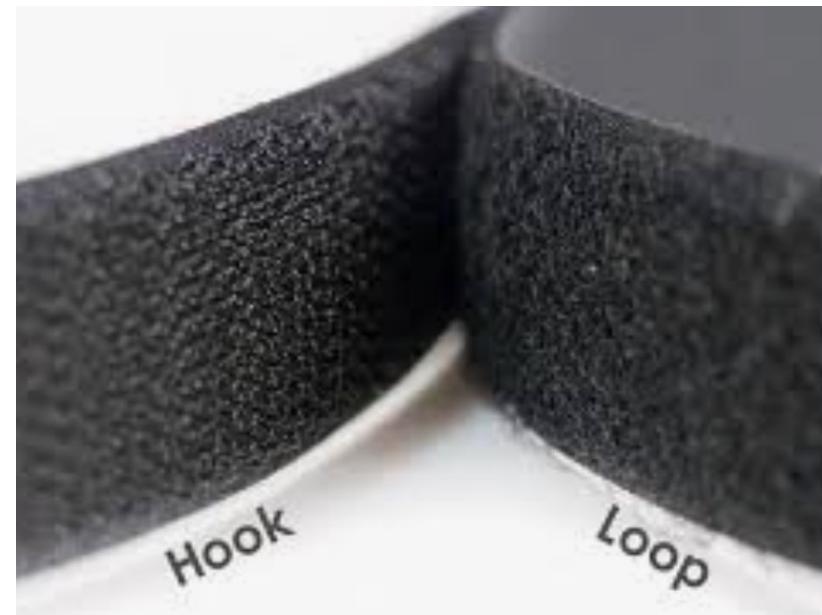


Fractal Consulting LLC
www.fractalconsultingllc.com



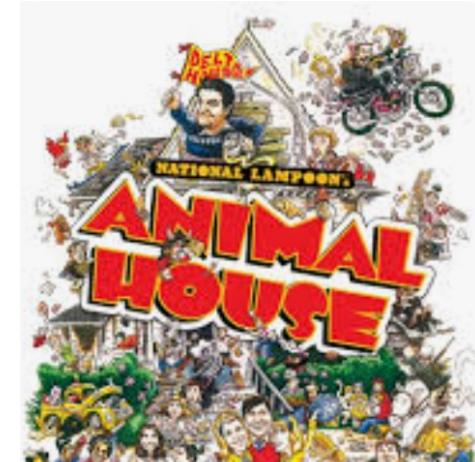
1955

- The Soviet Union and 7 east European countries sign Warsaw Pact
- The Montgomery bus boycott set off the civil rights movement
- Velcro was invented
- The TV remote was invented
- The first home microwave oven was sold
- The first McDonald's opened



1978

- The largest ever march for women's rights
- The US and China normalized diplomatic relations
- National Lampoon's "Animal House"
- Penzias and Wilson win Nobel Prize for "Big Bang"
- "Don't drink the Kool-Aid" (Jonestown massacre)
- First designer jeans
- Homebrewing beer became legal

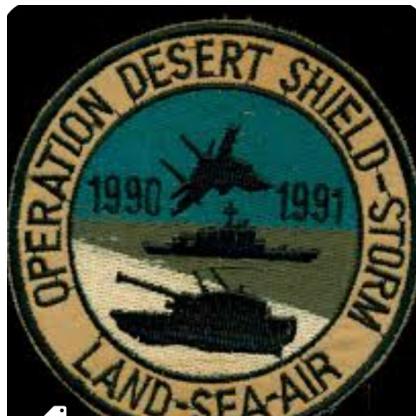


1990

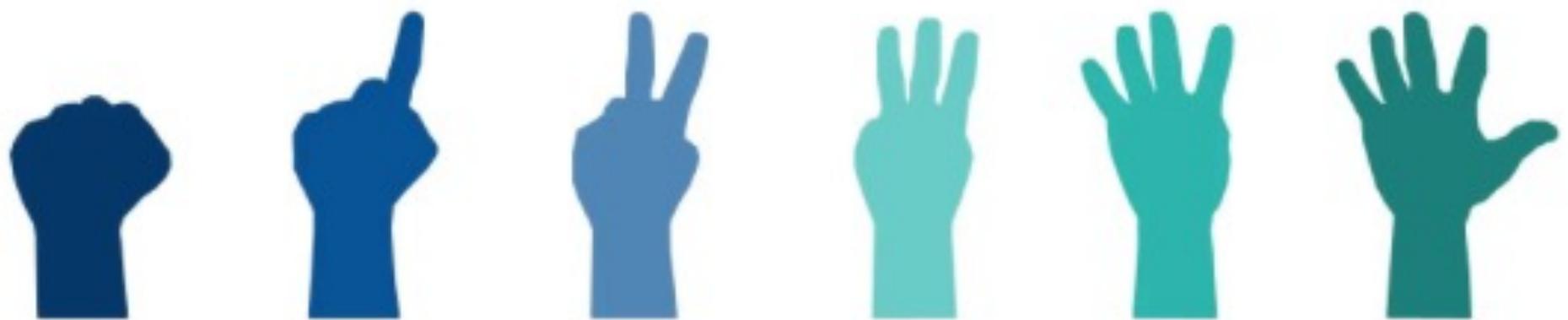
- Launch of the Hubble Space Telescope
- Reunification of Germany
- Nelson Mandela released from prison
- Browser / World Wide Web invented
- Iraq invades Kuwait / Operation Desert Shield



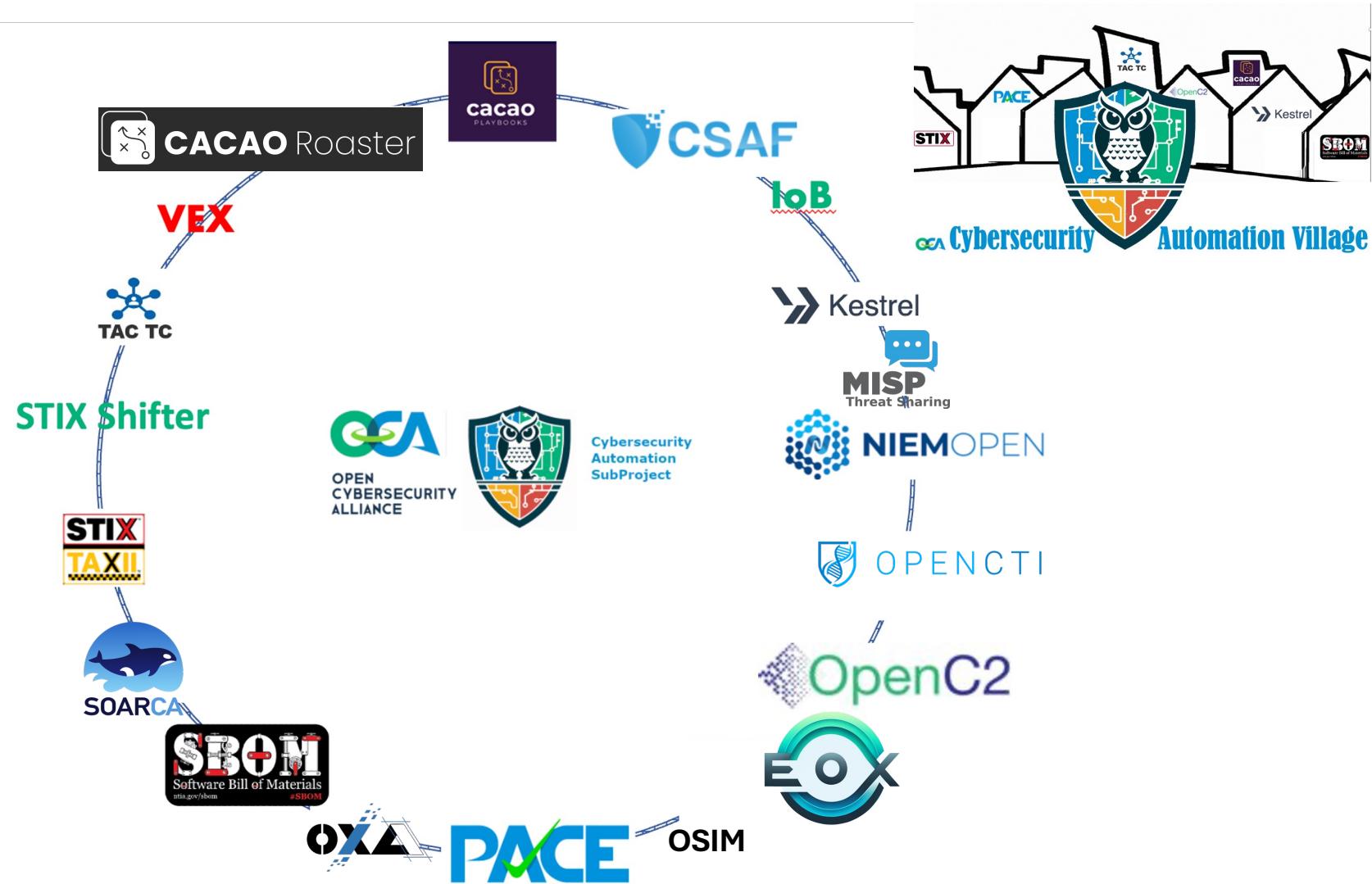
Credit: ESA/Hubble



✊ Fist to Five ✌







Takeaway



**Cybersecurity standards
enable automation
saving
time, people, and money**

6-Oct-2024 Washington Post

“I can’t remember when the cyber-people said ‘We’ve got nothing to report today’... Cyber-threats occupy about half of my time”.

Christopher Wray
Director, FBI

The Washington Post
Democracy Dies in Darkness

Opinion | Calamity in a keystroke: How the FBI copes with mounting threats

Christopher A. Wray: Cyberthreats are ‘diverse and constantly evolving.’

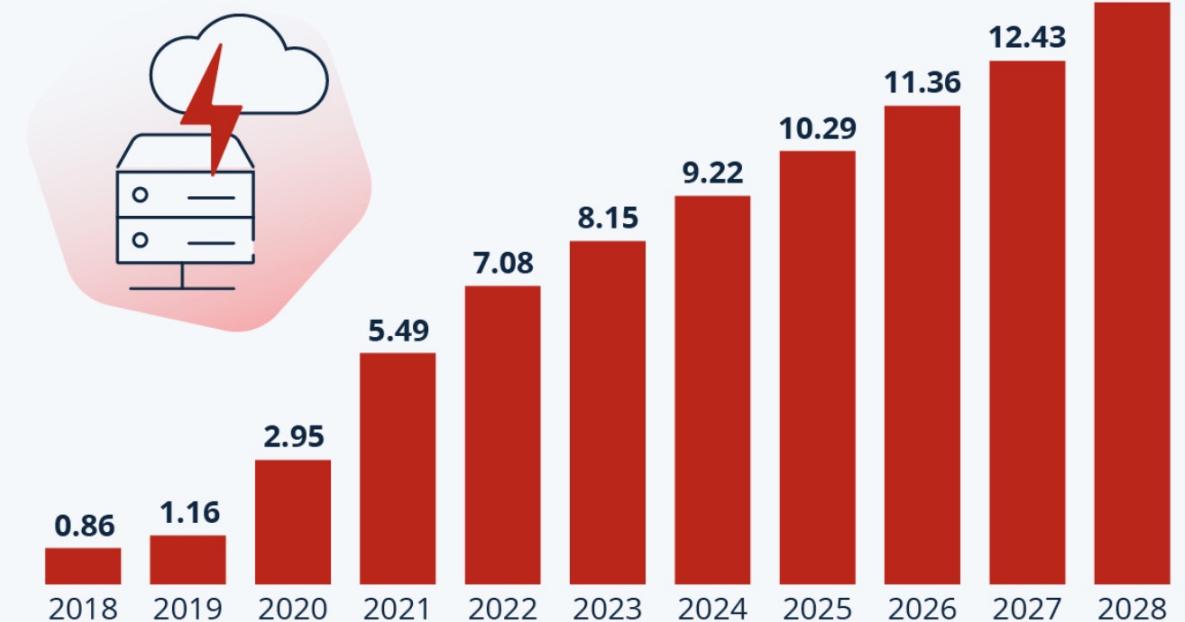


A close-up photograph of a man with brown hair, wearing a white shirt, shouting into a black mobile phone held to his ear with his right hand. He has a determined and intense expression. A large, white, rounded rectangular speech bubble originates from his mouth, containing the text "SHOW ME THE MONEY!" in bold, black, sans-serif capital letters.

**SHOW
ME THE
MONEY!**

Cybercrime Expected To Skyrocket

Estimated annual cost of cybercrime worldwide
(in trillion U.S. dollars)



As of Sep. 2023. Data shown is using current exchange rates.

Source: Statista Market Insights



Screenshot

statista

THE WHITE HOUSE



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybers>

THE WHITE HOUSE



**"In the end,
the trust we place in our digital infrastructure
should be proportional
to how trustworthy and transparent that infrastructure is,
and to the consequences we will incur
if that trust is misplaced."**

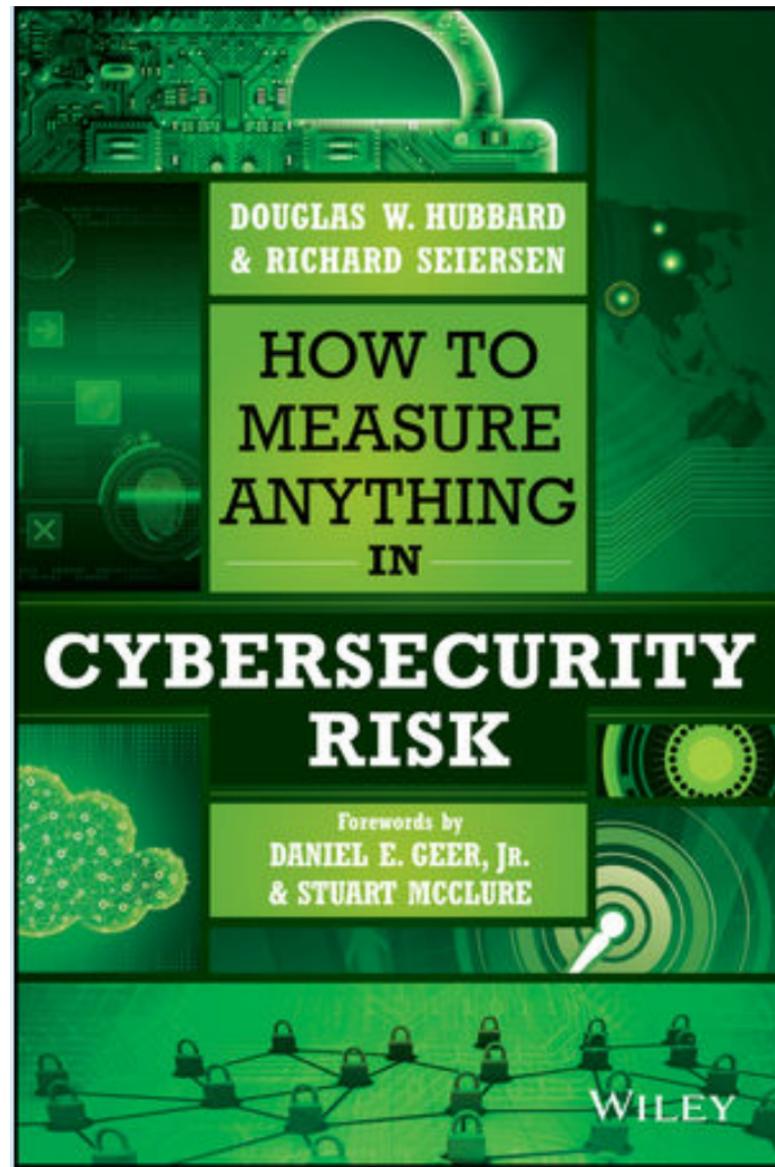


A close-up photograph of a man with brown hair, wearing a white shirt, shouting into a black mobile phone held to his ear with his right hand. He has a determined and intense expression. A large, white, rounded rectangular speech bubble originates from his mouth, containing the text "SHOW ME THE MONEY!" in bold, black, sans-serif capital letters.

**SHOW
ME THE
MONEY!**



The Power of the Federal Purse

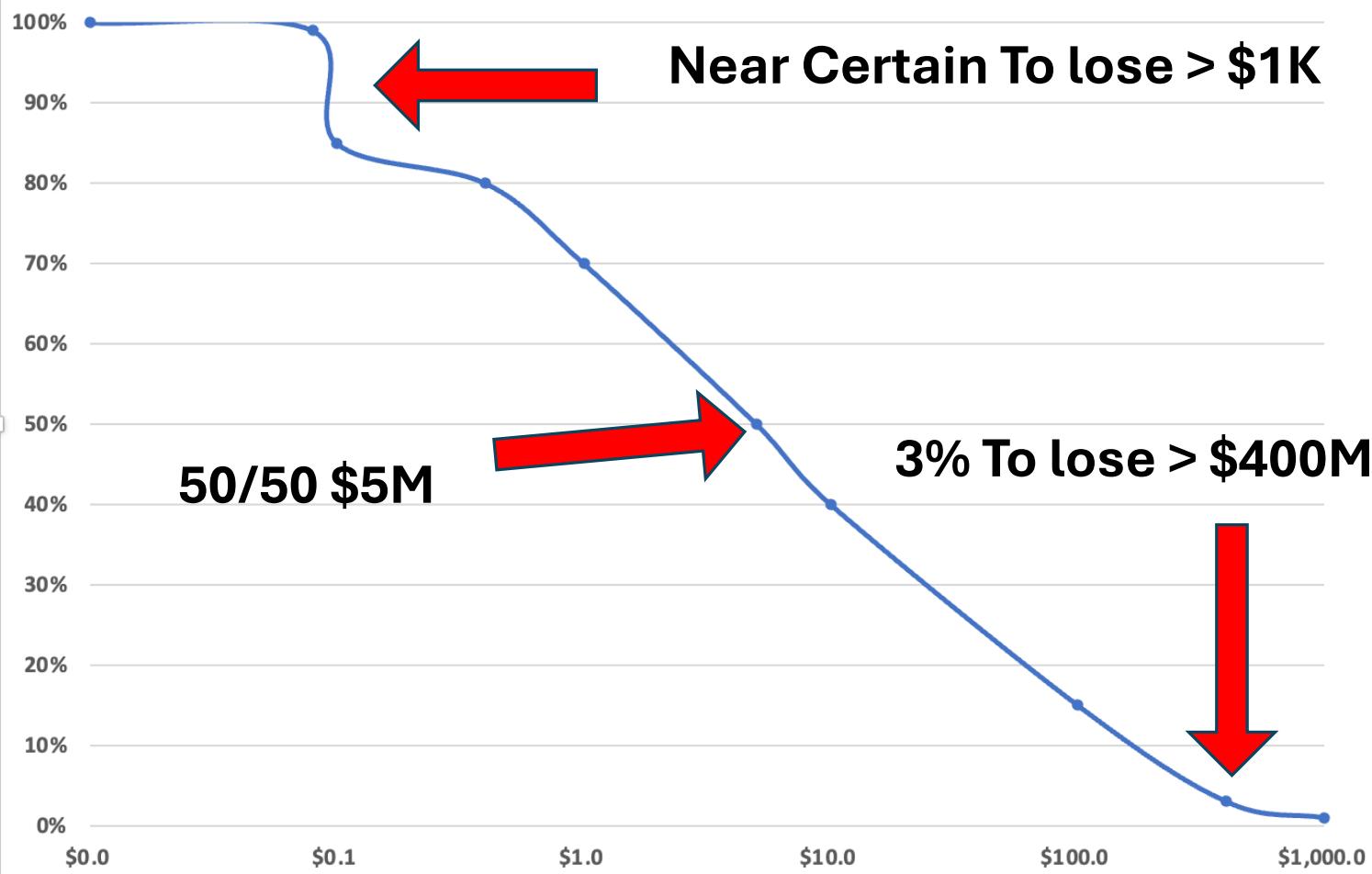


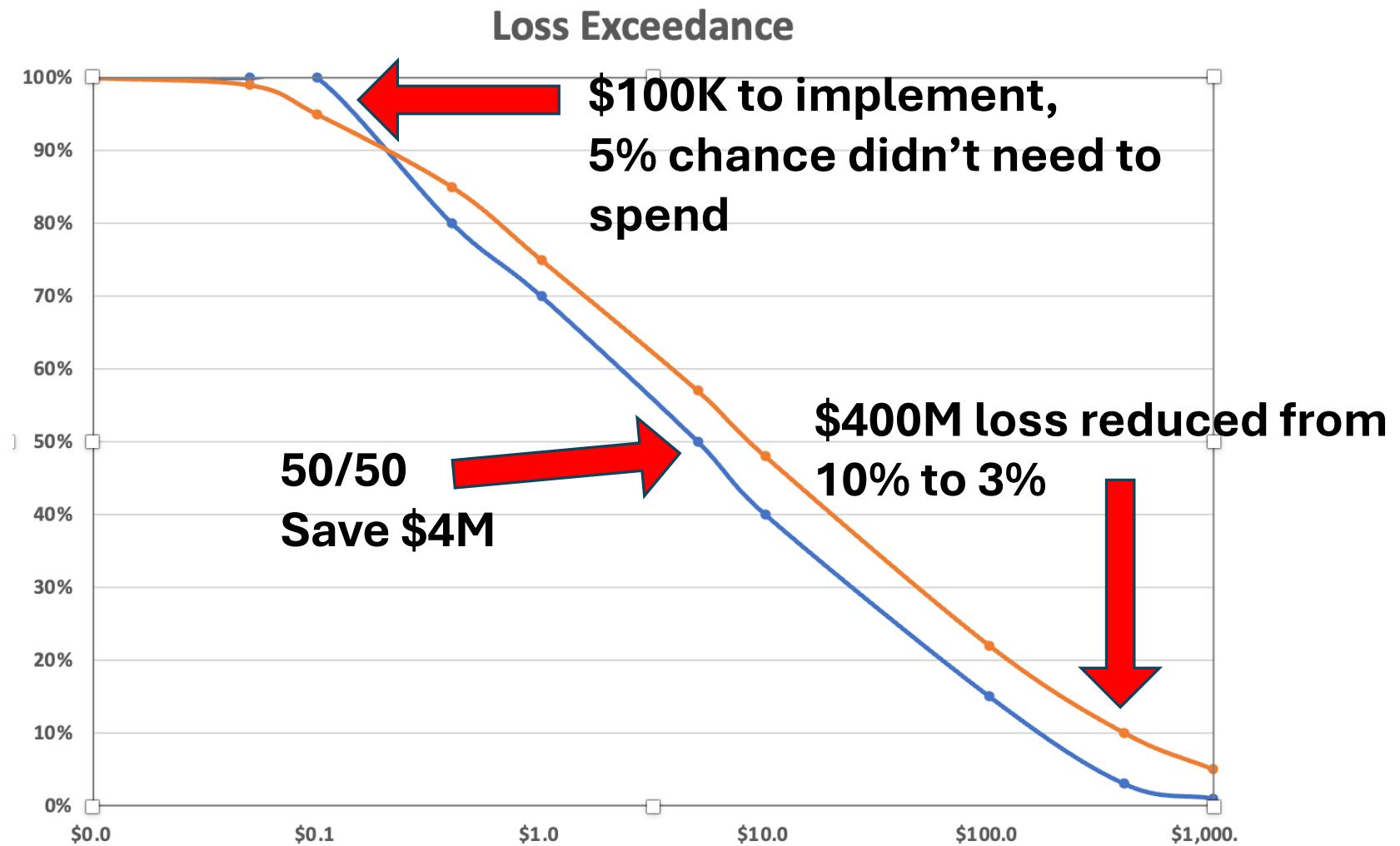
**"there are plenty of fields with massive risk,
minimal data, and profoundly chaotic actors
that are regularly modeled
using traditional mathematical methods"**

Hubbard & Seiersen

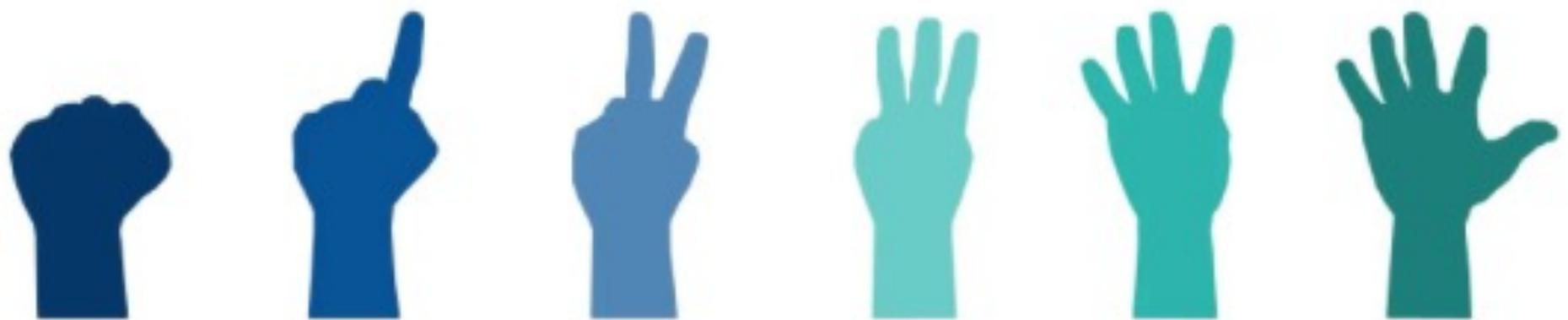
How to Measure Anything in Cybersecurity Risk

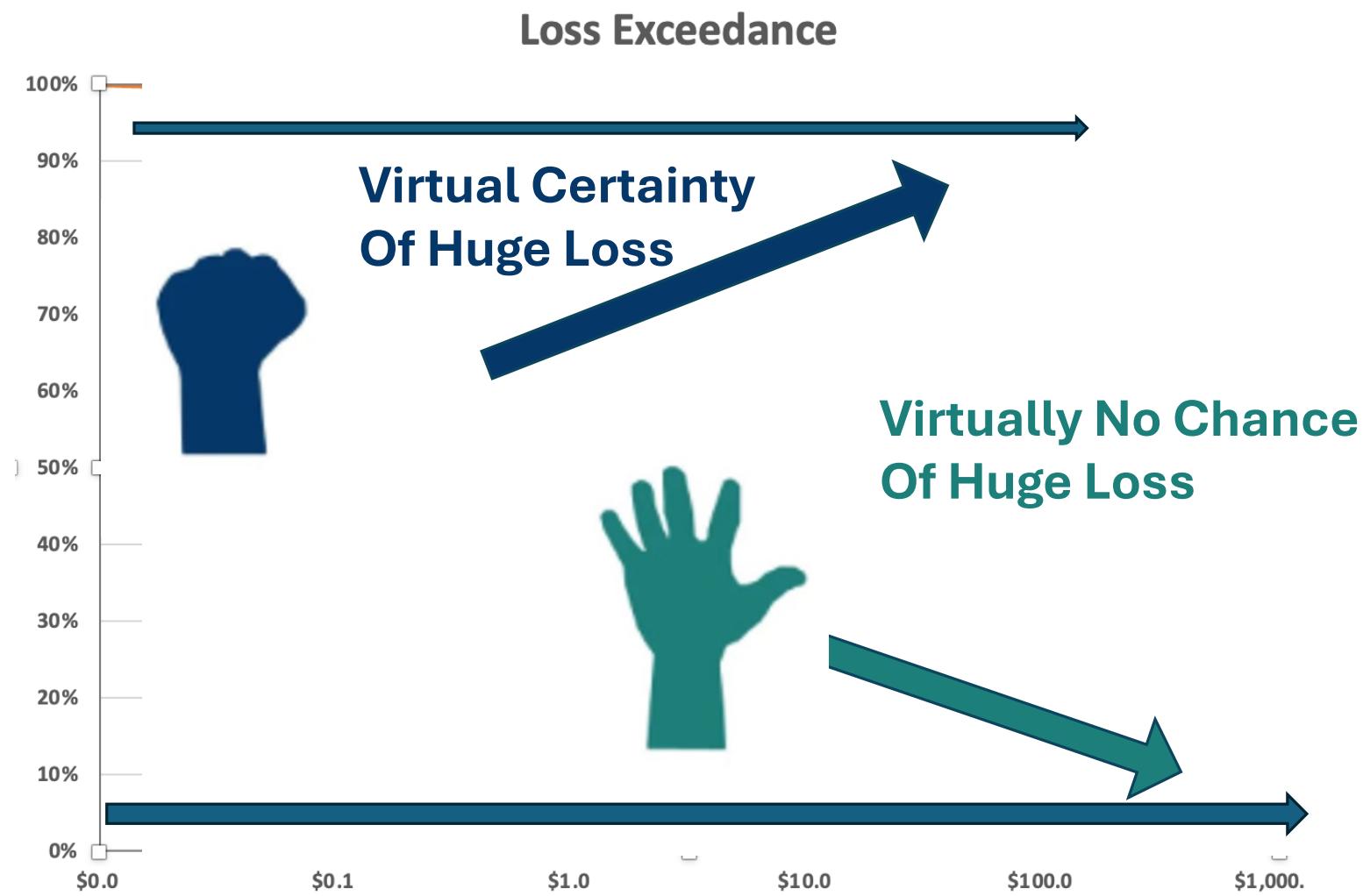
Loss Exceedance



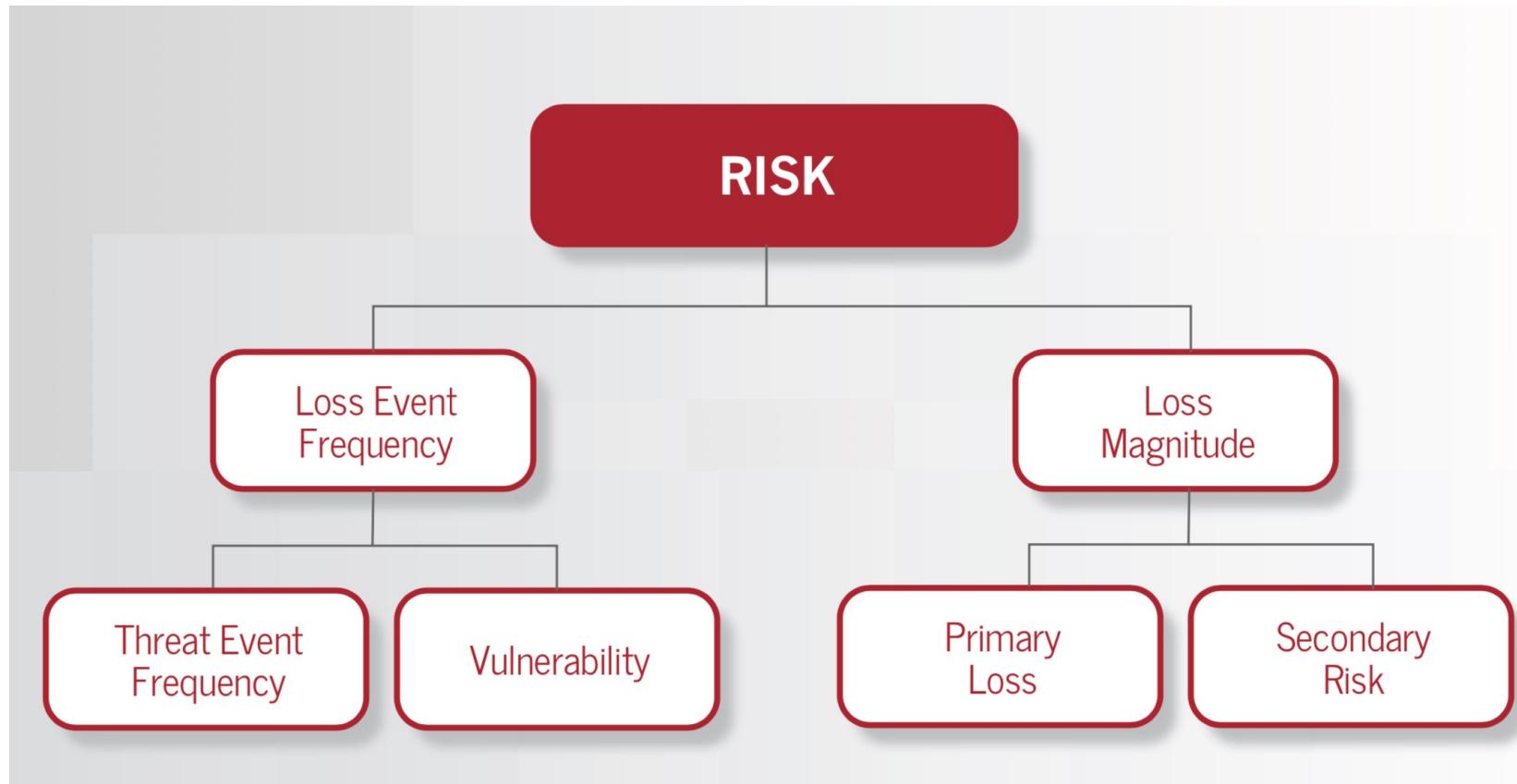


✊ Fist to Five ✌





Factor analysis of information risk (FAIR)



Time



Talent



Treasure





Demonstrated/Observed Gains So Far

10,000x increase in capacity

100-400x volume-to-mitigation c

Kicked out attackers

2 orders of magnitude faster
Hours instead of Weeks

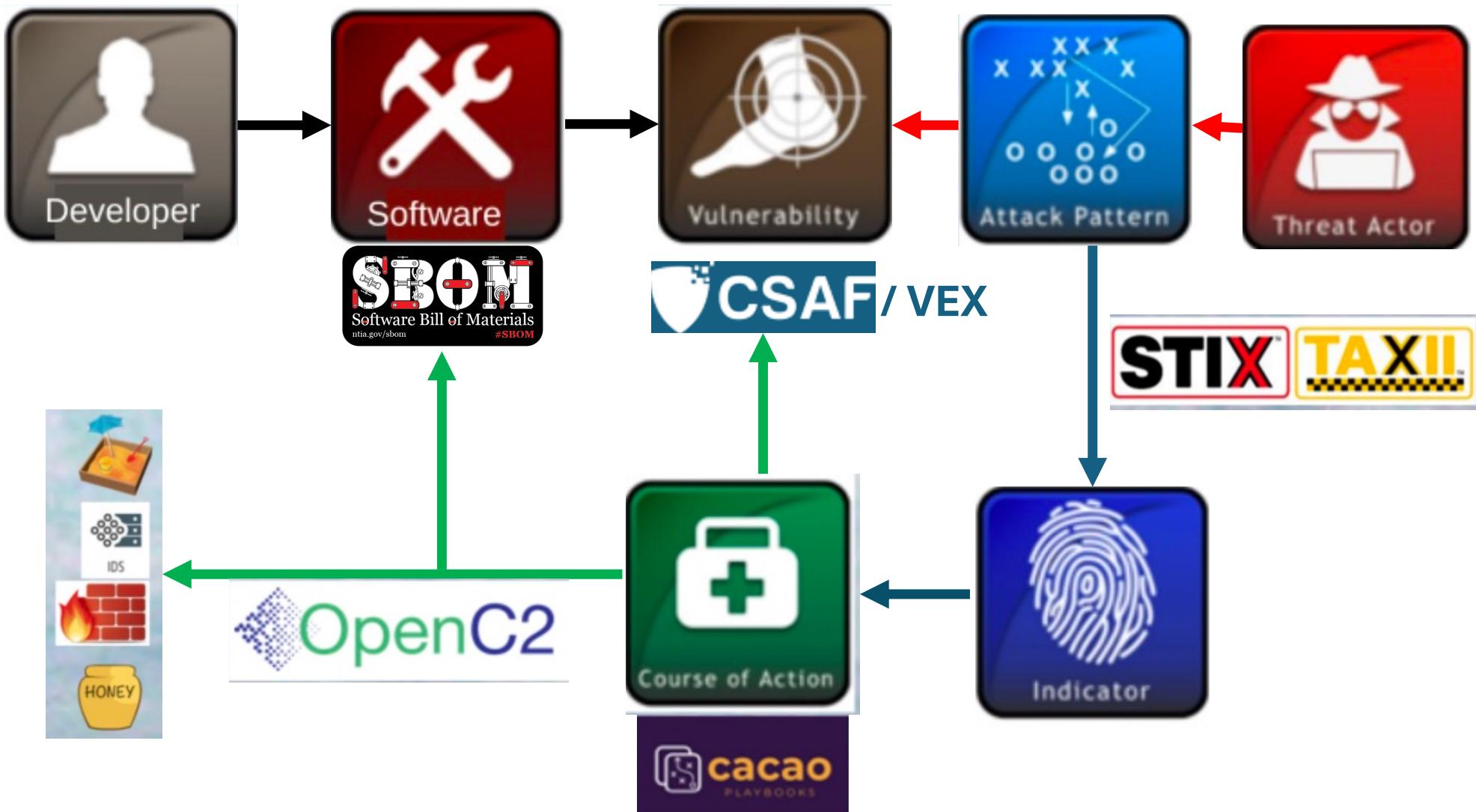
Reduced ops timeline on fully automated flows by over 99%

Timeline



Increasingly interoperable solutions
• 10-20-fold increase in orchestration

Version 1.0 of OpenC2 initial specification
Ability of both Government- and Commercially-source threat sources





United States of America



Russian Federation



Islamic Republic of Iran





Xkcd.org



Talent



- 25% - 30% efficiency increase for SOC Analysts by using standard command & control just from using vendor-agnostic playbooks
- £113k saving/yr

Treasure





Talent



- A customer reported automated handling of phishing improved fifty fold

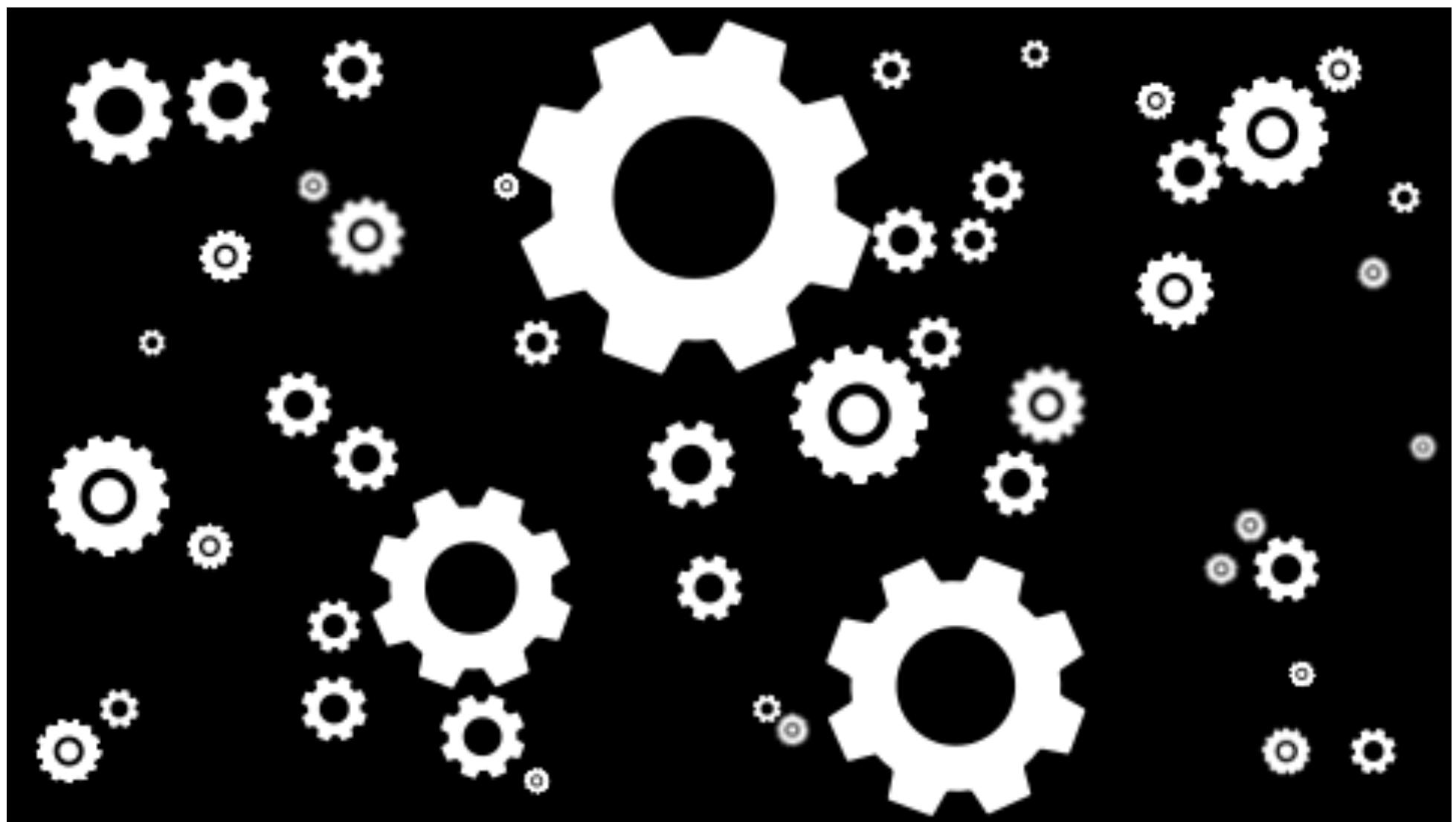
Treasure



- 98% savings in processing phishing emails - \$1.06M/yr



11-12 Sept 2024 Denver



Open Source Updates Have 75% Chance of Breaking Apps

- 95% of open source version upgrades contain at least one breaking change
- 75% of patches contain at least one breaking change
- 24% of security patches require a major version update
- 69% of security advisories are published AFTER the security release with a median delay of 25 days

<https://www.infosecurity-magazine.com/news/open-source-updates-75-breaking/>

RICHARD A. CLARK , 9/11 , & ACCOUNTABILITY



“...that’s a larger policy issue, which is, if we’re going to rely on these companies, shouldn’t they have to have some standards that they live up to? Or, be liable. They’re not liable. You can’t sue them. They make sure of that. **So, if you are a critical software that the world depends on, you need to have some regulation of your quality.**”

<https://www.cnn.com/videos/tech/2024/07/20/smr-clarke-on-summer-2024-blackout.cnn>



- Case Study

- Automation reduces assessment time by at least 90%
- 99% of **automated assessments agreed** with human assessments
- 83% **increased assessment accuracy** in one sub-system
- Potential three orders of magnitude labor **cost reduction saving \$6,000,000**

Time



Talent

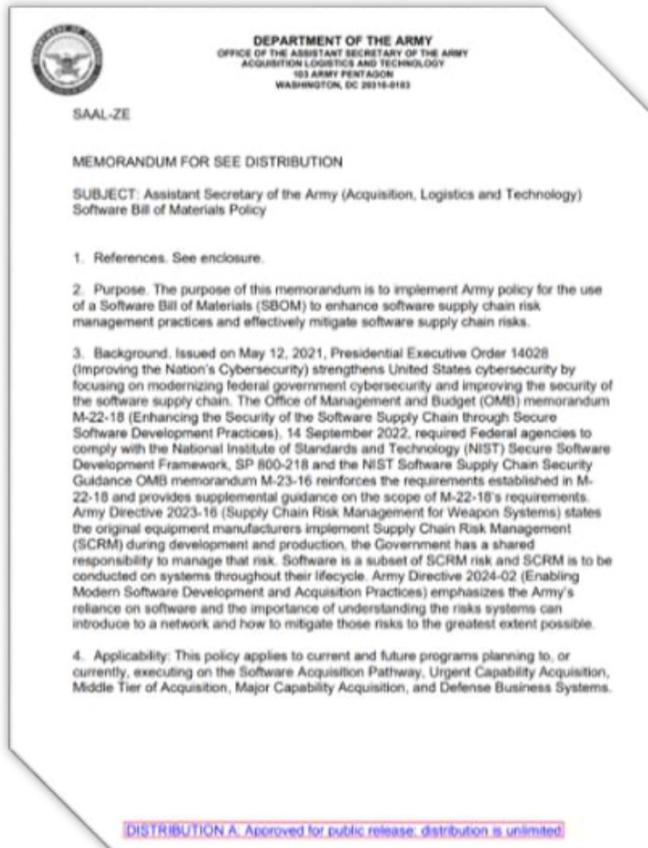


Treasure



Army

Securing the Software Supply Chain



New Contract Actions

- Incorporate contract language requiring vendors to generate and deliver SBOMs for covered computer software and COTS where commercially available

SBOM License Rights

- In solicitations, identify and negotiate for the associated SBOM data rights

Collect and Store

- Collect SBOMs for covered software and for COTS where commercially available
- Securely store and manage SBOMs
- Use and monitor SBOMs for vulnerability, incident, and supply chain risk management

Shift Left AND Shift Right



- Shift Left – create SBOMs
 - Developers in procurement, in choosing open-source libraries, during build
- Shift Right – manage SBOMs
 - After production, PSIRTS, customer vulnerability management





- One ICS customer saw a 76% efficiency improvement and saved 500 hours per open source project
- One customer reduced their vulnerability review timeframe from one day to under one hour

Time



Talent



Treasure





- One customer stated a 10% increase in developer efficiency since automating SBOM management
- Several other customers reported developer efficiency increased ~30%
- Some customers reported 50% cost reduction in tooling
 - Reducing appsec tools from 5-7 down to 1-2

Anonymous

- Just as Log4Shell happened, I was moving positions from one org-unit to a different one. Both did the same kind of SW development (mid-sized; ~40 product/projects).
- Org1 – had SBOMS - It took us all of 7 MINUTES to figure out which products to contact and have fixes online within the day.
- Org 2 - did not have SBOMs. It took a taskforce of ~5 People more than a week of communications with all of the products to figure out

Time



Talent



Treasure





- **80% reduction in time for PSIRT to Identify Vulnerable Component**
- **One of world's largest software suppliers reported value of SBOM when Log4j hit:**
 - full-response to thousands of customers
 - on thousands of products
 - within 2 hours
 - because they had SBOMs
 - vs most companies took weeks, and some took months, because they did not have SBOMs

Time



Talent



Treasure



Life Is On



- 80% reduction in staff hours for PSIRT Vulnerability Management

Time



Talent



Treasure



Time



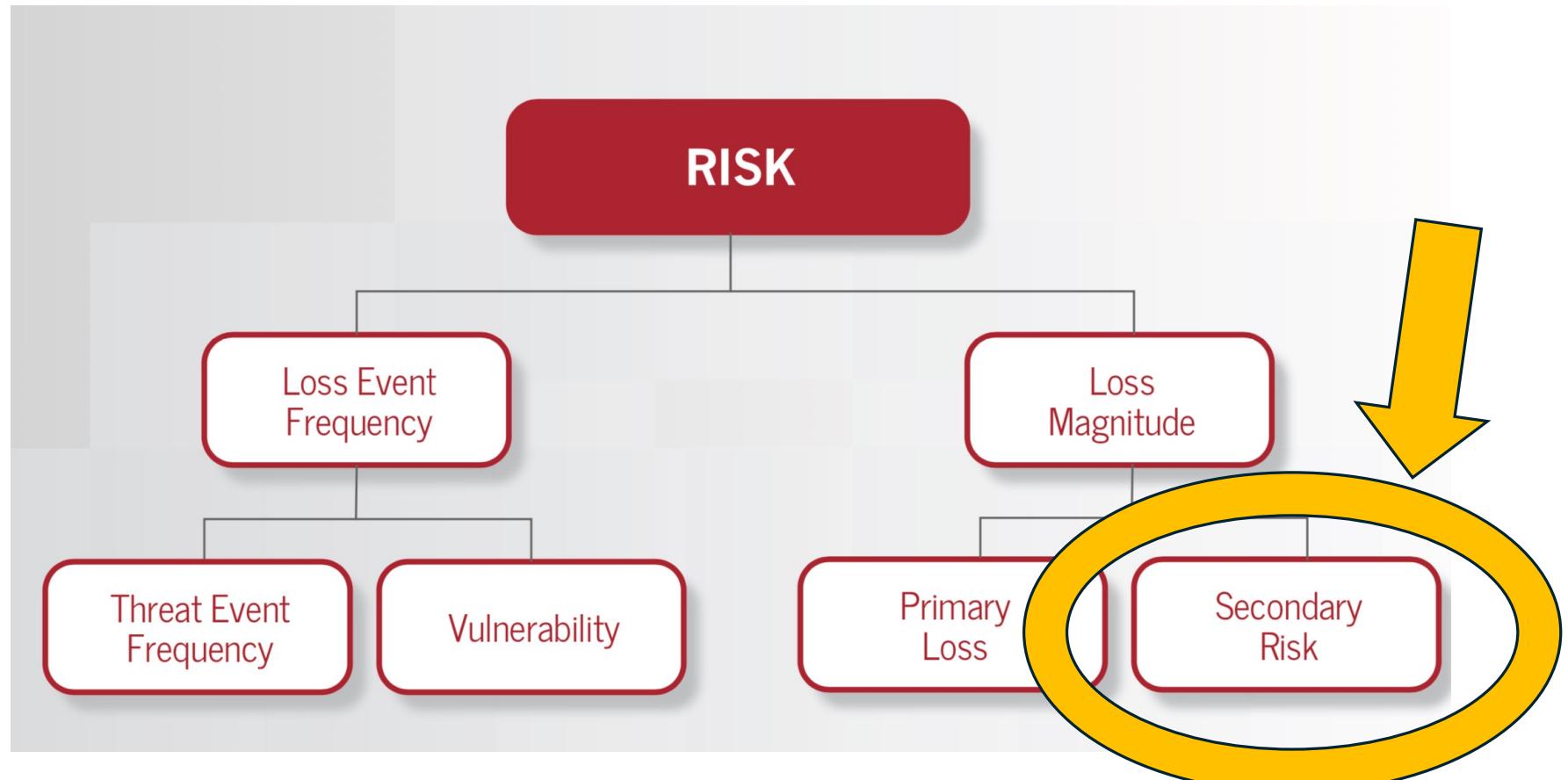
Talent



Treasure



Factor analysis of information risk (FAIR)



Duty of Care Risk Analysis (DoCRA)



What are the questions a judge would ask?





**Cybersecurity
Automation
SubProject**



 **Cybersecurity**

Automation Village



2020-Jan-27	CyberCommand	Columbia, MD	Denver Airport
2021- Jun-22	Borderless Cyber	Virtual	Comply-to-Connect
2021- Oct-28	Tech Transfer Days	New York, NY	SBOM Comply-to-Connect
2022-May-22	AT&T	Washington, DC	SBOM creation
2023-Jun-13	USC / SBOMarama	Los Angeles, CA	SBOM handling
2024-Apr-11,12	Peraton	Reston, VA	Olympic Destroyer



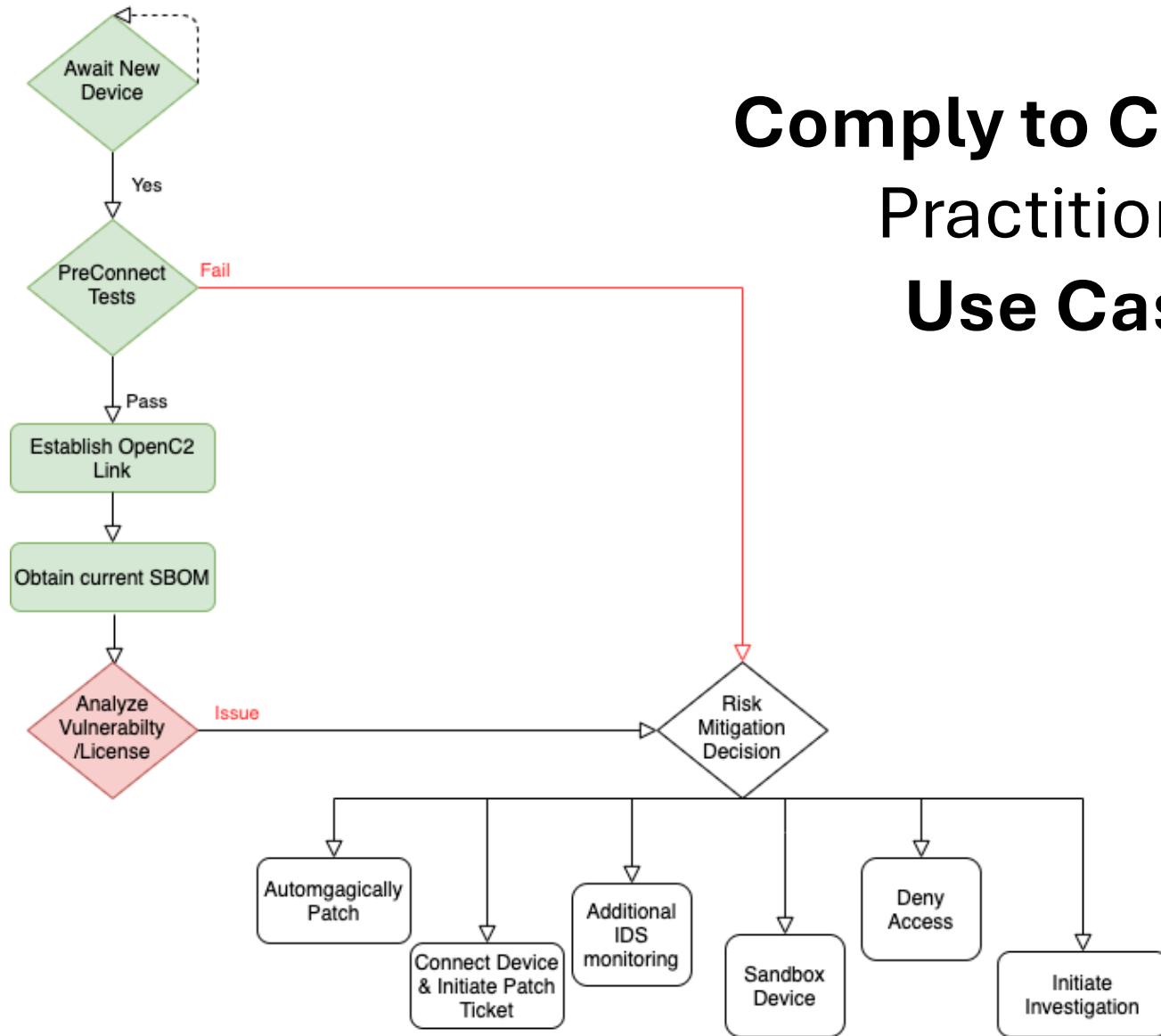
Jan 29-30 2025 AT&T Washington, DC Action!



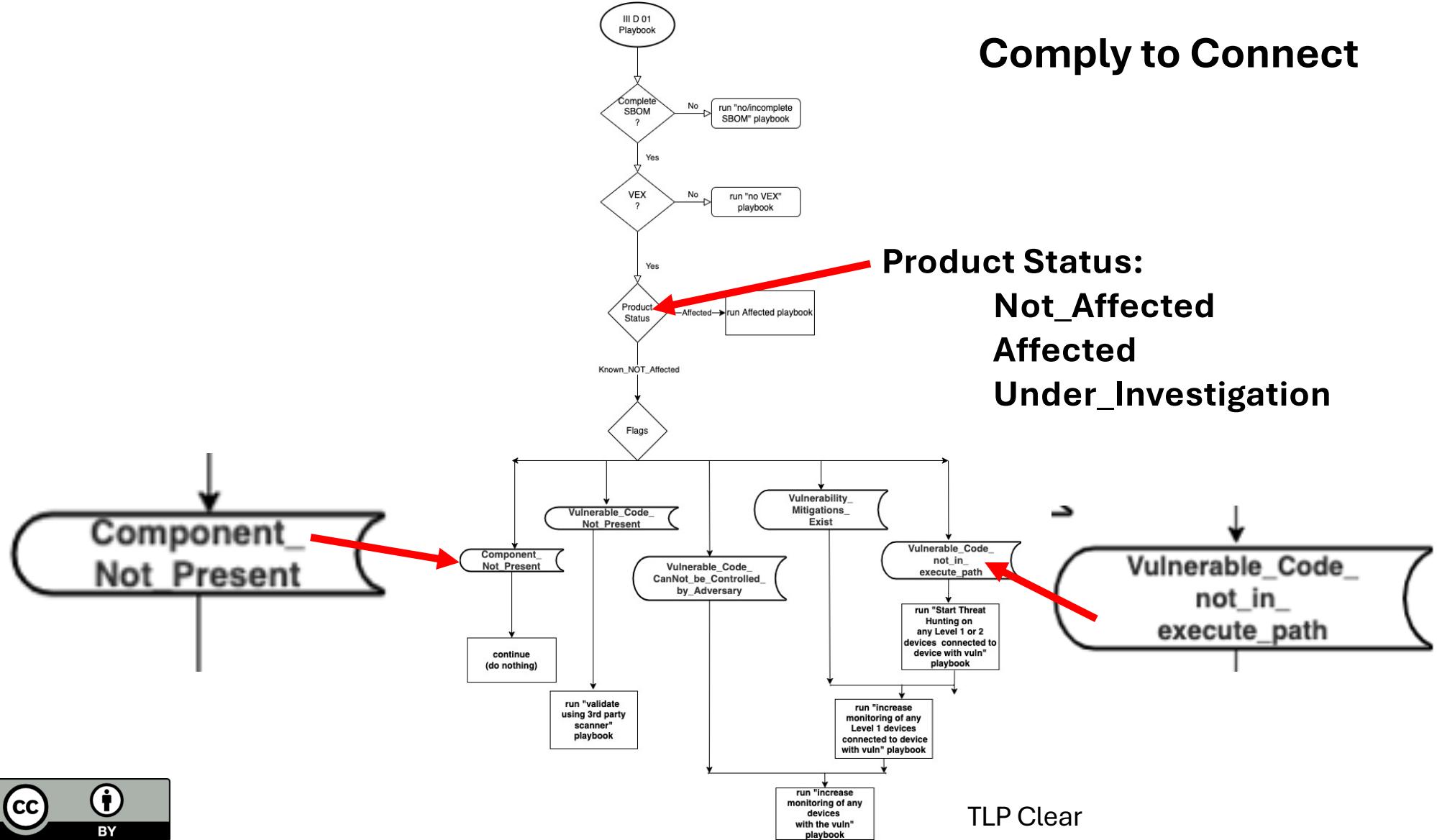
Comply to Connect

Practitioner

Use Case



Comply to Connect



The WhitchyWashy Ransomware Value Proposition

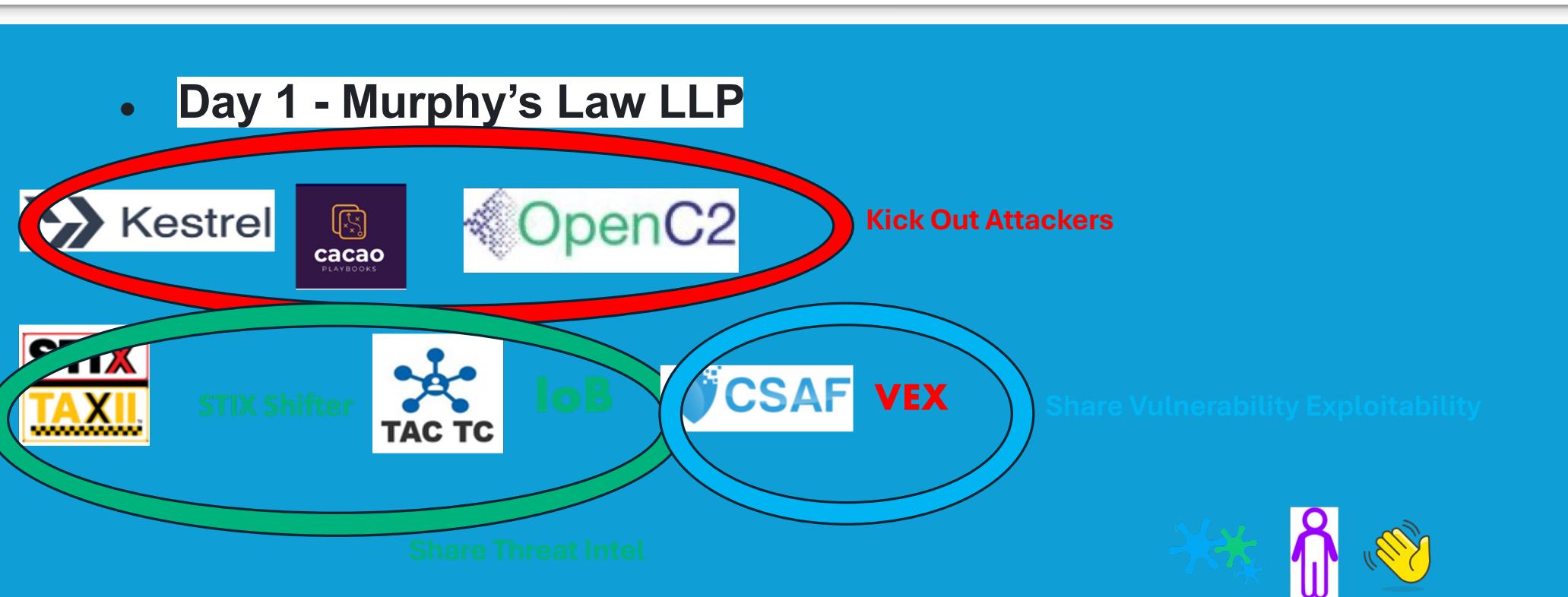
- Day 1 - Murphy's Law LLP
- Day 2 - On Deck Holdings
- Day 3 - Triumvirate CleanUp Inc
- Day 4 - NSAANSA
- Day 5 - Law Enforcement
- Day 6 - MilOps

Objective: As many projects on as many days as possible
- Machine API's, Humans, Handwaving



The WhitchyWashy Ransomware Use Case

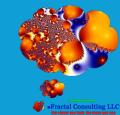
- Day 1 - Murphy's Law LLP



Plugfest

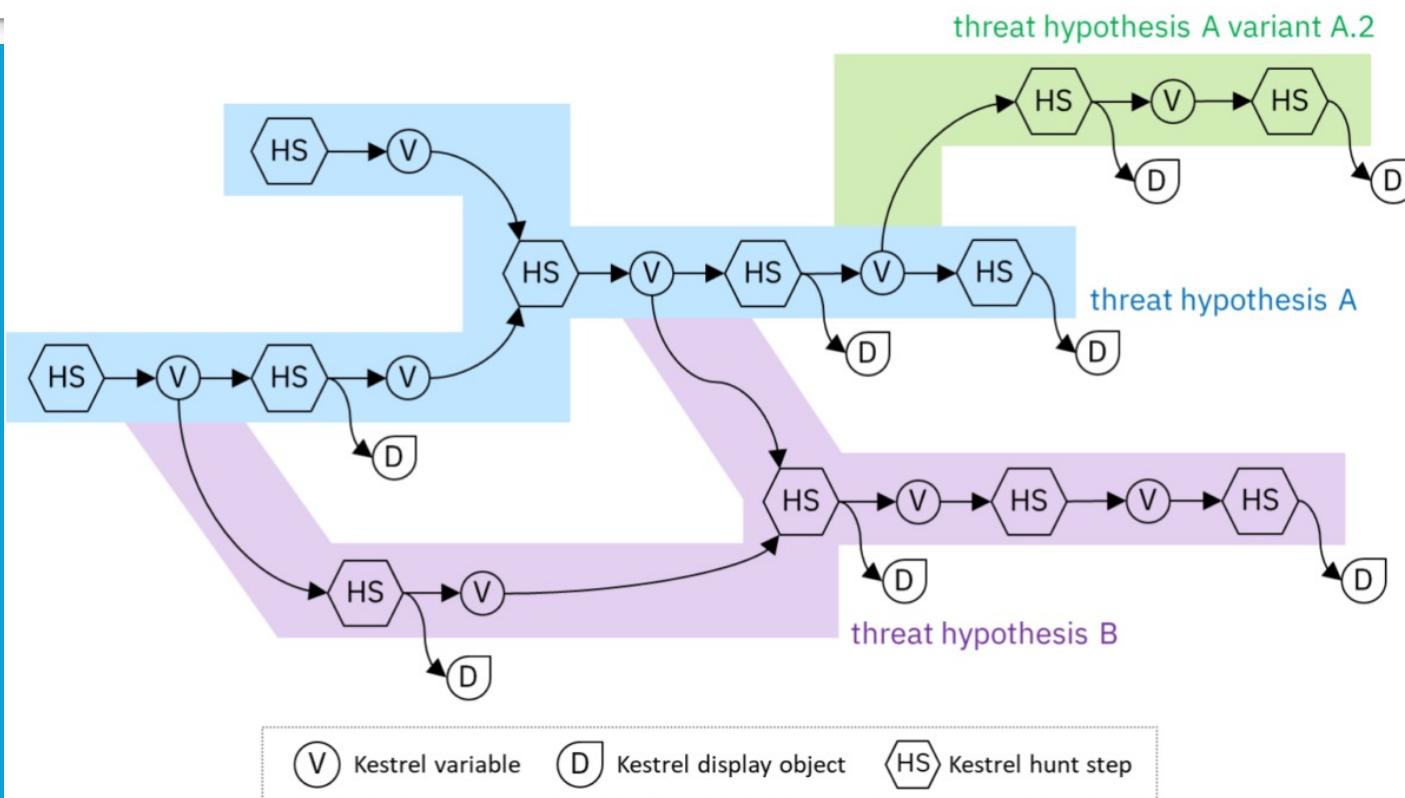


Machine to Machine



Kestrel

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



The WhitchyWashy Ransomware Use Case

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



STIX Shifter



IoB



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

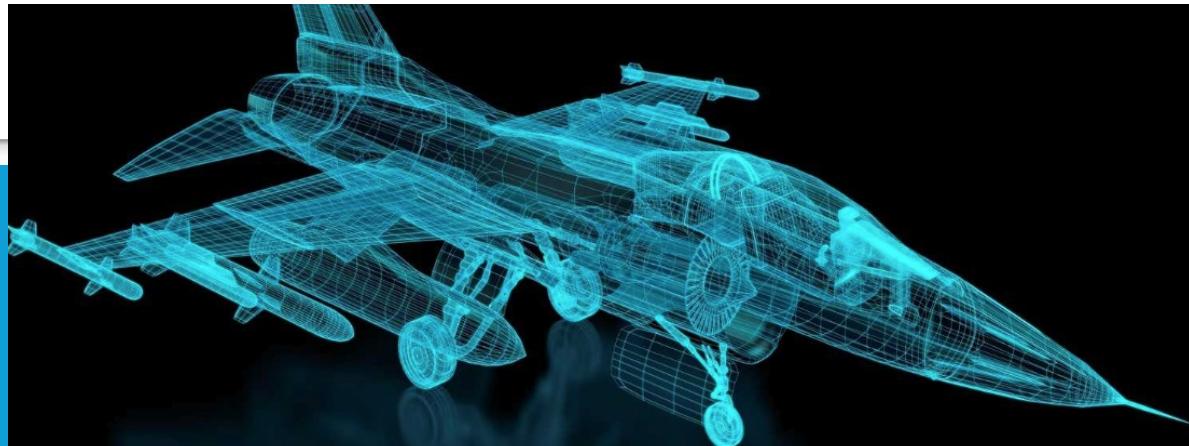
- Day 1 - Murphy's Law LLP, Day 2 - On Deck Holdings, Day 3 - Triumvirate CleanUp Inc
- Day 4 – NSAANSA



Day 5 - Law Enforcement



Day 6 - MilOps



Olympic Destroyer



Olympic Destroyer



IoB



QuadBlockQuiz

312

Score

Speed: fast

20 QuadBlocks

0 Rows

0 Answers

Tech Debt: 155



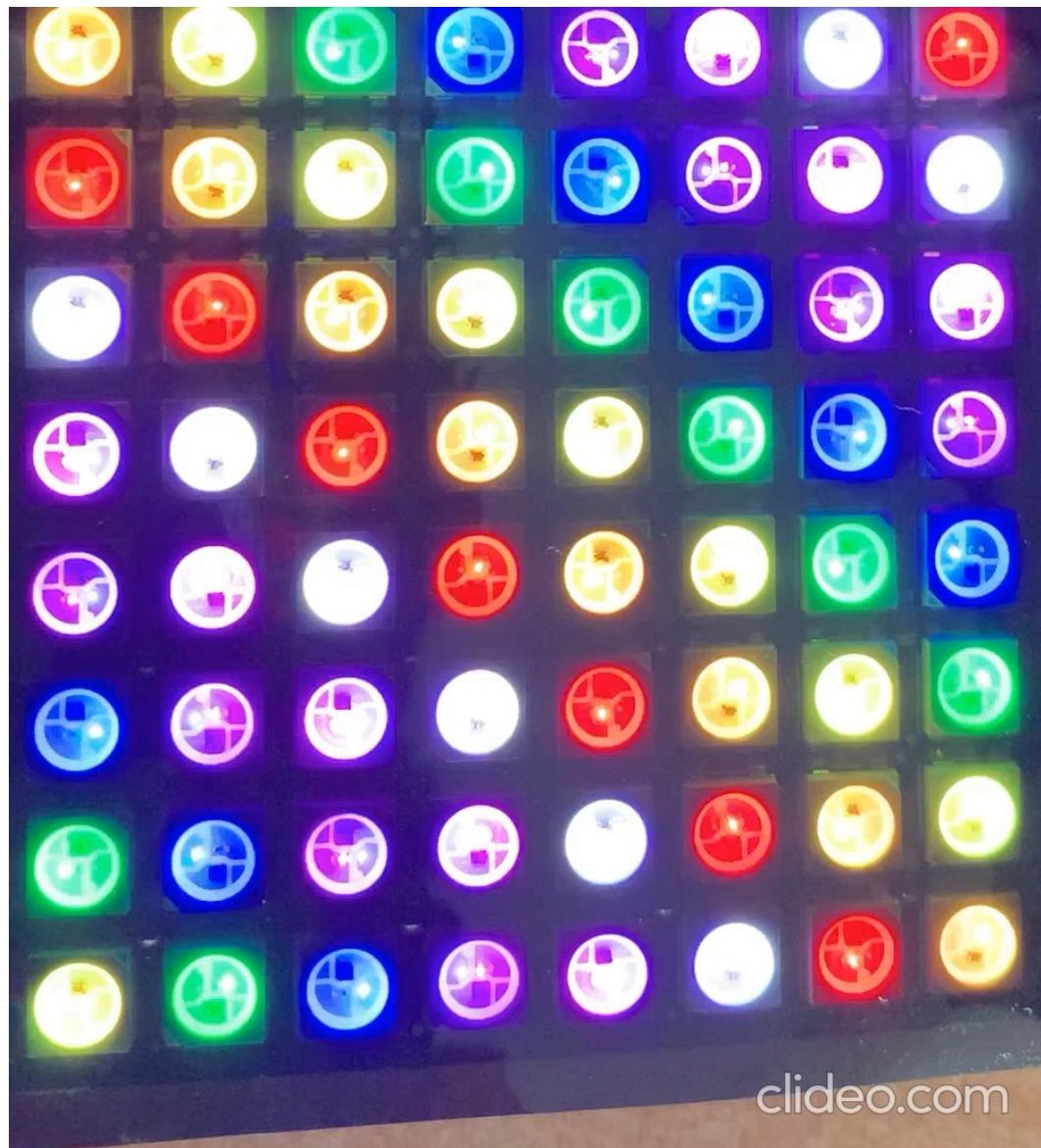
Click "How to

Don't let you
reaches the
bankrupt.

Over time, yo
some point, t
issues crop u

Vulnerabilitie
issues are bi
from being c

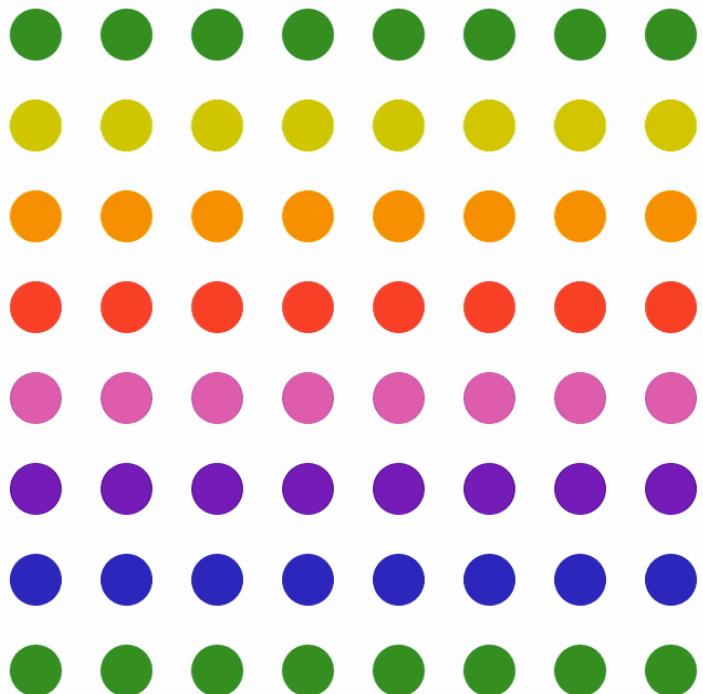




clideo.com



▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪ ▪



Rainbow



MADE WITH GIFOX

TURN LED OFF

Takeaways



**Cybersecurity standards
enable automation
saving
time, people, and money**

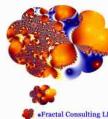




THINK EVILLY



Act Ethically



THE WHITE HOUSE

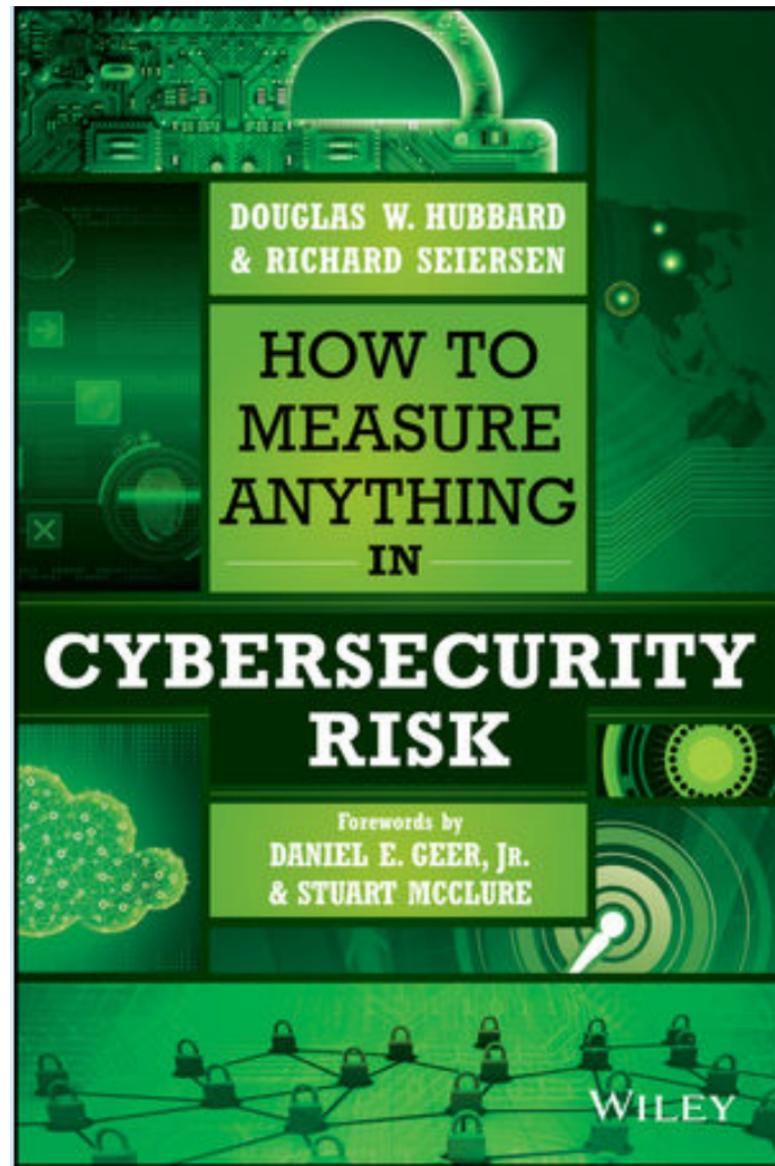


**"In the end,
the trust we place in our digital infrastructure
should be proportional
to how trustworthy and transparent that infrastructure is,
and to the consequences we will incur
if that trust is misplaced."**





**SHOW
ME THE
MONEY!**





GIVE ME A SIGN



I don't
understand



I kind of
understand



I get it!

There is never enough time.



Thank you for yours.

Q & A