From Threat Intelligence to Playbooks
The Evolution of the SOC

Bret Jordan, CISSP

Director, Office of the CTO
Symantec

Problem #1

Networks are starting to lose the war globally

Problem #2

Threat actors are advancing at a non-linear rate relative to cyber defense

Problem #3

How do you prevent, mitigate, and remediate in real-time?

Why is current cyber defense failing?

- Content and systems are moving outside the perimeter
- Network security has been traditionally inward focused
  - Find all vulnerabilities
  - Fix all vulnerabilities
  - Et voila we are magically “secure”
- This is based on a fallacy that we can know and/or fix all vulnerabilities
- Inward focus (hygiene) is necessary but inadequate

Why is current cyber defense failing? (cont.)

- Not all SOCs are created and staffed equally
- Security operations, procedures, and policies are:
  - Slow
    - Root cause analysis remains difficult
    - Detection is measured in terms of months or years
  - Manual
    - Organizations still perform a lot of manual investigations
    - Post infection analysis is manual and very hard to do
  - Reactive
  - Understaffed and underfunded
- One organization's defense stays their defense

What can we do about it?

- We need to respond more quickly
- We need to enable herd immunity for cyber defense
  - Learn what others have figured out and resolved
  - New attacks need to be shared quickly within the trust group
  - As networks become inoculated, the risk of wide-spread outbreak goes down
- We need a holistic approach to cyber defense

Holistic approach to cyber defense

- Understand ourselves
  - What are our assets?
  - What is our attack surface?
  - Where are we vulnerable?
- Understand the adversary
  - Who is the adversary?
  - Where and how are they acting?
  - What are they targeting?
  - What actions should we take?

Need for information sharing

- Holistic threat intelligence is not a single player sport
- Requires a wide-range of information
  - No single entity, **no matter how large**, has the full picture
  - Sharing is not completely new but is typically focused on very atomic, limited-sophistication indicators (IP lists, file hashes, URLS, email addresses, etc.)
  - Most sharing is unstructured and human-to-human
  - There is a need to share more sophisticated behavioral and contextual information

Need to ask the question

How can my detection today aid your prevention tomorrow?

Cyber Threat Intelligence (CTI) to the rescue

- What is STIX?
  - A way to document malicious activity in JSON
- Why is STIX 2 so valuable?
  - External relationships / graph model
  - Patterning
  - Clear semantics
- What is TAXII?
  - A definition for how to use HTTPs to transport CTI

The problems STIX solves

- Who is responsible for the attack?

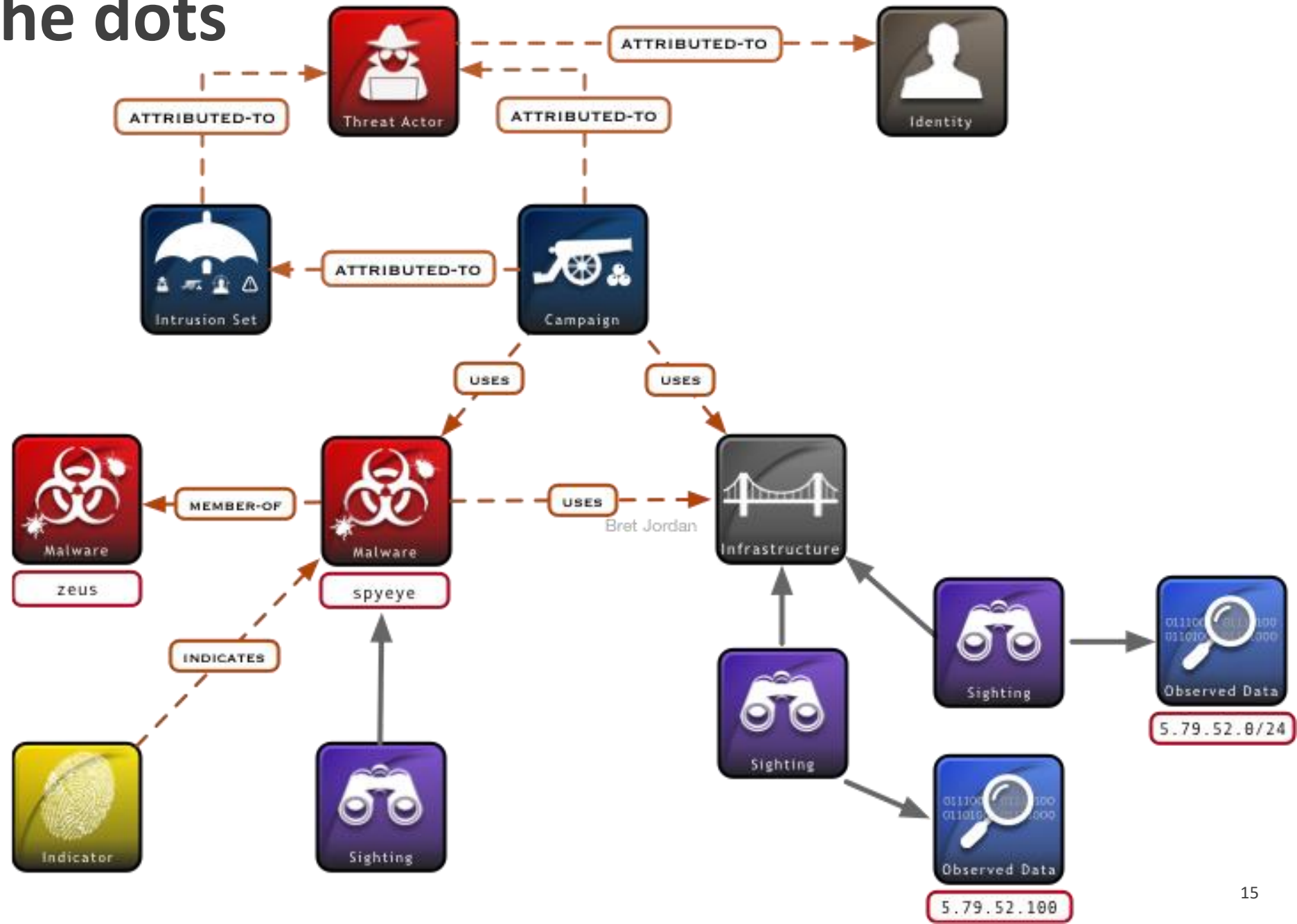
The problems STIX solves (cont.)

- How are they doing it, what is their modus operandi?

The problems STIX solves (cont.)

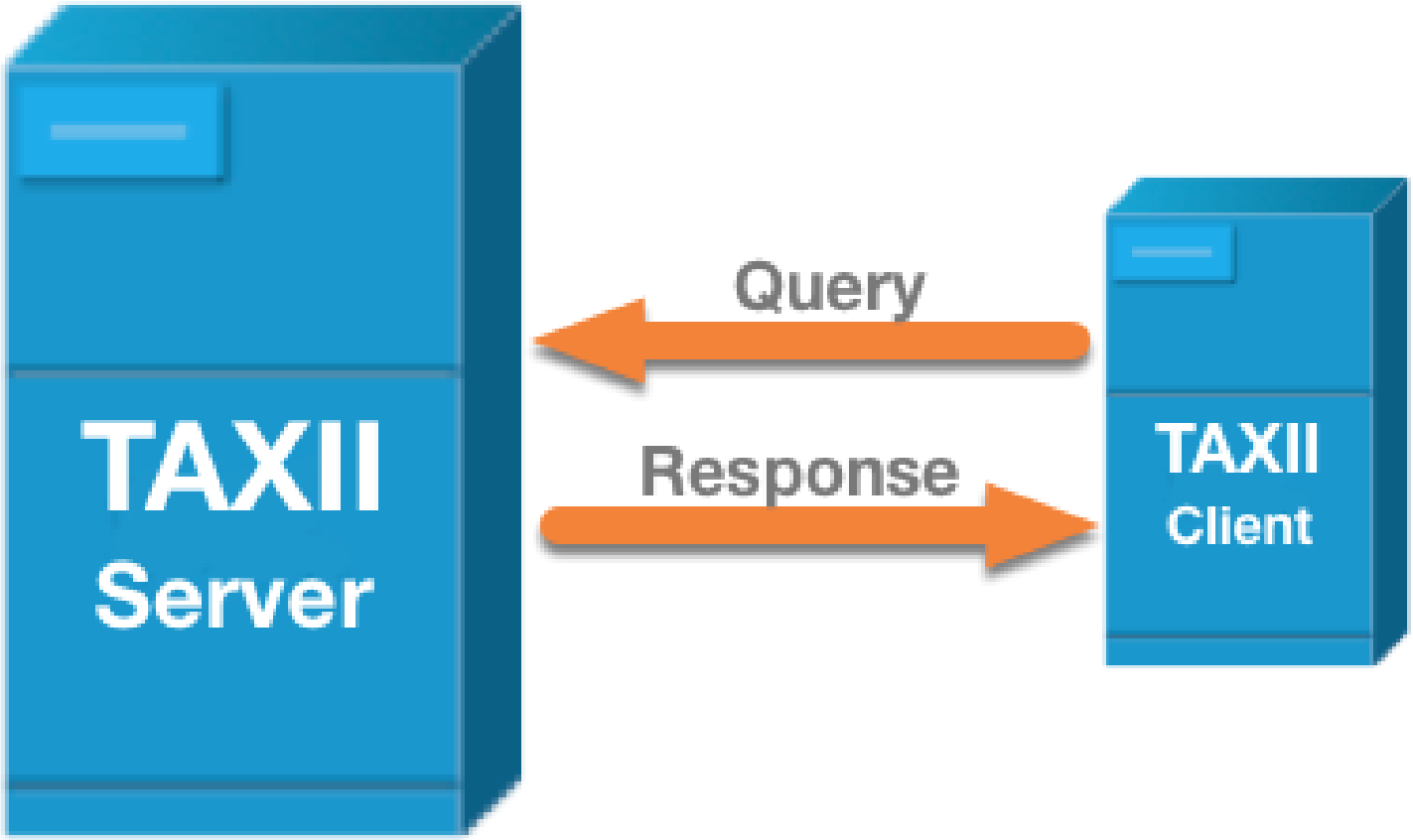
- How do you detect it and stop it?

Connecting the dots



TAXII 2.1

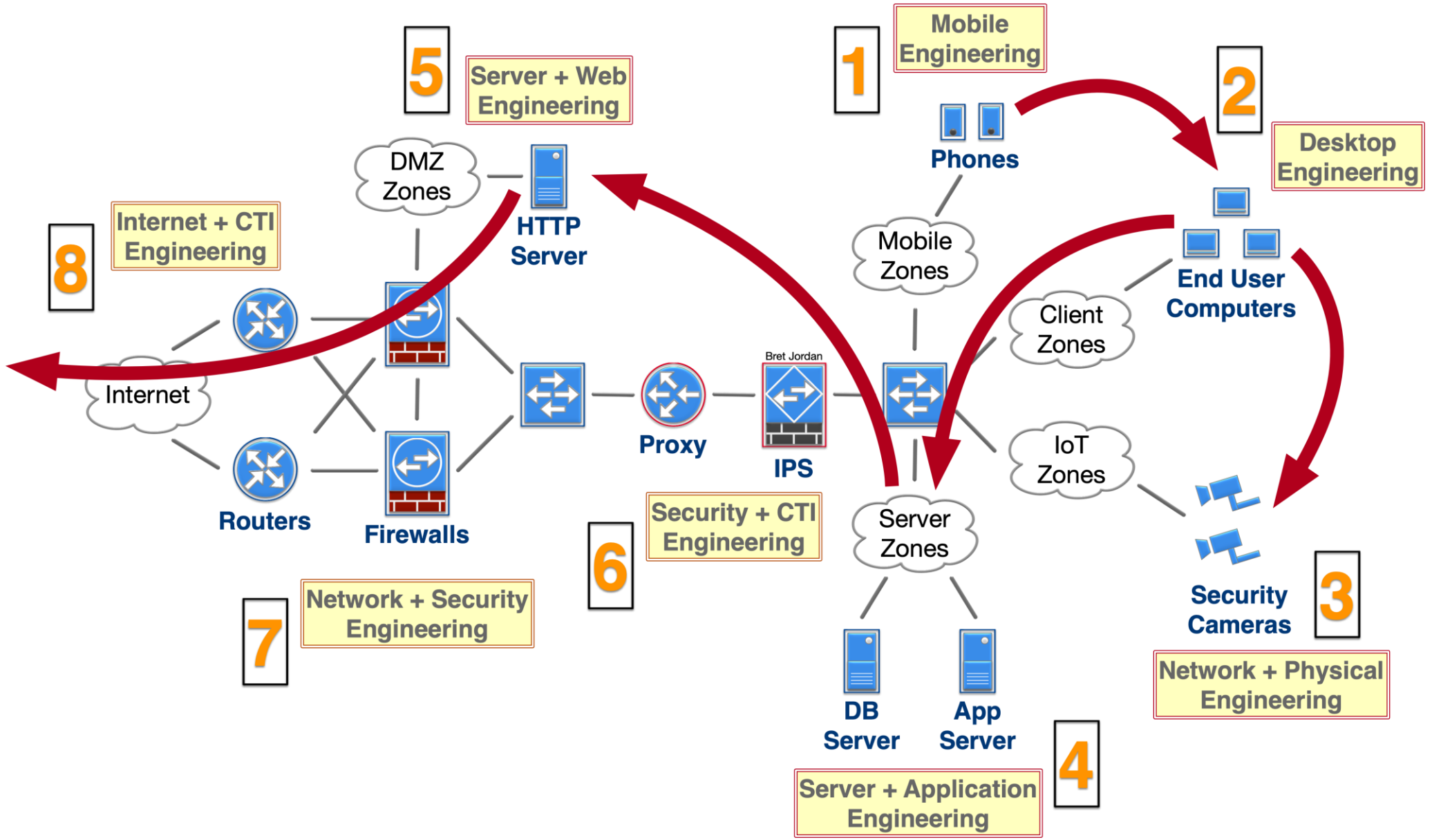
- Request / response over HTTPs



Problem - why we need playbooks

- Threats
  - Threat Actors and Intrusion Sets are advancing in speed and sophistication
  - Number of attacks are increasing and attack surface is growing
  - Time available to adequately respond and remain effective is decreasing
    - Automation and a standards-based machine-readable solution is needed
- Defense
  - Manual, slow, reactive, and siloed
  - Many disparate systems are usually involved
  - Many different groups are part of the response
  - Need to respond across multiple coordinated systems
  - No easy way to share threat response expertise

Problem & pain points – why we need playbooks



What are playbooks

- Collaborative Automated Course of Action Operations for Cyber Security
- A solution that defines structured and machine parsable playbooks
  - **Creation** of those playbooks
  - **Distribution** of those playbooks across systems
  - **Monitoring** the results of executed actions from those playbooks
- It includes documenting and describing the steps needed to **prevent**, **mitigate**, **remediate**, and **monitor** responses to a threat, an attack, or an incident
- It will build upon on existing underlying communication protocols and interfaces that enable the systems involved in CACAO

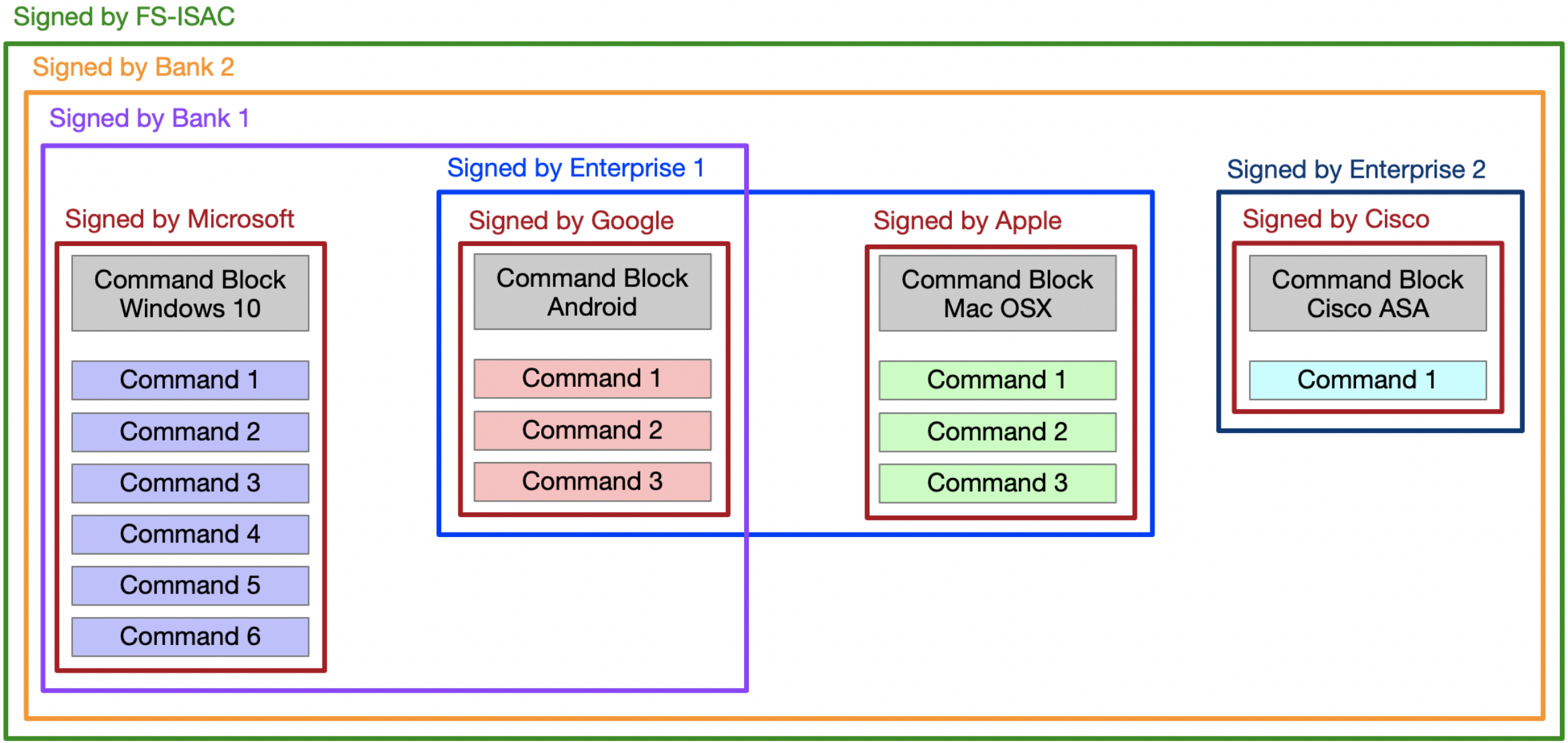
What are playbooks today?

- Documentation of security processes involving procedural, technical and human capabilities
- Defined and written procedures for operational security
- Typically kept in a binder on the shelf or in a KB article
- Used to orchestrate IT, cyber security, and physical security
  - For this work, physical security is out-of-scope
- Represented using manual and/or automated steps with conditional logic
- Used for **prevention**, **mitigation**, and **remediation**

Playbooks can span groups & technologies

- Many different groups are needed to respond to an attack
  - SOC / NOC / Network Support / Desktop Support / Mobile Support / Application Support
- Attack can span business units and enclaves
- Attack can target an entire industry sector requiring coordinated response
- Attacks can occur across multiple technologies in the same campaign and/or intrusion

Industry response example



Today

Future

Security Knowledge

Analysts / SOC

Vendors

National Certs

ISACs / ISAOs

Security Operation Center

Phase 1 Goal	Phase 1 Stretch Goal	Phase 2 Goal	Phase 3 Goal
Playbook Creation JSON Data Model Multiple Actions Temporal Logic Conditional Logic Versioning Targeting Syntax Verification	**Partial Automation** Digital Signatures Distribution Protocol	**Partial Automation + Reporting** Execution Interface Action Resource Response Resource Execution Verification Reporting Protocol	**Full automation**

Crawl Walk Jog Run

Conclusions

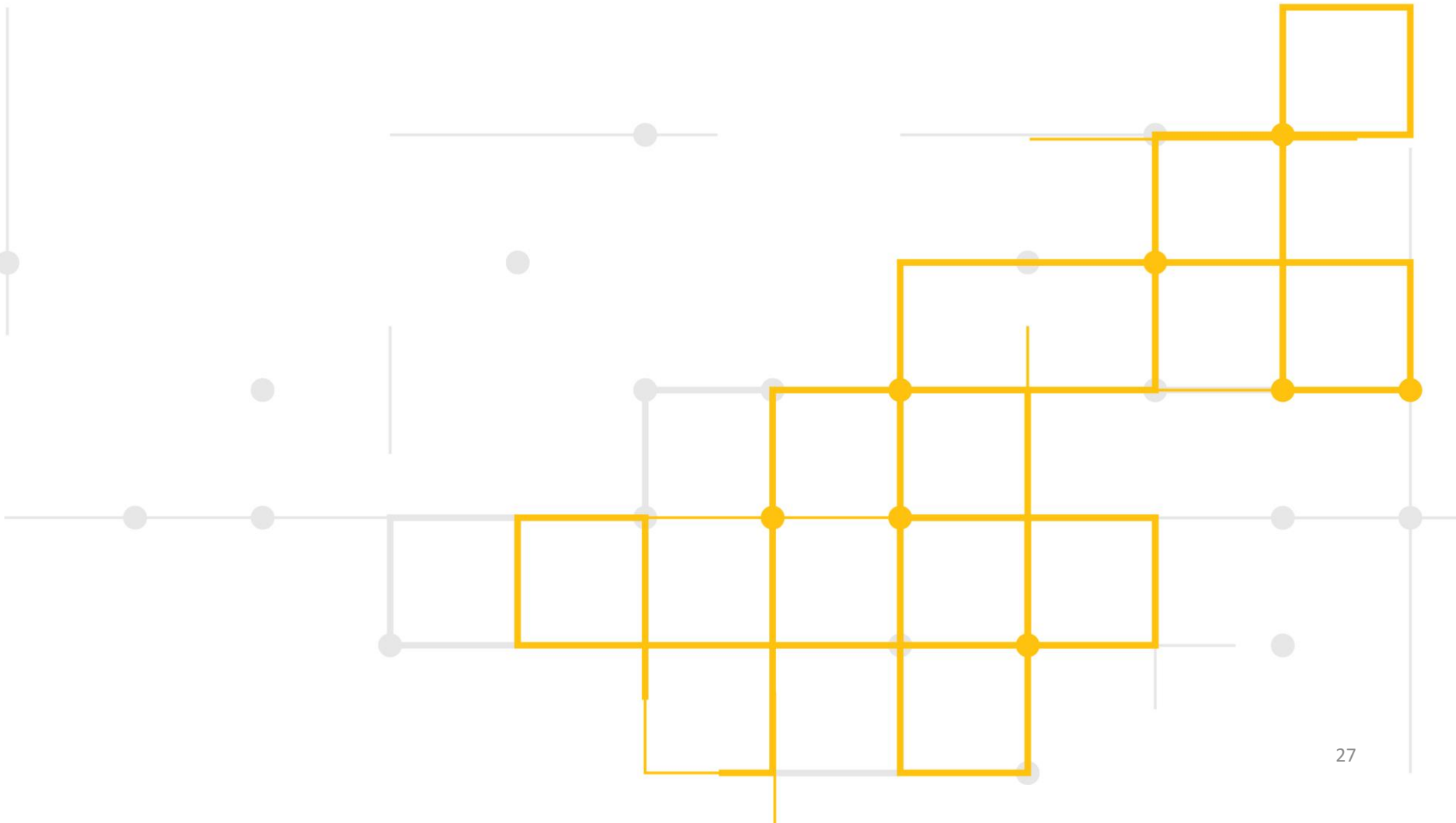
The dream

This dream of herd immunity is **only** possible when we share CTI in an automated machine-to-machine structured format

What Can and Should the ITU Do?

- Challenges for standardization
  - Coordination across SDOs
  - Understanding what is being done and where
  - Telco, Operator, and Enterprise use cases not always known
  - Individuals are spread to thin across SDOs
- ITU needs to get more involved and take a more active role
- ITU needs to standardize solutions that enable
  - Cyber defense
  - Threat intelligence and playbook sharing

Q&A



Thank you!

Bret Jordan, CISSP

bret_jordan@symantec.com