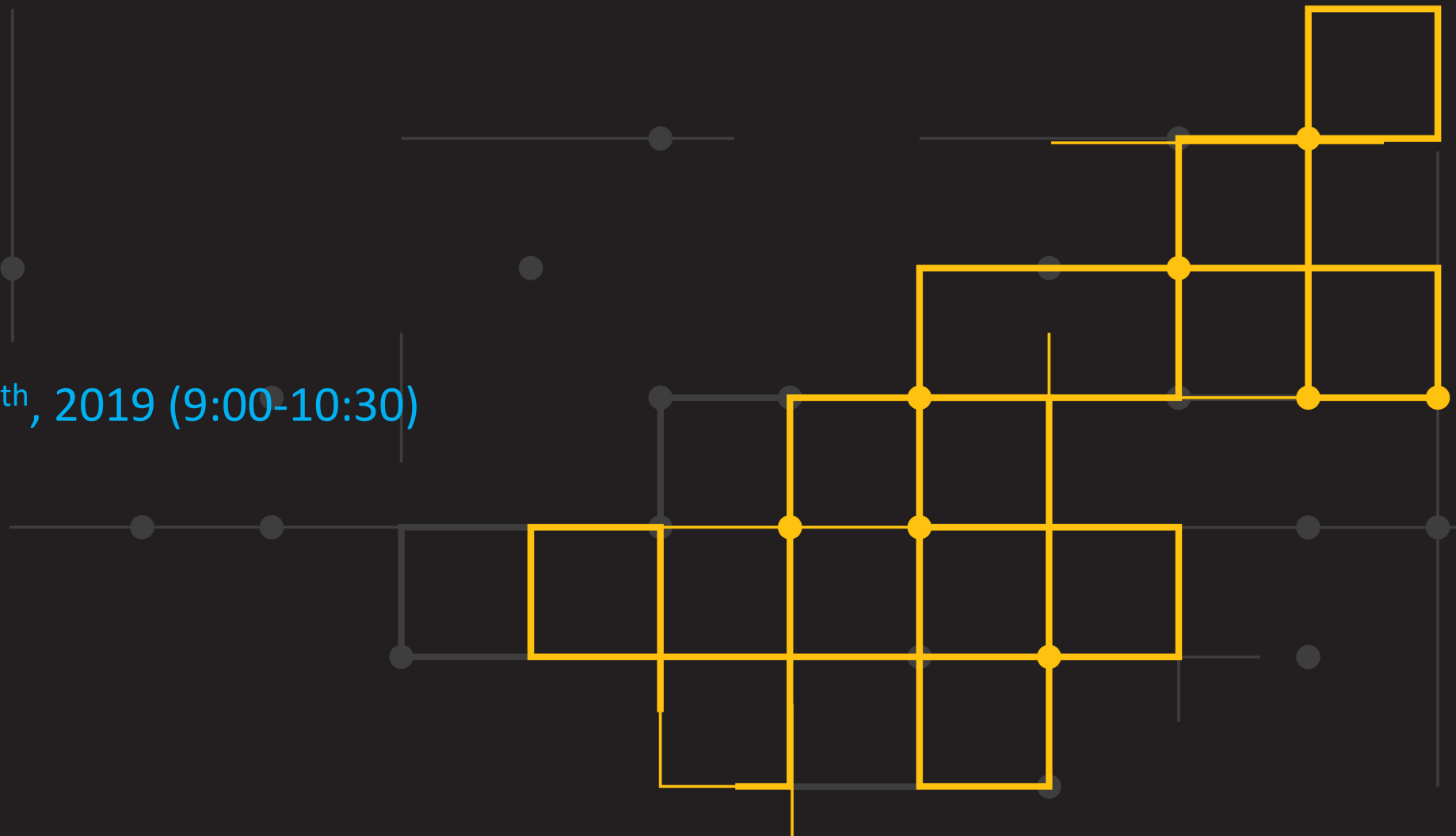
# CACAO BoF

IETF 104 Prague

Friday, March 29th, 2019 (9:00-10:30)

**Bret Jordan**
**Allan Thomson**
**Jyoti Verma**

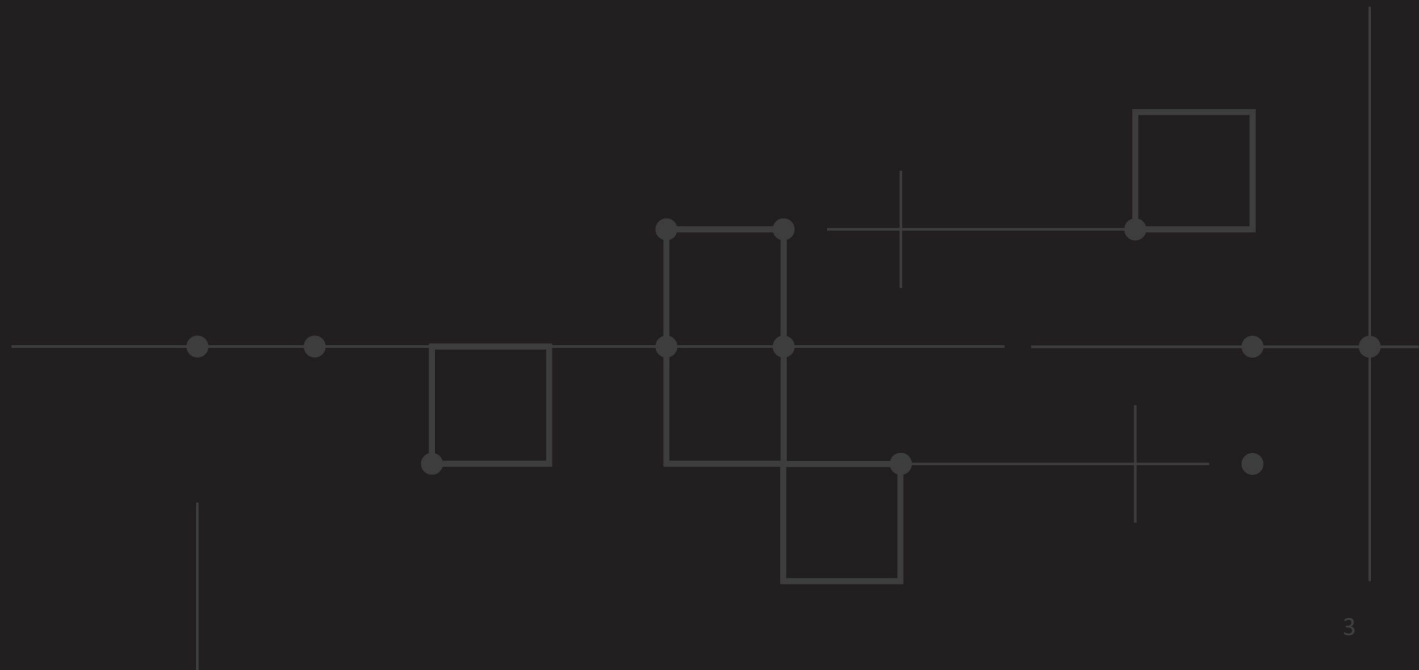


# IETF Note Well

- This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.
- As a reminder:
  - By participating in the IETF, you agree to follow IETF processes and policies.
  - If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
  - As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
  - Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
  - As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.
- Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:
  - BCP 9 (Internet Standards Process)
  - BCP 25 (Working Group processes)
  - BCP 25 (Anti-Harassment Procedures)
  - BCP 54 (Code of Conduct)
  - BCP 78 (Copyright)
  - BCP 79 (Patents, Participation)https://www.ietf.org/privacy-policy/ (Privacy Policy)

# Agenda

- Administrivia [5 min]
- Problem Statement Presentation and Discussion [45 min]
- Charter Discussion [40 mins]

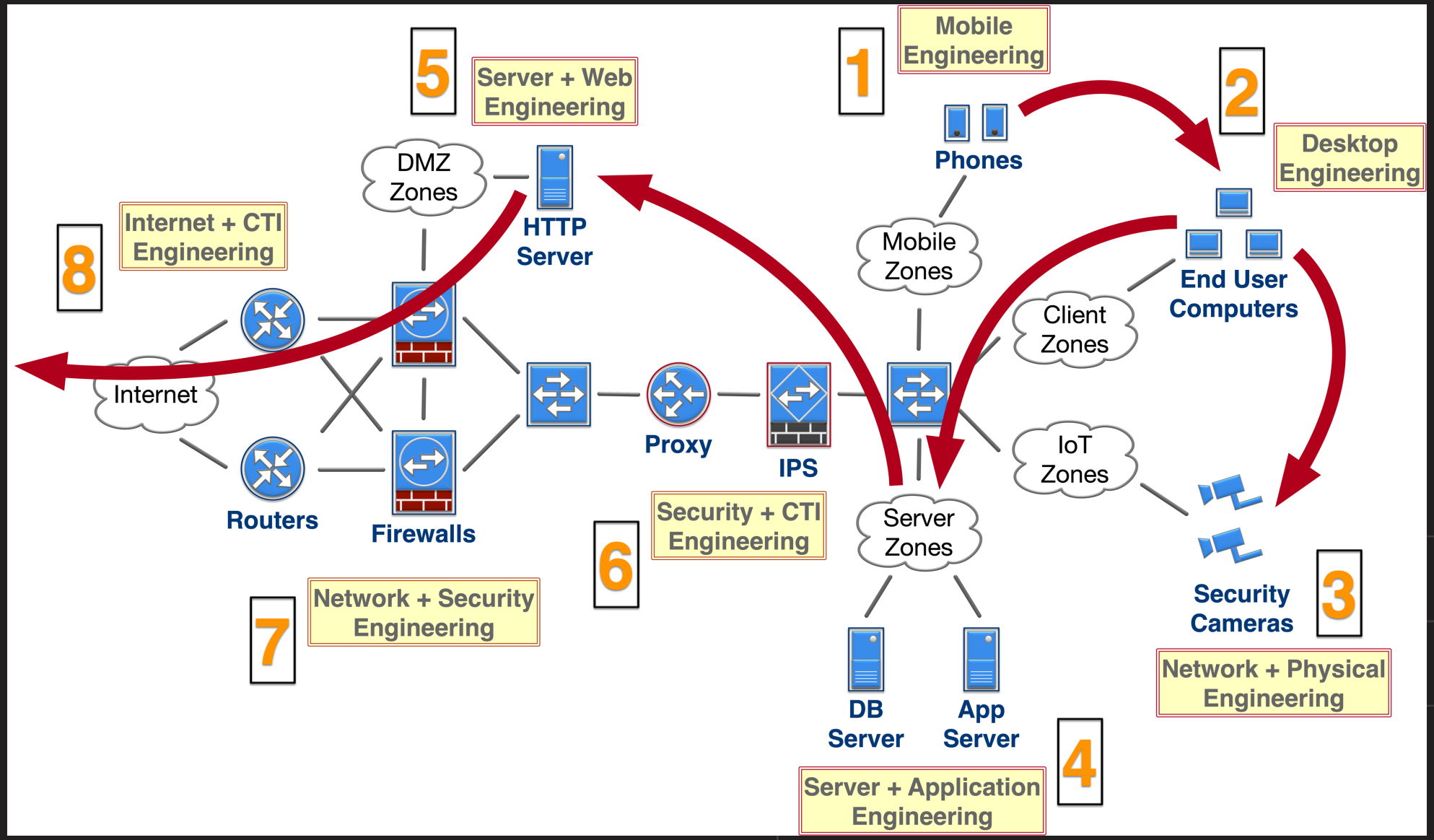


# Overview and Introduction

# Problem - Why we need CACAO

- 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 CACAO



# What is CACAO?

- 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 CACAO is NOT!

- This is not a standard for sharing arbitrary content or data
- This is not about documenting an incident, indicators of compromise, or threat actor behavior
- This is not an effort to redefine standards like I2NSF, NetConf, STIX, TAXII, OpenC2, SUIT, etc.

# 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**

# Example Playbook

## Windows Fuzzy PandaX

- **Security Operations Center**
  - Open ticket with priority level 2
  - Call level one network support
    - If they do not respond within 10 minutes
    - Escalate to level 2, then level 3, then management
- **Network Support**
  - Quarantine system to sandbox VLAN

# Example Playbook – cont.

## Windows Fuzzy PandaX

- **Security Operations Center**
  - Call level level one desktop support
    - If they do not respond within 30 minutes
    - Escalate to level 2, then level 3, then management

# Example Playbook – cont.

## Windows Fuzzy PandaX

- **Desktop Support**
  - Delete run at start reg keys and triggers
  - Reboot into SafeMode
  - Kill process sysmg.exe then winsrvx.exe then xnc.exe
  - Delete temp files
  - Delete compromised files defined in KB article 311
  - Delete other registry keys defined in KB article 312
  - Reboot system in to safe mode

# Example Playbook – cont.

## Windows Fuzzy PandaX

- **Desktop Support**
  - Verify processes do not restart after cleanup
    - If this does not work, escalate
  - Patch AV system and run updated AV scan
  - Patch OS
  - Run additional on-demand special AV scanners
  - Reboot system to normal mode
  - Update ticket

# Example Playbook – cont.

## Windows Fuzzy PandaX

- **Network Support**
  - Monitor traffic from system for 90 minutes
  - If no abnormal behavior is detected move system out of sandbox VLAN in to a restricted watch VLAN for 24 hours
  - If no user issues or abnormal behavior is detected move system to production VLAN
  - Update and close ticket

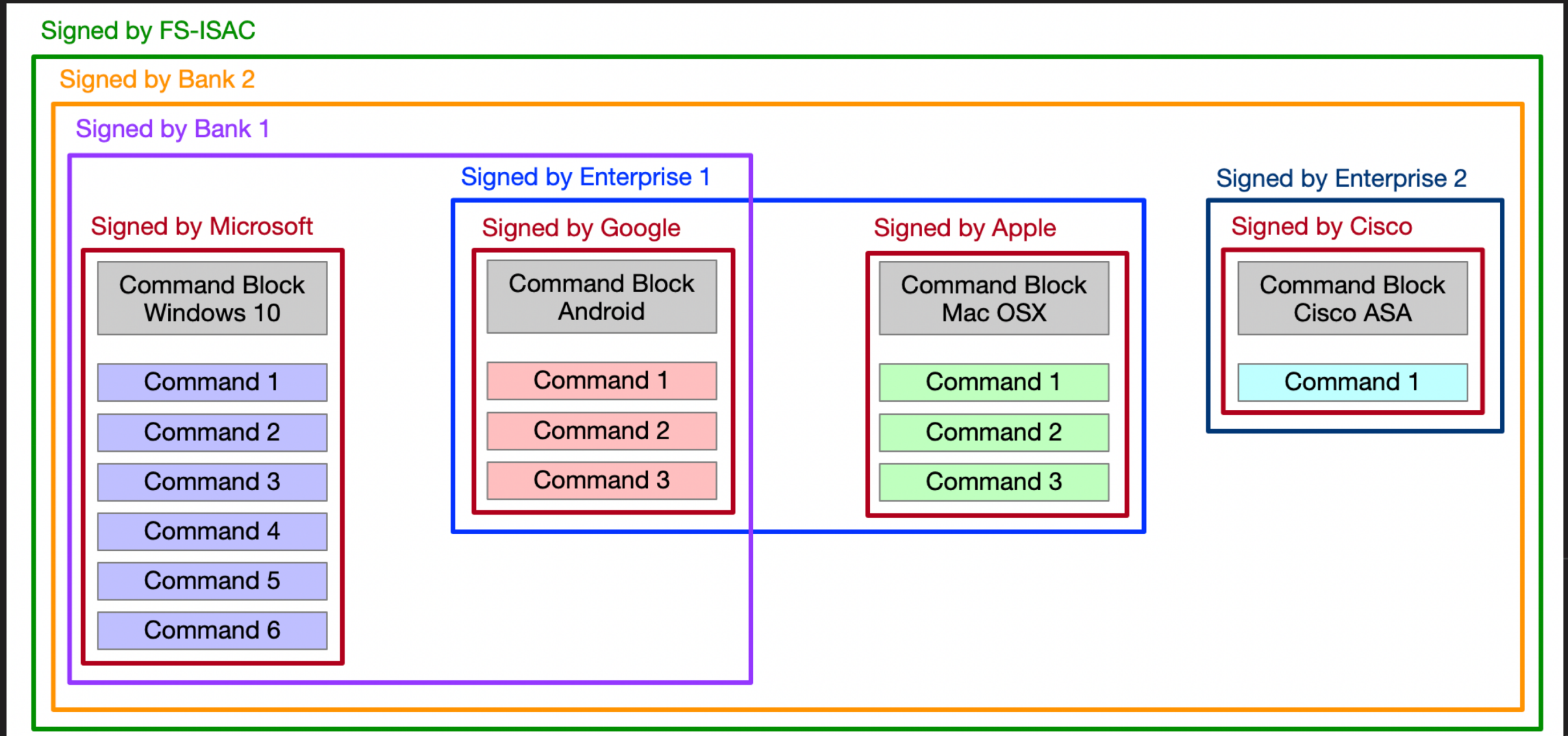
# Playbooks Can Span Groups & Technologies

- 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

# How We Get There - Coordinated Response

| | |
|---|---|
| Define | Playbook is defined based on various automated and manual inputs |
| Verify | Playbook is reviewed for accuracy and correctness. It is optionally verified in an test or sandbox environment |
| Distribute | Playbook actions are distributed to the systems that will execute them. Distribution includes checking that the playbook has been deployed correctly and follows rules defined within the playbook |
| Execute | Playbook is evaluated by one or more systems and execution events are communicated to the monitoring step |
| Monitor | Playbook execution is monitored and metrics are determined on the playbook to enable further refinement or improvement |

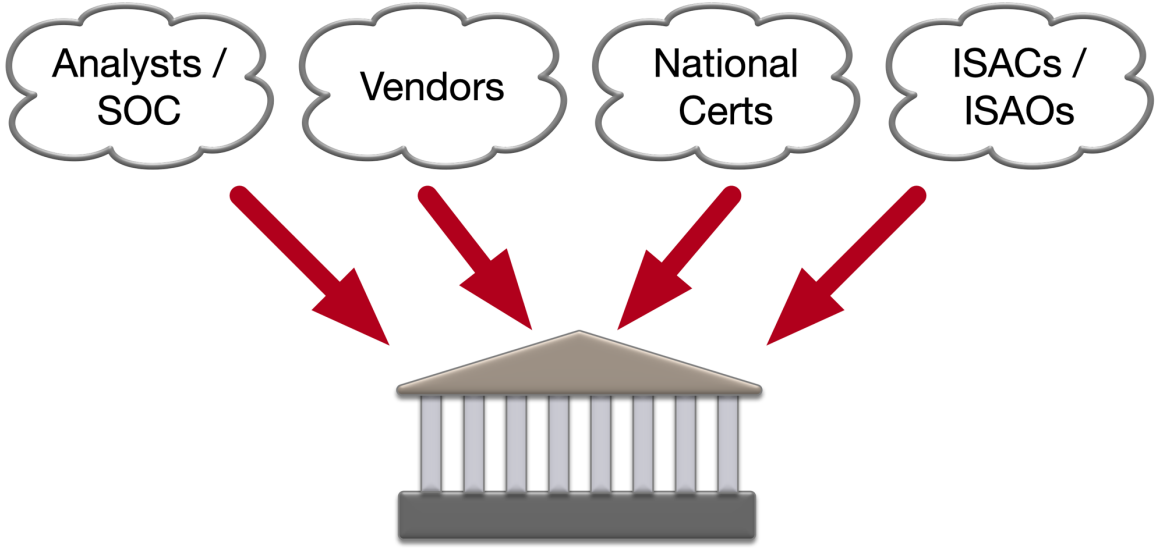
# How - Industry Response Example



Today


Future


# Security Knowledge




# Security Operation Center

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

Crawl Walk Jog Run

# Key Requirements

This solution needs to support the following:

# Key Requirements - Summary

- Multiple Actions (Sequencing and Backout)
- Decision Logic (Temporal and Conditional)
- Unique Identifiers
- Versioning and Targeting
- Testing, Verification, and Reporting
- Digital Signatures, Security, and Transport
- Management Separation

# Charter Review

# Detailed Key Requirements

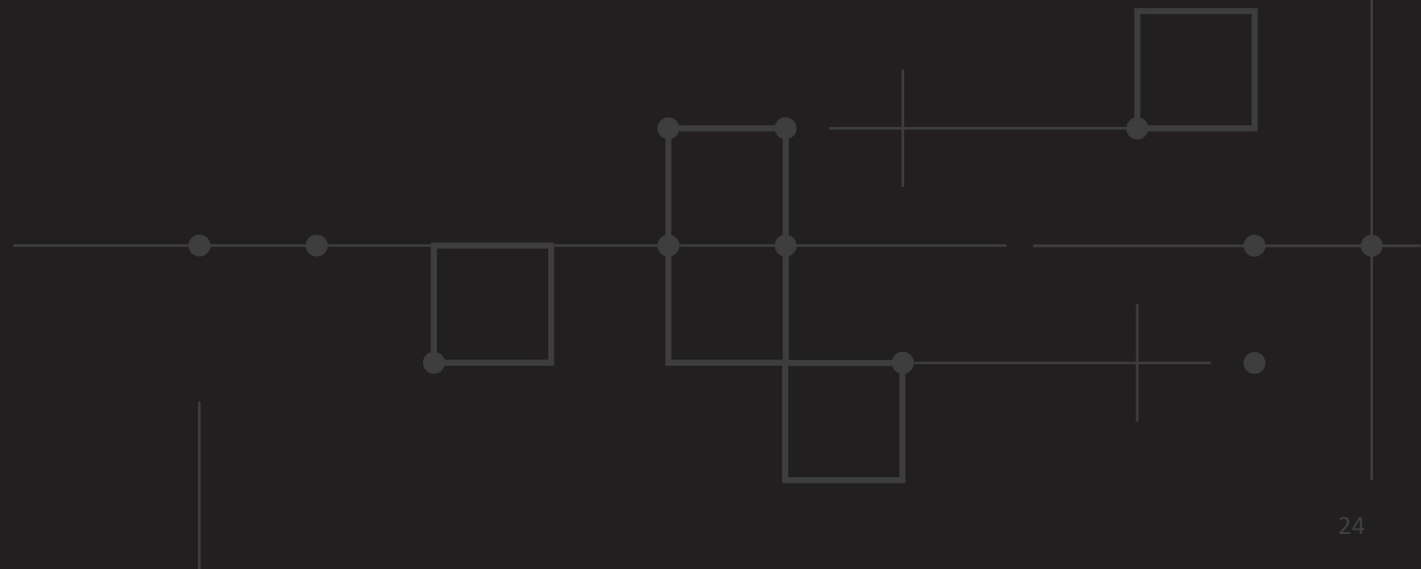
This solution needs to support the following:

# Actions

- Single Atomic Actions
- Multiple Actions
  - To respond to threats one must often perform many steps across many different pieces of infrastructure
- Sequencing of Actions
  - Actions often have to be done in a very specific order
- Back Out Steps

# Decision Logic

- Temporal Logic
  - Sometimes actions can only be performed at certain times or after a certain amount of time has passed after the previous action
- Conditional Logic
  - Often actions need to be performed based on environmental data or outcomes of previous actions

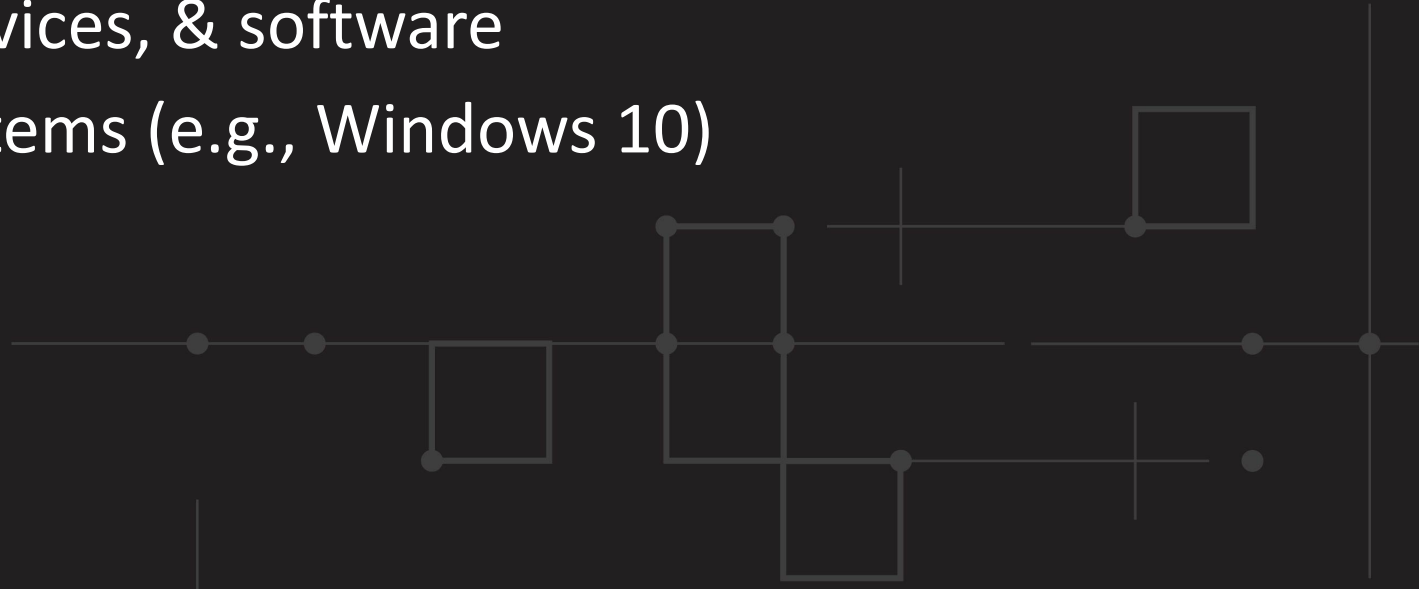


# Unique Identifiers

- System Integration
  - Needs to integrate with other systems globally
  - Support a globally unique ID like a UUIDv4 for projects and individual actions
- All transactions need to be able to be monitored
  - This means responses and notifications need a way to be tied back to the original request

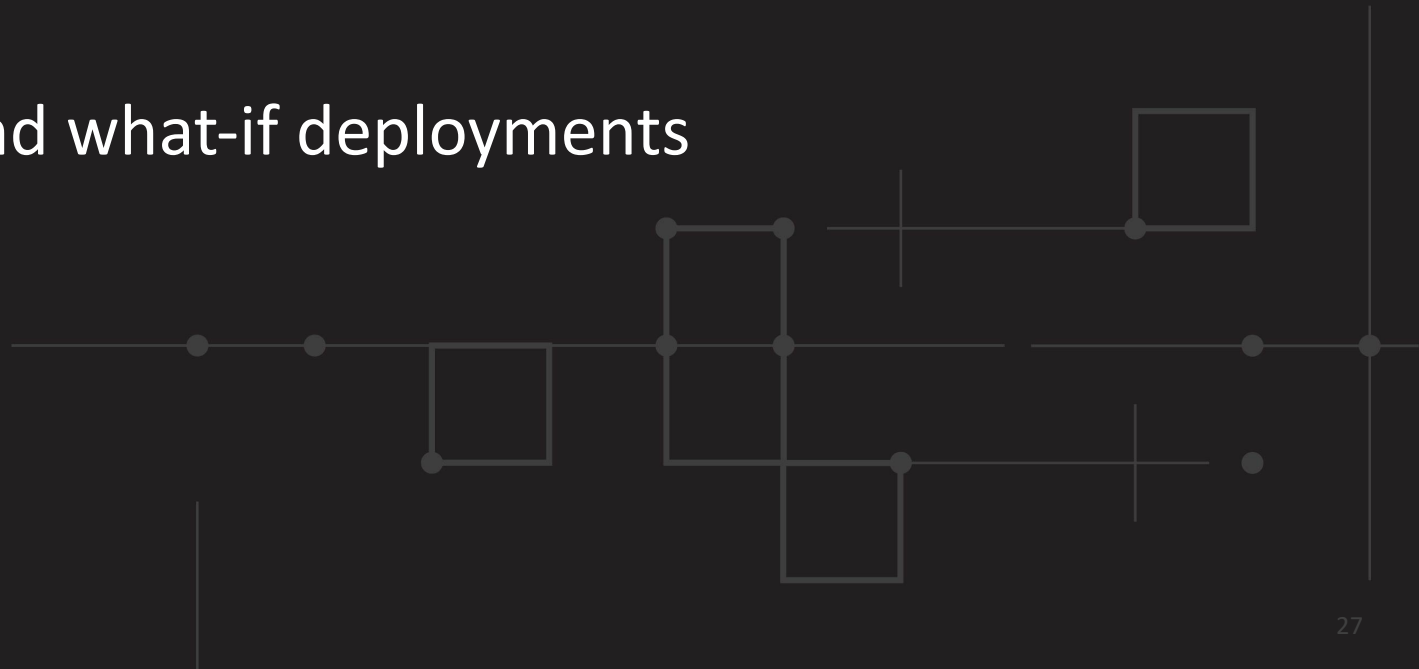
# Versioning and Targeting

- Versioning
  - Allow actions, projects, and templates to be versioned
  - Support both incremental and semantic versioning
- System Targeting
  - Identify specific machines, devices, & software
  - Identify general classes of systems (e.g., Windows 10)



# Use Cases and Testing

- Scope
  - Machine automation
  - Human actions / intervention
  - High level conceptual actions
- Testing
  - Provide dry run capabilities and what-if deployments



# Reporting

- Provide full reporting on the processing of each action
- Accommodate mandatory reporting and auditing
- Must have a timestamp and information about original request or rule that caused the event
- Could be either synchronously requested or an asynchronous event (syslog) with periodic updates

# Digital Signatures

- Ability to digitally sign COAs and their parts
- Ability to support multiple digital signatures
- Ability for multiple independent organizations to sign and verify the correctness, accuracy, and validity of the COA

# Security

- Security
  - Support full data protection, integrity and authentication
  - Support data markings like TLP
- Transport
  - Encrypted and authenticated
  - Both direct delivery and publish/subscribe solutions

# Management Separation

- COAs may be defined in one environment and executed or deployed to a different operational environment
- For a COA to execute correctly must have authorization in the operational environment where it is executed
- Security environment executing the COA will likely be different from where the COA was defined

# Milestones

# Major Milestones

- Refine requirements and use cases
  - Achieve WG consensus on requirements
- Define JSON data model
  - Simple actions and action groups
  - Temporal and conditional logic
  - Reporting, monitoring, and response
- Identify signature and encryption solution
- Identify protocols to layer on and interact with
  - Define specification for MTI protocol(s)