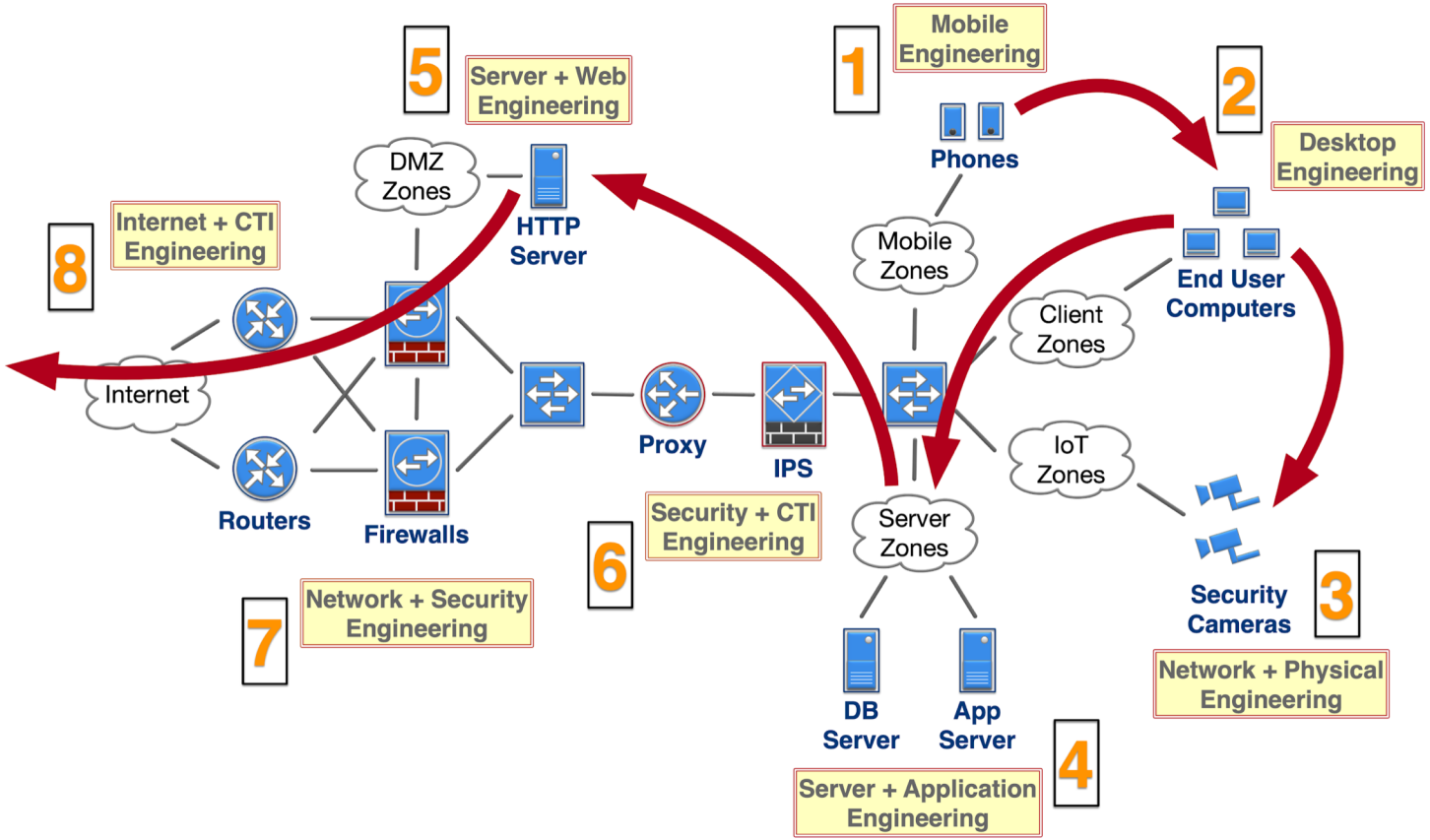
Collaborative Automated Course of Action Operations (CACAO)

Allan Thomson (LookingGlass Cyber Solutions)
Bret Jordan (Symantec)
Oct 2019

OASIS
Open standards. Open source.

Why CACAO - Threat Detection and Mitigation Today



What is CACAO

- Collaborative Automated Course of Action Operations for Cyber Security
  - A standard that defines structured and machine parsable playbooks
    - Creation of those playbooks
    - Distribution of those playbooks across systems
    - Monitoring of those playbooks and their results
  - It includes documenting and describing the steps needed to prevent, mitigate, remediate, and monitor responses to a threat, an attack, or an incident

- What it 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

Coordinated Security Response in 5 Steps

Definition
- Where a Coordinated Response is defined based on various inputs both automated and manually derived

Verification
- Where a Coordinated Response is reviewed for accuracy and correctness. It is optionally verified in an environment that can verify by executing the project in a way that provides an additional level of verification

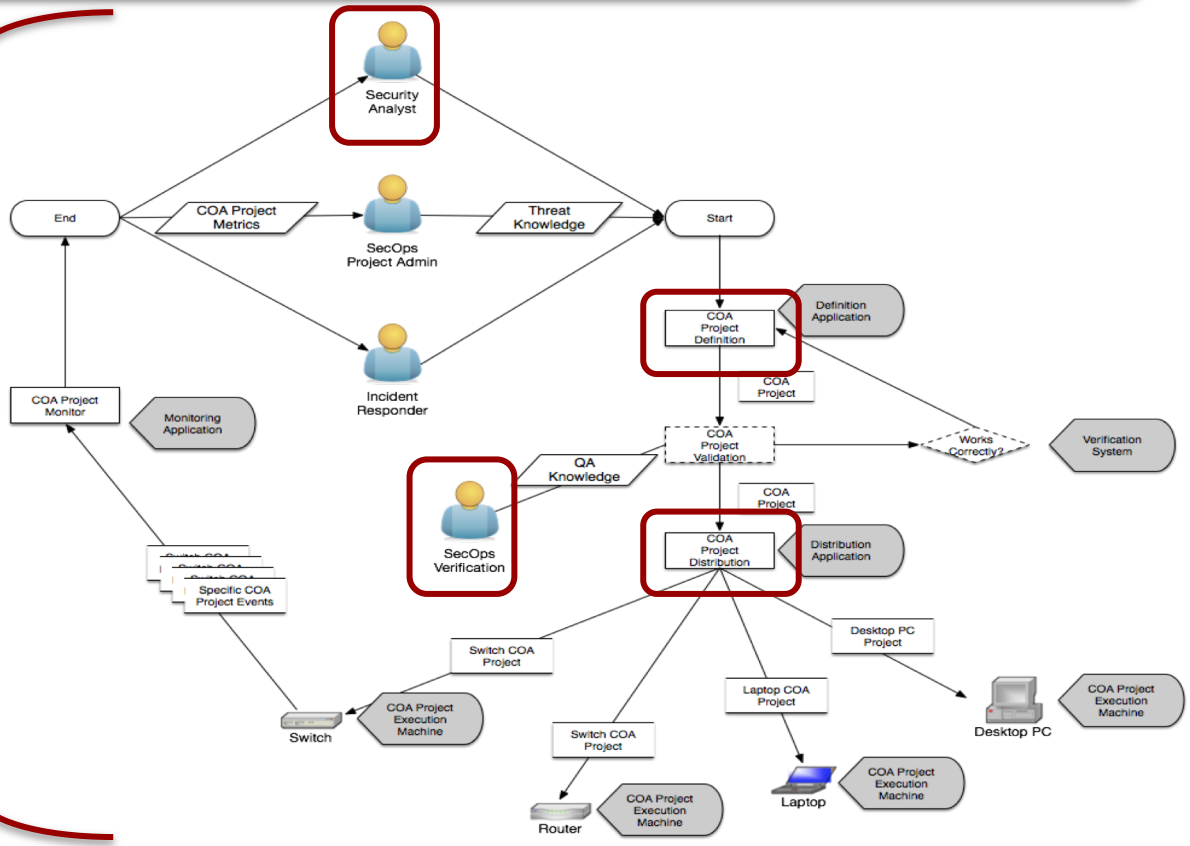
Distribution
- Where a Coordinated Response is distributed to the systems that will execute it. Distribution includes checking that the Coordinated Response has been deployed correctly and follows rules defined within the project for atomic transactions

Execution
- Where a Coordinated Response is evaluated by one or more security infrastructure systems and execution events are communicated to the monitoring step

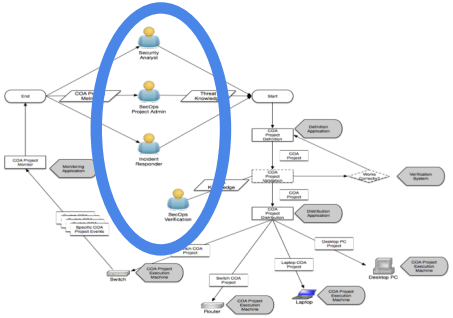
Monitoring
- Where a Coordinated Response execution is monitored and metrics are determined on the Playbook to enable further refinement or improvement to the definition

CACAO - System Coordination

- System Coordination
  Roles and requirements of system architectural components & behavior
- Interfaces
  Interfaces & API across components
- Protocols
  Protocols transporting CACAO content securely
- Schema
  Standard JSON Schema for Playbooks



CACAO Roles



Security Analyst

- Senior role where the person performs analysis of all available threat intelligence; malware research; active threats that may be relevant to their environment to determine a set of recommended steps to both detect and respond to threats
- Aware of the capabilities of the organization to respond where they have knowledge of the security infrastructure deployed on both network; servers and endpoints as well as the services running on those systems

SecOps Project Admin

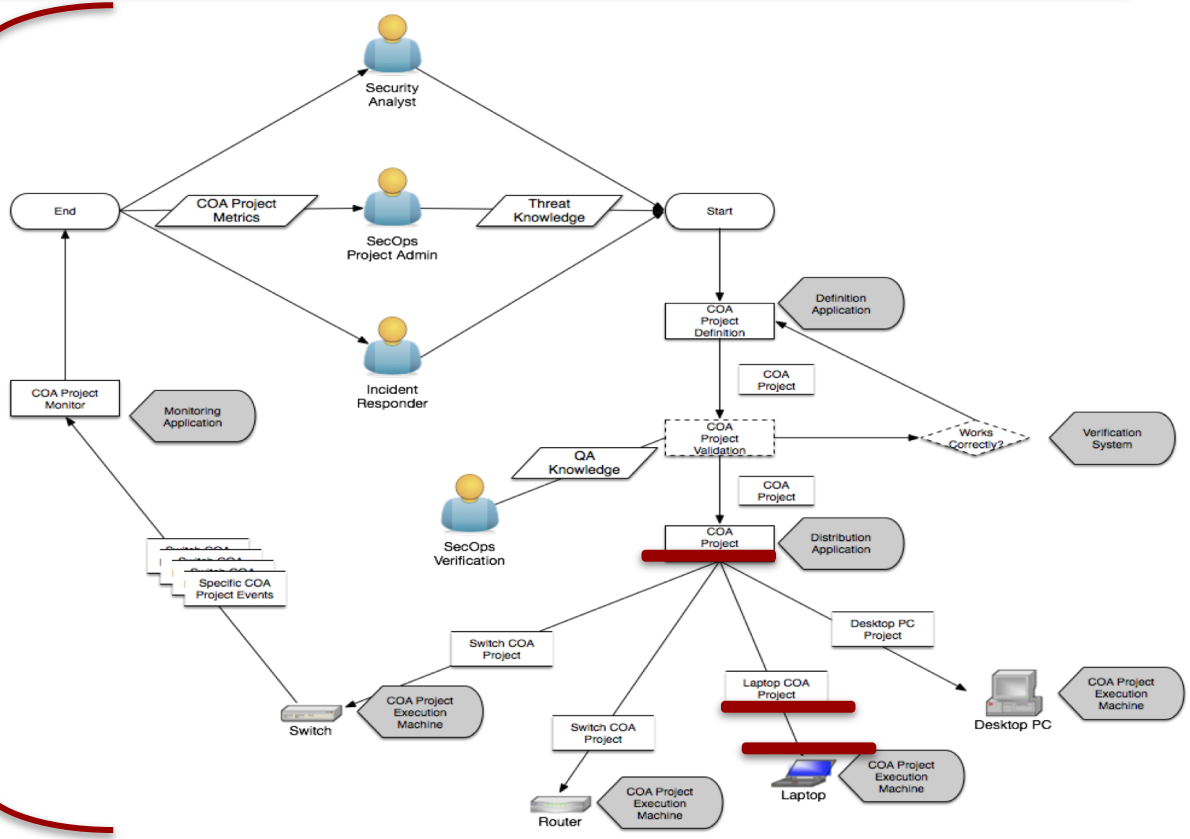
- Senior role that oversees and manages the security operations of the network
- May work closely with the Security Analyst to determine response playbooks to proactively manage risk in the enterprise environment.
- May either define Playbooks themselves or review/refine Playbooks defined by the Security Analyst

Incident Responder

- Focused on responding to an active threat to the enterprise where they have limited time to respond and most of their actions are focused on mitigation and remediation
- Any outcomes and results of the incident may be fed back into the other 2 teams involved to enable enhancement future responses that reduce the risk of threat incidents

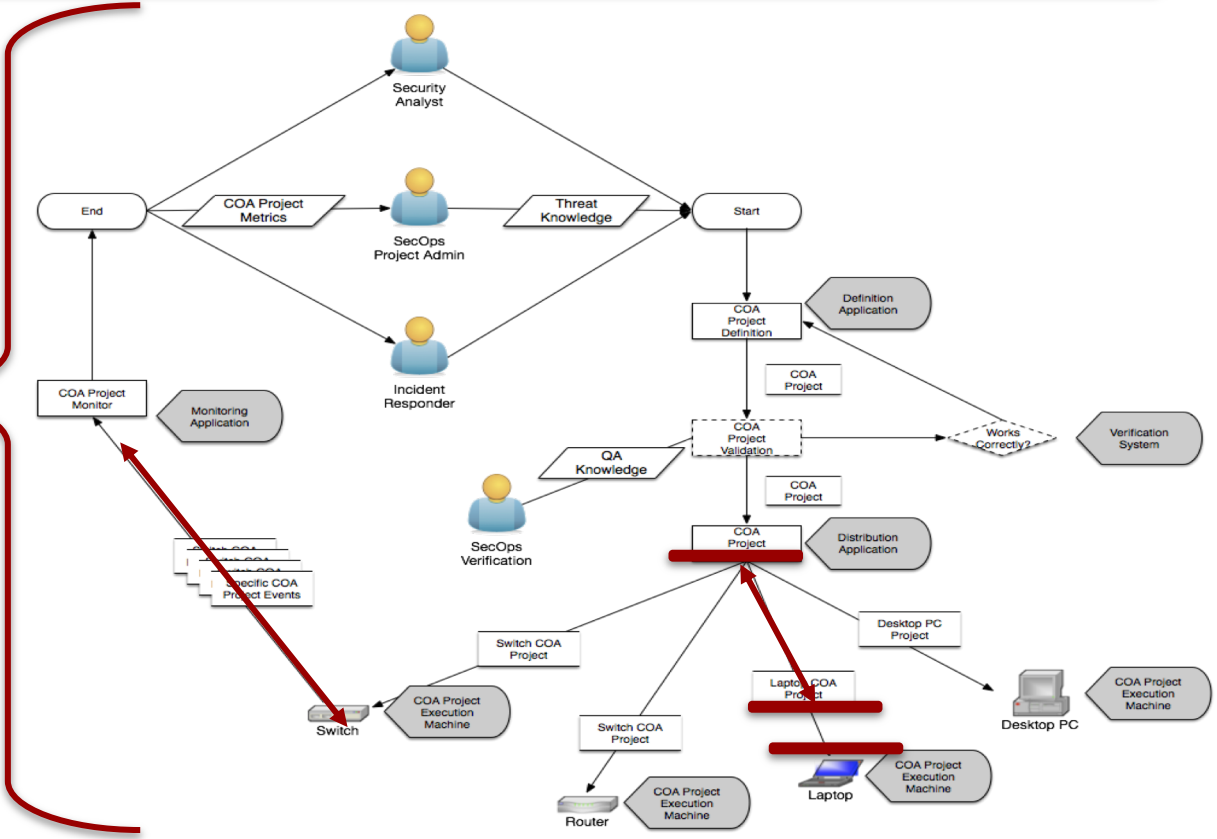
CACAO - Interfaces

- System Coordination
  Roles and requirements of system architectural components & behavior
- Interfaces
  Interfaces & API across components
- Protocols
  Protocols transporting CACAO content securely
- Schema
  Standard JSON Schema for Playbooks



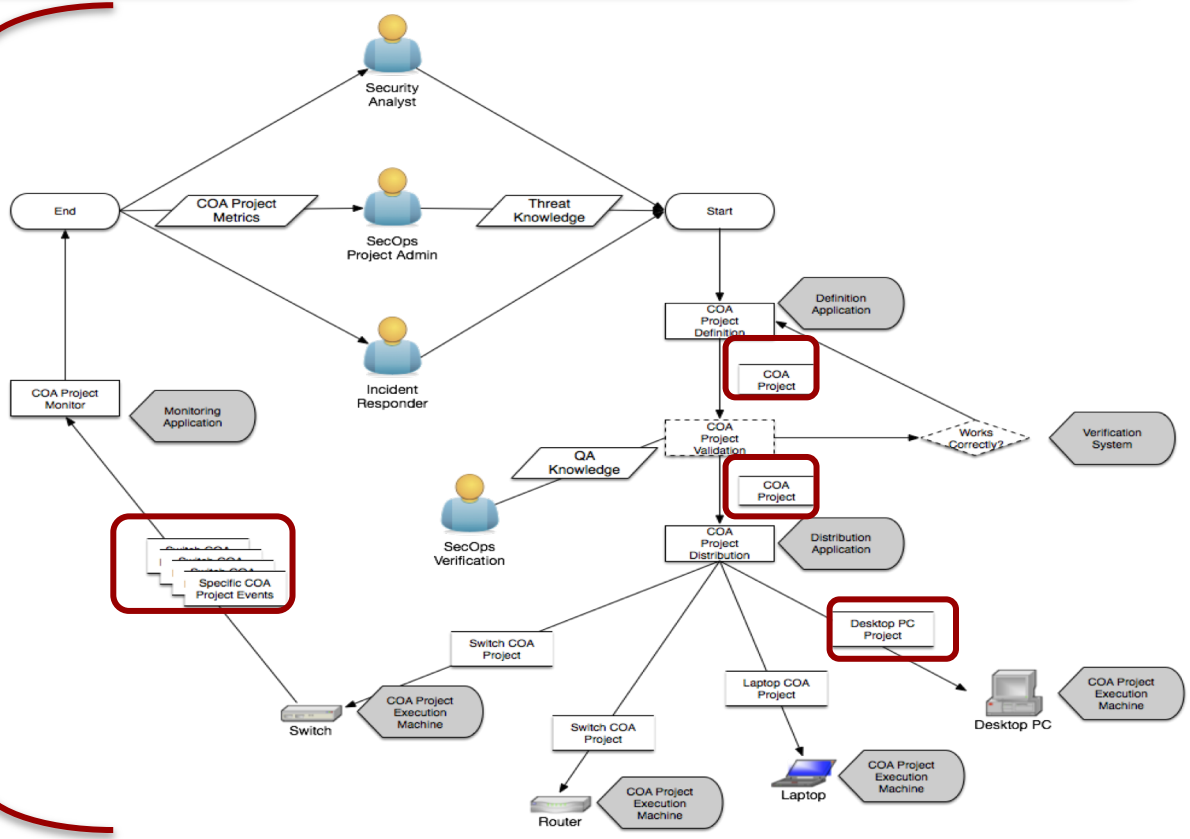
CACAO - Protocols

- System Coordination
  Roles and requirements of system architectural components & behavior
- Interfaces
  Interfaces & API across components
- Protocols
  Protocols transporting CACAO content securely
- Schema
  Standard JSON Schema for Playbooks

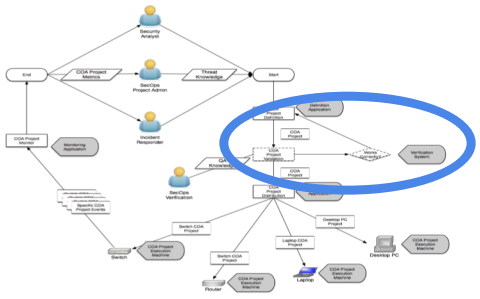


CACAO - Schema

- System Coordination
  Roles and requirements of system architectural components & behavior
- Interfaces
  Interfaces & API across components
- Protocols
  Protocols transporting CACAO content securely
- Schema
  Standard JSON Schema for Playbooks



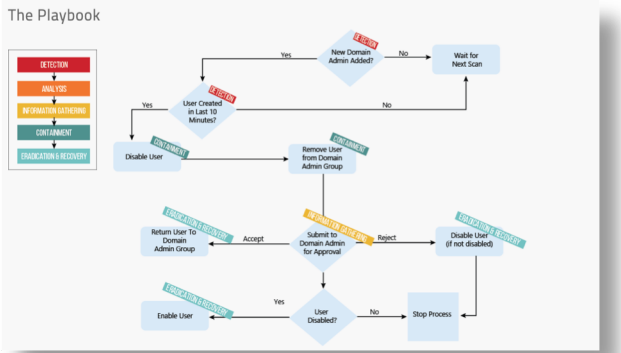
Verification



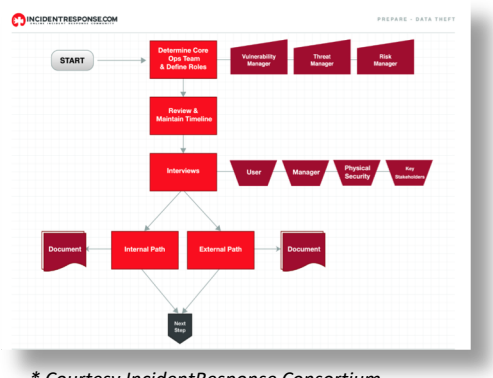
- Ability to **validate** the project will **execute correctly** once deployed in an operational environment
- Verification includes
  - All Playbook Sequence Elements are connected so that the complete sequence will complete when executed
  - All Playbook Conditional Elements have connections to defined Playbook Steps
  - Each Playbook Step is well-formed and parses correctly according to the Playbook JSON schema

CACAO Behavioral Construction

- Multiple Actions
  - 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
- 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



** Courtesy ayehu*



** Courtesy IncidentResponse Consortium*

CACAO Operations

- System Integration
  - Playbooks integrate with other systems globally (e.g. Cyber Threat Intelligence). To do this, Playbooks will need a globally unique ID like a UUIDv4
- Reporting
  - Provide full reporting on the processing of each action
  - Allow for full auditing
  - Accommodate mandatory reporting
  - Provide dry run capabilities
  - Define procedural back out steps
- Versioning
  - Playbooks are versioned

CACAO Implementation

- System Targeting
  - Ability to define
    - specific machine, operating system, software
    - general classes of systems (ex. Windows 10 sp3)

- Security
  - Ensures full data protection, integrity and authentication
  - Provides digital signatures of the COAs and their parts
  - Encrypted and authenticated delivery

- Transport
  - Supports both direct delivery and publish/subscribe solutions

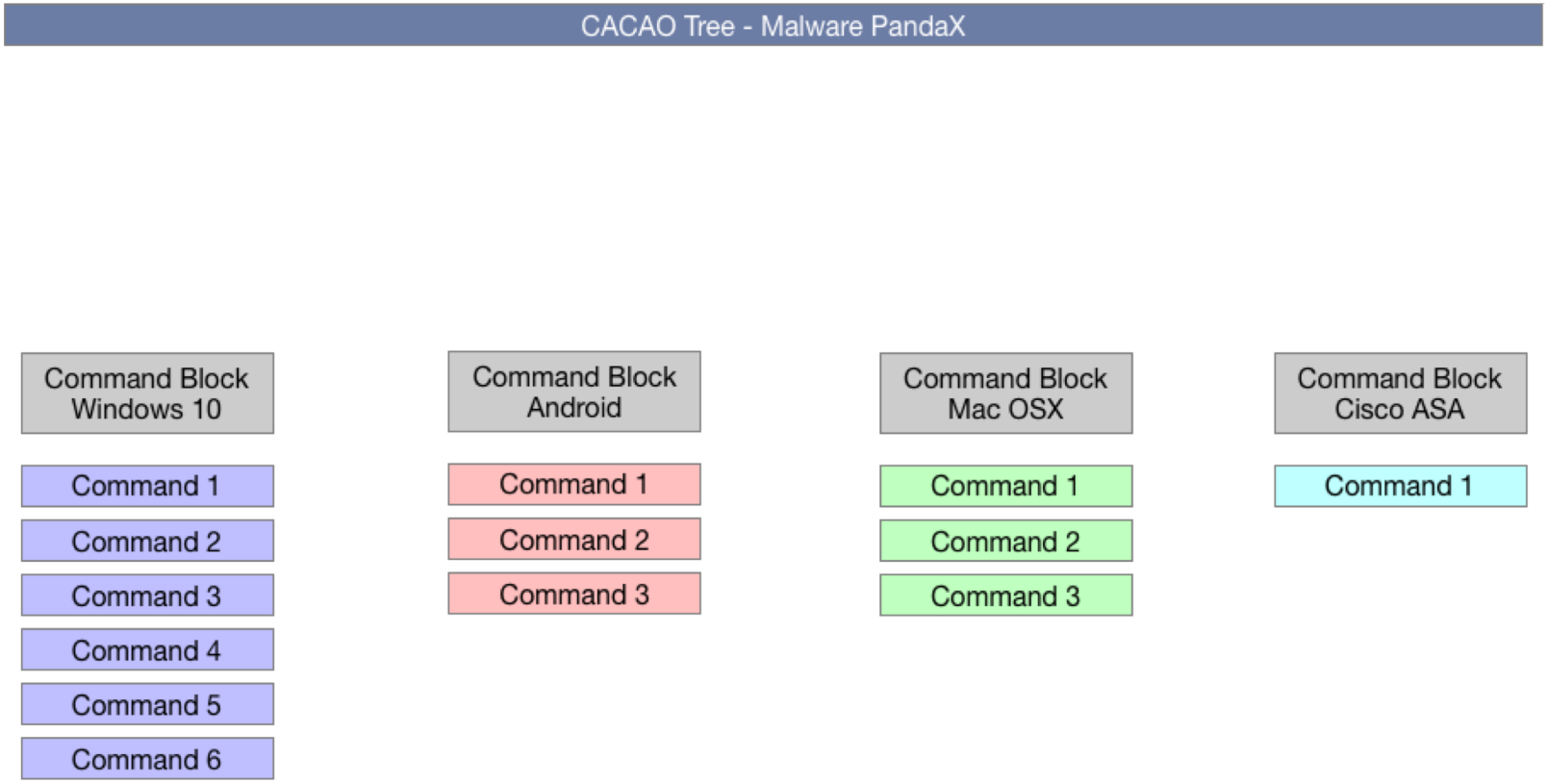
Playbook Examples

Example

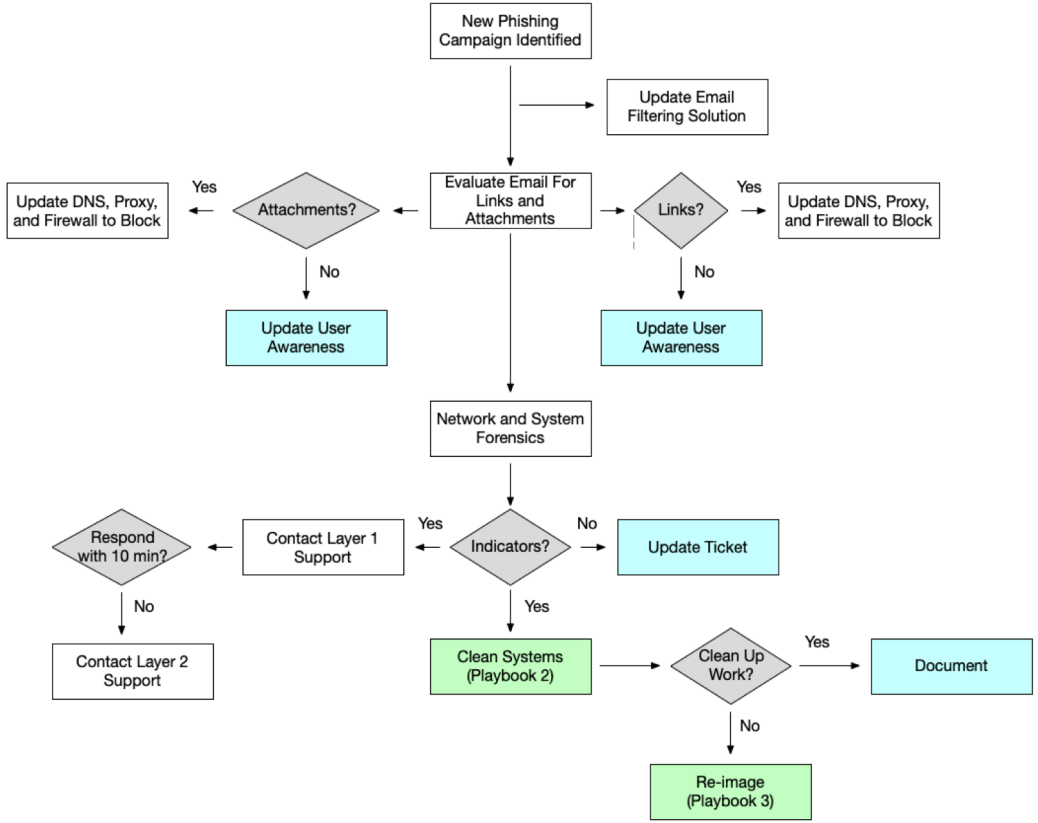
- As we go through these requirements, we are going to talk about this from a single use-case, that is mitigating or remediating a specific piece of malware
  - There are many more use-cases that can and will use CACAO

- Mitigation Response for Malware "Happy Panda" - Example
  - Windows 10 (performed by Desktop Support Team)
    - <6 steps>
  - Android (performed by Mobile Support Team)
    - <3 steps>
  - Mac OSX (performed by Apple Desktop Support Team)
    - <3 steps>
  - Cisco ASA Firewall (performed by Network Operations)
    - <1 steps>

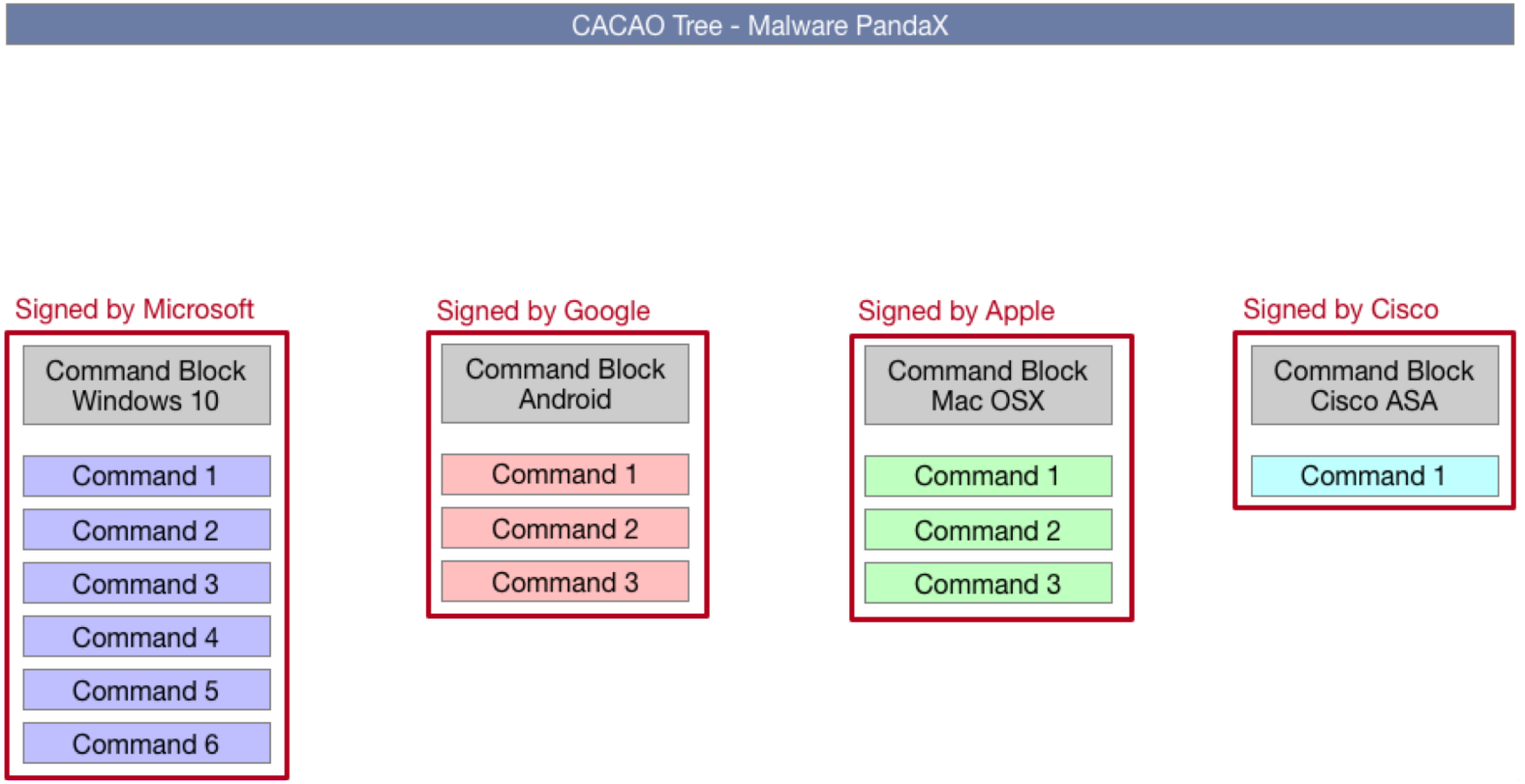
Single Organization Response



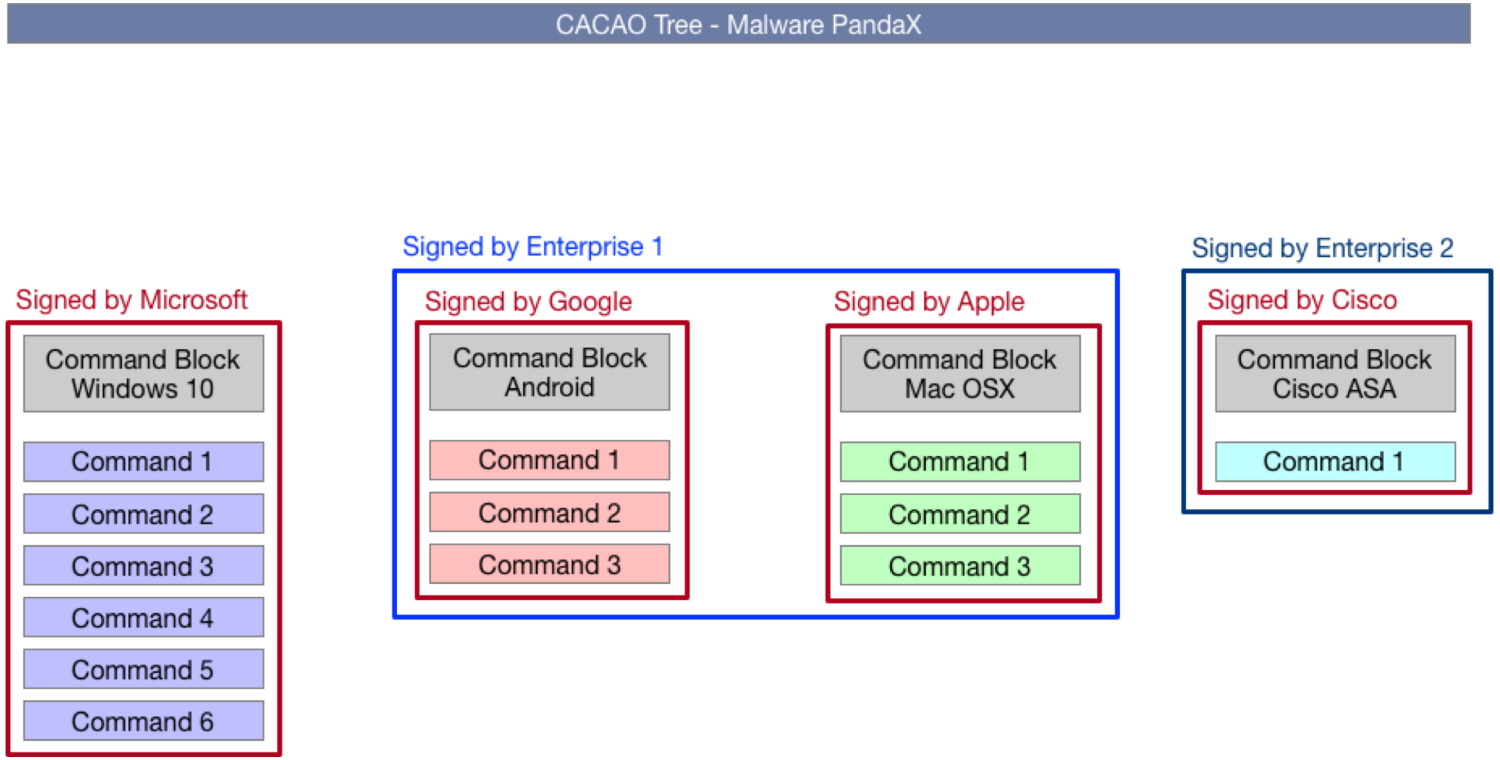
Phishing Campaign Response Example



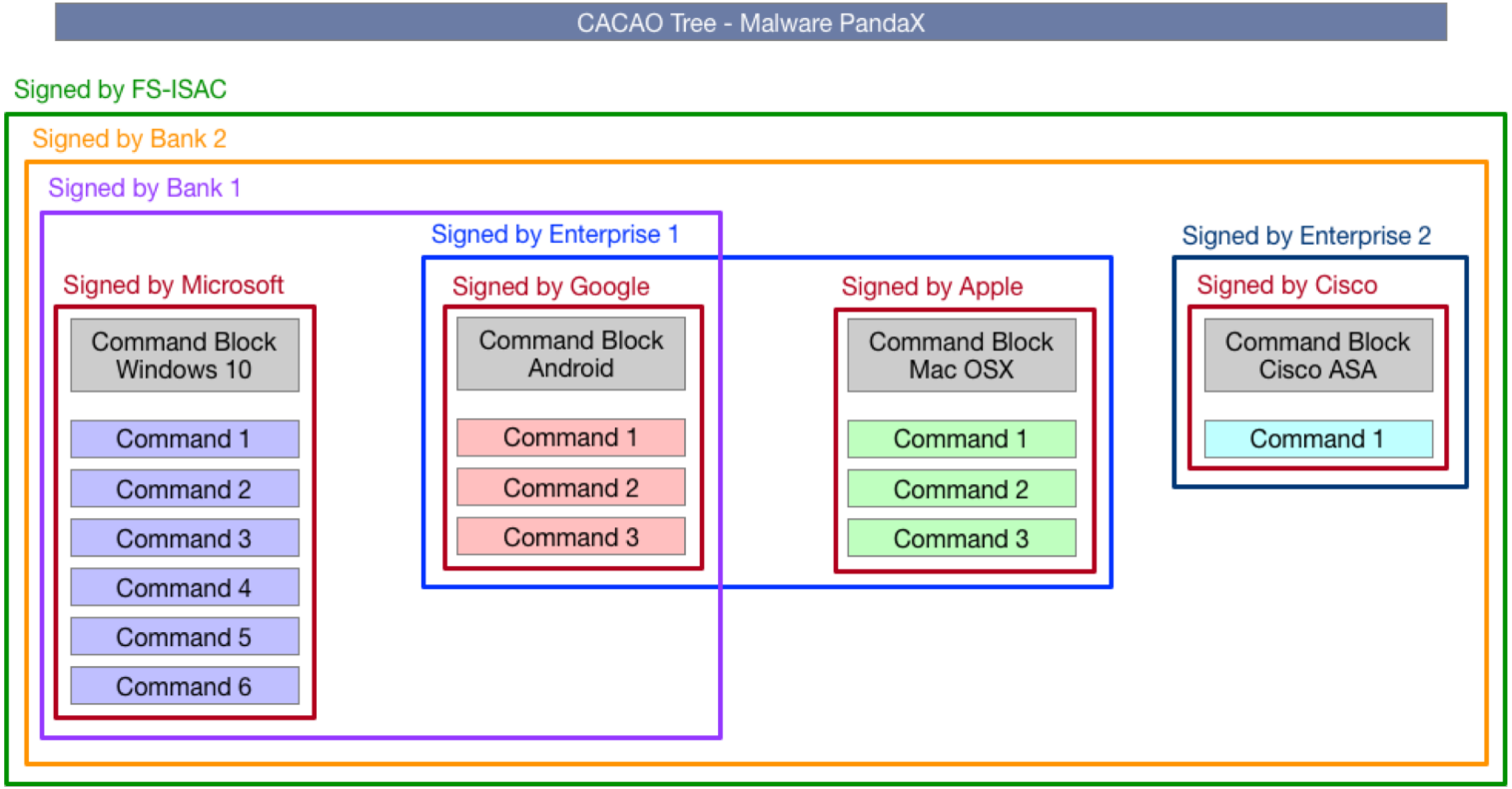
Vendor Source Signing



Combinational Signing



Industry Consortium Signing



Get Involved

cacao@lists.oasis-open.org