CACAO Introduction

(https://www.ietf.org/mailman/listinfo/Cacao)

Bret Jordan, Allan Thomson

October 24, 2018

What is CACAO?

- **C**ollaborative **A**utomated **C**ourse of **A**ction **O**perations for Cyber Security
  - A standard that defines actions for threat response, including
    - **Creation** of those actions
    - **Distribution** of those actions across systems
    - **Monitoring** of those actions 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 or indicators of compromise

Why CACAO?

- Threats
  - Threat Actors and Intrusion Sets are advancing
  - Number of attacks are increasing
  - Attack surface is growing
  - More valuable electronic data and connected systems
- Defense
  - Manual and reactive
  - Solutions are siloed
    - Organizations become system integrators with mixed results
  - Many different groups inside an organizations are part of the response
  - No easy way to share threat response expertise
  - Organizations need to respond in machine relevant time across multiple coordinated systems
  - ISACs and ISAOs could disseminate solutions with Threat Intelligence

Goals of CACAO

- Design key architectural interactions to allow **coordinated** threat response
  - **System Level:**
    Identify roles and requirements of system architectural components
  - **Interface Level:**
    Identify key requirements for interfaces across components
  - **Protocol Level:**
    Identify protocols that can/must transport CACAO content securely
  - **Schema Level:**
    Design a standard JSON structure for COAs / Playbooks

Goals of CACAO cont.

- Allow for manual (e.g. human-performed), process, and automatic actions

- Integrate with other security systems
  - E.g. Cyber Threat Intelligence; Identity; Risk Management
  - This will allow pivoting, sharing, collaboration, and enrichment

- Provide preventative, mitigative, and remediative solutions that are measurable and scalable

Core Requirements - Example Use Case

- 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>

Core Requirements

- 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

- 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

Core Requirements cont.

- System Integration
  - COA Projects need to integrate with other systems globally (e.g. Cyber Threat Intelligence). To do this, COA Projects 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
  - Need to allow COA Projects to be versioned

Core Requirements cont.

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

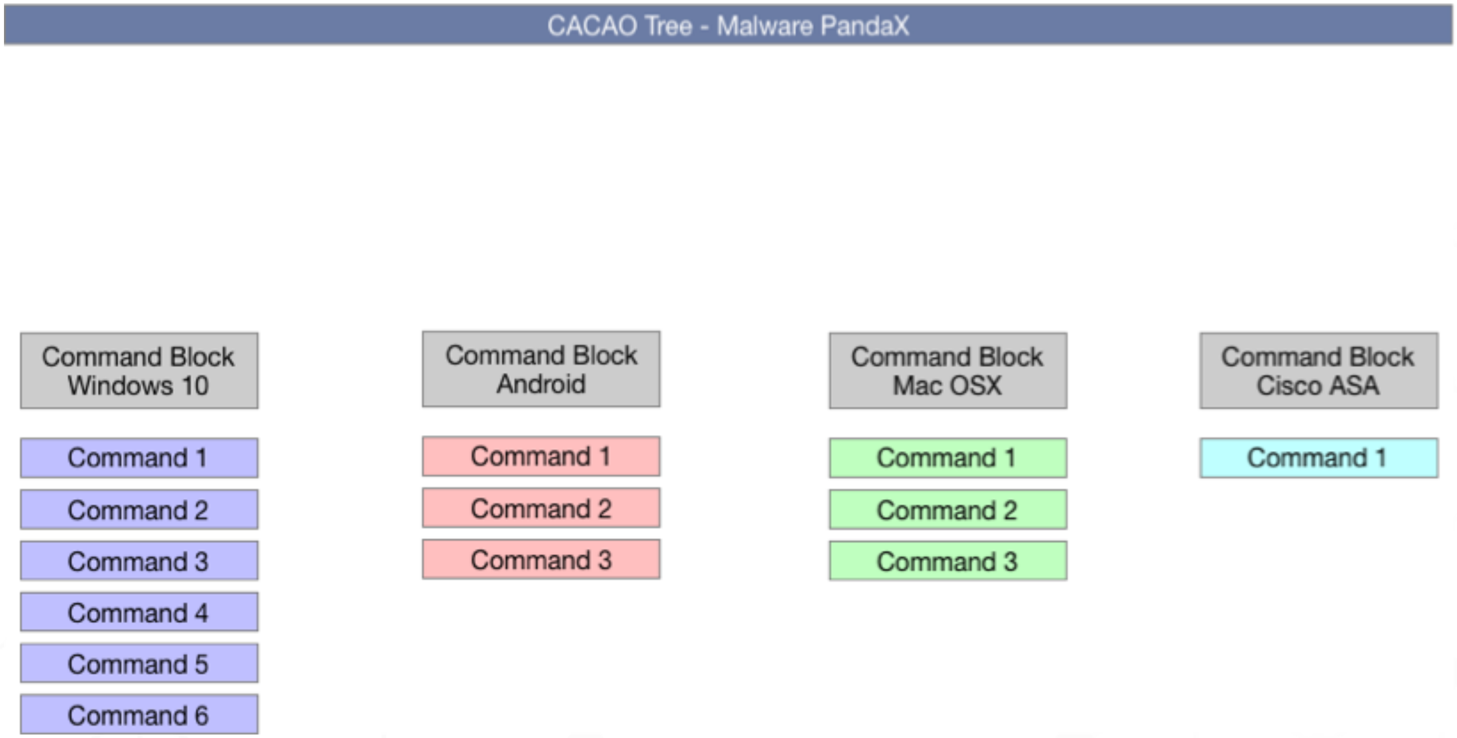
- Security
  - Need to ensure full data protection, integrity and authentication
  - Provide digital signatures of the COAs and their parts
  - Encrypted and authenticated delivery

- Transport
  - Needs to support both direct delivery and publish/subscribe solutions

Collaboration Examples

Collaboration Example

- One or more organizations/vendors create a series of commands for various platforms that mitigate malware "PandaX"



CACAO Tree - Malware PandaX

Command Block Windows 10
- Command 1
- Command 2
- Command 3
- Command 4
- Command 5
- Command 6

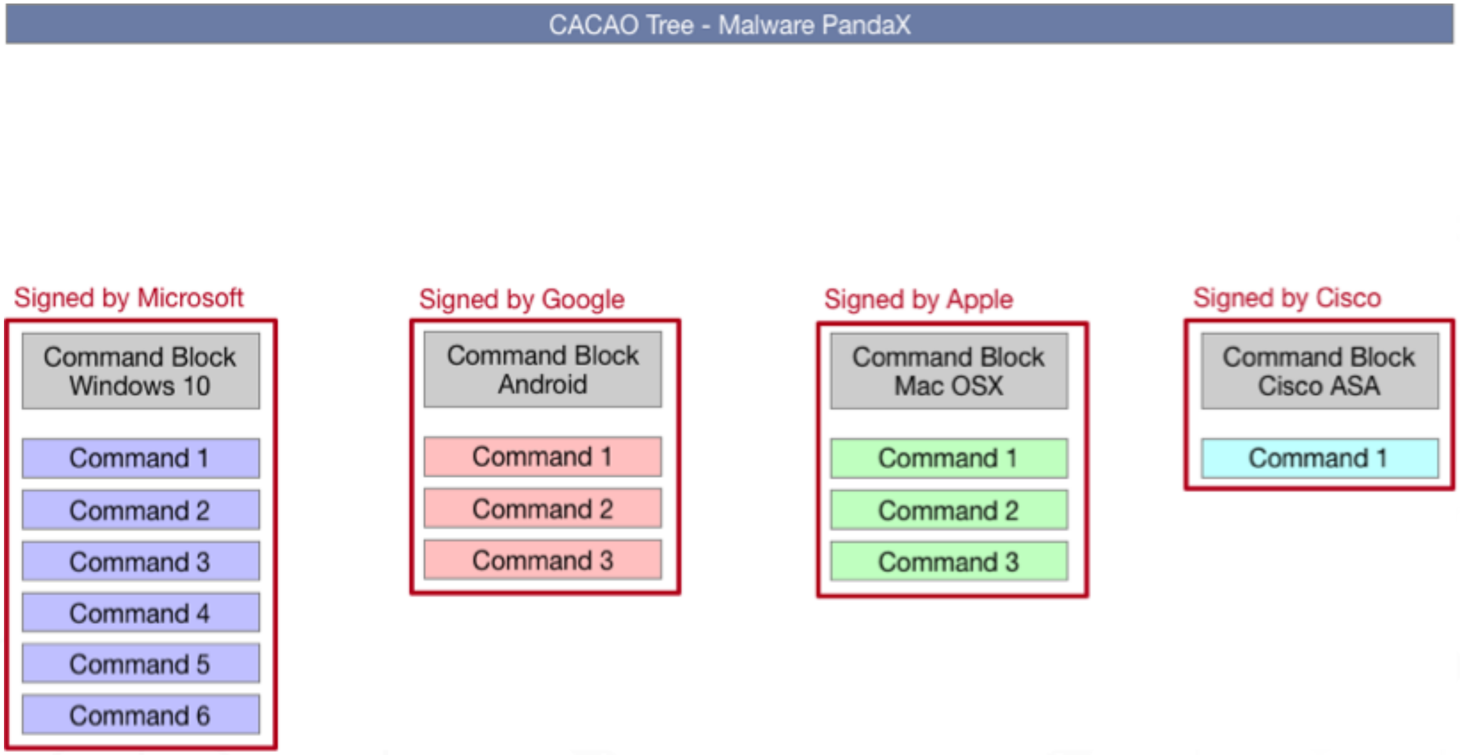
Command Block Android
- Command 1
- Command 2
- Command 3

Command Block Mac OSX
- Command 1
- Command 2
- Command 3

Command Block Cisco ASA
- Command 1

Collaboration Example - Individual Enterprise Response

- Various vendors sign their solutions for mitigating PandaX



CACAO Tree - Malware PandaX

Signed by Microsoft

Command Block Windows 10

Command 1

Command 2

Command 3

Command 4

Command 5

Command 6

Signed by Google

Command Block Android

Command 1

Command 2

Command 3

Signed by Apple

Command Block Mac OSX

Command 1

Command 2

Command 3

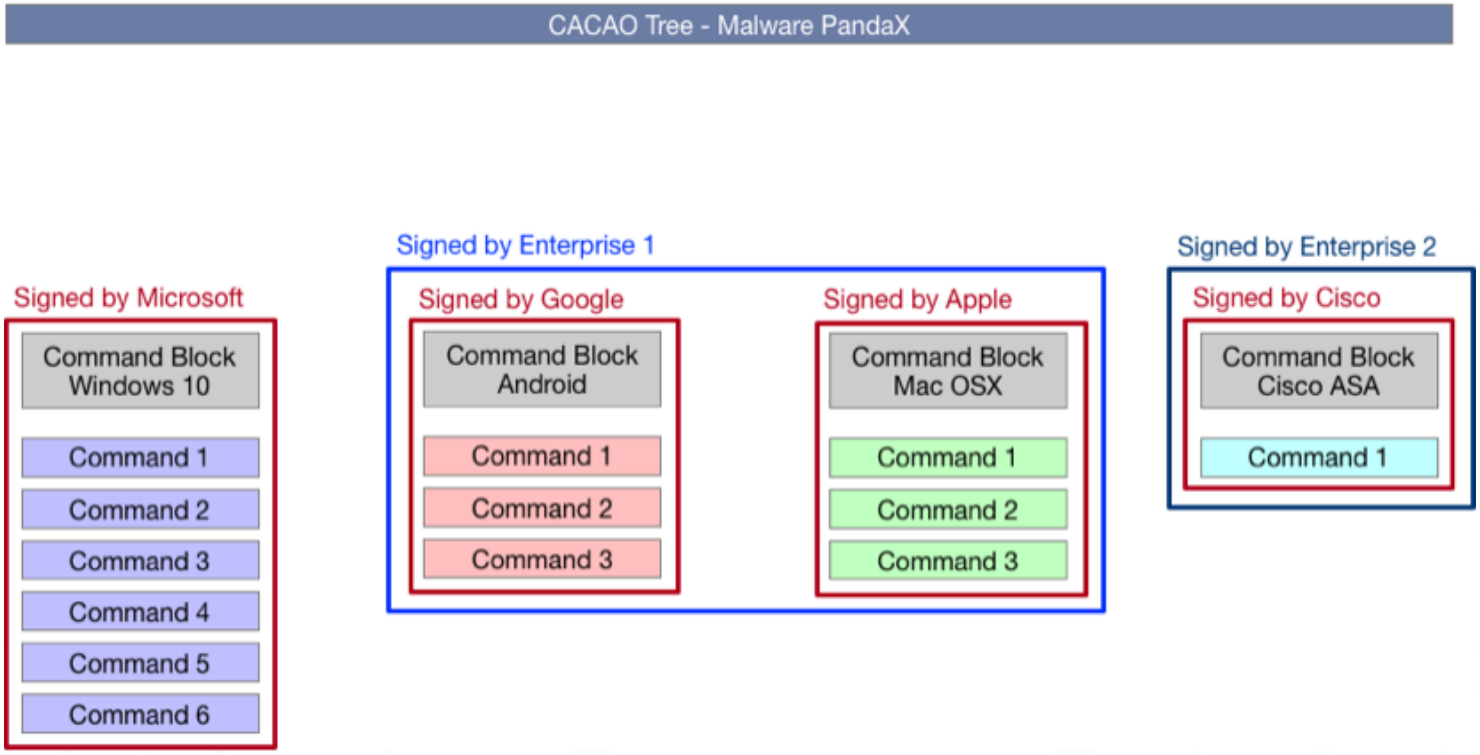
Signed by Cisco

Command Block Cisco ASA

Command 1

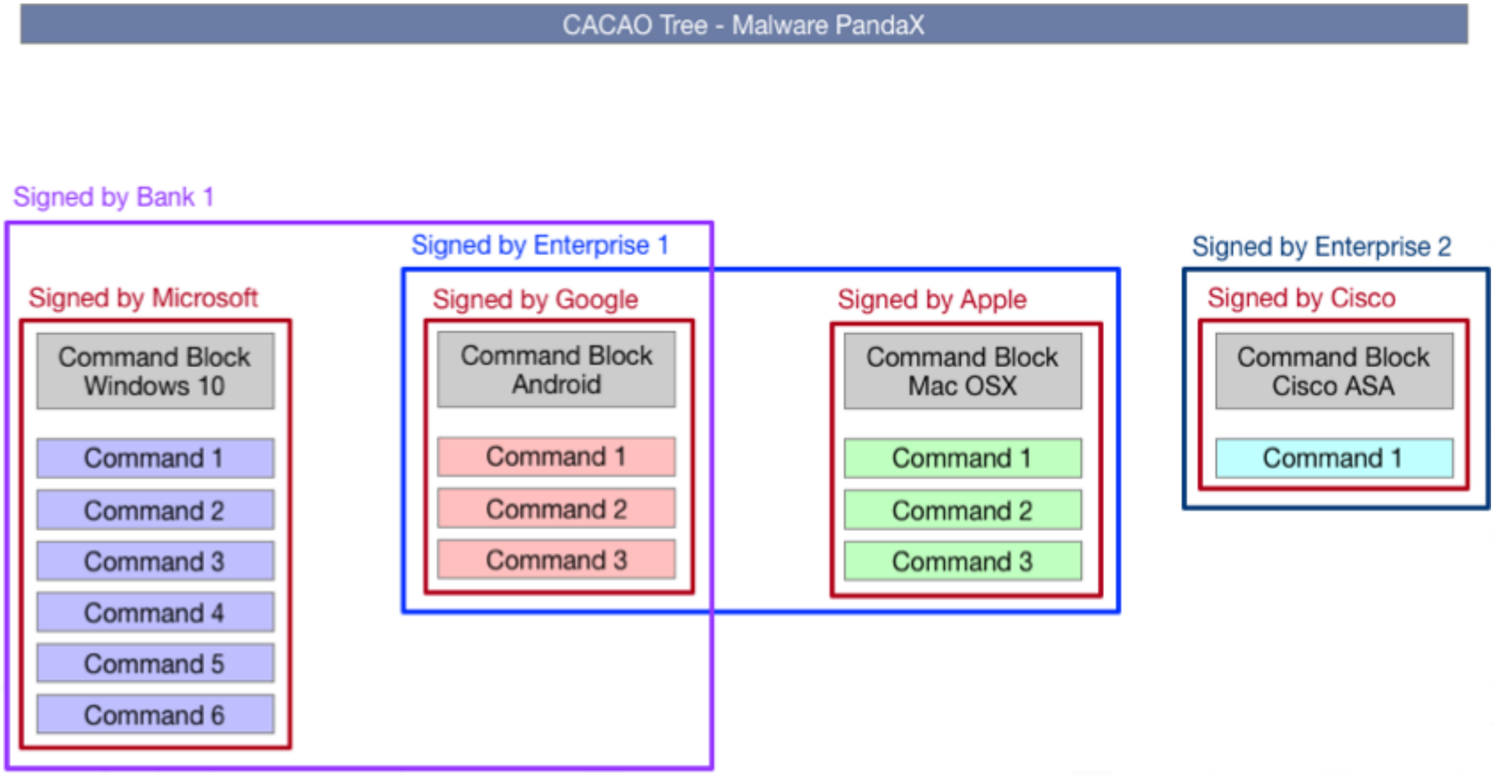
Collaboration Example - Combined Response

- Various organizations sign their solutions for mitigating PandaX



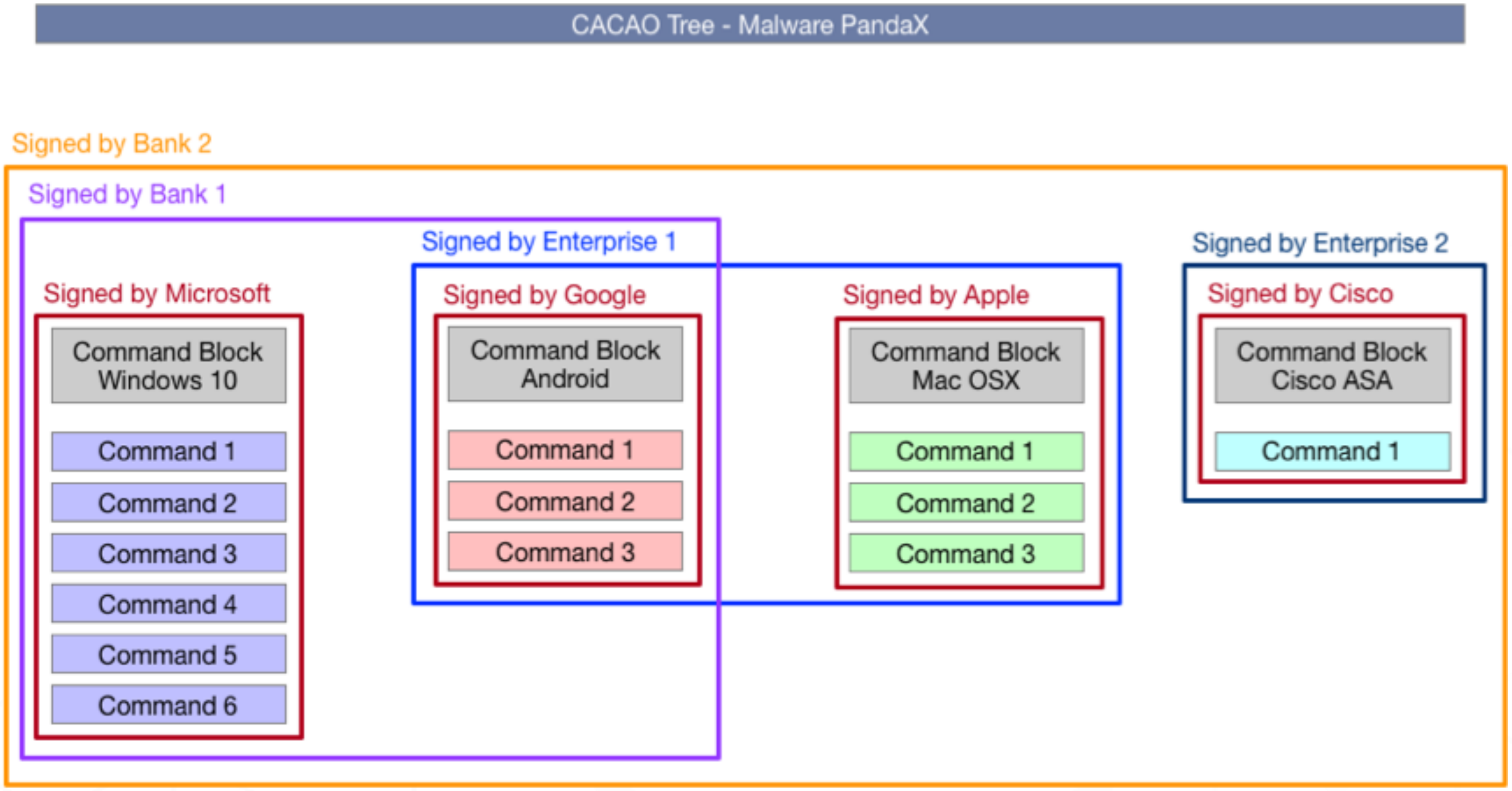
Collaboration Example - Big Bank 1 Response

- Big Bank 1 signs the entire solutions for mitigating PandaX



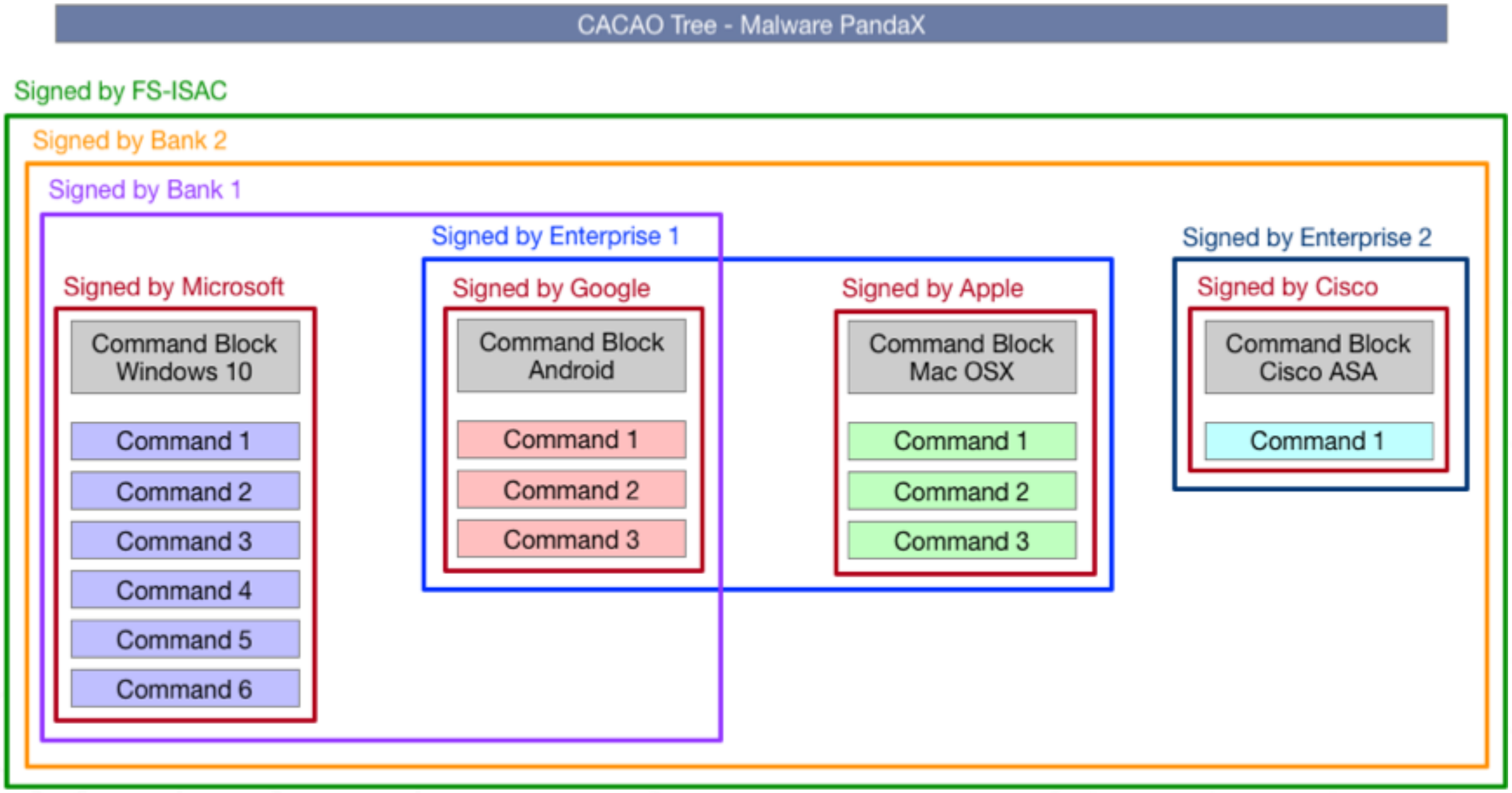
Collaboration Example - Big Bank 2 Response

- Big Bank 2 signs the entire solutions for mitigating PandaX



Collaboration Example - Industry Wide Response

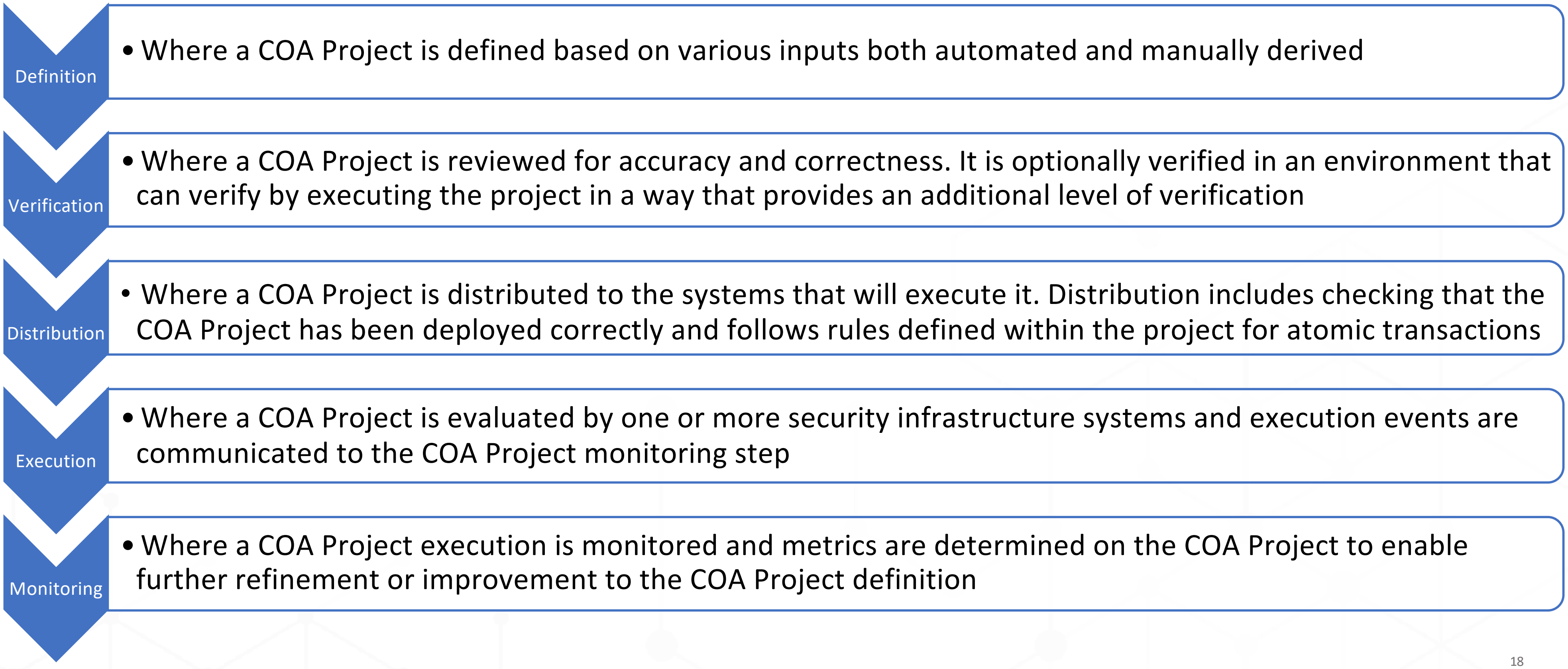
- FS-ISAC signs the entire solutions for mitigating PandaX



Architectural Introduction

CACAO Process

5 process steps involved in COA Project for use within a security environment



Definition

- Where a COA Project is defined based on various inputs both automated and manually derived

Verification

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

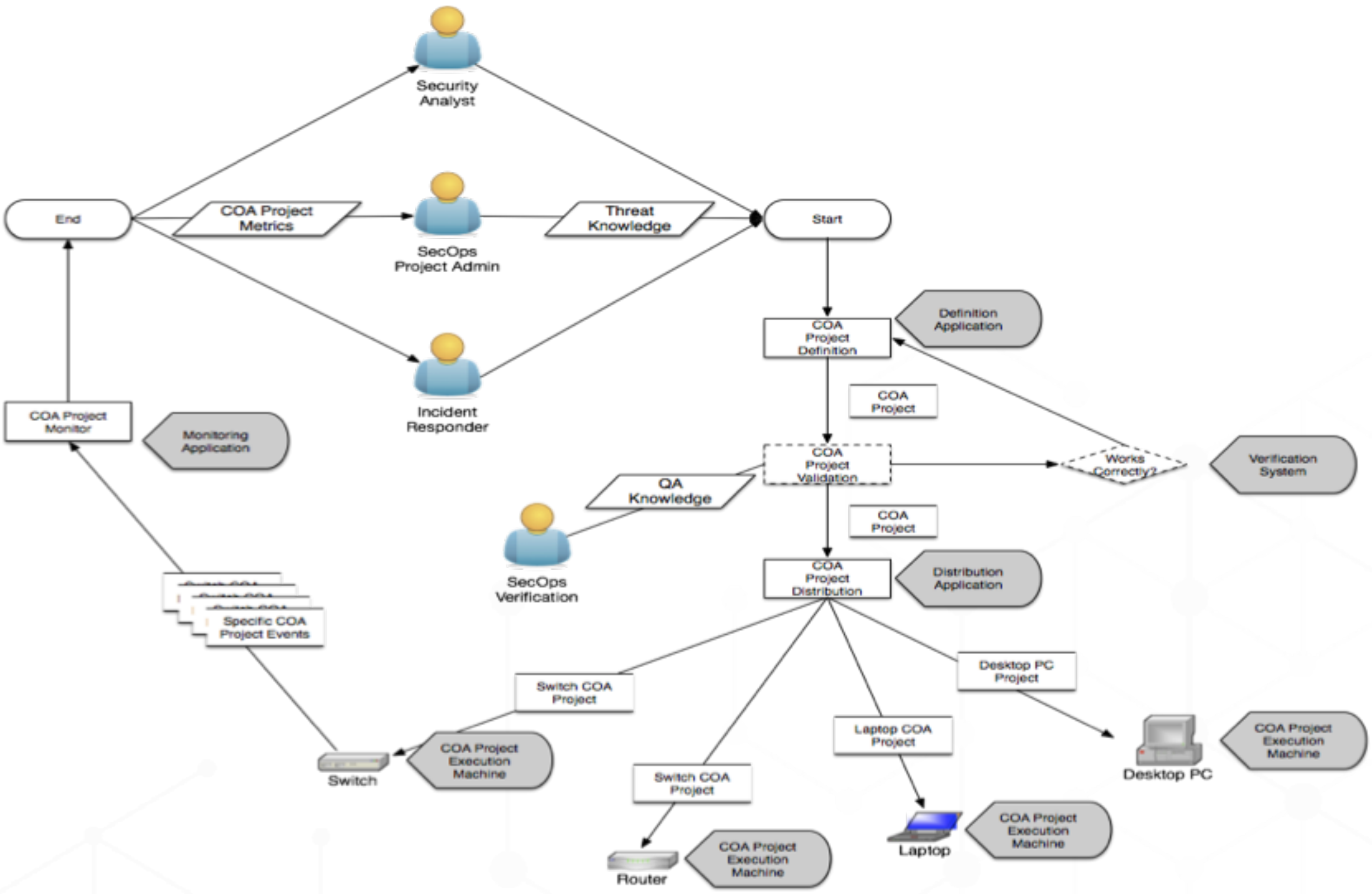
Execution

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

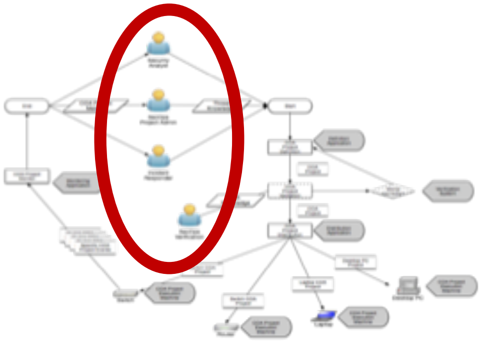
Monitoring

- Where a COA Project execution is monitored and metrics are determined on the COA Project to enable further refinement or improvement to the COA Project definition

CACAO High Level Architecture



CACAO Actors



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 COA Projects themselves or review/refine COA Projects 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

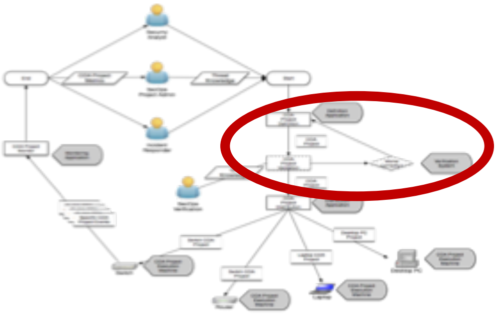
CACAO Project Elements

- One or more **Element Triggers** that would initiate a COA Project being executed
  - A **Element Trigger** may be
    - a network packet
    - a network session state
    - A file registry value
    - A memory state
    - A user event and associated identity
    - a time (absolute or interval)
    - or a combination of all the above

- One or more **Element Steps** defined within the COA Project that encapsulates the response to the threats they wish the COA Project should be responding to

- One or more **Element Outputs** that are provided as the COA Project is executed in the enterprise

CACAO Verification Step

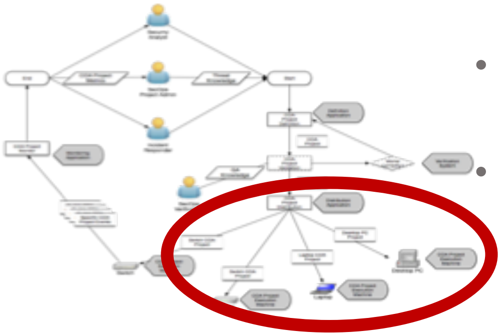


- Ability for an actor who has created or updated a COA Project Definition to **validate** that the project will **execute correctly** once deployed in an operational environment

- Key verifications
  - All COA Project Sequence Elements are connected so that the complete sequence will complete when executed
  - All COA Project Conditional Elements have connections to defined COA Project Steps
  - Each COA Project Step is well-formed and parses correctly according to the COA Project JSON schema

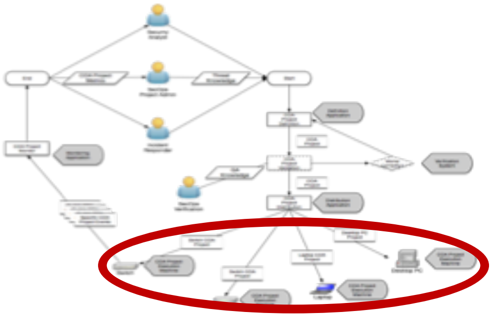
- More advanced verification may take place but those advanced verification processes are considered out of scope for this specification

CACAO Distribution



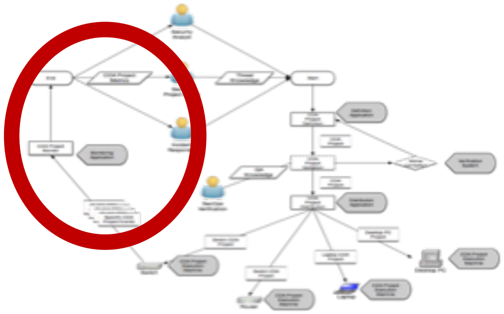
- A COA Project is deployed to an operational environment after the COA Project has been defined & verified
- Requires the following:
  - One Source distribution system (and associated actor) that executes the **COA Distribution Application**
  - One or more COA Execution systems that execute the **COA Project Execution Machine**
  - One or more COA Distribution protocols, including associated authentication and authorization methods that provides a secure transport of the COA Project between the COA Distribution Application and the COA Project Execution Machines
- The COA Distribution Application has the following functional requirements
  - It must support and track distribution of the COA Project Definition such that it can identify both successful and unsuccessful deployment of the COA Project
  - It must be able to parse a COA Project and determine which COA Project Execution systems are required to have the COA Project pushed to them
  - It must support all COA Distribution protocols required to distribute a COA Project to all specified systems required to execute that project
  - It must be able to detect and report on errors found as part of the distribution process

CACAO Execution



- COA Project Execution Machine executes one or more Elements of the project
- The COA Project Execution Machine has the following functional requirements
  - It must support at least one COA Distribution protocols to be able to receive COA Projects
  - It must support at least one COA Event Reporting protocols to be able to send COA Project execution status and events
  - It must support ability to parse received COA Projects and determine if that project can be executed correctly on the local machine
- A COA Project Execution Machine can run on any network-connected compute device such as (not limited to): laptop, server, iot sensor, network switch, router, firewall, ids, phone.

CACAO Monitoring



- COA Monitoring captures logs, data, statistics related to the COA Project execution across all systems

- The COA Project Monitoring has the following functional requirements
  - It must support at least one COA Event Reporting protocol to be able to receive COA Project execution status and events
  - It must be able to provide reports back to operations and analysts defining the COA Projects to allow refinement of the COA Project definition and verification steps

- A COA Project Monitoring system can run on any network-connected compute device such as (not limited to): laptop, server, iot sensor, network switch, router, firewall, ids, phone.

Next Steps

Next Steps (Proposed)

- Identify additional use cases
- Update Requirements
- Update Architecture
- Define
  - Schema
  - Interfaces
  - Behaviors

Getting Involved

- Bangkok IETF
  - Meetup 6th Nov (Tue) 5pm
  - Pagoda (4th floor)

- Prague IETF
  - tbd

- Subscribe to List
  - https://www.ietf.org/mailman/listinfo/Cacao

- Email List
  - cacao@ietf.org

- Draft Document
  - https://datatracker.ietf.org/doc/draft-jordan-cacao-introduction/

Thank You