CACA0 Introduction
(https://www.ietf.org/mailman/listinfo/Cacao)

Bret Jordan
November 04, 2018
What is CACAO?

- **Collaborative Automated Course of Action Operations 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

• Defense
  - Manual, reactive, and siloed
  - 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
Core Requirements

- Multiple Actions
- Sequencing of Actions
- Temporal Logic
- Conditional Logic
- System Integration

- Reporting
- Versioning
- System Targeting
- Security
- Transport
Collaboration Example - Industry Wide Response

Signed by FS-ISAC

Signed by Bank 2

Signed by Bank 1

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