CACA O Introduction - HotRFC
IETF 104 Prague
Sunday, March 24th, 2019

Bret Jordan
Allan Thomson
Jyoti Verma
Introduction

• Collaborative Automated Course of Action Operations for Cyber Security

• Mailing List: cacao@ietf.org
  – https://www.ietf.org/mailman/listinfo/

• CACAO Draft: draft-jordan-cacao-introduction-00

• BoF: Friday 9:30 - 10:00 in Berlin/Brussels
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 and standards-based machine-readable operational behavior 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 - Why we need CACAO
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

• 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.
  
  – CACAO will try and make use of other standards from the IETF and other SDOs
What are Playbooks?

- 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 Industry 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 Enterprise 1
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
BoF: Friday 9:30 - 10:00
Berlin/Brussels