Collaborative Automated Course of Action Operations (CACAO)

Technical Committee

•••

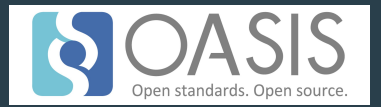
First TC Meeting

2019-09-04 - 11:00 US-Eastern

OASIS
Open standards. Open source.

IPR Mode

This TC will operate under the Non-Assertion IPR mode as defined in Section 10.3 of the OASIS IPR Policy document.



Agenda

- Call to Order and Welcome
- Volunteer for Note Taking
- Roll Call
- OASIS Admin
  - Nominations for Chair/Co-Chairs.
  - Election of Chair or Co-Chairs
  - Welcome from OASIS Staff
  - CACAO Overview
- Review of the TC Charter
- Other Business
  - Discussion of Contributed Work
  - Adoption of Standing Rules
  - Assignment of Other Responsibilities
  - Ongoing Meeting Schedule
  - Any other business
- Adjourn

OASIS
Open standards. Open source.

Roll Call

1) Verbally identify your name

2) Verbally identify your organization that you represent

To participate in this TC your organization must be an OASIS member

OASIS
Open standards. Open source.

Nominations & Elections

Nominations for Chair/Co-Chair

Election

OASIS
Open standards. Open source.

OASIS Welcome

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

OASIS
Open standards. Open source.

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

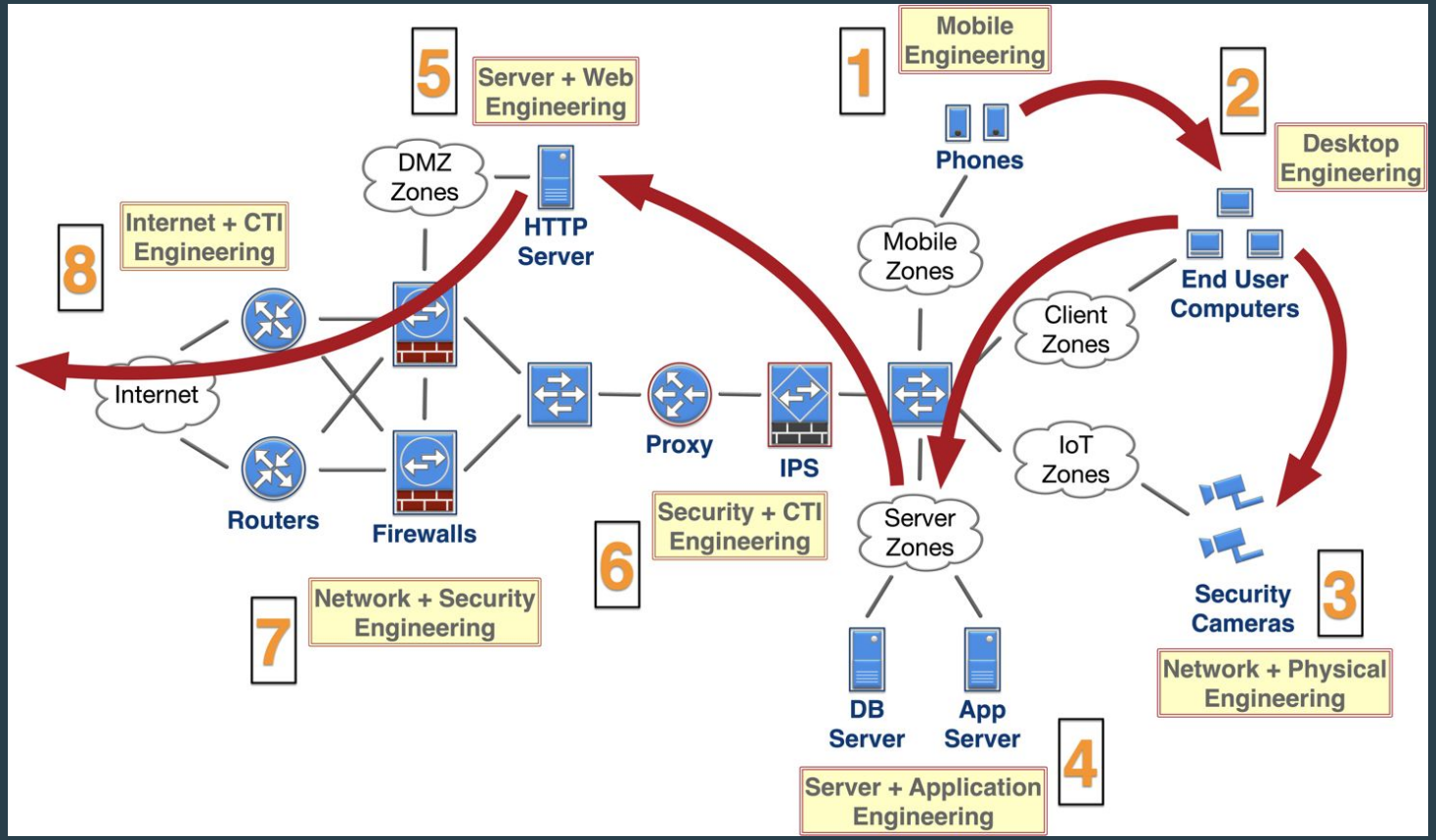
OASIS
Open standards. Open source.

Playbooks Can Span Groups & Technologies

- Different functional roles are often needed to respond to an attack
  - SOC / NOC / Network Support / Desktop Support / Mobile Support / Application Support
- Attacks can span business units, geolocations, and enclaves
- Attacks can target an entire industry sector or large organization requiring coordinated response
- Attacks can occur across multiple technologies in the same campaign and/or intrusion

OASIS
Open standards. Open source.

Problem & Pain Points – Why we need CACAO



OASIS
Open standards. Open source.

Review Charter Text - Statement of Purpose

This TC will create a standard that implements the course of action playbook model for cybersecurity operations. Each type of collaborative course of action playbook, such as prevention, mitigation and remediation will consist of a sequence of cyber defense actions that can be executed by the various technological solutions that can act on those actions.

OASIS
Open standards. Open source.

Review Charter Text - Statement of Purpose (cont.)

These course of action playbooks should be referenceable by other cyber threat intelligence that provides support for related data such as threat actors, campaigns, intrusion sets, malware, attack patterns, and other adversarial techniques, tactics, and procedures.

This TC may submit the specifications produced by this TC to other standards bodies (e.g., ITU-T, ETSI) for additional ratification.

OASIS
Open standards. Open source.

Review Charter Text - Scope of Work

This solution will specifically enable:

1) The creation and documentation of course of action playbooks in a structured machine-readable format

2) Organizations to digitally sign course of action playbooks

3) The securely sharing and distribution of course of action playbooks across organizational boundaries and technological solutions

4) The creation and documentation of processing instructions for course of action playbooks in a machine readable format

OASIS
Open standards. Open source.

Review Charter Text - Scope of Work (cont.)

It is out of scope of the TC to define or recommend actual investigation, detection, prevention, mitigation, and remediation steps for a given specific threat (e.g., defining how to remediate Fuzzy Panda on Windows™ 10). The TC will not consider how shared actions are operationalized on specific systems, except where it is necessary for those actions to interact with the playbook including the response expected for a specific action or step.

OASIS
Open standards. Open source.

Review Charter Text - Deliverables

This TC has the following major goals and deliverables:

1) CACAO Use Cases and Requirements

2) CACAO Functional Architecture: Roles and Interfaces

3) CACAO Protocol Specification

4) CACAO Data Model

5) CACAO Interoperability Test Documents

OASIS
Open standards. Open source.

Suggested TC Working Model

- The cyber security industry is a quickly evolving space - we can not afford complacent or slow-moving standards work to occur
- Lessons Learned from other standards to embrace in CACAO TC
  - Our industry can not afford to take years to define specs and implementations
  - We should not specify anything without validating with implementations or robust practice-based support for a feature
  - Weight and prioritize according to core use cases that most of the industry require
  - Let perfection not be the enemy of **good enough**
  - **Interoperability is key to success of standards**

OASIS
Open standards. Open source.

Proposed Agenda for 1st Working Meeting

Review existing CACAO use cases and requirements

Capture any additional use cases and requirements

If you have any contributions please send them to the list:

cacao@lists.oasis-open.org

OASIS
Open standards. Open source.

Other Business

Discussion of contributing work

Adoption of any standing rules

Other roles and positions in the TC (Secretary)

Ongoing Meeting Schedule

- Every other Tuesday at 11:00 US-Eastern (voting rights)

Other Business

OASIS
Open standards. Open source.

Requirements - 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

OASIS
Open standards. Open source.

Requirements - 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

OASIS
Open standards. Open source.

Requirements - 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

OASIS
Open standards. Open source.

Requirements - Versioning and Targeting

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

OASIS
Open standards. Open source.

Requirements - Use Cases and Testing

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

OASIS
Open standards. Open source.

Requirements - 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

OASIS
Open standards. Open source.

Requirements - 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

OASIS
Open standards. Open source.

Requirements - 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

OASIS
Open standards. Open source.

Requirements - 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

OASIS
Open standards. Open source.