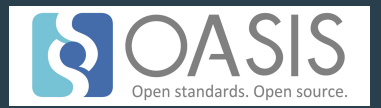
# Collaborative Automated Course of Action Operations (CACAO)

## Technical Committee

•••

TC Working Meeting
2019-09-17 - 11:00 US-Eastern



# IPR Mode

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

# Agenda

Administrivia

External Events

Discuss Requirements

# Administrivia

Excuse Allan

Welcome new secretaries

- Emily Ratliff (IBM)
- Lior Kolnik (Palo Alto Networks)
- Vasileios Mavroeidis (University of Oslo)

These meetings count for voting right

# External Events

Update on ITU Telecom World Meeting

Borderless Cyber

- Washington DC
- October 8-10th

# Discuss Requirements

# 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

# 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

# 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

# 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

# Requirements - Use Cases and Testing

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

# 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

# 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

# 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

# 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

# Wrap Up

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

cacao@lists.oasis-open.org