

IETF  
Internet-Draft  
Intended status: Informational  
Expires: August 4, 2019

B. Jordan  
Symantec Corporation  
A. Thomson  
LookingGlass Cyber  
J. Verma  
Cisco Systems  
January 31, 2019

Collaborative Automated Course of Action Operations (CACAO) for Cyber  
Security  
draft-jordan-cacao-charter-03

Abstract

This is the charter for the Working Group: Collaborative Automated  
Course of Action Operations (CACAO) for Cyber Security

Status of This Memo

This Internet-Draft is submitted in full conformance with the  
provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering  
Task Force (IETF). Note that other groups may also distribute  
working documents as Internet-Drafts. The list of current Internet-  
Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months  
and may be updated, replaced, or obsoleted by other documents at any  
time. It is inappropriate to use Internet-Drafts as reference  
material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 4, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the  
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal  
Provisions Relating to IETF Documents  
(<https://trustee.ietf.org/license-info>) in effect on the date of  
publication of this document. Please review these documents  
carefully, as they describe your rights and restrictions with respect  
to this document. Code Components extracted from this document must  
include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Goals and Deliverables . . . . .	3
Authors' Addresses . . . . .	4

## 1. Introduction

To defend against threat actors and their tactics, techniques, and procedures, organizations need to manually identify, create, and document prevention, mitigation, and remediation steps. These steps when grouped together into a course of action (COA) / playbook are used to protect systems, networks, data, and users. The problem is, once these steps have been created there is no standardized and structured way to document them, verify they were correctly executed, or easily share them across organizational boundaries and technology stacks.

This working group will create a standard that implements the playbook model based on current industry best practices for cybersecurity.

This solution will specifically enable:

1. the creation and documentation of COAs in a structured machine-readable format
2. organizations to perform attestations on COAs
3. the sharing and distribution of COAs across organizational boundaries and technology stacks
4. the verification of deployed COAs.

This solution will contain (at a minimum) a standard JSON based data model, a defined set of functional capabilities and associated interfaces, and a mandatory to implement protocol. This solution will also provide a data model for actuators to confirm the status of the COA execution, however, it will be agnostic of how the COA is implemented by the actuator.

Each collaborative course of action will consist of a sequence of cyber defense actions that can be executed by the various systems that can act on those actions. Further, these COAs will be coordinated and deployed across heterogeneous cyber security systems

such that both the actions requested and the resultant outcomes may be verified. These COA actions will be referenceable in a connected data structure like the OASIS STIX V2 model that provides support for connected data such as threat actors, campaigns, intrusion sets, malware, attack patterns, and other adversarial techniques, tactics, and procedures (TTPs).

Where possible the working group will consider existing efforts, like OASIS OpenC2 and IETF I2NSF that define the atomic actions to be included in a process or sequence. The working group will not consider how shared actions are used/enforced, except where a response is expected for a specific action or step.

## 2. Goals and Deliverables

This working group has the following major goals and deliverables. Some of the deliverables may be published through the IETF RFC stream as informational or standards track documents.

- o CACAO Use Cases and Requirements
  - \* Specify the use cases and requirements
- o CACAO Functional Architecture: Roles and Interfaces
  - \* Specify the system functions and roles that are needed to enable Collaborative Courses of Action
- o CACAO Protocol Specification
  - \* Specify and standardize the configuration for at least one protocol that can be used to distribute courses of action in both a direct delivery and publish-subscribe method
- o CACAO Distribution and Response Application Layer Protocol
  - \* Identify and document the requirements to effectively report and alert on the deployment of CACAO actions and the potential threat response to those actions
- o CACAO JSON Data Model
  - \* Create a JSON data model that can capture and enable collaborative courses of action
- o CACAO Interoperability Test Documents

- \* Define and create a series of tests and documents to assist with interoperability of the various systems involved.

The working group may decide to not publish the use cases and requirements and test documents as RFCs. That decision will be made during the lifetime of the working group.

#### Authors' Addresses

Bret Jordan  
Symantec Corporation  
350 Ellis Street  
Mountain View CA 94043  
USA

Email: [bret\\_jordan@symantec.com](mailto:bret_jordan@symantec.com)

Allan Thomson  
LookingGlass Cyber  
10740 Parkridge Blvd, Suite 200  
Reston VA 20191  
USA

Email: [athomson@lookingglasscyber.com](mailto:athomson@lookingglasscyber.com)

Jyoti Verma  
Cisco Systems  
170 West Tasman Dr.  
San Jose CA 95134  
USA

Email: [jyoverma@cisco.com](mailto:jyoverma@cisco.com)

IETF  
Internet-Draft  
Intended status: Informational  
Expires: December 22, 2019

B. Jordan  
Symantec Corporation  
A. Thomson  
LookingGlass Cyber  
J. Verma  
Cisco Systems  
June 20, 2019

Collaborative Automated Course of Action Operations (CACAO) for Cyber  
Security  
draft-jordan-cacao-charter-06

Abstract

This is the charter for the Working Group: Collaborative Automated  
Course of Action Operations (CACAO) for Cyber Security

Status of This Memo

This Internet-Draft is submitted in full conformance with the  
provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering  
Task Force (IETF). Note that other groups may also distribute  
working documents as Internet-Drafts. The list of current Internet-  
Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months  
and may be updated, replaced, or obsoleted by other documents at any  
time. It is inappropriate to use Internet-Drafts as reference  
material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 22, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the  
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal  
Provisions Relating to IETF Documents  
(<https://trustee.ietf.org/license-info>) in effect on the date of  
publication of this document. Please review these documents  
carefully, as they describe your rights and restrictions with respect  
to this document. Code Components extracted from this document must  
include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Goals and Deliverables . . . . .	3
Authors' Addresses . . . . .	4

## 1. Introduction

To defend against threat actors and their tactics, techniques, and procedures, organizations need to manually identify, create, and document prevention, mitigation, and remediation steps. These steps when grouped together into a course of action playbook are used to protect systems, networks, data, and users. The problem is, once these steps have been created there is no standardized and structured way to document them or easily share them across organizational boundaries and technological solutions.

This working group will create a standard that implements the course of action playbook model for cybersecurity operations. Each collaborative course of action, such as recommended prevention, mitigation and remediation steps, will consist of a sequence of cyber defense actions that can be executed by the various systems that can act on those actions. These courses of actions 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.

It is out of scope of the WG to define or recommend actual investigation, detection, prevention, mitigation, and remediation steps for a given threat. The working group 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.

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

.

This solution will contain at a minimum a data model that can be used to specify course of action playbooks; a defined set of functional capabilities and associated interfaces; and an exchange protocol between products. Where possible the working group may reuse and/or reference existing data models, like OASIS OpenC2 and other IETF standards (e.g., NETCONF, RESTCONF, DOTS, I2NSF, etc.) that define the atomic actions of a course of action playbook.

## 2. Goals and Deliverables

This working group has the following major goals and deliverables

- o CACAO Use Cases and Requirements
  - \* Specify the use cases and requirements
- o CACAO Functional Architecture: Roles and Interfaces
  - \* Specify the system functions and roles that are needed to enable Collaborative Courses of Action
- o CACAO Protocol Specification
  - \* Identify and standardize the configuration for at least one protocol that can be used to distribute course of action playbooks over the interfaces identified in the CACAO functional architecture. The WG may choose to use one or more protocols to address the requirements of both a direct delivery and publish-subscribe method
- o CACAO JSON Data Model
  - \* Create a JSON data model that can capture and enable collaborative courses of action
- o CACAO Interoperability Test Documents
  - \* Define and create a series of tests and documents to assist with interoperability of the various systems involved.

The working group may decide to not publish the use cases and requirements; and test documents. That decision will be made during the lifetime of the working group.

Authors' Addresses

Bret Jordan  
Symantec Corporation  
350 Ellis Street  
Mountain View CA 94043  
USA

Email: [bret\\_jordan@symantec.com](mailto:bret_jordan@symantec.com)

Allan Thomson  
LookingGlass Cyber  
10740 Parkridge Blvd, Suite 200  
Reston VA 20191  
USA

Email: [athomson@lookingglasscyber.com](mailto:athomson@lookingglasscyber.com)

Jyoti Verma  
Cisco Systems  
170 West Tasman Dr.  
San Jose CA 95134  
USA

Email: [jyoverma@cisco.com](mailto:jyoverma@cisco.com)



IETF  
Internet-Draft  
Intended status: Informational  
Expires: September 9, 2019

B. Jordan  
Symantec Corporation  
A. Thomson  
LookingGlass Cyber  
J. Verma  
Cisco Systems  
March 08, 2019

Collaborative Automated Course of Action Operations (CACAO) for Cyber  
Security  
draft-jordan-cacao-introduction-01

Abstract

This document describes the need for defining a standardized language and associated protocols to capture and automate a collection of coordinated cyber security actions and responses. This collection of actions is called a Course of Action (COA) Playbook.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 9, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Definitions . . . . .	2
2. Introduction . . . . .	3
3. Examples . . . . .	4
4. Requirements . . . . .	9
5. Architecture . . . . .	11
6. Deliverables . . . . .	12
7. IANA Considerations . . . . .	12
8. Security Considerations . . . . .	12
9. Privacy Considerations . . . . .	13
Contributors . . . . .	13
Authors' Addresses . . . . .	14

## 1. Definitions

**System:** A system is an heterogeneous set of any IT capabilities including hardware, software, endpoints (including IoT), networks, data centers and platforms with no assumptions on deployment form factor (physical, virtual, microservices), deployment scenario, geographic distribution, or dispersion.

**COA:** A Course of Action is a manual or automated action applicable to a given system or human process.

**COA Playbook:** A COA Playbook is the instantiation of a sequence of COAs that can be executed on a system or set of systems to protect it against Cyber threats and attacks.

**COA Playbook Template:** A set of high level COA actions defined by an organization on how they might respond generically to a specific threat scenario without the specific details of the threat included. Example: high level steps for mitigating or remediating malware in general.

**CACAO:** A Collaborative Automated Course of Action Operation represents a COA Playbook that can be coordinated and deployed with verified responses across a set of heterogeneous cyber security systems.

## 2. Introduction

To defend against threat actors and their tactics, techniques, and procedures, organizations need to identify, create, and document prevention, mitigation, and remediation steps. These steps when grouped together into a course of action (COA) Playbook are used to protect systems, networks, data, and users. The problem is, once these steps have been created there is no standardized and structured way to document them, verify they were correctly executed, or easily share them across organizational boundaries and technology stacks.

A COA Playbook with automated steps would enable system and network operators to respond to incidents in machine relevant time.

While some attacks may be well known to certain security experts and cyber researchers they are often not documented in a way that would enable automated mitigation or remediation. A documented way of describing prevention, mitigation, and remediation actions is critical for cyber defenders to respond more quickly and reduce the exposure from an attack.

In a similar manner, this will allow organizations to prevalidate the course of actions and potentially simulate the course of actions and understand their implications in terms of potential overall cost, revenue loss, user experience, risk of churn, risks in general, and liabilities. Indeed certain COAs might lead to radical mitigations in the system which might lead to more or less acceptable collateral damages to answer a certain cyber threat. Like at war, 'officers' responsible to engage or trigger the execution of a COA could be offered a chance to understand their options first in selecting the most appropriate COA.

While many attempts have been made over the years in the IETF and other SDOs to address certain elements of this problem space, there is currently no consolidated and standardized language or means that would allow cyber actions to be automatically coordinated, sequenced, processed and shared to enable cyber defenders to respond in machine relevant time. Some efforts such as BPMN have traditionally focused on higher-level non-cyber constructs for process definition, and other efforts like OpenC2 have focused purely on atomic actions, but none have focused on the overlay processes required for this to be used in a broader cyber security response use case.

To enable and assist cyber defense, a solution needs to be created to securely document, share, and automate the actions needed to prevent, mitigate, and remediate threats. This effort will focus on providing an information model, data serialization, and transport for defining,

sharing, and processing Collaborative Automated Course of Action Operations (CACAO).

Every COA Playbook will consist of a sequence of cyber defense actions that can be coordinated and deployed with verified responses across a set of heterogeneous cyber security systems. The primary focus will be on the definition of the higher level sequence of actions (perhaps a tree or graph) and where possible we will leverage existing efforts that may define the atomic actions to be included in a process or sequence.

A key use of CACAO is to enable more senior cyber defenders to document and share detailed step by step actions and solutions for a given threat that can be deployed en masse across heterogeneous system and network solutions. It also enables less experienced or junior personnel to have greater confidence in their efforts to defend their networks based on shared COA Playbooks defined by other organizations and other experts in the field of cyber security. These suggested steps, that may be executed automatically, provided by the senior personnel can also help guide the junior personnel in the correct ways to handle a variety of the security response without requiring senior personnel being involved.

This effort is intended to define a way for chaining atomic security actions together. The atomic actions themselves could be formed from a variety of languages such as STIX COA; OpenC2; Cisco IOS; Juniper JunOS....etc.

This effort will primarily focus on defining a semantic representation and information model to allow the construction of a COA Playbook. Our secondary focus will be on defining a serialization and transport protocol to enable COA Playbooks to be used between systems.

### 3. Examples

The following 2 simplified examples explain CACAOs that are written in pseudo programmatic terms to explain how the COA Playbook contains both human and machine defined actions that are executed in response to a threat. For each COA Playbook, the initial trigger event is defined and then followed by a set of COAs that can be sequential, conditional-based-flow, or a combination of both.

**Example 1: Infected Host Mitigation COA Playbook** This example defines the COA Playbook for an organization to respond to threat detection on a host within their internal network after a specific type of threat has been detected on the host. The playbook defines both machine and human steps to describe the mitigation response.

BEGIN-PLAYBOOK

Playbook-Name: InfectedHostMitigation1

Playbook-Trigger-Event:

- o Indicator indicator-8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f defines a command and control server based on CIDR 192.0.2.x that has been communicated to and from the host 198.51.100.12.
- o A trigger event may be defined in STIX2
- o A trigger defines an entry point into the playbook steps as follows.

BEGIN-COAs

COA:

- o Id: 1
- o Type: Human
  - \* Question: Ask the user whether they wish to review the mitigation procedures before proceeding?
  - \* Answer-Y-or-N
    - + If Y: Proceed to Id: 2
    - + If N: Proceed to Id: 3

COA:

- o Id: 2
- o Type: Human
  - \* Operation: Display mitigation procedures.

COA:

- o Id:3
- o Type: Machine
  - \* Operation: Vlan-Move

- \* Variable: "HostVLANID ="infected-host.vlan
- \* Target: \$\$infected-host
- \* Destination: Quarantine VLAN ID

COA:

- o Id:4
- o Type: Machine
  - \* Operation: Host-Image
  - \* Target: \$\$infected-host
  - \* ImageName: Windows-Good-Image1

COA:

- o Id:5
- o Type: Machine
  - \* Operation: Vlan-Move
  - \* Target: \$\$infected-host
  - \* Destination: \$\$HostVLANID

END-COAs

END-PLAYBOOK

Example 2: Find and Remove Malware COA Playbook This example describes a COA Playbook for an organization to find malware and then if found to remove the malware from an infected host. The playbook defines a more complicated sequence of machine instructions as identified by the MACHINE-SEQUENCE operation in COA-Id{4}.

BEGIN-PLAYBOOK

Playbook-Name: FindRemoveMalware1

Playbook-Trigger-Event:

- o Indicator indicator-8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f defines a malware hash \$\$inserthash that is known to identify a specific malware file if found on a host system
- o A trigger event may be defined in STIX2
- o A trigger defines an entry point into the playbook steps as follows.

BEGIN-COAs

COA:

- o Id: 1
- o Type: Human
  - \* Question: Ask the user whether they wish to review the mitigation procedures before proceeding?
  - \* Answer-Y-or-N
    - + If Y: Proceed to Id: 2
    - + If N: Proceed to Id: 3

COA:

- o Id: 2
- o Type: Human
  - \* Operation: Display mitigation procedures.

COA:

- o Id:3
- o Type: Machine
  - \* Operation: Vlan-Move
  - \* Variable: "HostVLANID ="infected-host.vlan
  - \* Target: \$\$infected-host
  - \* Destination: Quarantine VLAN ID

COA:

- o Id:4
- o Type: Machine-Sequence {
  - \* Delete run at start reg keys and triggers
  - \* Reboot into SafeMode
  - \* Kill process 3 then 1 then 2
  - \* Delete temp files
  - \* Delete compromised files from the system
  - \* Delete other Reg keys
  - \* Reboot system in to safe mode
  - \* Verify processes do not restart
  - \* Patch AV system
  - \* Run updated AV scan
  - \* Patch OS
  - \* Run additional on-demand special AV scanners
  - \* Reboot system to normal mode }
  - \* Target: \$\$infected-host

COA:

- o Id:5
- o Type: Machine
  - \* Operation: Vlan-Move
  - \* Target: \$\$infected-host
  - \* Destination: \$\$HostVLANID

END-COAs



## END-PLAYBOOK

## 4. Requirements

Below is a list of high level requirements that this effort needs to address.

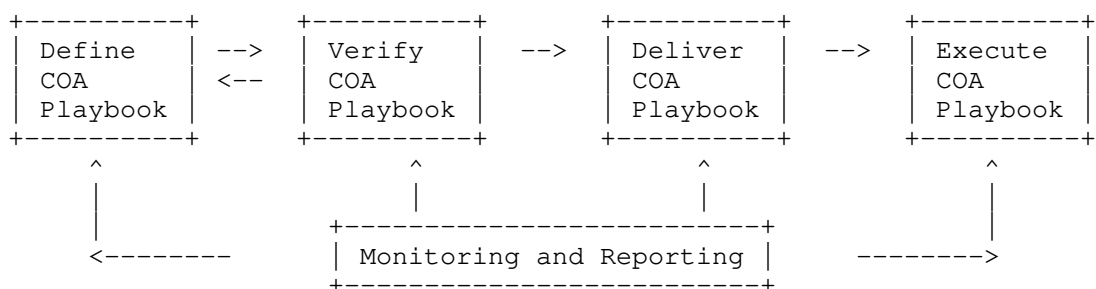
- o **Multiple Actions:** The solution needs to support the ability to describe one or more actions that can be processed in a batch manner or as-a-group.
- o **Data Protection, Integrity and Authentication (Rules for data in motion and at rest):** All requests and responses must be confidential and therefore a secure protocol should be used to convey these messages such as TLS (but not limited to). The COA Playbooks and actions must be able to be encrypted (and optionally signed) to ensure integrity and that they are only accessible by authenticated and authorized users.
- o **Globally Unique Identifiers:** All transactions (requests, responses, and notifications) need to be able to be tracked, monitored, and recorded for security and operational reasons, including the ability to backout failed actions. This means responses and notifications need a way to be tied back to the original request. Globally unique identifiers apply to both the COA Playbook and the COAs within the playbook. All transactions tracked, monitored and recorded will be restricted to the same management zone as the systems initiating the transactions and operating on the results. All systems operating in that management zone will support a common and agreed set of privacy associated with those transactions such that no concerns over loss of privacy or unexpected data exposure occurs.
- o **Reporting:** Provide the ability to gather single and batch reports of events for responses. All report events must have a timestamp, identifier of original request or rule causing event, and option for a full dump of matching data (network, endpoint config....etc) to be included in the event record. The report could be either synchronously requested or be an asynchronous event (syslog) with periodic updates.
- o **Sequences of Atomic Actions:** The ability to define an ordered list of atomic actions that must be executed as a combined set rather than as a sequence.
- o **Projects & Project Templates:** These should support actions for machine automation, human actions / intervention, and high level conceptual actions.

- o Customization: Provide the option to include custom actions in a batch or set of atomic actions.
- o Conditional Logic: This solution needs the ability to include action sequences that can support conditional logic, logical and comparative operators, and behavioral logic.
- o Project Testing: Ability to support what-if deployments where a defined COA Playbooks can be verified before deploying to a real system or environment, and perhaps be able to identify all the organizations that have tested it and verified it.
- o Auditability: The solution needs the ability to provide full confirmation (tracking and logging) of each COA at every transaction state.
- o Digital Signature Chain / Attribution with Identified Signed Topic: The solution needs the ability to track multiple digital signatures to show a chain of trust where it identifies the specific Signed Topic that is being signed. This solution should also support multiple independent organizations signing and verifying the correctness, accuracy, and validity of the COA Playbook or individual COA where the Signed Topic being signed by that independent entity is specified.
- o Input: One or more technical indicators, prioritization indicators, and rule names (optional).
- o Transport Methods: This solution needs to support the ability for clients to send COAs directly to an end device (request/response) and also to a communications channel (publish/subscribe).
- o Versioning: The solution needs to support both incremental versioning and semantic versioning, along with assertions that the COA works with certain products. This will enable support of multiple versions of a COA across products so that not all systems are required to be the same version to implement COA Playbooks. Newer COA Playbooks will provide information that allows consumers to relate the new version to prior versions.
- o Transactions: Needs the ability for systems to have the option to support both atomic and non-atomic transactions.
- o System Targeting: The solution needs the ability to identify the type, version, patch level of one or more systems that this COA is applicable for.

- o **Project Versioning:** Need ability to version (and track) COA Playbooks and Templates
- o **Data Markings:** Need ability to support data marking at a COA Playbook level such as the Traffic Light Protocol (TLP) for the project.
- o **Command and Control Management Separation (Definition vs Execution Environment):** A COA Playbook (and the contained atomic COAs) may be defined in one system by one or more authors, but the COA Playbook may be executed in an operational environment where the systems and users of those systems have different authentication and authorizations for the COA. In order for the COA Playbook to execute correctly it must have authorization in the operational environment where it is executed. Therefore the credentials of the authors should not be relied upon to execute correctly in the execution environment. Also, the security environment executing the COA Playbook will likely be different from where the COA Playbook was defined.
- o **Integration:** Ensure that COA Playbooks can be used in and work with existing threat intelligence data models, for example STIX.
- o **Flexibility:** Allow the COA Playbook to benefit and leverage existing capabilities available in 'the system' such as atomic ways to exchange security commands 'a la openc2', or read from available security capabilities in a standard way 'a la i2nsf' to understand what it can actually do or to allow conditional COA sequences

## 5. Architecture

A Collaborative Course of Action workflow will consist of several components, including at least:



- o Define: Where a COA Playbook is defined based on various inputs both automated and manually derived.
- o Verify: Where a COA Playbook is reviewed for accuracy, correctness, and is properly defined to execute correctly in a target environment without making any changes to the target environment.
- o Deliver: Where a COA Playbook is distributed to the systems that will execute the COA Playbook. Distribution includes checking that the COA Playbook has been deployed correctly and has followed the rules defined within the project for atomic transactions.
- o Execute: Where a COA Playbook is evaluated by one or more security infrastructure systems and execution events are communicated to the COA Playbook monitoring step. It can run either in full execution or in verification mode.
- o Monitoring: Where a COA Playbook execution is monitored and metrics are determined on the COA Playbook to enable further refinement or improvement to the COA Playbook definition.

## 6. Deliverables

This effort will need to produce and deliver the following documents:

1. An overview and architecture document
2. A COA Playbook data model in JSON / CBOR
3. Define how COA Playbooks will be distributed between each system within the process including leveraging existing transport mechanisms and any new APIs/Protocols required.

## 7. IANA Considerations

This memo includes no request to IANA.

## 8. Security Considerations

The solution described by this document provides a mechanism to define a series of actions that can be applied to a network or host system to prevent, mitigate, or remediate some threat. Discussion is needed about how to protect such a mechanism and the information it is managing from unauthorized access or disclosure.

In a principle of "who guards the guards" ("quis custodiet Ipsos custodes" Juvenal, Satire VI, lines 347-348) it is essential to armor

the COA service against itself and to consider a COA-SELF project for consistency and coherency where the target system of the COA is the COA service itself.

A breach in the COA service would break the integrity of an entire target system, potentially at extra large scale.

## 9. Privacy Considerations

Discussion is also needed about privacy considerations around how the endpoint devices and systems are identified and to ensure that any commands are encoded in a safe way and if the COA Playbook needs to collect private data it is still compliant to privacy regulations and offers all the mechanisms to guarantee compliance to such frameworks such as auditability, security, encryption, right to be forgotten, consents, etc.

### Contributors

- o Allen Hadden  
IBM  
ahadden@us.ibm.com
- o David Waltermire  
NIST  
david.waltermire@nist.gov
- o Efrain Ortiz  
Symantec  
efrain\_ortiz@symantec.com
- o Jason Keirstead  
IBM  
jason.keirstead@ca.ibm.com
- o Jason Webb  
LookingGlass Cyber  
jwebb@lookingglasscyber.com
- o Kyle Mackenzie  
JPMC  
Mackenzie.kyle@jpmorgan.com
- o Subodh Kumar  
JPMC  
subodh.kumar@jpmorgan.com
- o Swaroop Pradhan

JPMC  
swaroop.s.pradhan@jpmorgan.com

- o Vivek Jain  
JPMC  
vivek.jain@jpmchase.com

#### Authors' Addresses

Bret Jordan  
Symantec Corporation  
350 Ellis Street  
Mountain View CA 94043  
USA

Email: [bret\\_jordan@symantec.com](mailto:bret_jordan@symantec.com)

Allan Thomson  
LookingGlass Cyber  
10740 Parkridge Blvd, Suite 200  
Reston VA 20191  
USA

Email: [athomson@lookingglasscyber.com](mailto:athomson@lookingglasscyber.com)

Jyoti Verma  
Cisco Systems  
170 West Tasman Dr.  
San Jose CA 95134  
USA

Email: [jyoverma@cisco.com](mailto:jyoverma@cisco.com)