IETF
Internet-Draft
Intended status: Informational
Expires: November 3, 2019

B. Jordan
Symantec Corporation
A. Thomson
LookingGlass Cyber
J. Verma
Cisco Systems
May 02, 2019

Collaborative Automated Course of Action Operations (CACAO) for Cyber Security
draft-jordan-cacao-charter-04

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 November 3, 2019.

Table of Contents

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 for cybersecurity operations.

This solution will specifically enable:

1. the creation and documentation of COAs in a structured machine-readable format

2. organizations to perform attestation including verification and authentication on COAs

3. the sharing and distribution of COAs across organizational boundaries and technology stacks that may include protocols, apis, interfaces and other related technology to support sharing.

4. the verification of COA correctness prior to deployment.

5. the monitoring of COA activity after successful deployment.

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

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. 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 data structure like the OASIS STIX V2 model that provides support for related data such as threat actors, campaigns, intrusion sets, malware, attack patterns, and other adversarial techniques, tactics, and procedures.

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

- CACAO Use Cases and Requirements
  - Specify the use cases and requirements
- CACAO Functional Architecture: Roles and Interfaces
  - Specify the system functions and roles that are needed to enable Collaborative Courses of Action
- 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
- CACAO Distribution and Response Application Layer Protocol
  - Specify the protocol which may include apis, interfaces and other related technology to support the requirements identified for the protocol.
- CACAO JSON Data Model
  - Create a JSON data model that can capture and enable collaborative courses of action
- 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

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

Email: athomson@lookingglasscyber.com

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

Email: jyoverma@cisco.com