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.

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 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

- 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
  - 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
- 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