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

Abstract

This is the charter for the Working Group: Collaborative Automated Course of Action Operations (CCAO) 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 July 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.
1. Problem

Threat Actors and Intrusion Sets are advancing at an increasing rate relative to an organization’s ability to defend against and respond to cyber attacks. In addition, it is common that defenders need to manually identify and process prevention, mitigation, and remediation steps in order to protect their systems, networks, data, and users. There is also currently no standard means to easily and dynamically share proposed prevention, mitigation, or remediation steps and the operational experience gained from these attacks or their associated successful responses among a trusted set of organizations.

Due to the increasing sophistication and amplitude of cyber attacks the need for a secure collaborative set of systems providing coordinated detection and response across hosts, networks, and security infrastructure has raised significantly. This solution is necessary to effectively respond to threats in machine relevant time. While some attacks may be well known to certain security experts and researchers they are often not documented in a way that would enable automated prevention, mitigation, or remediation.

Key to this coordinated cyber attack response is a coordinated threat response including a standard information model; a set of functional capabilities, associated interfaces, and protocols. These key requirements would be defined in each of the system components across host; network and security infrastructure to ensure that each system can work together in a coordinated manner.

2. Working Group

To enable efficient collaboration and facilitate the rapid sharing of preventative, mitigative, and remediative actions this working group will focus on defining the set of technologies (protocols, interfaces, functional capabilities, and information model) required to detect, prevent, mitigate, and remediate threats. This solution will also define the machine-readable actions to enable an action-oriented defensive system. This effort will focus on providing the functionality requirements for each system that would participate in a coordinated threat response; the interfaces they should support including the transport mechanism used and finally the information
model across those systems to enable the coordinated actions in a structured secure manner.

Each collaborative course of action will consist of a sequence of cyber defense actions that can be executed by the various systems that those actions target. Further, these COAs can be coordinated and deployed across heterogeneous cyber security systems such that both the actions requested and the resultant outcomes may be monitored and verified. These actions will be referenceable in a connected data structure that provides support for connected data object and efficient operational use of those data objects such as Threat Actors, Campaigns, Intrusion Sets, Malware, Attack Patterns, and other adversarial techniques, tactics, and procedures (TTPs).

Where possible the working group will leverage existing efforts that _may_ 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 such a received shared action by a receiving party. It will also focus on the requirements for the correct construction and correct distribution of the structured actions and their corresponding interfaces and protocols.

3. Goals

This working group has the following major goals: * Document the use cases and requirements * Identify and document the system functions and roles that must exist with associated protocols for a coordinated threat response system to operate effectively * Identify and document the configuration for a series of protocols that can be used to distribute courses of action in both direct delivery and publish-subscribe methods * Identify and document the mechanism(s) required to monitor, report and alert on effective distribution of CACAO actions and the potential threat response to those actions * Create an information and data model that can capture and enable collaborative courses of action (sometimes called playbooks) that will be used in the coordinated threat response systems * Define and create a series of tests and documents to assist with interoperability of the various systems involved in the coordinated threat response system.

4. Deliverables

The working group plans to create informational and standards track documents, some of which may be published through the IETF RFC stream. * CACAO Use Cases and Requirements * CACAO Functional Architecture: Roles and Interfaces * CACAO Interface Specification *
The working group may decide to not publish the use cases and requirements 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

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

Email: athomson@lookingglasscyber.com