IETF
Internet-Draft
Intended status: Informational
Expires: July 6, 2019

B. Jordan
Symantec Corporation
A. Thomson
LookingGlass Cyber

January 02, 2019

Collaborative Automated Course of Action Operations (CACAO) for Cyber Security
draft-jordan-cacao-charter-00

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 July 6, 2019.

Table of Contents

1. Problem

Threat Actors and Intrusion Sets are advancing at an increasing rate relative to cyber defense. Further, cyber defenders typically have to manually identify and process prevention, mitigation, and remediation steps in order to protect their systems, networks, data, and users.

Due to this increase and sophistication of cyber attacks the need for a secure mechanism that would enable system and network operators to respond to threats in machine relevant time has raised significantly. 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 language for describing prevention, mitigation, and remediation actions is critical for cyber defenders to respond more quickly and reduce the exposure from an attack.

2. Working Group

To enable and assist cyber defense, the Collaborative Automated Course of Action Operations (CACAO) for Cyber Security working group will focus on creating a solution to securely document and share 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).

Each collaborative course of action will consist of a sequence of cyber defense actions that can be coordinated and deployed across a set of heterogeneous cyber security systems such that both the actions requested and the resultant outcomes may be monitored and verified.

The primary focus of this proposed working group will be the definition and the distribution of the sequence of actions (perhaps in a tree or graph). Where possible we will leverage existing efforts that _may_ define the atomic actions to be included in a process or sequence.

3. Goals

This working group has the following major goals: * Identify and document the use cases and requirements * Create an information and data model that can capture and enable collaborative courses of action (sometimes called playbooks) that can be used to automate some parts of cyber defense * Identify and document the system functions and roles that must exist with associated protocols to exchange information between those system functions * 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 * Define and create a series of tests and documents to assist with interoperability

4. Deliverables

The working group plans to create informational and standards track draft documents some of which may be published through the IETF RFC stream.

Within the first year, the working group aims to: * Identify a solution for capturing and distributing multiple sequenced atomic actions, whether they be manual or automated. * Publish a standards track draft solution that can be used by organizations and vendors to create and distribute Courses of Action / Playbooks.

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