---
title: Collaborative Automated Course of security Action Operations (CACAO) ~~for Cyber Security~~
abbrev: CACAO
docname: draft-jordan-cacao-charter-00
date: 2018-11-30
keyword: course of action

Commentaire [Med1]: I suggest to use « attack Defense » instead of « cyber security »
CJ: “protecting against cyber-attacks”?

ipr: trust200902
area: General
workgroup: IETF
keyword: Internet-Draft
category: info

stand_alone: yes
pi: [toc, sortrefs, symrefs]

coding: us-ascii

author:
 -
   ins: B. Jordan
   name: Bret Jordan
   organization: Symantec Corporation
   street: 350 Ellis Street
   city: Mountain View
   code: CA 94043
   country: USA
   email: bret_jordan@symantec.com
 -
   ins: A. Thomson
   name: Allan Thomson
   organization: LookingGlass Cyber
   street: 10740 Parkridge Blvd, Suite 200
   city: Reston
   code: VA 20191
   country: USA
   email: athomson@lookingglasscyber.com

Mis en forme : Français (France)

--- abstract

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

--- middle

Problem

Threat ~~Actors~~ actors and i~~I~~ntrusion ~~Sets~~ sets are advancing at an increasing rate relative to ~~cyber~~ security attacks defense (including, attack detect and mitigation). ~~Further~~Yet, ~~cyber~~ defenders who detect an attack is ongoing usually ~~typically~~ have to manually identify and process prevention, mitigation, and (candidate) remediation ~~steps~~ actions ~~in order~~ to protect their systems, networks, data, and users. Moreover, there are no standard means to easily

Commentaire [CJ2]: I don’t understand this sentence. “The diversity and the amplitude of cyber-attacks are ever increasing. But the mitigation toolkit is not progressing accordingly.”?

and dynamically share (candidate) mitigation actions and operational experience among a trusted set of network operators facing similar attacks.

Due to ~~this~~ the ~~increase~~increasing ~~, and~~ sophistication, and amplitude of ~~cyber~~ security attacks, the need for a secured collaborative mechanism that would enable system and network operators to ~~respond~~ efficiently react (or proactively act) 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~~hardly documented in a way that would enable automated mitigation or remediation. Also, new attacks may emerge and candidate mitigation actions may not be widely and promptly disseminated among networks and systems under or (being targets to) such attacks.

Commentaire [CJ3]: Not sure what a system operator is.

~~A~~ Standard data models~~documented language~~ for describing attacks, prevention and mitigation actions, ~~and~~ as well as proposed remediation actions ~~is~~ are ~~critical~~ necessary for collaborative ~~cyber~~ security defenders to respond more quickly and reduce the ~~exposure from an attack~~risk of being exposed to an attack. Distributed responses and coordination means would thus help to efficiently soften and mitigated distributed attacks at the largest scales.

# Working Group

To enable efficient collaboration and ~~assist~~facilitate the sharing of security practices among network operators for the sake of optimized, anticipating and dynamically responsive security policy enforcement ~~cyber~~ defense, the Collaborative Automated Course of security Action Operations (CACAO) ~~for Cyber Security~~ working group will focus on ~~creating~~ documenting a solution to securely ~~document and~~ share the actions needed to anticipate, prevent, mitigate, and remediate threats among trusted parties. This effort will ~~focus on providing~~include the specification of ~~an information~~a data model, data serialization, and a transport mode for ~~defining,~~ sharing, and processing ~~Collaborative Automated Course of Action Operations~~ security actions~~(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. Means to link an action with an attack will be considered.

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, the wg ~~we~~ will leverage existing efforts that *may* define the atomic actions to be included in a process or sequence. The WG won’t consider how shared actions are used/enforced by a receiving party, but will focus on the required data to be shared among trusted parties, and the companion interfaces and protocol exchanges.

Commentaire [CJ4]: Already said

Commentaire [Med5]: Not sure to understand what is meant here.

The mechanisms for sharing actions must be reliable and must be immune against mis~~ues~~use that would lead to exacerbate an attack or by introducing new attack vectors.

The WG will reuse existing protocols, wherever appropriate. Modifications to existing protocols will be achieved in coordination with the corresponding WGs.

# Goals

This working group has the following major goals:

- ~~Identify and d~~Document the use cases and requirements

- Describe a functional architecture which identifies the required functional entities and required interfaces and protocols for CACAO.
- Create ~~an information and~~a data model that can capture and enable collaborative courses of action among a set of trusted parties ~~(sometimes called playbooks)~~ that can be used to automate ~~some parts of security cyber defense~~the enforcement of appropriate security policies or the execution of proper mitigation actions
- ~~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
- Document applicability statements for some attack types (DDoS, for example).

Commentaire [Med6]: I don't understand what is meant here.

Commentaire [CJ7]: I don't get the whole sentence.

Commentaire [Med8]: Not sure this one is required. At least, I don't think an RFC is needed

# Deliverables

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

- CACAO Use Cases
- CACAO Requirements
- CACAO Functional Architecture: Roles and Interfaces
- CACAO Data Model
- CACAP Applicability Statement: The DDoS Case

The WG may decide to not publish the uses cases and requirements as RFCs. The decision will be made during the lifetime of the WG.

Within the first year, the working group aims to:

- ~~Identify~~ Describe 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~~.

Commentaire [Med9]: I'm not sure I would keep this text.