Published on *OASIS* (https://www.oasis-open.org)

Call for Participation: OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC

Submitted by censign on Sun, 2019-08-04 14:10
Type:
Call for Participation

A new OASIS technical committee is being formed. The OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security Technical Committee (TC) has been proposed by the members of OASIS listed in the charter below. The TC name, statement of purpose, scope, list of deliverables, audience, IPR mode and language specified in this proposal will constitute the TC's official charter. Submissions of technology for consideration by the TC, and the beginning of technical discussions may occur no sooner than the TC's first meeting.

The eligibility requirements for becoming a participant in the TC at the first meeting are:

(a) you must be an employee or designee of an OASIS member organization or an individual member of OASIS, and

(b) you must join the Technical Committee, which members may do by using the Roster "join group" link on the TC's web page at [a].

To be considered a voting member at the first meeting:

(a) you must join the Technical Committee at least 7 days prior to the first meeting (on or before 28 August 2019); and

(b) you must attend the first meeting of the TC, at the time and date fixed below (03 September 2019).

Participants also may join the TC at a later time. OASIS and the TC welcome all interested parties.

Non-OASIS members who wish to participate may contact us about joining OASIS [b]. In addition, the public may access the information resources maintained for each TC: a mail list archive, document repository and public comments facility, which will be linked from the TC's public home page at [c].

Please feel free to forward this announcement to any other appropriate lists. OASIS is an open standards organization; we encourage your participation.

----------?

[a] https://www.oasis-open.org/apps/org/workgroup/cacao/ [1]

[b] See http://www.oasis-open.org/join/ [2]

[c] http://www.oasis-open.org/committees/cacao/ [3]

?CALL FOR PARTICIPATION?
OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security Technical Committee Charter

The charter for this TC is as follows.

Section 1: TC Charter

(1)(a) TC Name

OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security

(1)(b) Statement of Purpose

This TC will create a standard that implements the course of action playbook model for cybersecurity operations. Each type of collaborative course of action playbook, such as prevention, mitigation, and remediation will consist of a sequence of cyber defense actions that can be executed by the various technological solutions that can act on those actions. These course of action playbooks 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.

This TC may submit the specifications produced by this TC to other standards bodies (e.g., ITU-T, ETSI) for additional ratification.

Business Benefits

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 form a course of action playbook that can be used to protect systems, networks, data, and users. The problem is, once these course of action playbooks have been created there is no standardized and structured way to document them or easily share them across organizational boundaries and technological solutions.

(1)(c) Scope

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

It is out of scope of the TC to define or recommend actual investigation, detection, prevention, mitigation, and remediation steps for a given specific threat (e.g., defining how to remediate Fuzzy Panda on Windows? 10). The TC 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.

(1)(d) Deliverables

This TC has the following major goals and deliverables

- CACAO Use Cases and Requirements

The TC will identify and document the core requirements needed to support the common use cases that are done today.

- CACAO Functional Architecture: Roles and Interfaces

The TC will specify the system functions and roles that are needed to enable collaborative courses of action playbooks.

- CACAO Protocol Specification

The TC will 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.

- CACAO Data Model

This TC will define a normative data model for CACAO using property tables similar to how the OASIS STIXv2 data model was defined. This data model will be designed to explicitly work with I-JSON and all examples will be done in JSON. The TC will also define JSON as the mandatory to implement serialization for this version of CACAO. The TC may decide to also document the data model in other non-normative forms that would be located in an appendix.

- CACAO Interoperability Test Documents

This TC will define and create a series of tests and documents to assist with interoperability of the various systems involved. These documents can be used by technological solutions adopting the CACAO course of action playbooks to help ensure that they do so in an interoperable manner. The TC will decide how best to publish these documents.

(1)(e) IPR Mode

The TC will operate under the Non-Assertion Mode of the OASIS IPR Policy.

(1)(f) Audience

Security Vendors, Incident Responders, Security Operation Centers (SOCs), Cyber Defense Centers, Threat Intelligence Analysts, Large Enterprise, Governments

(1)(g) Language

The TC will operate and publish its work in English.

(Optional References for Section 1)

https://www.lookingglasscyber.com/blog/cacao-a-future-for-collaborative-... [4]

Section 2: Additional Information

(2)(a) Identification of Similar Work

We do not know of any existing open source or open standard solutions that address security playbooks. There are several proprietary solutions that exist, but those are not shareable in an open standards way. Some solutions like BPMN exist that deal with process management for a business in XML format. However, this group does not believe that BPMN is the best solution for trying to solve the cyber security playbook problem. Some additional frameworks such as:

https://nifi.apache.org/ [5]
https://camunda.com/ [6]

may be utilized or referenced in the design of CACAO playbooks.

(2)(b) First TC Meeting

Tuesday, September 3rd, 2019 at 11:00 AM US-ET and will be done via Zoom.

(2)(c) Ongoing Meeting Schedule

The TC will plan on having bi-weekly meetings on Tuesdays at 11:00 AM US-ET.

(2)(d) TC Proposers

Colby Derodeff, FireEye - colby.derodeff@fireeye.com [7]
Allen Hadden, IBM - ahadden@us.ibm.com [8]
Ryan Hohimer, DarkLight - ryan.hohimer@darklight.ai [9]
Bret Jordan, Symantec - Bret_Jordan@symantec.com [10]
Jason Keirstead, IBM - Jason.Keirstead@ca.ibm.com [11]
Terry MacDonald, Individual - terry.macdonald@gmail.com [12]
Vasileios Mavroeidis, University of Oslo - vasileim@ifi.uio.no [13]
Shawn Riley, DarkLight - shawn.p.riley@darklight.ai [14]
Arnaud Taddei, Symantec - arnaud_taddei@symantec.com [15]
Allan Thomson, LookingGlass Cyber Solutions - athomson@lookingglasscyber.com [16]

(2)(e) Primary Representatives' Support

"DarkLight, Inc. fully supports the creation of the OASIS CACAO Technical Committee. We will actively participate in the creation of specifications to achieve intelligent, sharable, and automated courses of action.? ?

Ryan Hohimer, CTO of DarkLight, Inc.

?FireEye fully supports creation of the OASIS CACAO Technical Committee. The ability for one organization to create a playbook that can be shared and leveraged by other organizations creates a true force multiplier across the security industry. Threat actors are constantly changing their tactics and leveraging new techniques as they target organizations. By creating a standardized response framework that works with disparate technologies, security teams will be able to thwart and respond to future attempts without prior knowledge of the attack,? Paul Patrick, Chief Engineering Architect & Distinguished Engineer, FireEye.

"The ability to efficiently collaborate across vendors on incident response actions and playbooks, will fill a critical gap in the cybersecurity operations ecosystem, and enable better outcomes for our clients. IBM Security is proud to support the formation of this TC and the participation of our proposers listed above." - Jason Keirstead - Chief Architect of Threat Management, IBM Security.

?CACAO Technical Committee represents a significant opportunity to define a standard mechanism for security playbook for security operations and incident response. LookingGlass Cyber Solutions firmly supports the creation of this TC and will provide active support in creating the specifications? - Allan Thomson, CTO, LookingGlass Cyber Solutions.

?The need for automated and shareable cyber security playbooks is critical to improving operational cyber security. CACAO will enable organizations, both big and small, to prevent, mitigate, or remediate cyber threats more quickly and with greater confidence. Symantec Corporation fully supports the creation of this TC and the participation of our proposer(s) listed above.? - Bret Jordan, Director Office of the CTO, Symantec Corporation.

?The Information and Cyber Security group of the University of Oslo fully supports the creation of CACAO TC. The automation of security playbooks will aid dramatically security operations and incident response. We are looking forward to work towards that goal.? - Vasileios Mavroeidis, Information and Cyber Security, University of Oslo

(2)(f) TC Convener

Bret Jordan, Symantec Corp. - bret_jordan@symantec.com [17]

(2)(g) OASIS Member Section

N/A

(2)(h) Anticipated Contributions

Introduction https://datatracker.ietf.org/doc/draft-jordan-cacao-introduction/ [18]

(2) FAQ Document

N/A

(2)(j) Work Product Titles and Acronyms

CACAO

Associated TC:
Collaborative Automated Course of Action Operations (CACAO) for Cyber Security
Deadline:

Links:
[1] https://www.oasis-open.org/apps/org/workgroup/cacao/
[2] http://www.oasis-open.org/join/
[3] http://www.oasis-open.org/committees/cacao/
[4] https://www.lookingglasscyber.com/blog/cacao-a-future-for-collaborative-cybersecurity-course-of-action/
[5] https://nifi.apache.org/
[6] https://camunda.com/
[7] mailto:colby.derodeff@fireeye.com
[8] mailto:ahadden@us.ibm.com
[9] mailto:ryan.hohimer@darklight.ai
[10] mailto:Bret_Jordan@symantec.com
[11] mailto:Jason.Keirstead@ca.ibm.com
[12] mailto:terry.macdonald@gmail.com
[13] mailto:vasileim@ifi.uio.no
[14] mailto:shawn.p.riley@darklight.ai
[15] mailto:arnaud_taddei@symantec.com
[16] mailto:athomson@lookingglasscyber.com
[17] mailto:bret_jordan@symantec.com
[18] https://datatracker.ietf.org/doc/draft-jordan-cacao-introduction/