OASIS Committee Note

Playbook Requirements Version 1.0

Working Draft 01

28 January 2020

Technical Committee:
[OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC](https://www.oasis-open.org/committees/cacao/)

Chairs:
Bret Jordan (bret.jordan@broadcom.com), [Broadcom](https://www.broadcom.com/)
Allan Thomson (athomson@lookingglasscyber.com), [LookingGlass](https://www.lookingglasscyber.com/)

Editors:
Bret Jordan (bret.jordan@broadcom.com), [Broadcom](https://www.broadcom.com/)
Allan Thomson (athomson@lookingglasscyber.com), [LookingGlass](https://www.lookingglasscyber.com/)

Additional artifacts:
<TBD>

Related work:
This document is related to:

- CACAO Introduction Version 01. Edited by Bret Jordan, Allan Thomson, and Jyoti Verma. Latest version: https://tools.ietf.org/html/draft-jordan-cacao-introduction-01

Abstract:
To defend against threat actors and their tactics, techniques, and procedures, organizations need to identify, create, document and test investigative, preventive, mitigative, and remediative steps. These steps, when grouped together, form a cyber security playbook that can be used to protect organizational systems, networks, data, and users.

This document defines the core requirements for how cyber security playbooks can be created, documented, and shared in a structured and standardized way across organizational boundaries and technological solutions.

Status:
This [Working Draft](https://www.oasis-open.org/policies-guidelines/tc-process#dWorkingDraft) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](https://www.oasis-open.org/policies-guidelines/tc-process#committeeDraft) as a Committee Note Draft. The OASIS document [Approval

Process](https://www.oasis-open.org/policies-guidelines/tc-process#standApprovProcess) begins officially with a TC vote to approve a WD as a Committee Note Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Note Draft.

This committee note is provided under the [Non-Assertion](https://www.oasis-open.org/policies-guidelines/ipr#Non-Assertion-Mode) Mode of the [OASIS IPR Policy](https://www.oasis-open.org/policies-guidelines/ipr), the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page https://www.oasis-open.org/committees/cacao/ipr.php. Note that any machine-readable content ([Computer Language Definitions](https://www.oasis-open.org/policies-guidelines/tc-process#wpComponentsCompLang)) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

URI patterns:

Initial publication URI:
https://docs.oasis-open.org/cacao/playbook-requirements/v1.0/cnd01/playbook-requirements-v1.0-cnd01.docx.
Permanent "Latest stage" URI:
https://docs.oasis-open.org/cacao/playbook-requirements/v1.0/playbook-requirements-v1.0.docx.
(Managed by OASIS TC Administration; please don't modify.)

Notices

Table of Contents

1 Introduction

To defend against threat actors and their tactics, techniques, and procedures, organizations need to identify, create, document and test investigative, preventive, mitigative, and remediative steps. These steps, when grouped together, form a cyber security playbook that can be used to protect organizational systems, networks, data, and users.

To enable organizations to respond to threats in cyber relevant time, security teams need to be able to automate the creation, sharing, parsing, and execution of cyber security playbooks.

Each type of cyber security playbook, such as investigation, prevention, mitigation and remediation will consist of a sequence of actions that can be executed by the various technological solutions that can act on those actions whether those actions are executed by a machine, a human, or a combination of the two. These playbooks need to be referenceable by other shared cyber threat intelligence that provides support for related data such as threat actors, campaigns, intrusion sets, malware, attack patterns, and other adversarial tactics, techniques, and procedures.

This document defines the core requirements for how cyber security playbooks can be created, documented, and shared in a structured and standardized way across organizational boundaries and technological solutions.

1.1 References (non-normative)

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, http://www.rfc-editor.org/info/rfc4122.

1.2 IPR Policy

This document is provided under the [Non-Assertion](https://www.oasis-open.org/policies-guidelines/ipr#Non-Assertion-Mode) Mode of the [OASIS IPR Policy](https://www.oasis-open.org/policies-guidelines/ipr), the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/cti/ipr.php).

1.3 Terminology

Investigative Action - This is an action that is used to gather information relevant to the construction or modification of cyber security playbooks. This includes gathering of information about a possible incident, problem, attack, or compromise. In some cases, an investigative action could require changes to the systems, networks or application behaviors in order to facilitate a deeper understanding of the investigation and resultant potential response.

Mitigative Action - This is an action that is used to respond to problems that can occur from an incident, problem, attack, or compromise. This is often done when a remediative action is not currently possible. For example, when a system patch is not yet available, one might deploy compensating controls such as moving the system into a sandbox virtual lan (vlan) or deploying more stringent firewall rules.

Remediative Action - This is an action that is often used with a goal of eradicating an issue, problem, attack, or compromise on one or more systems that have been determined to be compromised or involved in the particular event.

Preventative Action - This is an action that is used to help ensure that an issue, problem, attack, or compromise does not happen in the first place. In some cases, preventative actions may overlap with certain mitigative and remediation actions.

Playbook - This is a collection of one or more actions that defines a behavior and provides guidance on how to address a certain incident, problem, attack, or compromise. A playbook may be triggered by some automated or manual event or observation. A playbook may contain automated and manual actions.A playbook may be defined in one system by one or more authors but the playbook may be executed in an operational environment where the systems and users of those systems have different authentication and authorizations. A playbook may also reference or include other playbooks in such a manner that allows composition from smaller, more specific function playbooks similar to how software application development leverages modular libraries of common functions shared across different applications.

Action - This provides detailed information about a specific step or command that is either executed manually or automatically. The individual actions may be defined in other specifications, and when possible will be mapped to the JSON structure of this specification. When that is not possible, they will be base64 encoded.

1.4 Overview

The requirements for cyber security playbooks naturally fall into several Playbook Information Domains (PID) as depicted in Figure 1 (below). Requirements in each PID are listed in the indicated section of this requirement document.

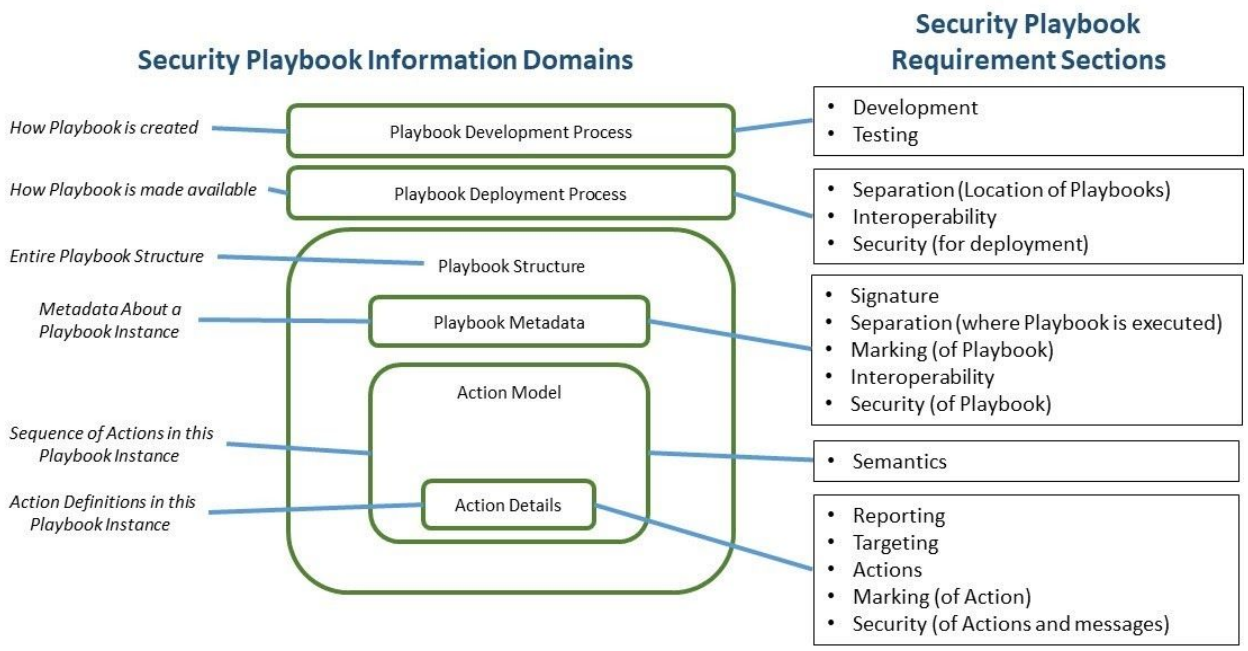

Figure 1 - Playbook Requirements Domains

Playbook Development Process (PID.Dev) Requirements

- Provides guidance on the playbook development/testing process such as: acceptable development practices and verification/validation testing necessary for acceptance of new playbooks.

Playbook Deployment Process (PID.Dep) Requirements

- Provides guidance on how to make a playbook available to the community where each community have their own defined requirements for acceptance of intelligence including playbooks.

Playbook Structure (PID.Struct) Requirements

- Defines the overarching structure of a playbook including mandatory/optional sections and overarching structure and formatting.

Playbook Metadata (PID.Meta) Requirements

- Defines the mandatory/optional data that goes with each playbook instance.

Action Model (PID.ActModel) Requirements

- Defines the flow of actions within a playbook including the sequence, control flow and logic, temporal requirements, flow decisions, and alternate paths.

Action Detail (PID.ActDetail) Requirements

- Defines the mandatory/optional data that goes with each action in the playbook. Note that each unique action is defined only once, even though the action may be referenced multiple times in the action model.

2 Requirements

The following section defines the core requirements that are needed to support the creation, sharing, and deployment of cyber security playbooks.

2.1 Development

Requirement	Details	PID
DEV.1	**Release In Phases** Break the CACAO playbook work into release phases	PID.Dev
DEV.2	**Minimally Viable Product (MVP)** Try to get "minimally viable product" out sooner rather than later (i.e., do not wait until a full and "complete" standard done, which will take much more time.)	PID.All

2.2 Interoperability

Requirement	Details	PID
INTEROP.1	**Vendor and Source Agnostic** Support deployment and use within an enterprise consisting of different vendors. Allow sharing of playbooks between enterprises with different environments, solutions, and vendors	PID.Dep
INTEROP.2	**Extensions** Support vendor-specific extensions	PID.Dep

2.3 Actions

Requirement	Details	PID
ACT.1	**Multiple Actions** The solution needs to support the ability to document one or more actions that can be processed in a batch manner or as-a-group concept	PID.Struct; PID.ActModel
ACT.2	**Sequencing of Actions** Actions often have to be done in a very specific order	PID.Struct; PID.ActModel

ACT.3	**Back Out Steps**	PID.Struct; PID.ActModel
ACT.4	**Combination of Actions** The ability to define an ordered list of atomic actions that must be executed as a combined set rather than as a sequence. For example: deny + log, allow + log, redirect + log.	PID.Struct; PID.ActModel
ACT.5	**Support Different Action Types** The solution needs to support the following types of actions: Machine automation, Human actions / intervention, High level conceptual actions	PID.Struct; PID.ActModel PID.ActDetail
ACT.6	**Handle Atomic and Non-Atomic Actions** Needs ability for systems to have option to support both atomic and non-atomic transactions Example: 1 sequence of actions provided but a system can be provisioned with option to treat entire sequence as atomic (i.e. one failure causes the entire sequence to be rejected) or non-atomic where the system can continue to operate through the sequence with errors being recorded but not treated as data	PID.Struct; PID.ActModel PID.ActDetail

2.4 Control Logic

Requirement	Details	PID
LOGIC.1	**Temporal Logic** Sometimes actions can only be performed at certain times or after a certain amount of time has passed after the previous action. (Window of opportunity. Example: Must I act now? If I don't act now, will the opportunity close? Will the response action be different later?)	PID.Struct; PID.ActModel
LOGIC.2	**Conditional Logic** Often actions need to be performed based on environmental data or outcomes of previous actions	PID.Struct; PID.ActModel

2.5 Identifiers

Requirement	Details	PID
IDENT.1	**System Integration**	PID.Dep; PID.Meta

	Needs to integrate with other systems globally. Needs to support a globally unique ID like a UUIDv4 [RFC4122] for projects and individual actions.	
IDENT.2	**Monitoring** All transactions need to be able to be monitored. This means responses and notifications need a way to be tied back to the original request	PID.Dep; PID.Meta

2.6 Targeting

Requirement	Details	PID
TARGET.1	**Versioning** Allow actions, projects, and templates to be versioned. Support both incremental and semantic versioning.	PID.Meta; PID.ActModel; PID.ActDetail
TARGET.2	**System / Group Targeting** Identify specific machines, devices, software, general classes of systems (e.g., Windows 10), teams (SoC Team / Network Team), and individuals (CISO).	PID.Meta; PID.ActModel; PID.ActDetail

2.7 Testing

Requirement	Details	PID
TEST.1	**Scope** Machine automation Human actions / intervention High level conceptual actions	PID.Dev; PID.Dep; PID.Meta; PID.ActModel; PID.ActDetail
TEST.2	**Dry-Run Capabilities** Including what-if deployments	PID.Dev; PID.Dep; PID.Meta; PID.ActModel; PID.ActDetail
TEST.3	**Playbook Validation Before Deployment** Ability to validate that a playbook is correctly formed syntactically and semantically would execute without significant failures	PID.Dev; PID.Dep PID.Struct PID.ActModel PID.ActDetail

2.8 Reporting

Requirement	Details	PID
REPORT.1	**General Reporting** Provide full reporting on the processing of each action including supporting the needs for mandatory reporting requirements.	PID.Dep PID.Meta
REPORT.2	**Auditing** Must have a timestamp and information regarding the original request or rule that caused the event for full auditing capabilities.	PID.Dep PID.Meta
REPORT.3	**Report Delivery** Could be either synchronously requested or an asynchronous event (syslog) with periodic updates	PID.Dep PID.Struct

2.9 Signatures

Requirement	Details	PID
SIG.1	**Basic Digital Signatures** Ability to digitally sign playbooks and their various parts and even sub parts	PID.Meta PID.Struct PID.ActModel
SIG.2	**Layered / Multiple Signatures** Ability to support multiple digital signatures of the same thing	PID.Meta PID.Struct PID.ActModel
SIG.3	**Semantic Signatures** Ability for multiple independent organizations to sign and verify the correctness, accuracy, and validity of the playbook	PID.Meta PID.Struct PID.ActModel

2.10 Security

Requirement	Details	PID
SEC.1	**Integrity and Authentication** Support full data protection, integrity and authentication	PID.Dep PID.Struct
SEC.2	**Transport**	PID.Dep PID.Struct

	All requests and responses must be conveyed over a secure (encrypted and authenticated) transport protocol such as HTTPS (but not limited).	
SEC.3	**Delivery Options** Both direct delivery and publish/subscribe solutions	PID.Dep PID.Struct

2.11 Separation

Requirement	Details	PID
SEP.1	**Portability** Playbooks may be defined in one environment and executed or deployed to a different operational environment. Meaning, the security environment executing the playbook will likely be different from where the playbook was defined.	PID.Dep
SEP.2	**Authorization Requirements** For a playbook to execute correctly it must have authorization in the operational environment where it is executed.	PID.Dep PID.Meta

2.12 Marking

Requirement	Details	PID
MARK.1	**Object Level Markings** Need ability to support data marking at a Playbook level such as TLP Red for the entire playbook	PID.Dep PID.Meta PID.Struct PID.ActModel PID.ActDetail
MARK.2	**Granular Markings** Need ability to support data marking at specific control blocks within a Playbook	PID.Dep PID.Meta PID.Struct PID.ActModel PID.ActDetail

Appendix A. Acknowledgments

Participants:
The following individuals were members of the OASIS CACAO Technical Committee during the creation of this document and their contributions are gratefully acknowledged:

Anup Ghosh, Accenture
Patrick Maroney, AT&T
Dean Thompson, Australia and New Zealand Banking Group (ANZ Bank)
JR Jewczyk, Bank of Montreal
Bret Jordan, Broadcom
Arnaud Taddei, Broadcom
Alexandre Dulaunoy, CIRCL
Omar Santos, Cisco Systems
Naasief Edross, Cisco Systems
Jyoti Verma, Cisco Systems
Arsalan Iqbal, CTM360
Avkash Kathiriya, Cyware Labs
Ryan Joyce, DarkLight, Inc.
Ryan Hohimer, DarkLight, Inc.
Shawn Riley, DarkLight, Inc.
Preston Werntz, DHS Office of Cybersecurity and Communications (CS&C)
Michael Rosa, DHS Office of Cybersecurity and Communications (CS&C)
Marko Dragoljevic, EclecticIQ
Christopher O'Brien, EclecticIQ
Aukjan van Belkum, EclecticIQ
Vincent Lopez, Financial Services Information Sharing and Analysis Center (FS-ISAC)
Colby DeRodeff, FireEye, Inc.
Henry Peltokangas, FireEye, Inc.
James Meck, FireEye, Inc.
Paul Patrick, FireEye, Inc.
Gerald Stueve, Fornetix
Ryusuke Masuoka, Fujitsu Limited
Toshitaka Satomi, Fujitsu Limited
Koji Yamada, Fujitsu Limited
Danny Martinez, G2, Inc.
Stephanie Hazlewood, IBM
Mahbod Tavallaee, IBM
Srinivas Tummalapenta, IBM
Emily Ratliff, IBM
Jason Keirstead, IBM
John Morris, IBM
Joerg Eschweiler, Individual
Terry MacDonald, Individual
Anil Saldanha, Individual

Frans Schippers, Individual
Rodger Frank, Johns Hopkins University Applied Physics Laboratory
Jorge Aviles, Johns Hopkins University Applied Physics Laboratory
Nam Le, Johns Hopkins University Applied Physics Laboratory
Tim Zhan, Johns Hopkins University Applied Physics Laboratory
Karin Marr, Johns Hopkins University Applied Physics Laboratory
Allan Thomson, LookingGlass
Chris Dahlheimer, LookingGlass
Jason Webb, LookingGlass
Ivan Kirillov, Mitre Corporation
Bob Natale, Mitre Corporation
David Kemp, National Security Agency
Daniel Dye, NC4
Hiroshi Takechi, NEC Corporation
Christian Hunt, New Context Services, Inc.
Andrew Storms, New Context Services, Inc.
Stephen Banghart, NIST
David Darnell, North American Energy Standards Board
Cheolho Lee, NSRI
Lior Kolnik, Palo Alto Networks
Duncan Sparrell, sFractal Consulting LLC
Tom Maier, Siemens AG
Marco Caselli, Siemens AG
Curtis Kostrosky, Symantec Corp.
JP Bourget, Syncurity
Andrew Pendergast, ThreatConnect, Inc.
Ryan Trost, ThreatQuotient, Inc.
Franck Quinard, TIBCO Software Inc.
Toby Considine, University of North Carolina at Chapel Hill
Vasileios Mavroeidis, University of Oslo

Appendix B. Revision History

Revision	Date	Editor	Changes Made
01	2020-01-27	Bret Jordan, Allan Thomson	Initial version