Memorandum

www.tno.nl

Aan Nationaal Cyber Security Centrum (NCSC)

Datum
18 december 2023

Van ir. H.L.J. Bijmans
ir. H. Kerkdijk
ir. G. de Roode
ir. T.G. Sierink

Onderwerp Security Playbooks & het NCSC

Automatisch delen van security playbooks

1. Inleiding

Het NCSC deelt vanuit haar unieke informatiepositie cyberdreigingsinformatie met tal van organisaties in haar achterban. Middels het delen van informatie en het faciliteren van samenwerking tussen rijksoverheidsorganisaties en vitale industrieën op het gebied van cyber security tracht het NCSC Nederland beter te beschermen tegen cyberaanvallen. Het NCSC biedt organisaties een zogenaamde *feed* van (cyber) dreigingsinformatie (CTI) aan. Veel van deze dreigingsinformatie wordt door het zelf NCSC verzameld en gevalideerd. Organisaties kunnen echter ook zelf dreigingsinformatie (bijvoorbeeld voortkomend uit eigen dreigingsonderzoeken of incidenten) via het NCSC met de andere organisaties delen. Het belangrijkste doel van deze uitwisseling is de weerbaarheid van deze organisaties (en daarmee de Nederlandse samenleving) tegen digitale dreigingen te verhogen. Het NCSC bedient verschillende doelgroepen. Een deel van haar doelgroep werkt samen in het NDN, het Nationaal Detectie Netwerk. Dit samenwerkingsverband bestaat uit zowel vitale (private) organisaties als Rijksoverheidsorganisaties.

Alle doelgroepen van het NCSC ontwikkelen zich en bereiken zo een hoger volwassenheidsniveau. Een belangrijke trend in deze ontwikkeling is dat operationele securityprocessen, zoals die worden verricht door SOC's en CSIRT's meer worden geautomatiseerd. Veel organisaties richten zich daarbij op het automatiseren van simpele security taken, zoals het raadplegen van interne of externe bronnen. Daarnaast bestaat de trend om ook meer incident response vraagstukken te automatiseren, dit kan bijvoorbeeld door middel van security playbooks (Bijmans, Kerkdijk, & Tesink, 2020). Deze machine-leesbare workflows beschrijven hoe bepaalde triggers tot een gestandaardiseerde response leiden en worden vastgelegd in zogeheten "*security playbooks".* Dergelijke security playbooks worden typisch ingezet in zogeheten Security Orchestration and Reponse (SOAR) producten, welke in verbinding staan met de verschillende securityproducten binnen een bedrijfsnetwerk, om vervolgens deze te gebruiken binnen de response. Verscheidene cybersecurity leveranciers bieden dergelijke SOAR-producten aan en de verwachting is dat het gebruik hiervan in de toekomst enkel zal groeien (Bijmans, Kerkdijk, & Tesink, 2020). Het technische formaat waarin security playbooks worden vastgelegd is op dit moment product specifiek, maar er wordt binnen het standaardisatie-orgaan OASIS gewerkt aan een standaard, Collaborative Automated Course of Action Operations (CACAO) (OASIS, 2023).

Met het verstrekken van security playbooks zou de response op geconstateerde dreigingen bij organisaties binnen de doelgroepen versneld kunnen worden. Nu wordt veel van de response op een geconstateerde dreiging

handmatig uitgevoerd. Na een detectie worden handmatig andere logbronnen geraadpleegd, verdere context verkregen of configuratie wijzigingen doorgevoerd. Wanneer er bijvoorbeeld een grote kwetsbaarheid in een veelgebruikt softwarepakket wordt gevonden, dan dient iedere organisatie dezelfde stappen uit te voeren om deze dreiging te analyseren en te mitigeren. Precies dit proces kan door middel van een security playbook worden vergemakkelijkt, gestandaardiseerd en versneld. Immers, bij het uitvoeren van een goed opgesteld playbook hoeft niet iedere organisatie zelf alle stappen voor een succesvolle mitigatie te definiëren. Versnelling van de response op cyberincidenten zal uiteindelijk resulteren in beter beschermde organisaties.

Dit memorandum biedt een overzicht van de huidige SOAR-standaarden. Dit om de huidige ontwikkelingen binnen playbook-gedreven security automatisering te schetsen vanuit het perspectief van technologie, standaardisatie en de markt.

2. Security playbooks en de standaardisatie van (cyber) dreigingsinformatiedeling

Een belangrijke ontwikkeling in de automatisering van SOC- en CSIRT-processen is de opkomst van *security workflow orchestration*. Dit houdt in dat bepaalde gebeurtenissen een gestandaardiseerde respons activeren, bestaande uit een vaste (vooraf gedefinieerde) workflow. Dergelijke workflows worden beschreven in zogeheten *security playbooks*. In de context van dit memo gaat het specifiek om security playbooks die “machine-readable” zijn en geautomatiseerd kunnen worden uitgevoerd. Hiervoor wordt in de regel een zogeheten Security Orchestration Automated Response (SOAR) product gebruikt. Security playbooks kunnen verschillende operationele security taken volgens een vaste workflow afhandelen, al dan niet (semi-) geautomatiseerd. Denk bijvoorbeeld aan situaties waarin veel repetitieve taken moeten worden verricht, situaties waar alles volgens afspraak en consistent moet worden afgehandeld (compliance eisen), of bij tijdrovende taken zoals het doorzoeken van grote hoeveelheden log data.

Security playbooks zijn momenteel nog volop in ontwikkeling. Om playbooks te delen is nodig dat deze in een gestandaardiseerd formaat worden verspreid om zo door verschillende partijen te kunnen worden verwerkt. De volgende secties beschrijven de huidige stand van zaken met betrekking tot de standaardisatie van security playbooks alsmede gerelateerde standaarden voor (cyber) informatiedeling. Hierin wordt zowel het technische aspect als de mate van adoptie door de industrie onder de loep genomen.

2.1. CACAO – Collaborative Automated Course of Action Operations

CACAO, Collaborative Automated Course of Action Operations, is een standaard voor het definiëren van security playbooks die op dit moment wordt ontwikkeld door OASIS (OASIS, 2023). Op moment van schrijven is versie 2.0 aanstaande, en is de laatste draft op 24 oktober uitgekomen. Binnen deze standaard worden in serie of parallel incident response workflows beschreven in machine-leesbaar formaat (JSON). Deze workflows bevatten verschillende opdrachten die zo nodig automatisch kunnen worden uitgevoerd. Opdrachten via SSH, bash, API-interactie over HTTP, en OpenC2 worden standaard ondersteund. Natuurlijk kan er soms ook een menselijke blik op zaken nodig zijn. CACAO ondersteunt daarom handmatige acties en handmatige beslissingen bij een ‘splitsing’ in de workflow. Daarnaast kan in het CACAO-formaat ook meer context worden toegevoegd met behulp van datavelden die de dreiging beschrijven, zoals specifieke labels, impact en prioriteit. Tot slot kunnen CACAO-playbooks digitaal worden ondertekend, waarmee het mogelijk is de integriteit en authenticiteit van een playbook bewijzen.

OASIS onderscheidt verschillende typen security playbooks die uiteenlopen qua inzetbaarheid en doel. Een overzicht van alle soorten is beschreven in onderstaande tabellen. Inzetbaarheid bestaat uit twee klassen. *Executable* playbooks zijn bedoeld om meteen toegepast te worden in een organisatie zonder enige aanpassingen van de specifieke opdrachten. Een playbook *template* is een veralgemeniseerde variant, welke wel het proces schetst, maar welke een organisatie eerst dient aan te passen naar de eigen omgeving voordat het playbook kan worden toegepast. Dergelijke templates zijn bij uitstek geschikt om in een gemeenschap te delen.

Type	Beschrijving
Executable	Directe implementatie zonder enige aanpassingen
Template	Slechts algemene structuur en stappen, aanpassingen zijn noodzakelijk

Tabel 1: Playbook types (inzetbaarheid)

Type playbook (doel)	Beschrijving
Notification	Melden van dreiging
Detection	Opsporen van (bekende) dreiging
Investigation	Onderzoeken van plaatsgevonden incident
Prevention	Voorkomen van bekend of verwachte dreiging
Mitigation	Beperken van impact van incident
Remediation	Herstellen na incident
Attack	Uitvoeren van pentests of simulaties

Tabel 2: Playbook types (doel)

OASIS definieert het gebruik van CACAO-playbooks in verschillende scenario's voor verschillende doeleinden. In totaal zijn er zeven van dit soort doelen te onderscheiden, welke zijn weergeven in bovenstaande tabel. Een *detection* playbook zou bijvoorbeeld kunnen worden opgesteld op basis van specifieke IoC's die horen bij een aanval van een specifieke Advanced Persistent Threat (APT), terwijl voor een algemene kwetsbaarheid die veel systemen raakt (bijvoorbeeld log4j) een *prevention* playbook zou kunnen worden opgesteld.

De ontwikkeling van de CACAO standaard is begonnen in 2019, maar bij het schrijven van dit memo bieden nog maar weinig SOAR-producten ondersteuning. Zoals weergeven in Tabel 3 werken alle SOAR-oplossingen met machine-leesbare playbooks, maar ondersteunen de meeste slechts een eigen ("proprietary") bestandsformaat. In een door TNO verrichte inventarisatie kwamen slechts twee commerciële SOAR-producten in beeld die de CACAO standaard ondersteunen.

Aanbieder	Machine-leesbare playbooks?	Bestandstype	CACAO-ondersteuning?
Activiti (Activiti, 2023)	Ja	BPMN	Nee
Airflow (Idealista, 2023)	Ja	Ansible (YAML)	Nee
Shuffle (Shuffle, 2023)	Ja	JSON (Shuffle native)	Nee
Cortex XSOAR (Cortex, 2023)	Ja	COPS (YAML)	Nee
IBM QRadar (IBM, 2022)	Ja	.resz Qradar-native	Nee
Splunk Phantom (Splunk, 2021)	Ja	JSON (Splunk native)	Nee
Microsoft Sentinel (Microsoft, 2023)	Ja	JSON (Sentinel native)	Nee
Google Chronicle (Google, 2023)	Ja	JSON (Chronicle native)	Nee
The Incident Response Tool (Sphynx, 2023)	Ja	JSON (CACAO)	Ja
Cyberalytics CYBerSOAR platform (Cyberalytics, 2023)	Ja	JSON (CACAO)	Ja

Tabel 3: Inventarisatie CACAO-ondersteuning door SOAR-producten

Op het eerste gezicht is te zien dat bekende oplossingen nog geen CACAO ondersteunen. Echter, de conclusie die men uit deze tabel kan trekken is allerminst negatief. Het verleden heeft geleerd dat de eerdere OASIS-standaarden succesvol zijn gebleken. Zo is STIX is binnen veel relevante oplossingen erkend, zowel in MISP als in andere CTI-oplossingen van IBM en EclecticIQ. Wat het meest positief stemt is het grote aantal commerciële partijen die hun steun aan het CACAO project hebben verleend. Denk hierbij aan IBM, NIST en Cisco (OASIS, 2023). Omdat STIX een vergelijkbare ontwikkeling in volwassenheid heeft doorgemaakt, is daarom ook nu de verwachting CACAO een brede adoptie zal gaan krijgen in de komende jaren. Het feit dat een eerste partijen daar al mee begonnen is bevestigt dit vermoeden.

2.2. Gerelateerde standaarden voor het delen van (cyber) dreigingsinformatie

Naast de CACAO standaard voor het standaardiseren van security playbooks, bestaan er een aantal gerelateerde standaarden die kunnen worden gebruikt om (cyber) dreigingsinformatie uit te wisselen. Deze standaarden worden in de volgende secties besproken.

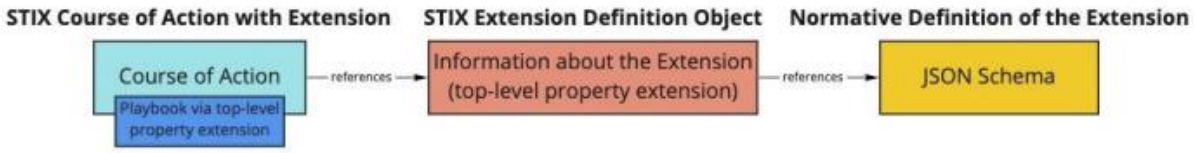
2.2.1. STIX – Structured Threat Information Expression

Voor STIX is het delen van de context van een aanval juist wel het hoofddoel, in tegenstelling tot CACAO. Deze standaard, ontwikkeld door OASIS en beschreven in een JSON-formaat, heeft als doel het delen en innemen van CTI te vergemakkelijken. Verschillende STIX Domain Objects (SDO's) kunnen worden gevuld met allerlei dreigingsrelevante gegevens. Deze SDO's kunnen vervolgens weer onderling naar elkaar verwijzen met STIX Relationship Objects (SRO's) om het beeld van de dreiging gestructureerd en gedetailleerd te beschrijven. Een STIX-object om de response op een aanval te definiëren is het Course of Action SDO. Dit object is echter nog niet volledig gedefinieerd. In de documentatie schrijft OASIS hierover het volgende:

"The Course of Action object in STIX 2.1 is a stub. It is included to support basic use cases (such as sharing prose courses of action) but does not support the ability to represent automated courses of action or contain properties to represent metadata about courses of action. Future STIX 2 releases will expand it to include these capabilities." (OASIS, 2021)

Hieruit blijkt dat de STIX-standaard op dit aspect nog niet is uitontwikkeld. Er is voorgesteld om (CACAO) playbooks te integreren in STIX (Mavroeidis & Zych, 2022). Dit kan op verschillende manieren: als losstaand

Extension Definition Object, een property extension, of juist als extension binnen in een Course of Action SDO, zie Figuur 1. Uiteindelijk is het doel van deze extensie om een playbook, gecodeerd in base64, in zijn geheel te verwerken binnen het STIX-object.



Figuur 1: Voorbeeld van integratie van een JSON playbook in STIX, als extensie van een Course of Action SDO.

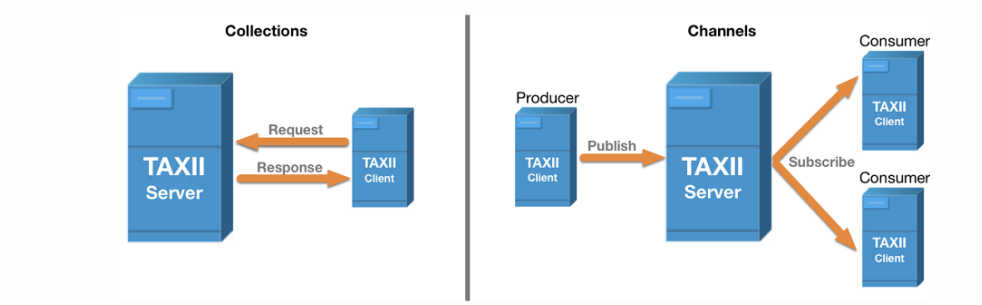
2.2.2. OpenC2 – Open Command and Control

De volgende, door OASIS ontwikkelde, standaard is OpenC2. Deze standaard wordt gebruikt voor machine-to-machine communicatie, specifiek om operationele securityproducten binnen de IT-infrastructuur van een organisatie geautomatiseerd met elkaar te kunnen laten communiceren. De gespecificeerde opdrachten staan los van applicaties, wat het mogelijk maakt om in één taal alle securityproducten in een omgeving aan te sturen. OpenC2 kan bijvoorbeeld aanpassingen doen aan de configuratie van een IDS, firewall, EDR-oplossing, etc. Zoals eerder benoemd kunnen CACAO-playbooks OpenC2 commando's uitvoeren. Een OpenC2-commando bestaat hoofdzakelijk uit een actie, en een target. Daarop volgt een reactie van het doel. Belangrijk om te realiseren is dat dit wel vereist dat het ontvangende product wel "*OpenC2 aware*" is, en dat de inhoud van de commando's nauwkeurig moet aansluiten met specifieke infrastructuur details. Zo bevestigt OASIS dat er altijd maatwerk zal zijn, met als reden en ook doel dat veel bestaande en nieuwe producten eigenlijk al OpenC2-aware zijn, maar elk op hun eigen manier (OASIS, 2021). Op dit moment ondersteunt alleen Symantec, software voor end-point security, OpenC2 opdrachten (OASIS, 2022).

OpenC2 is een kansrijke standaard voor het automatiseren van operationele security taken, omdat het de mogelijkheid biedt tot geautomatiseerde herconfiguraties van cybersecurityproducten. Echter, het is onzeker binnen welke termijn organisaties hier klaar voor zijn. Omdat SOC's vaak niet het mandaat hebben om geautomatiseerd aanpassingen in de infrastructuur te maken zullen organisaties voor dergelijke automatische herconfiguraties zowel hun technische- als beheersprocessen moeten veranderen.

2.2.3. TAXII - Trusted Automated Exchange of Intelligence Information

TAXII is ontworpen door OASIS met het doel om STIX Objects te verzenden en delen. In de laatste versie, v2.1, wordt verzonden STIX-data gebundeld in een STIX Envelope Object met daarin alle STIX Objects. Voor het delen maakt TAXII gebruik van HTTPS en definieert een REST API met duidelijke vereisten voor client en server. Er zijn twee manieren van interactie tussen client en server, zie Figuur 2 (OASIS, 2021). De *collections* manier is een traditionele client en server benadering, terwijl de *channels* manier een soort uitzendkanaal definieert, waarbij meerdere afnemers geabonneerd kunnen worden op de TAXII-server van een producent.



Figuur 2: De twee verschillende manieren van TAXII client-server interactie (OASIS, 2021)

2.2.4. MISP - Malware Information Sharing Platform and Threat Sharing

MISP (Malware Information Sharing Platform and Threat Sharing) is een open-source softwareoplossing om dreigingsinformatie te delen, compleet met een GUI. MISP geen standaard zoals CACAO en STIX, maar vanwege haar populariteit kan het gezien worden als één van de standaard manieren voor het delen van dreigingsinformatie. Zoals beschreven in 2.2, wordt MISP ook ingezet door het NCSC. Binnen het platform worden MISP Objects gedefinieerd. Dit is een eigen datastructuur waarmee data aan o.a. Objects, Events, en Attributes kan worden gekoppeld. MISP volgt hierbij een vergelijkbare, maar niet exact gelijke, structuur als STIX. MISP Objects zijn op eenzelfde manier machine-leesbaar, maar de focus ligt op het opslaan en analyseren van gegevens, met name IoC's. Desondanks ondersteunt MISP zelf ook het delen van informatie in STIX-formaat. Tot slot kent MISP het object security playbook als vooraf gedefinieerd veld.

3. Conclusie

In dit memo is de stand van zaken rondom het automatiseren van security playbooks in kaart gebracht. Hierbij is vooral gekeken naar de verschillende standaarden en hoe deze zich ontwikkelen.
Uit die uiteenzetting is gebleken dat de CACAO standaard voor security playbooks een belangrijke rol gaat spelen. Hoewel de standaard nog jong en volop in ontwikkeling is, zijn er verscheidene (prominente) commerciële partijen die hun steun hebben toegezegd. Dit, samen met gerelateerde standaarden zoals STIX, TAXII en OpenC2, schept de mogelijkheid voor een verrijkte informatiedeling

Om deze stapsgewijze werkwijze voor het werken met geautomatiseerde security playbooks te realiseren zijn een aantal nieuwe competenties benodigd. Allereerst vereist het opstellen van CACAO template playbooks kennis van de standaard, maar ook gedegen kennis van incident response processen. Een organisatie dient te bepalen onder welke omstandigheden een playbook wordt opgesteld en wanneer niet. Hierbij kan gedacht worden aan de ernst van de dreiging of de complexiteit in het incident response proces. Ook dient te worden bepaald hoe gedetailleerd een playbook per dreiging is en hoe om te gaan met het updaten ervan. Wanneer er tijdens een dreiging nieuwe informatie binnenkomt, wanneer dient dan het playbook te worden aangepast?

Bij de organisaties die playbooks ontvangen zal het verrijken van een template playbook tot een executable playbook waarschijnlijk geautomatiseerd plaatsvinden. Mogelijk kan een template playbook in de toekomst zelfs rechtstreeks in een SOAR geladen worden, welke het dan specifiek maakt voor de organisatie. Echter, in het begin zal dit proces nog handmatig verlopen.

Bronnen

OASIS. (2021, June 10). *STIX Version 2.1*. Opgehaald van OASIS OPEN: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_a925mpw39txn

Mavroeidis, V., & Zych, M. (2022, August). *Arxiv.* Opgehaald van https://arxiv.org/ftp/arxiv/papers/2203/2203.04136.pdf

OASIS. (2021). Opgehaald van OASIS OPEN Github: https://github.com/oasis-tcs/openc2-tc-ops/blob/main/oc2-companion.md#because-of-this-you-will-often-feel-like-youre-missing-concrete-definitions-of-what-openc2-is

OASIS. (2022). *OpenC2 in the News*. (OASIS) Opgeroepen op March 21, 2023, van https://openc2.org/news.html

OASIS. (2021). *OASIS OPEN Github*. Opgehaald van https://oasis-open.github.io/cti-documentation/taxii/intro.html

Activiti. (2023). *Github Activiti*. (Activiti) Opgeroepen op March 21, 2023, van https://github.com/Activiti/Activiti

Idealista. (2023). *Github Airflow*. (Idealista) Opgeroepen op March 21, 2023, van https://github.com/idealista/airflow-role

Shuffle. (2023). *Shuffle.io Workflows*. (Shuffle) Opgeroepen op March 21, 2023, van https://shuffler.io/search?tab=workflows

Cortex. (2023). *Cortex XSOAR Concepts*. (Cortex) Opgeroepen op March 21, 2023, van https://xsoar.pan.dev/docs/concepts/concepts

IBM. (2022). *QRadar SOAR Playbook Designer Demo*. (IBM) Opgeroepen op March 21, 2023, van https://mediacenter.ibm.com/media/QRadar+SOAR+Playbook+Designer+201+Demo+-+Import+Export/1_08sm5fjj

Splunk. (2021). *Use a Custom Script - Splunk Phantom*. (Splunk) Opgeroepen op March 21, 2023, van https://docs.splunk.com/Documentation/Phantom/4.10.7/PlatformAPI/RESTCustom

Microsoft. (2023). *Playbooks gebruiken met automatiseringsregels in Microsoft Sentinel*. (Microsoft) Opgeroepen op March 21, 2023, van https://learn.microsoft.com/nl-nl/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents

Google. (2023). *My First Automation - Chronicle SOAR*. (Google) Opgeroepen op March 21, 2023, van https://chronicle-soar.elevio.help/en/articles/228

IACD. (2019). *IACD*. (IACD) Opgeroepen op March 21, 2023, van https://www.iacdautomate.org/

Schlette, D., Caselli, M., & Günther, P. (2021). *A Comparative study on Cyber Threat Intelligence: The Security Incident Response Perspective.* IEEE Communications Surveys & Tutorials.

Demisto. (2018). *Github Demisto COPS*. (Demisto) Opgeroepen op March 21, 2023, van https://github.com/demisto/COPS

Bijmans, H., Kerkdijk, R., & Tesink, S. (2020). *Ontwikkelingen in de Automatisering van Operationele Security Taken Resultaten literatuurstudie.* Den Haag: TNO.

Sphynx. (2023). *Products - The SPHYNX SPA Suite*. Opgehaald van Sphynx Technology Solutions: https://www.sphynx.ch/products/

OASIS. (2023). *OASIS Collaborative Automated Course of Action Operations (CACAO) for Cyber Security TC*. Opgehaald van OASIS OPEN: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao

Cyberalytics. (2023). *CYBerSOAR platform*. Opgehaald van Cyberalytics: https://cyberalytics.com/cybersoar