

For citation, please be referred to the HTML version of this article:

<https://ercim-news.ercim.eu/en129/special/from-collaboration-to-automation-a-proof-of-concept-for-improved-incident-response>

PDF version of the full issue:

<https://ercim-news.ercim.eu/images/stories/EN129/EN129-web.pdf>

From Collaboration to Automation: A Proof of Concept for Improved Incident Response

by Lasse Nitz (Fraunhofer FIT), Martin Zadnik (CESNET), Mehdi Akbari Gurabi (Fraunhofer FIT), Mischa Obrecht (Dreamlab Technologies AG) and Avikarsha Mandal (Fraunhofer FIT)

Effective incident response relies on taking accurate and timely measures in reaction to cybersecurity incidents. The increase in both the number and variety of cyberattacks, however, makes it challenging for incident handlers to keep up with this task. In the H2020 project SAPPAN, we take a practical look at this problem and explore the sharing of incident handling information, the automation of incident response processes, as well as the relationship between these two topics, to assist human operators in their work.

Automation within and information sharing between computer security incident response teams (CSIRTs) have the potential to improve response times for both common and novel attacks, despite a seemingly ever-increasing number of cybersecurity incidents. High-quality detection systems and automation of common incident response processes can help CSIRTs to utilise the time and efforts of operators more effectively by allowing human experts to focus on critical and novel kinds of attacks. Sharing incident response and recovery playbooks for emerging kinds of attacks can further improve response across organisation borders and hence has the potential to diminish the damage caused by new attacks. Additionally, shared play-

books can provide a good starting point for the automation of respective response processes.

Sharing playbooks, however, requires a mutual understanding of what a playbook is. While the common understanding is that a playbook describes a conditional sequence of steps to take for the mitigation (and sometimes also prevention or analysis) of a certain kind of incident, the specific format may vary significantly between different organisations, ranging from full text descriptions over structured text to machine-readable descriptions. A standardised machine-readable playbook format has the benefit of providing a clean interface, which allows the building of tools

that take respective playbooks as input. This would also allow for easy integration of shared playbooks into locally deployed tools.

The SAPPAN project [L1] sets one of its goals to share incident handling information. While we were working on this goal, we came across a playbook standardisation effort organised within OASIS, called Collaborative Automated Course of Action Operations for Cyber Security (CACAO) [1]. Since this effort addresses the problem of providing a mutual understanding of what a playbook is by standardisation of the playbook representation and format, we decided to address the remaining problem of

Playbook standard
Playbook type
Description
Label
Abstraction
Validity
Playbook

Figure 1: Simplified structure of the MISP security playbook object.

how to share them. We settled on Malware Incident Sharing Platform (MISP [L2]) as the sharing platform, due to its high popularity and already existing object to capture textual Course of Action (CoA) playbooks. Our goal was to prepare a MISP data model, which allows capturing standardised playbooks (such as CACAO playbooks) without being restricted to just a single standard.

In collaboration with the Technical Committee of CACAO, we prepared a MISP playbook object with specific attributes for the playbook metadata [2]. The actual standardised playbook is stored as an attachment attribute in the object as is depicted in Figure 1. This allows sharing of playbooks in other formats and does not require the transformation of a playbook when it is shared and exported from MISP. After discussing the playbook object with the MISP developers, it is now available in the official MISP object repository [L3]. We also implemented a tool to read locally stored CACAO playbooks and to correctly publish them into MISP, and vice versa.

When considering automation of incident response workflows based on shared playbooks, the shared playbooks themselves should not be specific to the sharing organisation's infrastructure. One reason for this is that if a playbook contains infrastructure-specific information, it may pose a security risk, if the receivers are not fully trusted. A second reason is that infrastructure-specific playbooks have little to no value for organisations with differing infrastructure. Playbooks suitable for sharing should hence be infrastructure-independent. Automation of incident response workflows, on the other hand, is infrastructure-specific. Consequently,

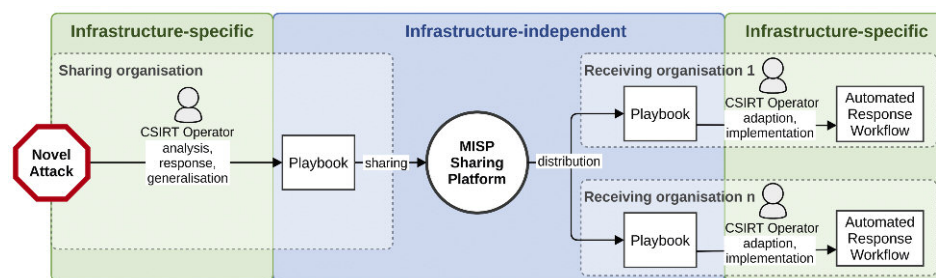


Figure 2: Overview of how collaborative playbook sharing can improve response across organisation borders. The sharing organisation detects a novel kind of attack. After mitigation, the incident is analysed and generalised to create a playbook, which is shared via MISP as a MISP security playbook object. The receiving organisations can then benefit from the sharing organisation's experience and potentially use the playbook description for preventative measures such as automated response to this kind of attack.

there is a gap between the level of detail in which shared materials should be provided and the level of detail required for automation of respective workflows. Even though some information for incident response automation can be automatically transferred from the playbook to the automation engine (e.g., the general structure of the workflow), there is still manual work required by human operators, due to this gap in the respective levels of detail. A schematic overview of how the sharing process aligns with the automation process is shown in Figure 2.

The process of adapting a playbook to a specific organisation was carried out as a prototype for the example of responding to suspected, outgoing malware communication. To this end, the playbook was adapted to an automated workflow using Apache Airflow as a workflow engine. This automated workflow was then integrated with the case management solution used by Dreamlab's Cyber Security Operation Centre (CySOC) [L4]. The goal of the workflow is to automatically resolve as many detections as possible by blocking suspected malicious traffic from and to affected hosts, whilst simultaneously keeping the risk of disruptions low. It does this by distinguishing between critical and uncritical assets (which is done through integration with an organisation-specific asset inventory) and applying a heuristic to automatically resolve alerts which affect normal (as in not critical) hosts. This achieves two things:

1. The majority of alerts are resolved quickly and automatically with minimal risk of disruptions, which frees up analyst-time in the Security Operation Centre (SOC).
2. Alerts affecting critical hosts can be examined more closely with the now

available, additional analyst-resources.

While the implementation and integration of the automated workflow into a real-world SOC environment showed that it requires non-negligible initial effort, it also revealed that it can improve response times for ordinary incidents significantly. Focusing automation efforts on incidents involving normal assets seems to provide the best trade-off between rapid incident response and the risk of disruption.

This work was done within the EU H2020 project SAPPAN [L1]. SAPPAN has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833418.

Links:

- [L1] <https://sappan-project.eu/>
- [L2] <https://www.misp-project.org>
- [L3] <https://kwz.me/hfE>
- [L4] <https://kwz.me/hfK>

References:

- [1] B. Jordan and A. Thomson eds.: "CACAO Security Playbooks Version 1.1" OASIS Committee Specification, 22 Oct. 2021. Available online: <https://kwz.me/hfH>
- [2] V. Mavroeidis, et al.: "On the Integration of Course of Action Playbooks into Shareable Cyber Threat Intelligence", IEEE Big Data, 2021.

Please contact:

Lasse Nitz
 Fraunhofer Institute for Applied Information Technology (FIT),
 Germany
lasse.nitz@fit.fraunhofer.de