RESEARCH NEWS

Fraunhofer at the Hannover Messe 2025

Standardized Security Playbooks improve protection against Cyberattacks

One attack, many responses — organizations use various solutions to ward off online attacks. The playbooks that outline countermeasures also vary in their specifics. In the CyberGuard project, Fraunhofer researchers are working on standardized playbooks to help companies optimize their security strategies and align them with each other. The playbooks are generated by large language models and support the automation of IT security.

Those responsible for IT security at companies and other organizations outline the defensive measures to counter cyberattacks in documents called playbooks. These documents serve as guides to what to do in case of a cyberattack, such as if an email contains a Trojan, a laptop is infected with malware or the organization’s website is attacked.

So far, each company has relied on its own security concepts and devised its playbooks individually. This means hardly any security-related information is shared between these organizations. And that is a problem, especially when business partners regularly exchange data, as is the case with industrial firms and their suppliers.

With that in mind, a team of researchers from the Fraunhofer Institute for Applied Information Technology FIT embarked on the CyberGuard project to build a standardized framework to ward off attacks. The project’s centerpiece is a set of standardized playbooks containing machine-readable process descriptions. In terms of standards, the researchers are relying on the Collaborative Automated Course of Action Operations (CACAO) open-source format from the Organization for the Advancement of Structured Information Standards (OASIS). The documents created using the CACAO standard are compatible with each other, so they can be shared freely between companies and organizations. “This means even small businesses or start-ups that can’t afford a big IT security department can get playbooks to prepare for an emergency and protect themselves,” adds Mehdi Akbari Gurabi, a data protection and data sovereignty expert at Fraunhofer FIT.

Large language model generates playbooks

The first step is to convert the existing manually generated playbooks, which often exist in text or table format, into machine-readable documents. To do this, the Fraunhofer researchers are harnessing the capabilities of AI-based large language models (LLMs).

The LLM analyzes the texts written by employees in natural language and converts them to the machine-readable CACAO format.

The finished playbooks and the valuable security expertise they contain can be shared with customers or business partners as needed, for example via protected trustworthy platforms. Internal data is left out. “For sharing purposes, the machine-readable step-by-step instructions are worded so abstractly that internal information simply doesn’t appear, including file or drive names,” Akbari Gurabi explains.

Cyberattacks are constantly evolving and becoming more and more refined. That is why Akbari Gurabi and his team of Fraunhofer researchers plan to empower the AI to learn on its own going forward. If a new version of an attack emerges, for example, the AI will update and optimize the relevant playbook based on the existing expertise. The virtual security expert is not left unsupervised in the process, though. Akbari Gurabi explains: “Mistakes are unacceptable in IT security. That’s why CyberGuard involves a stage in which IT managers review the AI-generated machine-readable documents and make sure all the steps make sense.”

Automated processes

The security experts at Fraunhofer FIT are also working to automate the steps defined in the playbooks. Once that is done, the IT system could do things like immediately take action if the intrusion detection system identifies an attack. This eases the burden on IT personnel while also accelerating the response to attacks.

The CyberGuard architecture and the additional research projects based on it promise a wide range of advantages for companies and other organizations: Jointly maintained playbooks allow for optimized responses to attacks by cybercriminals and hackers. Automated workflows accelerate responses and ease the burden on security experts. Business operations are more effectively protected against disruptions. And finally, even small businesses and start-ups gain access to high-quality, professional security solutions.

At present, CyberGuard is still in the pilot phase. Fraunhofer FIT will be showcasing a demonstrator at the Fraunhofer joint booth (Hall 2, Booth B24) at the Hannover Messe 2025 (March 31–April 4, 2025). The AI and security experts will be available during the event to take questions.

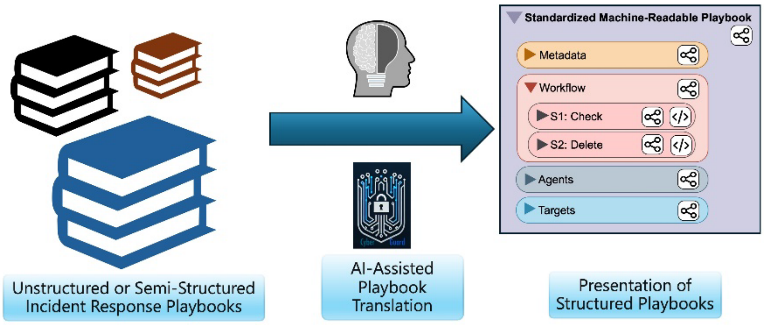
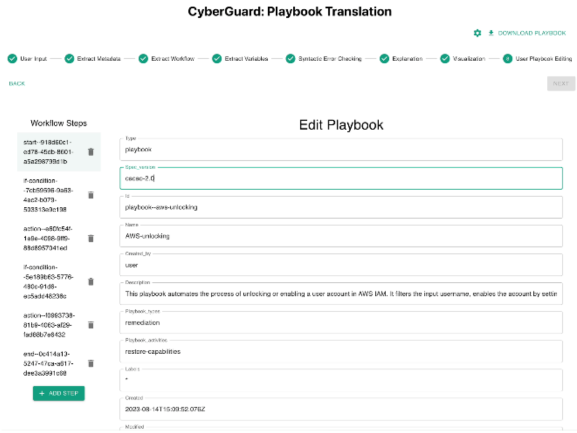


Fig. 1 **Improved protection against cyberattacks: In the CyberGuard project, an AI-based approach converts manually written playbooks into machine-readable ones that can be shared and automated.**

© Fraunhofer FIT



start--918d60c1-ed78-45db-8601-a5a298799d1b
if-condition--7cb59596-9a63-4ac2-b079-503313a9c198
action--a60fc54f-1a9e-4098-9ff9-88d8957041ed
if-condition--5e189b63-5776-480c-91d8-ec5add48238c
action--f0893738-81b9-4063-af29-fad88b7e8432
end--0c414a13-5247-47ca-a617-dee3a3991c89

Type: playbook
Spec_version: cacao-2.0
Id: playbook--aws-unlocking
Name: AWS-unlocking
Created_by: user
Description: This playbook automates the process of unlocking or enabling a user account in AWS IAM. It filters the input username, enables the account by settin
Playbook_types: remediation
Playbook_activities: restore-capabilities
Labels: *
Created: 2023-08-14T15:09:52.076Z
Modified

Fig. 2 **The playbooks generated by the AI through CyberGuard can be modified and edited manually by IT personnel.**

© Fraunhofer FIT