Cyber Shield

Automated Responses to Cyber Security Threats

Graduate

Marco Agostini

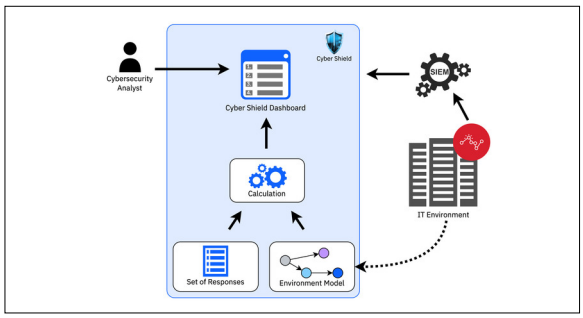
Dominik Ehrle

Initial Situation: Cyber security threats continue to pose a major challenge to organizations. There is an abundance of technologies and products assisting the detection and investigation of cyber security threats. However, supporting security operation teams to respond to threats has received limited attention. Modern Intrusion Prevention Systems (IPS) provide the possibility to react in real-time to cyber security threats but still lack the ability to predict the impact of the responses on the IT infrastructure.

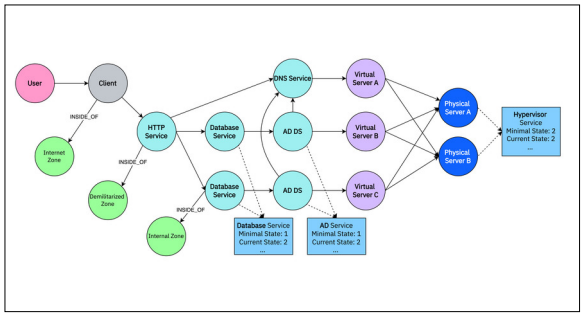
Approach: The work focuses mainly on supporting the cybersecurity analyst in the decision-making process to select the best-suited response to a cyber security threat. The decision making process is enhanced by additional information regarding the IT infrastructure. The responses of a predefined set are compared to the alert attributes to determine the possible responses and their impact on the IT environment. Additionally, the possible responses are prioritized by calculating their impact cost. Consequently, the analyst can decide on the preferred response, considering the impact on the IT environment. The application consists of a fronted, backend and persistency tier. The frontend provides a dashboard, containing relevant information about the alert in order to decide on the best-suited response. Furthermore, it allows the triggering of the desired response. The backend implements an API providing all the required endpoints for interaction, e.g., creating the abstract environment model of the IT infrastructure and persisting it in a graph database.

Result: The Cyber Shield application implements procedures to handle cyber security threats. It provides automated response determination capabilities, where the responses of the predefined set are matched to the alert, identifying the possible responses to the alert based on its attributes. Moreover, the impact calculation evaluates the impact of a response on the IT infrastructure being represented by the environment model. Finally, the possible responses are prioritized by calculating their impact cost with the defined cost function.

Cyber Shield Application Overview
Own presentment



Cyber Shield Environment Model
Own presentment



Cyber Shield Dashboard
Own presentment

Advisor
Prof. Dr. Mitra Purandare

Co-Examiner
Dr. Claudiu Duma, Credit Suisse, Zürich, ZH

Subject Area
Security, Software

Project Partner
IBM Research Europe, Zürich