Response Recommendations to Cyber Security Threats

Cyber Shield - a security incident response impact calculation application

Students

Marco Agostini

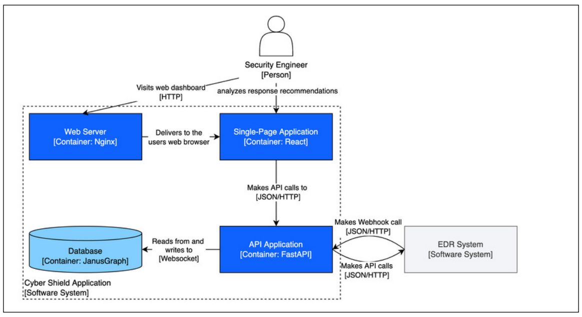
Dominik Ehrle

Initial Situation: Cyber security threats continue to pose a major challenge to organizations. While there is an abundance of technologies and products assisting the detection and investigation of threats, supporting security operation teams in responding to threats has received limited attention. Modern Endpoint Detection and Response (EDR) systems provide the possibility to react in real time to cyber threats, but still lack the ability to predict the impact of the responses on the infrastructure.

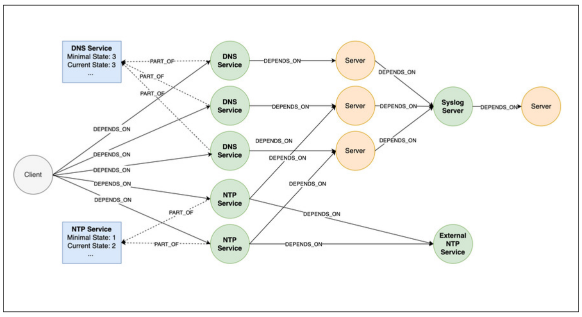
Approach: This student research project realizes a proof-of-concept application for impact calculation of cyber incident responses. The focus is on supporting the cyber security analyst in making a decision on the best suited response by providing additional information about the environment. The application receives security alerts from an EDR system and calculates the impact of possible responses which are then presented to the analyst. Consequently, the analyst can decide on the most suited response, considering its impact on the environment. The application itself is a three-tier architecture which consists of a frontend, a backend, and a persistency tier. The frontend presents the relevant information to the analyst and allows the inspection of alerts and their responses. The backend provides the calculation and alert data handling functionalities. To model and calculate the implications, the environment is abstracted in a graph data model implemented in a persistent graph database. This data model is pre-configured, based on the real environment, and serves as starting point for further elaboration by the analyst.

Conclusion: The application implements different subject areas such as data modelling, matching security responses to given incidents, as well as impact calculation of an incident response under consideration of an environment model. It can retrieve security alerts from an EDR system which are then processed by the backend. This data, together with additional information about the environment, is then visually presented to the analyst.

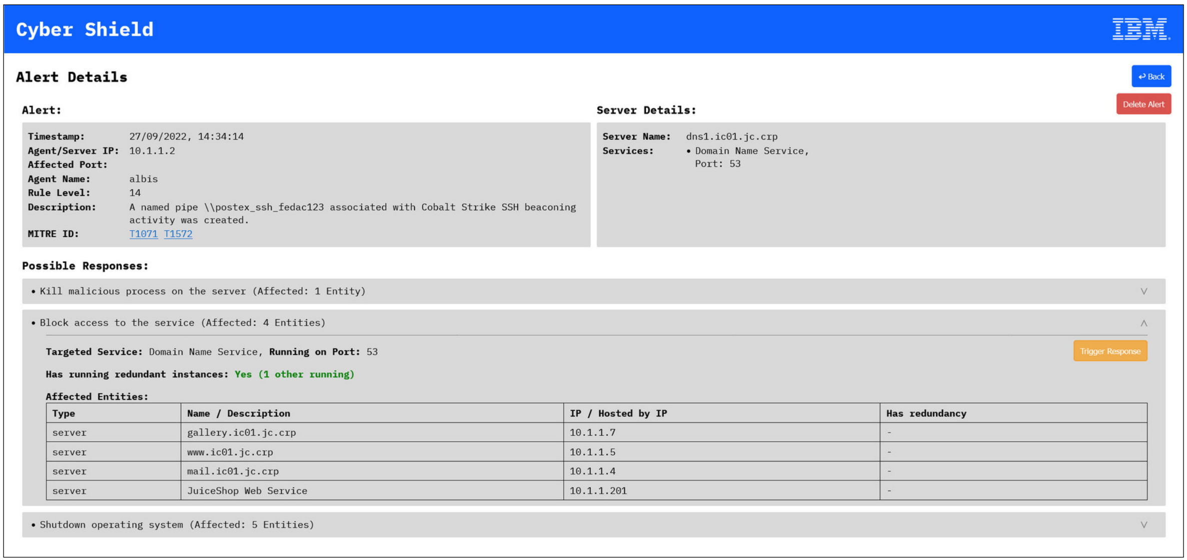
C4 Model - Container Diagram
Own presentment



Graph Data Model
Own presentment



Cyber Shield Dashboard
Own presentment



Alert Details

Alert:

Timestamp: 27/09/2022, 14:34:14
Agent/Server IP: 10.1.1.2
Affected Port:
Agent Name: albis
Rule Level: 14
Description: A named pipe \\postex_ssh_fedac123 associated with Cobalt Strike SSH beaconing activity was created.
MITRE ID: T1071 T1572

Server Details:

Server Name: dns1.ic01.jc.crp
Services:
- Domain Name Service, Port: 53

Possible Responses:

- Kill malicious process on the server (Affected: 1 Entity)
- Block access to the service (Affected: 4 Entities)

Targeted Service: Domain Name Service, **Running on Port:** 53

Has running redundant instances: **Yes (1 other running)**

Affected Entities:

Type	Name / Description	IP / Hosted by IP	Has redundancy
server	gallery.ic01.jc.crp	10.1.1.7	-
server	www.ic01.jc.crp	10.1.1.5	-
server	mail.ic01.jc.crp	10.1.1.4	-
server	JuiceShop Web Service	10.1.1.201	-

- Shutdown operating system (Affected: 5 Entities)

Advisor
Prof. Dr. Mitra Purandare

Co-Examiner
Prof. Dr. Nathalie Weiler

Subject Area
Security, Software

Project Partner
IBM Research Europe, Zurich