Assignment 2

Implementation and Demonstration of Configuration Management Database (CMDB)

Tobias Zeier, the 2nd of December 2024
University of Essex Online

1. Introduction

In this document, the student is going to describe the implementation of a prototype Configuration Management Database (CMDB), tailored to IT security requirements. The solution is built according to the previously submitted design document. For the implementation the student evaluated several products such as GLPI, i-doit, CMDBuild, iTop, ServiceNow and Microsoft Access. Since many of these solutions require setting up a virtual machine where the solution can be installed, the student decided to use ServiceNow's Developer Program because it can be used without any preconditions, the only thing needed is a browser. This was the students first interaction with ServiceNow, he had no prior experience working with such a platform. For better readability, the student has decided to add screenshots of configuration details for all components (i.e. tables, forms, automations, etc.) as an attachment.

2. Implementation Documentation

In the previously submitted document for the first assignment, the student has designed a solution for a CMDB which was tailored for IT security requirements. This includes managing vulnerabilities and compliance in relation to a company's assets and configuration items (CI). There are ready-to-use, preconfigured templates which are accessible on the internet. However, the student decided to start from an empty instance as the instruction prescribes that the implementation is to be carried out exactly as described in the design document.

2.1 Hosting environment

ServiceNow offers a free Personal Developer Instance (PDI), where basic applications can be built in a sandbox without much prior knowledge. They run the same software as paid ServiceNow however, they run on low-performance hardware and hence do not have the same performance as the paid ones. Furthermore, they are not eligible for professional support but there is a forum where developers can get community support.

2.3 Database Schema

As stated above, the task was to implement the solution according to the previously generated design document. In this document, the database schema was outlined as follows.

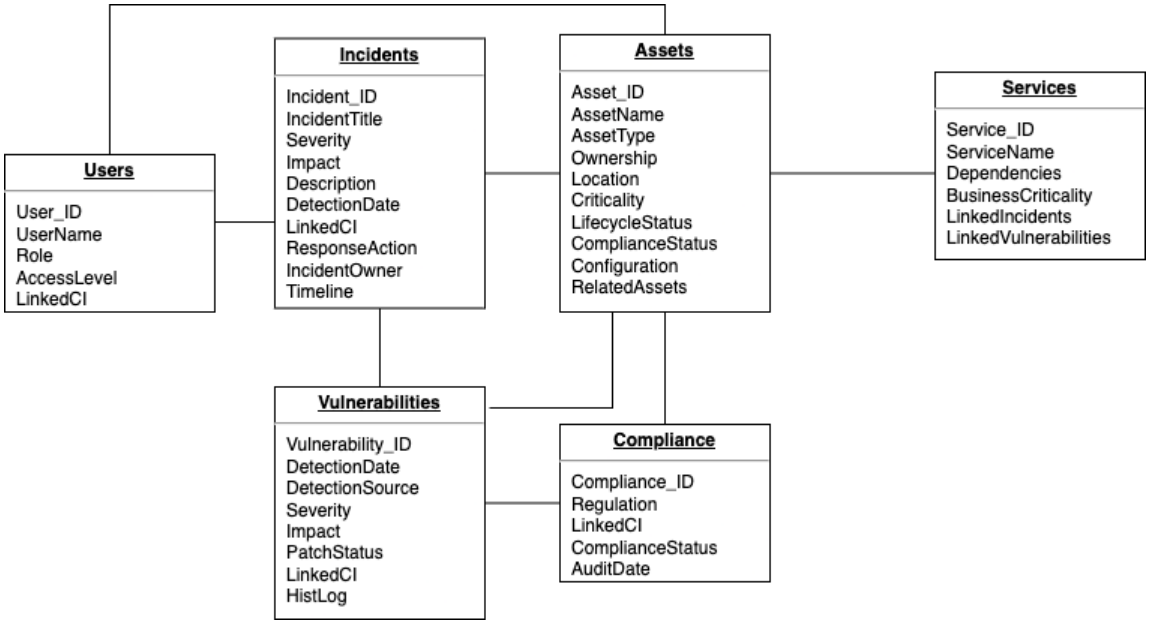

Figure 1: IT Security CMDB Data Schema (Zeier, 2024)

Based on that, the first action on the platform was to create a new application with the name CMDB-ITSecurity. In there, six new tables with the names and fields specified in figure 1 were added. From there relationships between the tables have been setup which allow to reference between each table, e.g. when a new asset is created, a look up to the users table gives the creator the possibility to assign ownership of this asset to a specific user.

2.4 Forms

To be able to populate these tables in a graphical user interface (GUI), a form for each table was created. There, the student chose which fields should be displayed in which position. The student has decided to split the forms into two parts. The upper part contains fields for entering new records. The lower part is for control purposes and shows which user created or changed a record on which date.

2.5 Dashboard

The design document described a dashboard as a home screen, where users can add and remove widgets, according to their preference. These widgets typically show all open incidents, open vulnerabilities, outdated assets and more. Hence, the student has created a dedicated dashboard which can be modified to personal preferences. Initially the dashboard shows the number of open incidents, compliance issues, vulnerabilities as well as outdated assets. Apart from that, users can open overviews for all tables and from there, create, update and delete records. For these lists, filters can be set in order to create and save personal views. Pre-configured lists as well as personal lists can be exported as Excel, CSV, JSON or PDF.

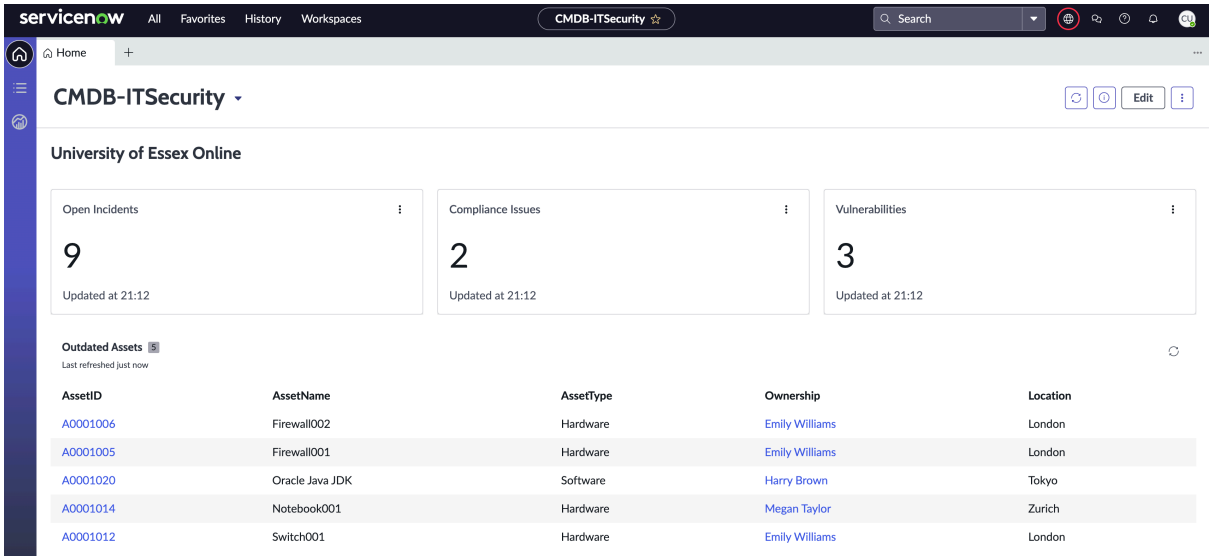

Figure 2: Home-Dashboard of CMDB Prototype

2.5 Security Configuration

Since the outlined solution is a prototype, only three security roles have been created. These roughly differentiate which rights a user can have. The following table outlines the configuration.

Role	Tables	Create	Read	Write	Delete
Admin	All	x	x	x	x
User	All	x	x	x	
Read-Only	All		x		

Table 1:Security Roles (Zeier, 2024)

2.6 Automation

ServiceNow's PDI offers to add automations such as flows, where a sequence of actions that execute based on a trigger can be assembled. Several flows or sub flows can then be put together as a process for an end-to-end business workflow. To bring in some automation, the student has decided to add two flows, one automatically creates an incident as soon as an asset, which is outdated, is created or updated. Another one automatically creates an incident immediately when a new vulnerability is created. Both automations are enriched with data from the record which triggered the action. For example, when an asset is outdated, the incident contains the information about the affected asset.

3. Critical Analysis

The importance of IT security increases steadily, by utilising integrated platform solutions, establishing logical environments, and incorporating CMDB systems with asset-centric secrets, organisations can enhance their cybersecurity measures, improve operational efficiency, and ensure compliance with regulatory standards (Pillala, 2024).

This analysis is supported by the student however, it needs to be added, that only by fully integrating these system with each other as well as setting up as much

automation as possible, the compounded systems can result in an advantage when it comes to staying on top with vulnerabilities and regulations. Otherwise the company is lagging behind which can result in sever financial losses. After critically analysing the submitted prototype, it can be argued that there could have been more automation which would minimise manual operations. For example when a new vulnerability is detected, not only an incident should be created but there should also be a flag on the asset itself so it correlates through the whole system.

To mitigate the impact of vulnerabilities within a software system, it is essential to implement a continuous monitoring process. This process should include regular scanning to identify vulnerabilities and generate reports documenting potential security breaches. Such monitoring must account for the system's evolution in response to attacks, consolidating resources to provide a comprehensive overview of the system. This enables the prediction of the potential effects of vulnerabilities on the system as a whole or on individual components (Aldea et al., 2020).
This could be done by using vulnerability scanners which automatically detect potential threats. Other tools such as Elasticsearch can detect annomalies by using Machine Learning (ML).

4. Conclusion

Dande and Li (2023) conclude in their literature review, that numerous organisations have faced challenges in implementing effective Enterprise Service Management (ESM) software equipped with robust configuration management modules, particularly in the era of cloud computing. Given the abundance of providers in the market and the increasing cybersecurity threats, employing a CMDB Selection Matrix Model (CSMM) as an initial framework offers organisations a validated approach for making well-informed decisions.
The author agrees whith this statement as he experiences an increasing number of IT security threats in his job as a teamlead of a DevOps team within the banking sector. It is crucial to every business to have an overview of all their assets in relation to possible threats in order to be able to react imediately once an issue occures. Furthermore, companies need to make sure to be complient to all regulations which apply to their business and hence need a system which allows them to stay on top of that. Hence, fully integrated CMDB which covers these aspects is crucial for successfully managing vulnerabilities, threats and compliance aspects.

Word count: 1247

References

Zeier, T. (2024) Assignment 1: Design and Demonstration of Configuration Management Database (CMDB) for IT Security Management. *ITSM November 2024*. Essay submitted to the University of Essex Online.

Zeier, T. (2024) Assignment 2: Implementation and Demonstration of Configuration Management Database (CMDB). *ITSM December 2024*. Essay submitted to the University of Essex Online.

Pillala, G. (2024) Fortifying the Digital Bastion: Pioneering Cybersecurity with Dynamic Secrets Management and CMDB Fusion in the Enterprise. *Journal of Information Security* 15(04): 411–418. DOI: https://doi.org/10.4236/jis.2024.154023

Aldea, M., Gheorghică, D. and Croitoru, V. (2020) 'Software Vulnerabilities Integrated Management System', *2020 13th International Conference on Communications (COMM)*. Bucharest, Romania, 18-20 June. 97-102. IEEE Xplore. DOI: https://doi.org/10.1109/COMM48946.2020.9141970

Dande, F., & Li, X. (2023) 'Enterprise Service Management Cybersecurity Threats: Exploring Cloud Configuration Management Database (CMDB) Implementation Within Community Colleges', *8th North America Conference on Industrial Engineering and Operations Management.* Huston, Texas, USA, 13-16 June.