CENTENE Corporation

2024 Internship Program

XSOAR Inventory Dashboard

Evan Marlo Anderson
Advanced Cybersecurity Technology

PROJECT OVERVIEW

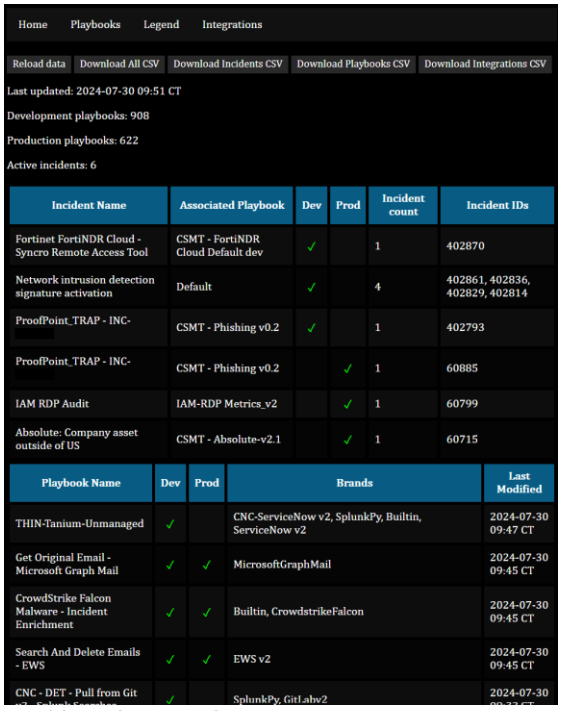
Cortex XSOAR is a SOAR (security orchestration, automation and response) platform used by many teams at Centene. XSOAR allows teams to automate security response tasks, enriches incident data, and offers threat intelligence. This inventory provides a summary of all playbooks, incidents, and integrations within XSOAR that isn't readily available within the platform.

OUTCOMES

Playbooks in XSOAR are automated security processes. Centene has hundreds of production playbooks and hundreds more that are currently in development. Multiple incidents of a playbook can exist at any time, and playbooks integrate with external tools. With so many parts, it can be difficult for XSOAR administrators to keep track of everything. This dashboard makes it easier to see and track all playbooks, incidents, and integrations in XSOAR.

Another feature of the dashboard is the ability to download the data as a CSV file. This allows users to take a "snapshot" of XSOAR at that moment in time.

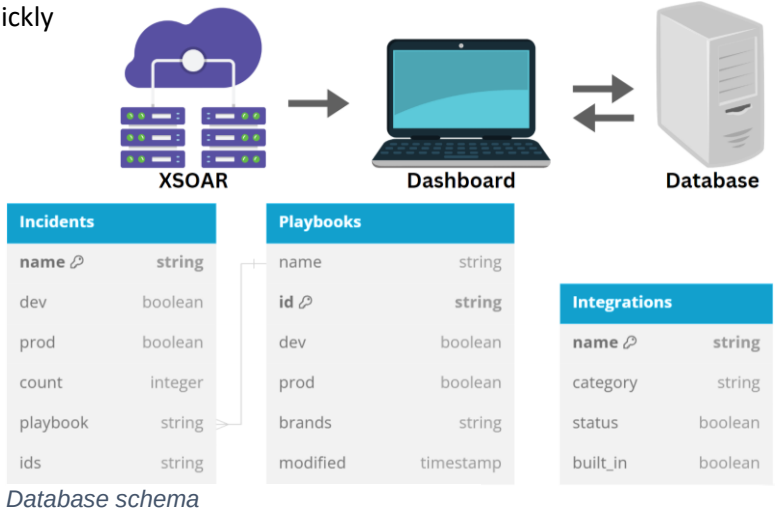
The dashboard also contains a legend, mapping team names to their acronyms in XSOAR. This allows users to quickly know which playbooks belong to which teams.



Dashboard screenshot

DESIGN

The dashboard is built in Django, a Python web framework. It pulls data from the XSOAR API, filters relevant fields, and stores it in a SQL database. Users can trigger an update process to replace the database with current data. This will be done periodically as it typically takes about five minutes to request and process all of the data.



Database schema

Institution: **Utah State University**
Manager: **Nick Isaacs**