

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.

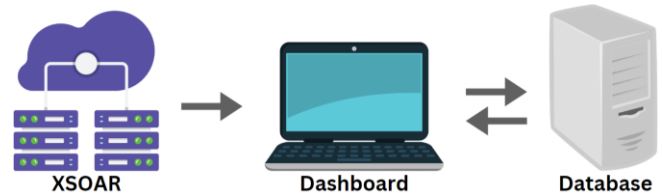
DESIGN

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.

Incident Name	Associated Playbook	Dev	Prod	Incident count	Incident IDs
Fortinet FortiNDR Cloud - Syncro Remote Access Tool	CSMT - FortiNDR Cloud Default dev	✓		1	402870
Network intrusion detection signature activation	Default	✓		4	402861, 402836, 402829, 402814
ProofPoint_TRAP - INC-	CSMT - Phishing v0.2	✓		1	402793
ProofPoint_TRAP - INC-	CSMT - Phishing v0.2		✓	1	60885
IAM RDP Audit	IAM-RDP Metrics_v2		✓	1	60799
Absolute: Company asset outside of US	CSMT - Absolute-v2.1		✓	1	60715

Playbook Name	Dev	Prod	Brands	Last Modified
THIN-Tanium-Unmanaged	✓		CNC-ServiceNow v2, SplunkPy, Builtin, ServiceNow v2	2024-07-30 09:47 CT
Get Original Email - Microsoft Graph Mail	✓	✓	MicrosoftGraphMail	2024-07-30 09:45 CT
CrowdStrike Falcon Malware - Incident Enrichment	✓	✓	Builtin, CrowdStrikeFalcon	2024-07-30 09:45 CT
Search And Delete Emails - EWS	✓	✓	EWS v2	2024-07-30 09:45 CT
CNC - DET - Pull from Git	✓		SplunkPy, Git1abw2	2024-07-30 09:45 CT

Dashboard screenshot



Incidents		Playbooks		Integrations	
name	string	name	string	name	string
dev	boolean	id	string	category	string
prod	boolean	dev	boolean	status	boolean
count	integer	prod	boolean	built_in	boolean
playbook	string	brands	string		
ids	string	modified	timestamp		

Database schema

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