Splunk Dashboard,alerts, and report

Daniel Cruz

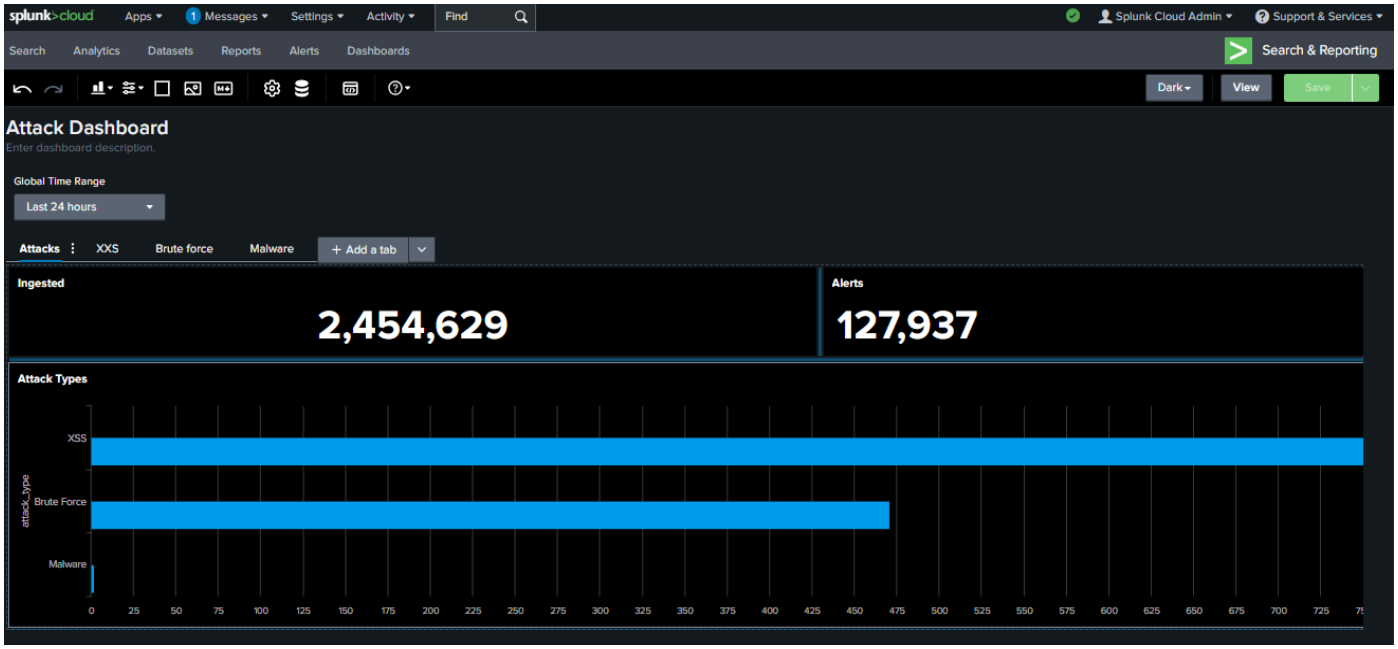
8/30/25

Logs created From AIT LDS V1_1

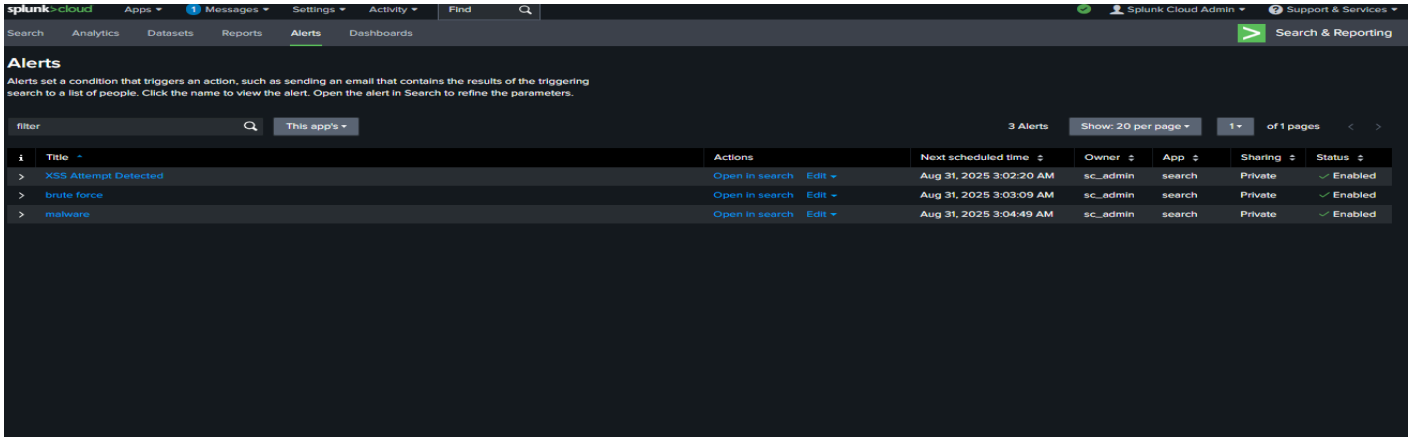
Summary

This Splunk project detects and visualizes XSS, Brute Force, and Malware activity across multiple sourcetypes, using dashboards, alerts, and aggregated SPL searches.

Overview Dashboard

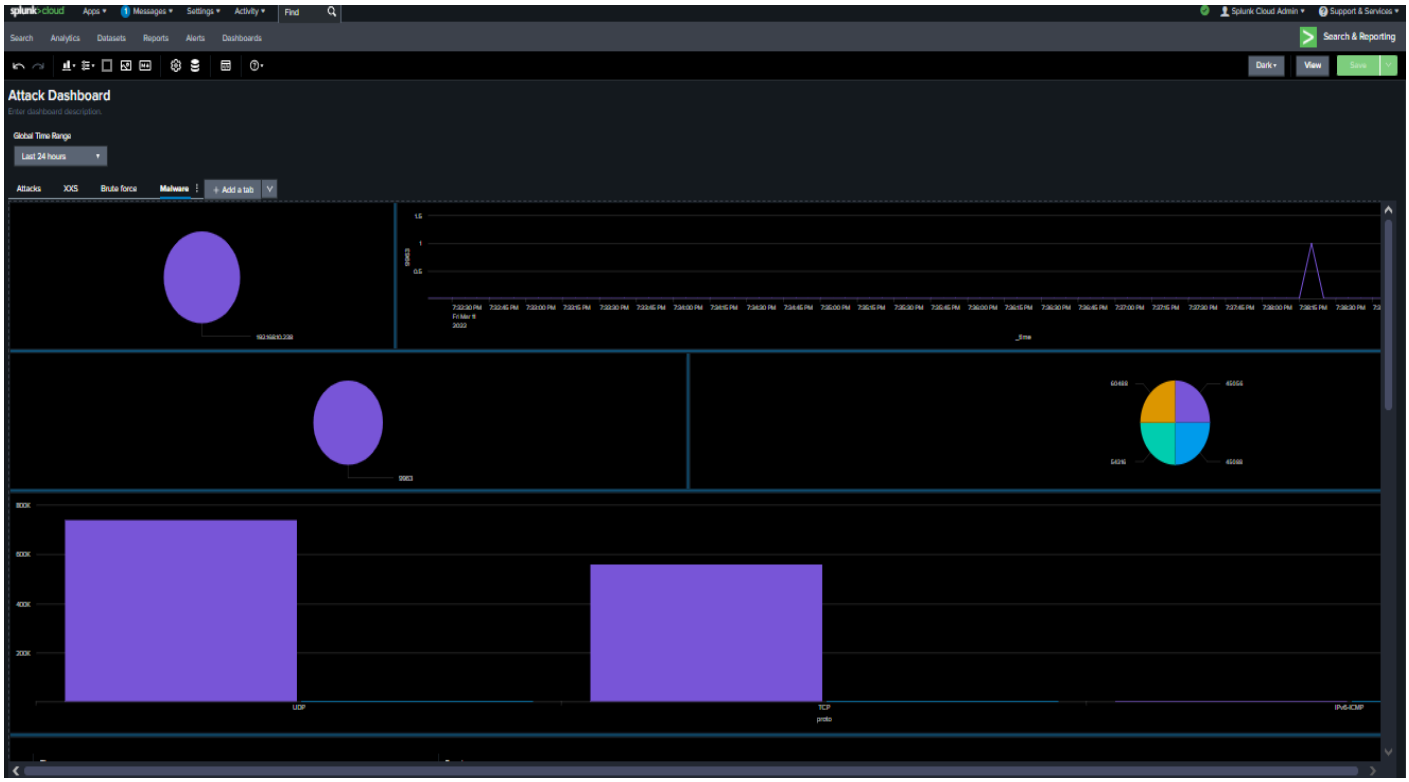


Alerts



Attack Type: XSS Injection Attempt
Number of Events: 263
Source IP: 192.168.10.238
Time Range: 2025-03-20 19:15:00
Behavior/Notes: Single-source automated scan

Attack Type: Malware
Number of Events: 2
Destination IP: 192.168.10.238
Destination Port: 9963
Time Range: 2020-03-04 19:38:24 – 19:39:29
Behavior/Notes: Small number of malicious events targeting port 9963



Attack Type: Brute Force
Number of Events: 429
Source IP (RIP): 127.0.0.1
User: Daryl
Time Range: 2024-03-04 19:29:33
Behavior/Notes: 429 failed login attempts under user “Daryl” at 7 PM