

Splunk Dashboard,alerts, and report

Daniel Cruz

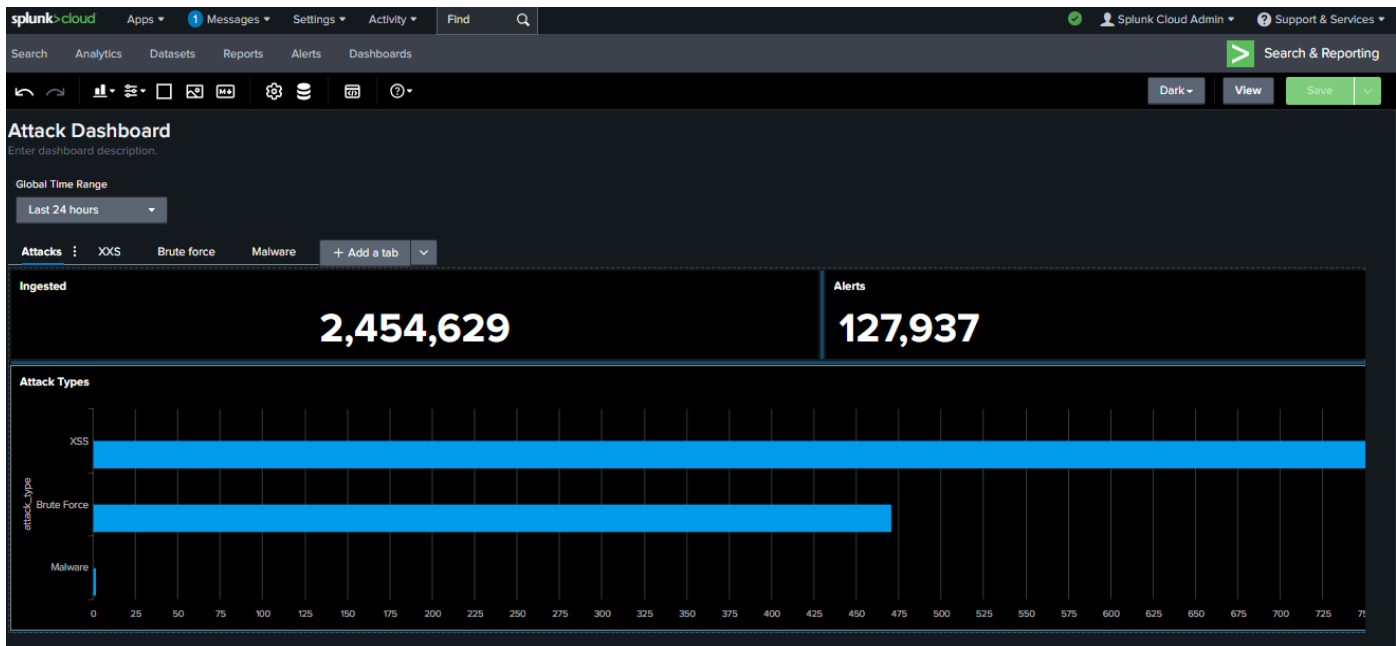
8/30/25

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

The screenshot displays the 'Alerts' page in Splunk Cloud. The top navigation bar includes 'splunkcloud', 'Apps', 'Messages', 'Settings', 'Activity', and a search bar. Below the navigation bar, there are tabs for 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The page title is 'Alerts' with a description 'Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.' Below the description is a search bar and a 'This app's' button. The main content area shows a table of alerts with columns: 'Title', 'Actions', 'Next scheduled time', 'Owner', 'App', 'Sharing', and 'Status'. There are 3 alerts listed.

Title	Actions	Next scheduled time	Owner	App	Sharing	Status
XSS Attempt Detected	Open in search Edit	Aug 31, 2025 3:02:20 AM	sc_admin	search	Private	Enabled
brute force	Open in search Edit	Aug 31, 2025 3:03:09 AM	sc_admin	search	Private	Enabled
malware	Open in search Edit	Aug 31, 2025 3:04:49 AM	sc_admin	search	Private	Enabled

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

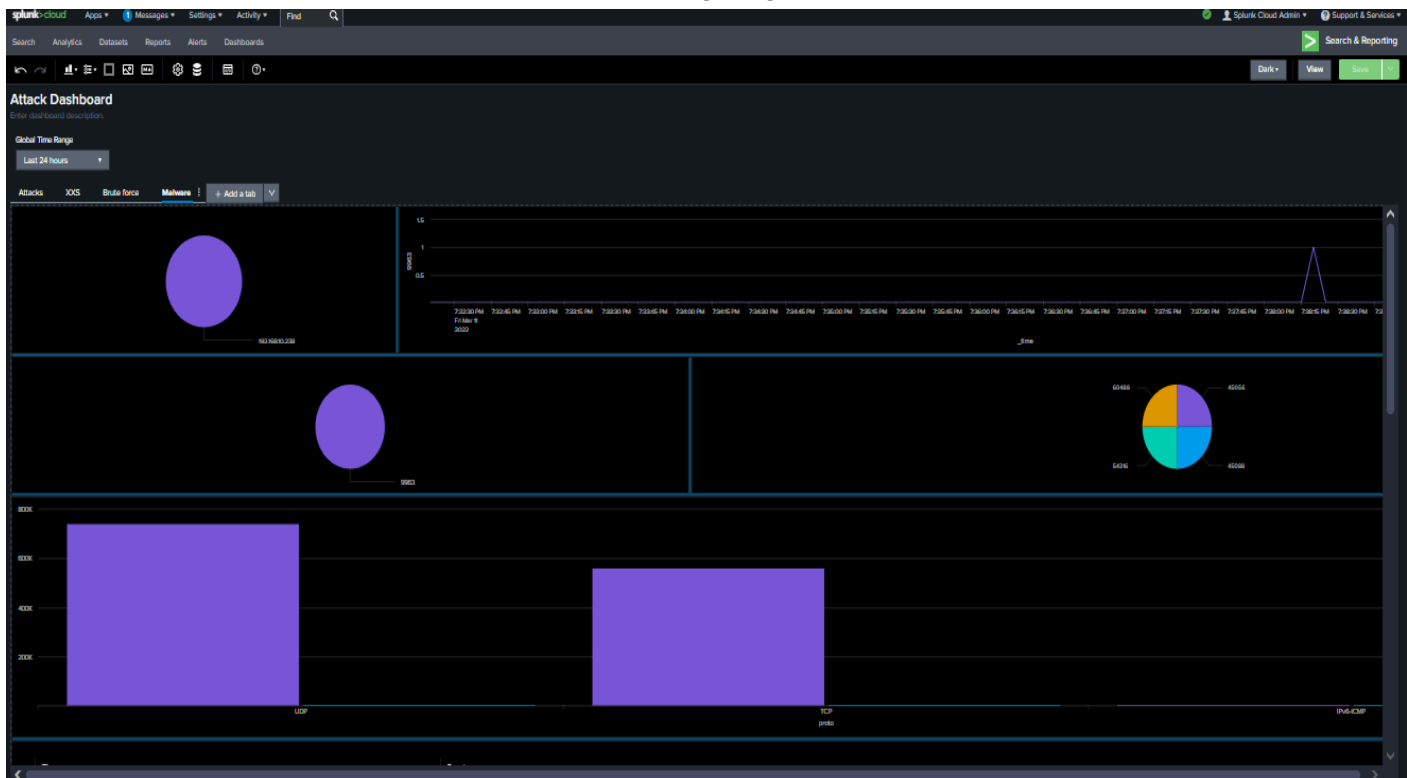
Number of Events: 2

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

