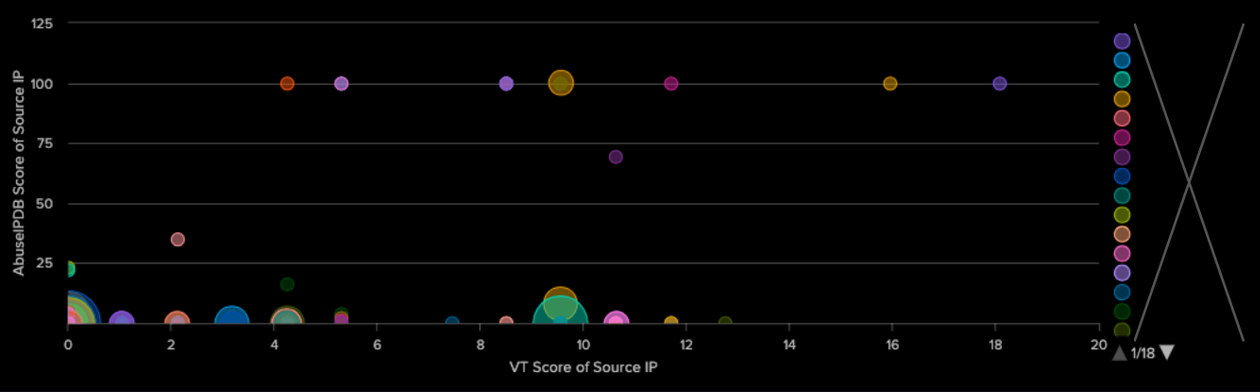
NGF...

Analyzer on NGFW logs

Time Range: 20:59:42 – 20:59:50, 16 Apr 2025 | TI Verdicts: All (1) | Connection Type: All | Source IP: * | Destination IP: * | Actions: All (1) | Applications: All (1)

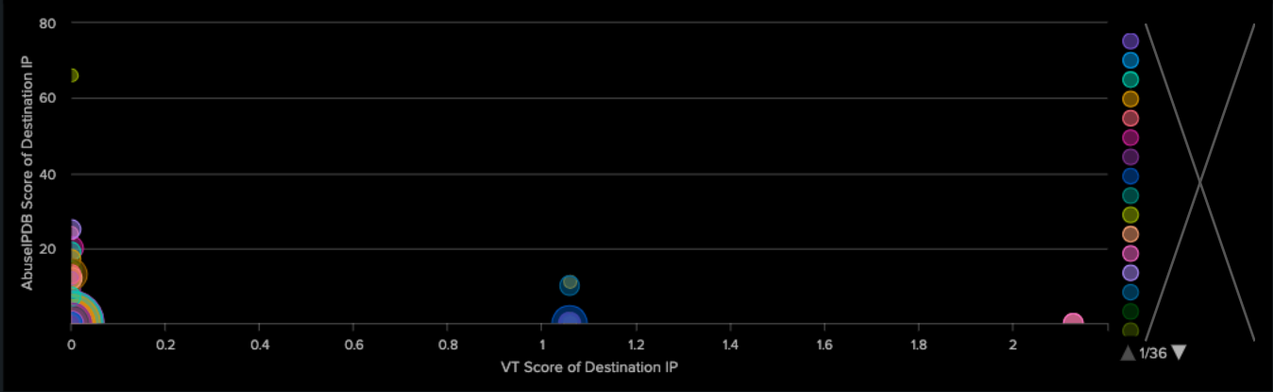
Source IPs Overview

Overview of public source IPs with enrichment from threat intelligence feeds, helping identify high-risk targets based on connection volume and TI scoring



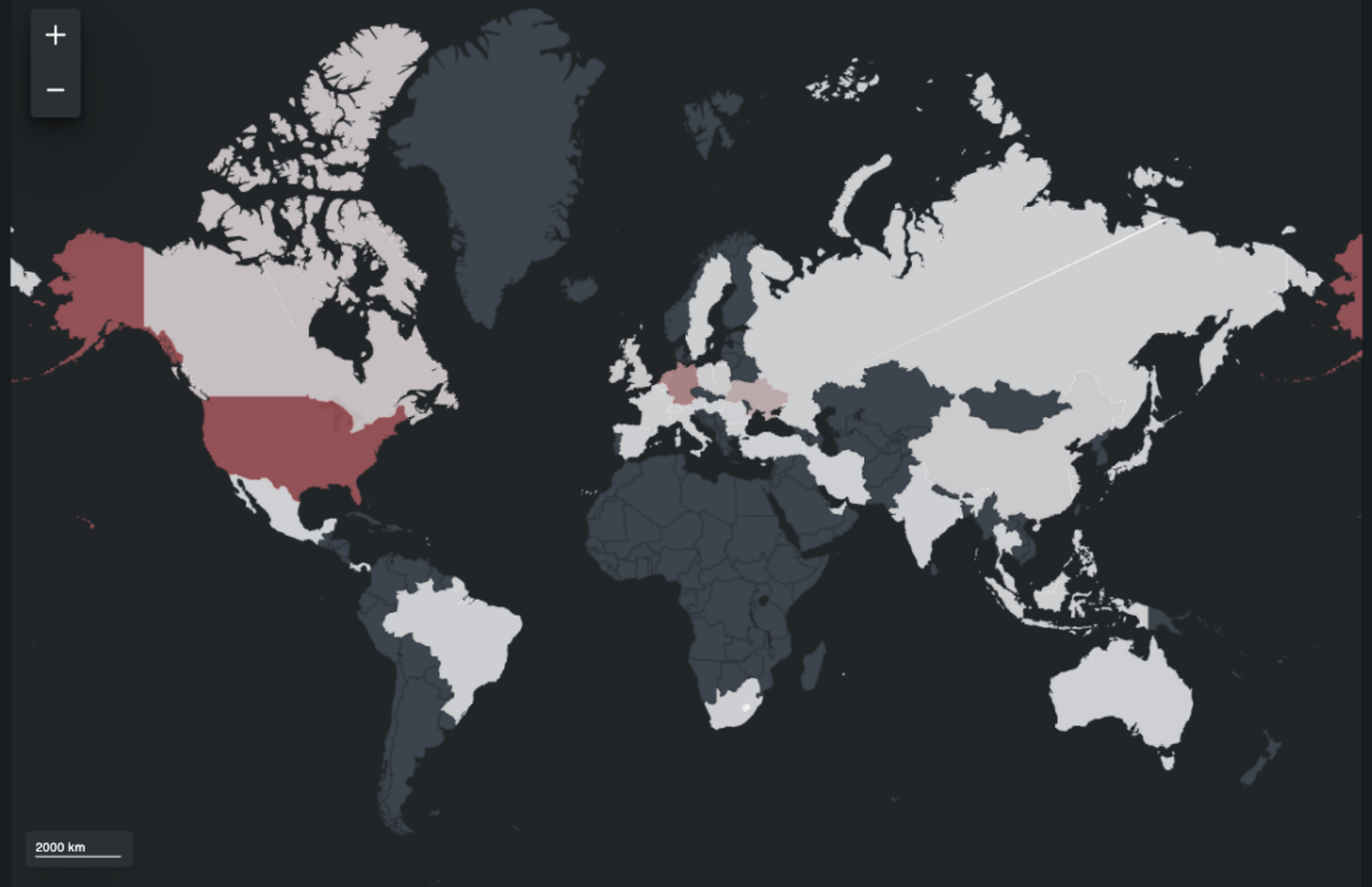
Destination IPs Overview

Overview of public destination IPs with enrichment from threat intelligence feeds, helping identify high-risk targets based on connection volume and TI scoring



Communications with countries

Displays the geographic distribution of public IPs involved in NGFW-detected events to highlight global activity patterns.



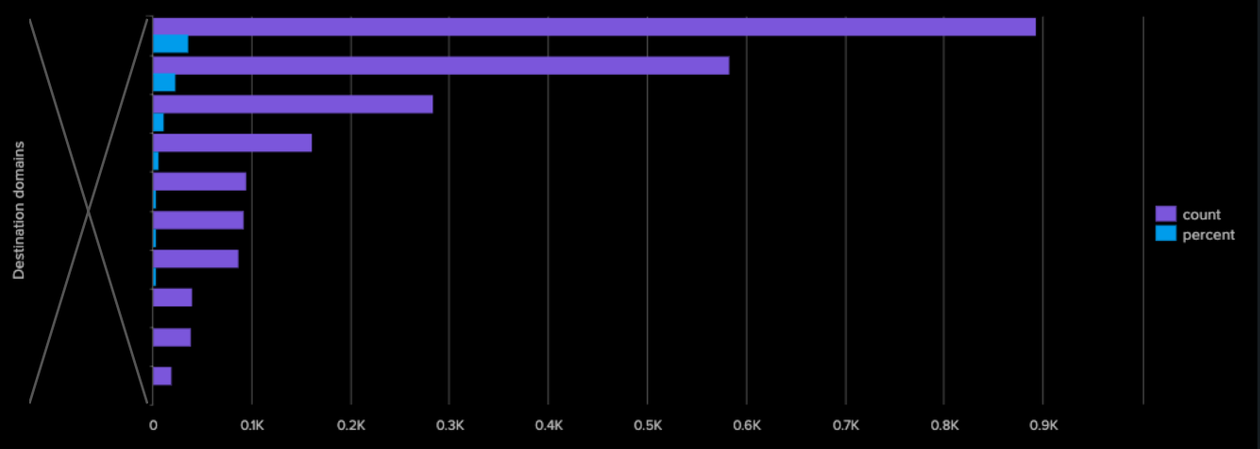
Connections from High-Risk Countries

Details connections originating from countries listed in lookup. Allows focused review of potentially dangerous communications.

Country	Total Connections From Country	Source IPs	TI verdict
Iran	1		Suspicious
Panama	1		Suspicious
Romania	1		Suspicious
Thailand	1		Suspicious
Brazil	7		Harmless
India	8		Harmless
Russia	11		Harmless Suspicious
Indonesia	13		Harmless Suspicious

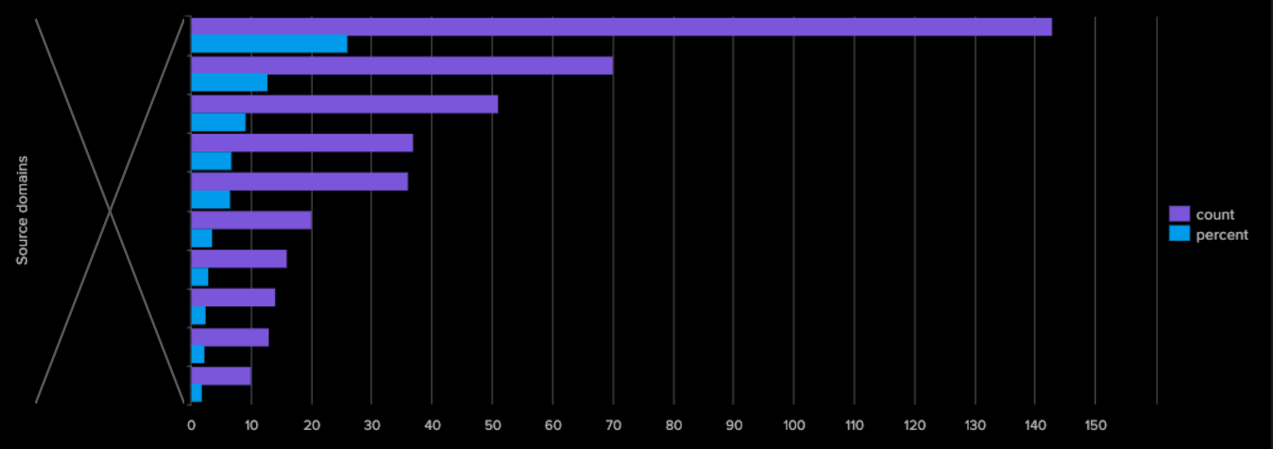
Top destination domains

Displays the most frequently accessed destination domains by users or systems within the network. Helps identify web usage trends and potential command-and-control (C2) domains.



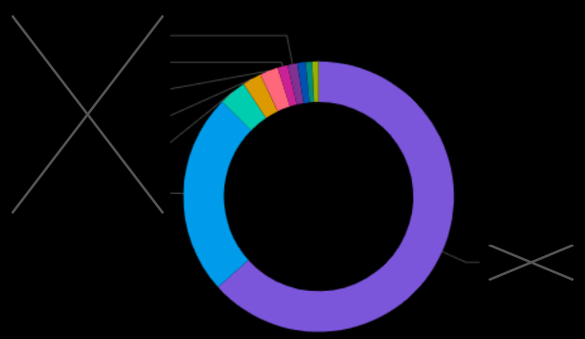
Top source domains

Shows domains associated with source IP addresses generating traffic, or domains from which traffic originates towards the organization's public resources.



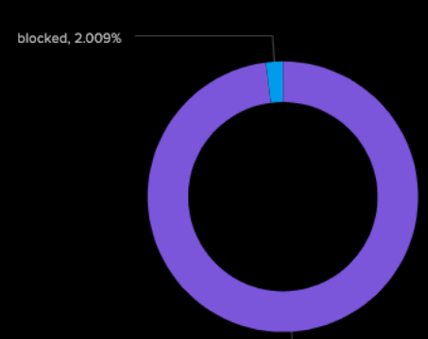
Top 10 most used applications

Shows the 10 most frequently used applications (as classified by Palo Alto Networks) by connection count.



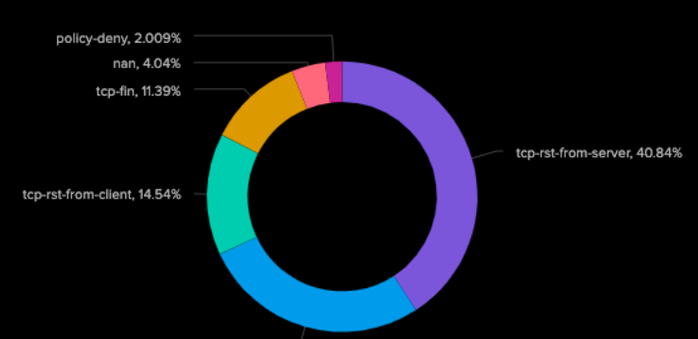
Statistic by the action

Shows the ratio of allowed traffic to blocked traffic



Session End Reason Distribution

Visualizes the primary reasons for network session termination. Aids in diagnosing network issues.



Network Connection Details

Shows the details abount network connections based on NGFW logs

#	Time	TI Verdict	AbuseIPDB Score for Source	VT Score for Source	Destination IP	Destination port	AbuseIPDB Score for Destination	VT Score for Destination	Action	Rule	Application
1	2025-04-16 20:59:46	Unknown	Private IP	Private IP		1500	Private IP	Private IP	allowed	Rule_66	informix
2	2025-04-16 20:59:46	Unknown	Private IP	Private IP		902	Private IP	Private IP	allowed	Rule_158	vmware
3	2025-04-16 20:59:46	Unknown	Private IP	Private IP		389	Private IP	Private IP	allowed	Rule_71	ldap
4	2025-04-16 20:59:46	Unknown	Private IP	Private IP		902	Private IP	Private IP	allowed	Rule_159	vmware
5	2025-04-16 20:59:46	Suspicious	16	4.26		465	0	0.00	blocked	Rule_14	not-applicable
6	2025-04-16 20:59:45	Harmless	0	0.00		80	0	0.00	allowed	Rule_124	web-browsing
7	2025-04-16 20:59:46	Harmless	0	0.00		10051	0	0.00	allowed	Rule_147	ssl
8	2025-04-16 20:59:46	Suspicious	0	7.45		9080	0	0.00	blocked	Rule_16	not-applicable
9	2025-04-16 20:59:45	Harmless	0	0.00		443	0	0.00	allowed	Rule_2	web-browsing
10	2025-04-16 20:59:45	Harmless	0	0.00		443	0	0.00	allowed	Rule_2	web-browsing

< Prev 1 2 3 4 5 ... Next >