## NGF... ▼ Analyzer on NGFW logs Time Range TI Verdicts Threat Severities Connection Type Source IP Destination IP Applications Actions Subtypes medium, low All All 20:59:42 – 20:59:50,... **▼** (2) 🕶 Threats by Severities Threats Severities over Time Line chart showing the count of threats at different Palo Alto Networks severity levels over the selected time period. Allows tracking of threat spikes and general trends. Displays the percentage distribution of detected threats by severity levels defined by Palo Alto Networks. low, 50% medium, 50% 20:59:42 Wed Apr 16 2025 20:59:43 20:59:44 20:59:45 20:59:46 20:59:47 20:59:48 20:59:49 \_time TI Verdicts over Time Threats by TI verdicts Demonstrates how detected threats are distributed according to TI verdicts for IPs associated with the threats. Displays how the count of threats with different TI verdicts has changed over time. Helps assess the evolution of the threat landscape. Harmless, 43.75% Unknown, 56.25% 20:59:42 Wed Apr 16 2025 20:59:43 20:59:44 20:59:45 20:59:46 20:59:47 20:59:48 20:59:49 **Detailed Threat Event Information** Provides a comprehensive table with details of threat events Source IP Source port AbuseIPDB VT Score Destination Destination Time \$ TI Verdict \$ AbuseIPDB TYPE Rule \$ Triggered Severity \$ Action \$ Application \$ Log Score for IΡ port Score for for Subtype Source Destination Destination 2025-04-16 62499 80 0.00 Harmless Private IP Private IP allowed Rule\_37 ms-update file 20:59:46 2025-04-16 38522 10050 Private IP Private IP Unknown Private IP Private IP allowed not-applicable nan scan 20:59:46 2025-04-16 Harmless 48908 Private IP Private IP 443 0.00 allowed not-applicable nan scan 20:59:46 2025-04-16 65321 Private IP Private IP 445 Private IP Private IP allowed Rule\_176 ms-ds-smbv3 file 20:59:46

2025-04-16

20:59:46

2025-04-16

20:59:46

2025-04-16

20:59:46

Unknown

Unknown

Harmless

37005

37005

20776

Private IP

Private IP

Private IP

Private IP

Private IP

Private IP

25

25

80

Private IP

Private IP

Private IP

Private IP

0.00

allowed

allowed

allowed

Rule\_168

Rule\_168

Rule\_202

smtp-base

smtp-base

web-browsing

file

file

file

<Prev 1 2 Next>