AI for Network Operations

AI-Powered Root Cause Analysis, Anomaly Detection, and Remediation

Instant Network Intelligence with Natural Language

Analyze billions of network events instantly. Identify outages, troubleshoot routing issues, and detect anomalies without complex query syntax.

Sample AI Prompt

> *"Generate an incident report for the last 2 hours comparing against yesterday's baseline. Correlate events across all network devices to identify root causes. Include anomaly detection, priority matrix, and vendor-specific remediation commands."*

From a single prompt, the AI analyzes billions of events and delivers:

What You Get

Executive Summary	Priority Matrix	Anomaly Detection
Cross-Device Correlation	Remediation Playbook	Escalation Contacts

Priority Matrix (from real report)

Priority	Issue	Affected Device
P0	FW Event Storm (+400%)	CORE-FW-01
P1	IP Spoofing Attacks	EDGE-FW-01
P2	DNS Amplification	dns-01/dns-02
P3	STP Loop Guard	sw-access-01 Gi1/0/24

Cross-Device Correlation

Device	Events	vs Baseline
CORE-FW-01	1.88M	+400%
ise-psn01	400K	+79%
app-server-01	409K	+115%

Anomaly Detection (from real report)

Metric	Current	Baseline	Delta
Total Events	6.65M	4.08M	+62.9%
Critical (Sev 3)	455K	442K	+2.9%
Emergency (Sev 1)	4	2	+100%
Events/Min	55K	34K	+62.9%

Vendor-Specific Remediation

```
# Cisco FTD — Reduce logging storm
show logging setting
configure logging level FirePower warning

# Cisco IOS — STP Loop Guard
show spanning-tree interface Gi1/0/24 detail
show cdp neighbors Gi1/0/24 detail

# Infoblox — Block attacking IPs
set threat_protection blocked_ip add 82.29.53.218
```

Key Capabilities

Root Cause Analysis	**Baseline Comparison**	**Cross-Device Correlation**
Instant identification of failure chains	*Automatic anomaly detection vs. normal*	*Link events across routers, switches, FWs*

Log Sources

LogZilla accepts logs from **any syslog-compatible source**. App Store integrations include:

Routing/Switching
Cisco IOS/Nexus, Juniper, HP

Wireless
Cisco WLC/Meraki, Ubiquiti, Ruckus

DNS/DHCP
Infoblox, Linux BIND/DHCPd

Firewalls
Palo Alto, Fortigate, Cisco ASA/FTD

Identity
Cisco ISE, Windows/AD

+ More
Any syslog, API, or file source