LOGZILLA

AI for Security Operations
www.logzilla.net

AI for Security Operations

AI-Powered Threat Detection, IOC Extraction, and MITRE ATT&CK Mapping

Transform Your SOC with Natural Language AI

Query billions of security events instantly. Get threat intelligence, IOC extraction, and automated remediation guidance without writing complex queries.

Sample AI Prompt

```
"Generate a security incident report for the last 24 hours.
Correlate events across firewalls, IDS, and endpoints to
identify attack chains. Include IOC extraction, MITRE
ATT&CK mapping, and remediation commands."
```

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

What You Get

Threat Intel
Attack Correlation
IOC Extraction
Remediation Playbook
MITRE Mapping
Escalation Contacts

AI-Generated Threat Intel

Source IP	Country	Threat	Action
45.142.xxx.xxx	Russia	Brute Force	Blocked
185.220.xxx.xxx	Germany	Port Scan	Blocked
23.94.xxx.xxx	US	DNS Amp	Rate Ltd

MITRE ATT&CK Mapping

Technique	Tactic	Evidence
T1110.001	Credential Access	12,453 SSH failures
T1498.002	Impact	DNS amplification
T1046	Discovery	Port scanning
T1071.004	C2	Suspicious DNS

AI-Generated Report (Excerpt)

Finding	Severity	Events
DNS Amplification Attacks	Critical	847
Failed SSH Authentication	High	12,453
Firewall Deny Events	Medium	156,892
Certificate Failures	Medium	2,341

Automated Remediation

```
# Cisco ASA - Block attacker
access-list OUTSIDE_IN deny ip host 45.142.xxx.xxx any

# Palo Alto - Create EDL block
set address "Threat-Actor-1" ip-netmask 45.142.xxx.xxx/32

# Fortinet - Block and log
config firewall address
  edit "blocked-attacker"
  set subnet 45.142.xxx.xxx/32
```

Security Frameworks

Framework	AI Capability
MITRE ATT&CK	Auto-mapping to techniques
NIST CSF	Identify/Protect/Detect/Respond
CMMC	Compliance evidence gathering
PCI-DSS	Log review and anomaly detection

Key Capabilities

Threat Hunting

Natural language queries across all security logs

IOC Extraction

Auto-identify malicious IPs, domains, hashes

MITRE ATT&CK Mapping

Auto-map events to techniques and tactics

Log Sources

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

Firewalls

Palo Alto, Fortigate, Cisco ASA/Firepower, Check Point, SonicWall, WatchGuard

IDS/IPS

Zeek, Snort, Fail2ban

Network

Cisco IOS/Nexus/WLC/Meraki, Juniper, Infoblox, Ubiquiti

Identity

Cisco ISE, Windows/AD, Linux PAM

Cloud

Palo Alto Prisma, AWS VPC Flow Logs

+ More

Any syslog, API, or file-based source

Contact: sales@logzilla.net | www.logzilla.net