LOGZILLA DOCUMENTATION

Snort

LogZilla App Store application: Snort

LogZilla App Store · Generated April 27, 2026 · logzilla.ai/docs/logzilla-appstore/snort

Overview

Snort is an open-source, free and lightweight network intrusion detection system (NIDS) and intrusion prevention system (IPS). It is capable of performing real-time traffic analysis and packet logging on IP networks. Snort uses a rule-based language combining signature, protocol, and anomaly inspection methods to detect malicious activity.

Developed by Sourcefire (now part of Cisco), Snort can be configured to run in three main modes: sniffer, packet logger, and network intrusion detection. It can detect a wide variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

App Function

- Parse Snort alert_fast and alert_syslog format log messages
- Extract network metadata (IPs, ports, protocol)
- Categorize events by Snort classification and severity
- Provide dashboards for threat hunting and alert triage
- Alert on critical severity, malware, privilege escalation, and DoS events

Vendor Documentation

- Snort Official Website (https://www.snort.org/)
- Snort Documentation (https://www.snort.org/documents)
- Snort 3 Alert Logging (https://docs.snort.org/start/alert_logging)

Device Configuration

Configure Snort to send alerts to syslog and forward to LogZilla:

Snort 3

Run Snort with the `alert_syslog` output module:

```
snort -A alert_syslog -c /etc/snort/snort.lua
```

Alerts are sent to the local system logger with program name `snort`.

Snort 2

Edit `/etc/snort/snort.conf` and enable syslog output:

```
output alert_syslog: LOG_LOCAL5 LOG_ALERT
```

Forward to LogZilla

Configure the local syslog daemon to forward Snort alerts to LogZilla:

rsyslog (`/etc/rsyslog.d/snort.conf`):

```
:programname, isequal, "snort" @@LOGZILLA_IP:514
```

syslog-ng:

```
destination d_logzilla { tcp("LOGZILLA_IP" port(514)); };
filter f_snort { program("snort"); };
log { source(s_local); filter(f_snort); destination(d_logzilla); };
```

Verification

Generate test traffic or trigger a rule, then verify events appear in LogZilla with program name `snort`.

Incoming Log Format

The Snort logs processed by the app follow the alert_fast format:

```
<date>  [**] [<gid>:<sid>:<rev>] <msg> [**] [Classification: <classification>] [Priority: <priority>]
{<proto>} <src_ip>:<src_port> -> <dst_ip>:<dst_port>
```

Where:

- `<date>` is the timestamp (MM/DD-HH:MM:SS.microseconds)
- `<gid>` is the Generator ID (rule group)
- `<sid>` is the Signature ID (rule identifier)
- `<rev>` is the rule revision
- `<msg>` is the alert message (may be quoted in Snort 3)

- <classification> is the threat classification category
- <priority> is the alert priority (1=highest, 4=lowest)
- <proto> is the network protocol (TCP, UDP, ICMP)
- <src_ip> and <src_port> are the source IP address and port
- <dst_ip> and <dst_port> are the destination IP address and port

Parsed Metadata Fields

Tag Name	Example	Description
Vendor	Cisco	Vendor name
Product	Snort	Product name
Event Class	security	LogZilla event classification
Protocol	TCP	Network protocol
SrcIP	192.168.1.100	Source IP address (HC)
DstIP	10.0.0.1	Destination IP address (HC)
DstPort	http	Destination port or service name
Snort Classification	Web Application Attack	Snort threat classification
Severity	critical	Normalized severity level
Snort SID	1:1000000	Snort Signature ID gid:sid (HC)

Severity Mapping

Snort priority values are mapped to human-friendly severity levels:

Priority	Severity
1	critical
2	high

Priority	Severity
3	medium
4	low

MITRE ATT&CK Mappings

Snort Classification	MITRE ID	Tactic
Attempted User/Admin Privilege Gain	T1068	Privilege Escalation
Web Application Attack	T1190	Initial Access
Network Trojan/Executable Code	T1204	Execution
Denial of Service	T1499	Impact
Detection of a Network Scan	T1046	Discovery
Attempted Information Leak	T1005	Collection

Triggers

Trigger	Description
`Snort: MITRE ATT&CK Threat Detected`	Catch-all for any MITRE-mapped threat
`Snort: Critical Severity Alert`	Priority 1 alerts requiring immediate attention
`Snort: High Severity Alert`	Priority 2 alerts for investigation
`Snort: Malware Detected`	Trojan or executable code detected
`Snort: Privilege Escalation Attempt`	User or admin privilege gain attempt
`Snort: Web Application Attack`	Web application attack detected
`Snort: Denial of Service`	DoS attack detected

Trigger	Description
`Snort: Network Scan Detected`	Network reconnaissance activity

Dashboard

The Snort Overview dashboard provides:

- Key metrics badges (total alerts, by severity, by protocol)
- Alert timeline
- Top classifications, source IPs, destination IPs, and ports
- Severity and protocol breakdowns
- Live alert stream

Log Examples

TCP Traffic (Priority 2)

```
01/23-12:34:56.789  [**] [1234:5678:0] This is a sample log message [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.1.100:12345 -> 10.0.0.1:80
```

UDP Traffic (Priority 3)

```
02/14-23:45:12.345  [**] [5678:1234:0] Another example log entry [**] [Classification: Misc Attack] [Priority: 3] {UDP} 172.16.254.254:53 -> 8.8.8.8:53
```

Snort 3 Format with Quoted Message (Priority 1)

```
07/16-09:23:39.153899  [**] [1:1000000:0] "SERVER-WEBAPP Apache Log4j arbitrary code execution attempt" [**] [Classification: Attempted User Privilege Gain] [Priority: 1] {TCP} 192.168.1.2:50284 -> 192.168.2.3:80
```