LOGZILLA DOCUMENTATION

Trendmicro

LogZilla App Store application: Trendmicro

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

Overview

Trend Micro TippingPoint is an Intrusion Prevention System (IPS) that provides network threat protection through deep packet inspection. TippingPoint devices detect and block exploits, malware, and suspicious traffic in real-time using signature-based and behavioral analysis.

App Function

- Parse TippingPoint UnityOne logs in TMEF (Trend Micro Event Format)
- Extract source/destination IPs, ports, protocols, and actions
- Map security events to MITRE ATT&CK techniques and tactics
- Identify permitted threats indicating IPS policy gaps
- Categorize events with `Event Class: security`
- Provide dashboards for threat analysis and attack investigation

Vendor Documentation

- SMS Syslog Settings (https://docs.trendmicro.com/en-us/documentation/article/security-management-system-6-5-1-edit-syslog-settings)
- SMS Syslog Log Types (https://docs.trendmicro.com/en-us/documentation/article/security-management-system-6-5-1-syslog-log-types)
- SMS Syslog Fields Reference (https://docs.trendmicro.com/en-us/documentation/article/security-management-system-6-5-1-syslog-fields)

Device Configuration

Configure TippingPoint SMS to send syslog to LogZilla:

Log in to the Security Management System (SMS) console
Navigate to **Admin > Server Properties > Syslog**
Click **Add** to create a new syslog destination
Configure the following:

- **Server**: LogZilla server IP address
- **Port**: 514
- **Protocol**: TCP recommended (UDP may cause data loss with URI strings)
- **Format**: CEF or TMEF
- **Delimiter**: TAB (default)

Click **OK** to save

Verification

Generate test traffic or trigger a filter match, then verify events appear in LogZilla with `Vendor` tag set to `Trend Micro`.

Incoming Log Format

UnityOne uses Trend Micro Event Format (TMEF), a customized event format developed by Trend Micro for reporting security event information. TMEF uses space-separated key-value fields for structured logging.

Parsed Metadata Fields

Global Tags

Tag Name	Example	Description
`Vendor`	`Trend Micro`	Vendor name
`Product`	`UnityOne`	Product name
`Event Class`	`security`	Cross-vendor event classification

UnityOne Tags

Tag Name	Example	Description
`Severity`	`Critical`	Event severity (Critical, Major, Minor, Low, Normal)
`Protocol`	`TCP`	Network protocol
`SrcIP`	`185.153.64.126`	Source IP address
`DstIP`	`134.122.53.164`	Destination IP address
`DstPort`	`mysql`	Destination port (translated to service name)
`Action`	`Block`	Action taken by IPS
`Device Host`	`bwi1-ips-01`	IPS device hostname

Tag Name	Example	Description
Category	Reputation	TippingPoint event category
Signature	DB-Market-BWI	IPS filter/rule name that triggered
Event Type	Threat	Security event classification (always "Threat")
MITRE Technique	RDP	MITRE ATT&CK technique name from event description
MitreId	T1076	MITRE ATT&CK technique ID
MITRE Tactic	Lateral Movement	MITRE ATT&CK tactic

Log Examples

Reputation Block

```
product="UnityOne" version="1.0.0.17" event_class="7610"
event_description="7610: RepDV: Reputation Block" severity="4" app="TCP"
cnt="1" src="203.0.113.50" sourceTranslatedAddress="203.0.113.50"
spt="54321" dst="192.168.1.100" dpt="443" act="Block"
cs1="Default-Block" cs5="sms.example.com" dvchost="ips-dc1-01"
cat="Reputation"
```

MITRE ATT&CK Detection (Lateral Movement)

```
product="UnityOne" version="1.0.0.17" event_class="5873"
event_description="5873: RDP: Windows Remote Desktop Access (ATT&CK T1076)"
severity="2" app="TCP" cnt="1" src="10.10.10.50"
sourceTranslatedAddress="10.10.10.50" spt="49152" dst="10.10.10.100"
dpt="3389" act="Permit" cs1="Allow-Internal" cs5="sms.example.com"
dvchost="ips-dc1-01" cat="Security Policy"
```

Triggers

Trigger	Description
UnityOne: MITRE ATT&CK Detection	Catch-all for MITRE-mapped events

Trigger	Description
`UnityOne: Permitted Threat (Policy Gap)`	Threat detected but permitted - review IPS policy
`UnityOne: Traffic Quarantined`	Traffic quarantined for analysis
`UnityOne: Lateral Movement (T1021)`	RDP/SSH lateral movement detected
`UnityOne: Credential Attack (T1110)`	Brute force or credential attack
`UnityOne: Critical Severity Event`	Critical severity (4) events
`UnityOne: Malware Detected`	Malware category events
`UnityOne: Command and Control`	C2 communication detected