Lastline Enterprise Syslog Integration

January 17, 2024

6950 Hollister Avenue, Suite 100
Goleta, CA 93117
lastline.com | 805.456.7076

1 Introduction

This guide describes the Syslog Integration into Lastline Enterprise.

The Syslog Integration allows Lastline Enterprise to automatically send syslog notifications to a SIEM server when events that match some specified criteria are triggered. Lastline supports sending notifications over syslog in CEF format (used by HP ArcSight) or LEEF format (used by IBM qRadar). Syslog Integration can send a notification when Lastline detects something on a monitored network. Furthermore, it can send notifications about the status of Lastline Appliances.

In the next sections this guide will explain how to configure and use the Syslog Integration.

2 Overview of the Syslog Integration

2.1 Glossary

This section will briefly explain the meaning of some of the terms used in this guide.

2.1.1 SIEM

Security information and event management, service that provides event monitoring with prioritized alert notification.

2.1.2 CEF

Common Event Format, an open log management standard introduced by ArcSight that improves the interoperability of security-related information from different security and network devices and applications.

2.1.3 LEEF

Log Event Extended Format, a customized event format for IBM Security QRadar.

2.1.4 Trigger category

A trigger category represents a type of event for which notifications should be sent. Notifications can be triggered by different classes of events. When configuring a notification the user must specify for which trigger notifications should be sent.

2.1.5 Appliance trigger

Trigger category related to events concerning appliances status. Can be either appliance-checkin (An occurrence of an appliance checkin) or appliance-message (Status messages from components of an appliance).

2.1.6 Audit trigger

Trigger category related to audit events (relevant actions performed by a user account on the web portal). The audit event categories are the following:

- authentication: authentication related actions (e.g., a user logged in to the portal) (available from format version 7.10)
- configuration: appliance related actions (e.g., the reconfiguration of an appliance)
- registration: customer/account/license related actions (e.g., the creation of a new customer)

2.1.7 Network trigger

Trigger category related to network events. These events are currently:

- malware Command and Control traffic
- drive-by download
- fake anti-virus software activity
- malicious file download
- suspicious network activity
- suspicious URL activity (available from format version 7.10)
- Lastline network test
- unwanted software activity (e.g., adware)

2.1.8 Mail trigger

Trigger category for email detection events. Suspicious or malicious emails can be detected because of attachments, URLs or other characteristics of the message.

2.1.9 Test trigger

Trigger category for testing events. A notification can be triggered from the UI to verify that the Syslog Integration was successfully configured.

2.1.10 Intrusion trigger

Trigger category related to intrusion events (Available from format version 8.1)

2.2 Architecture

When using Syslog Integration a Manager can be configured to send SIEM syslog notifications automatically to a chosen server whenever the configured events are triggered. The Manager can either send the notification directly to the specified server or through a Sensor.

Currently two formats are supported for SIEM notifications: CEF and LEEF. The current version of the format is "7.5".

The content of the notifications differs depending on the event that has been triggered and the log format which has been chosen for the syslog notification.
The guide will now list the fields that are included in SIEM notification for every trigger type and log format.

2.2.1 Choice of format

The choice between CEF and LEEF format may be dictated by the SIEM platform to which syslog notifications need to be sent. When both formats are an option, we recommend choosing the LEEF format for the following reasons:

- CEF format limits the number of non-standard, extension fields that can be included in a message. Because of this restriction, some Lastline notification messages contain additional information when encoded in LEEF format compared to CEF.
- LEEF format is easier to parse, as it consistently uses the TAB character as a separator between fields, while not allowing TAB as a value within a field. CEF on the other hand uses the SPACE character as separator, but does not forbid SPACE in values.

2.2.2 Transport Protocol

Sending SIEM syslog message can be done either using UDP or TCP transport protocols. One might prefer TCP for the reliability of messages, but this ultimately depends on what the SIEM platform supports.

UDP When using the UDP transport protocol, each notification message is sent as a single UDP message. It is the SIEM server's responsibility to parse each UDP message as a single notification.

TCP When using the TCP transport protocol, a stream of newline seperated messages is sent to the target SIEM server. It is the SIEM server's responsibility to parse out each newline seperated message as a single message. In the event of a connection disruption between the sender and receiver, there will be one single attempt to re-establish the TCP connection. If a connection can be established, messages sent will be resumed from the last message which failed to send. If the connection cannot be re-established, each message will not be sent, and ignored, until a successful connection is established with the server.

This feature is only available from format version 7.10.

2.2.3 CEF Format

A message in CEF log format is maily composed by a prefix common to all messages and an extension part, a collection of key-value pairs to give additional information about the event, each key can be part of a predefined set or a limited custom-defined set.

The structure of the prefix for the CEF notification remains the same for all types of trigger and is in the form "<date> <origin host> CEF:<CEF version>|<vendor>|<product>|<version>|<signature id>|<name>|<severity>":

- date: date of the notification generation in "MMMM dd HH:mm:ss" format
- origin_host: source of the SIEM notification
- CEF version: version of the CEF format, currently "0"
- vendor: name of the vendor (i.e., "Lastline")
- product: name of the product (e.g., "Enterprise")
- version: version of the application sending the syslog message, currently "8.1"
- signature_id: unique identifier of the reported event type. List of values for each event:
  - Appliance status events: "appliance-status"
  - Audit events: "audit-event" (available from format version 7.5)
  - Mail events:
    - "email-attachment" Detection of a malicious email from an email attachment.
    - "email-url" Detection of a malicious email based on a url. (available from format version 7.5)
    - "email-message" Detection of a malicious email based on a message characteristic. (available from format version 9.1)
  - Network events:
    - "dga-activity-domain"
    - "dga-activity-pattern"
    - "dns-resolution"
    - "file-download"
    - "network-connection"
    - "profile-match"

    - "signature-match"
    - "sinkhole-resolution"
    - "suspicious-url" (available from format version 7.10)

  - Intrusion events: "intrusion-event" (available from format version 8.1)

- name: human readable description of the event
- severity: integer ranging from 0 to 10, reflects the importance of the event

Action type	Description
account_blocked	Account blocked
account_created	Account created
account_deleted	Account deleted
account_permission_granted	Permission granted to an account
account_permission_revoked	Permission revoked from an account
account_unblocked	Account un-blocked
account_updated	Account details updated
api_token_reset	License API-token set to a new value
appliance_rebooted	The appliance has been rebooted
appliance_reconfigured	The appliance has been reconfigured
appliance_upgraded	The software version of the appliance has been upgraded
checkpoint_certificate_added	A checkpoint certificate was added
checkpoint_certificate_deleted	A checkpoint certificate was deleted
checkpoint_notification_created	Notifications via Checkpoint was configured
checkpoint_notification_updated	A checkpoint notification configuration configuration was updated
email_changed	Account email updated
failed_login	A user failed to login to the specified account
httppost_notification_created	Notifications via HTTP Post was configured
httppost_notification_updated	A HTTP Post notification configuration was updated
invalid_credentials	Invalid credentials
license_created	New license generated
license_updated	License details updated
mail_notification_created	Notifications via mail was configured
mail_notification_updated	A mail notification configuration was updated
notification_deleted	A notification configuration was deleted
password_changed	Account password updated
password_reset	Password reset performed
password_reset_request	Password reset requested
sensor_added	A sensor was added
sensor_updated	A sensor was updated
siem_notification_created	Notifications via SIEM was configured
siem_notification_updated	A SIEM notification configuration was updated
streaming_notification_created	Notifications via streaming API was configured
streaming_notification_updated	A streaming API notification configuration was updated
successful_login	A successful login was performed for the account
successful_logout	An account successfully logged out
tanium_server_added	A tanium server configuration was added
tanium_server_deleted	A tanium server configuration was deleted
tanium_server_updated	A tanium server configuration was updated
tippingpoint_notification_created	Notifications via TippingPoint was configured
tippingpoint_notification_updated	A TippingPoint notification configuration was updated
wmi_source_configured	A WMI source was configured for session management
wmi_source_deleted	A WMI source configuration was deleted

Table 1: Possible values for appliance trigger fields

The extension part contains different fields depending on the type of event:

1. Appliance trigger fields
   - predefined fields:
     - start: start time-stamp
     - end: end time-stamp
     - deviceExternalId: unique id of the appliance
     - cat: category, name of the component that sent the message. Possible values are listed in table 2.
     - deviceFacility: detailed name of the component (message event only). Possible values are listed in table 2.
     - msg: the actual message being sent by the component (message event only)
     - rt: receipt time of the event
     - dvc: ip address of the appliance
     - dvchost: fully qualified domain name of the appliance
   - custom fields:
     - deviceType: the type of the appliance
     - deviceStatusLink: link to the status page of this appliance
     - msgIdentifier: identifier of the appliance message (message event only). Possible values are listed in table 2.
     - impact: impact of this event, ranging from 0-100 (message event only)

2. Audit trigger fields (this fields are available only from format version 7.3)
   - predefined fields:
     - start: start time-stamp
     - src: ip address of the user that performed this action
     - suser: account of the user that performed the logged action
     - duser: customer to which the action refers
     - cat: category of the audit action, currently one of:
       - registration: account/customer/license related actions
       - configuration: appliance related actions
     - externalId: id of the audit event
     - deviceExternalId: unique id of the manager appliance (on-premise only)
   - custom fields:
     - AffectedEntityType: type of the object affected by this action (e.g., "license", "account", "appliance")
     - AffectedEntityID: identifier of the object affected by this action (e.g., the license key, name of the account, uuid of the appliance)
     - EventDetailLink: link to details about this action on the user website
     - AuditActionType:type of the audit action, some of the possible values are described in table 1 (available from format version 7.5)
     - ConfiguredSoftwareVersion: version of the software that has been reconfigured (appliance_upgraded events only)
     - impact: impact of this action, ranging from 0-100

3. Network trigger fields

   - predefined fields:
     - start: start time-stamp
     - end: end time-stamp
     - src: source ip address of the event
     - dst: destination ip address of the event
     - cnt: number of occurrences of this event
     - act: action taken in response to this event
     - cat: information about the event malware in the form "malware class name/malware name"
     - proto: transport layer protocol used by the event
     - externalId: identifier of the event
     - deviceExternalId: obfuscated identifier of the appliance
     - smac: source mac address of the event
     - sourceDnsDomain: hostname of the source
     - dhost: destination hostname of the event
     - reason: name of the source (if this particular event is due to a hit on custom intelligence)
     - msg: comment on the intel entry (if this particular event is due to a hit on custom intelligence)
     - fsize: size of the malicious file (malicious file download only)
     - fname: name of the malicious file (malicious file download only)
     - fileHash: MD5 hash of the malicious file (malicious file download only)
     - fileType: type of the malicious file (malicious file download only)
     - suser: string representation of the list of users that were logged on at the time of the event

   - custom fields:
     - detectionId: string representing the concatenation of threat, activity and detector id
     - EventDetailLink: link to details about this event on the user website
     - ResolvedDomain: resolved destination domain
     - EventUrl: URL of the network event, in case of a file download this will be the URL the file was downloaded from, otherwise it will be the URL directly associated with the network event (this field is available only from format version 7.2)
     - fileCategory: category of the malicious file (malicious file download only)
     - fileSHA1: SHA-1 hash of the malicious file (malicious file download only)
     - FileDetailLink: link to details about the malicious file on the user website (malicious file download only)
     - impact: impact of this event, ranging from 0-100
     - IncidentId: identifier of the incident related to this event (this field is available only from format version 7.2)
     - IncidentImpact: impact of the incident related to this event (this field is available only from format version 7.2)
     - URLDetailLink: link to details about the supicious URL (this field is available only from format version 7.8)

4. Mail trigger fields

   - predefined fields:
     - start: start time-stamp
     - end: end time-stamp
     - suser: sender of the email message
     - deviceExternalId: obfuscated identifier of the appliance

- fsize: size of the attachment (email-attachment type only)
- fname: name of the attachment (email-attachment type only)
- fileHash: MD5 hash of the attachment (email-attachment type only)
- fileType: type of the attachment (email-attachment type only)
- duser: recipients of the email message
- act: action taken in response to this event, some of the possible values are described in table 3 (available from format version 7.6)
- cat: information about the mail message in the form "threat class name/threat name" (email-message type only)

- custom fields:
  - EmailSubject: subject of the mail message
  - MessageID: id of the email message
  - impact: impact of this event, ranging from 0-100
  - fileCategory: category of the attachment (email-attachment type only)
  - fileSHA1: SHA-1 hash of the attachment (email-attachment type only)
  - FileDetailLink: link to details about the attachment on the user website (email-attachment type only)
  - mailUrl: URL found in the mail message (email-url type only) (available from format version 7.5)
  - mailUrlHash: MD5 hash of the URL (email-url type only) (available from format version 7.5)
  - EventDetailLink:link to details about this event on the user website (available from format version 7.5)

5. Test trigger fields
   - predefined fields:
     - devTimeFormat: format of the devTime (MMM dd yyyy HH:mm:ss z)
     - devTime: timestamp of the event
     - externalId: unique identifier for the test

   - custom fields:
     - impact: impact of this event, always 10 for tests
     - notification_config_id: unique identifier for the notification configuration

6. Intrusion trigger fields
   - predefined fields:
     - start: start time-stamp
     - end: end time-stamp
     - externalId: unique identifier of the intrusion
     - deviceExternalId: obfuscated identifier of the appliance
     - msg: detailed information about the intrusion event (e.g., "Correlated 3 incidents into an intrusion")
     - deviceFacility: the correlation rule that caused the event, if any
     - cat: the most advanced attack stage
     - dvc: a sequence of each host with the threats and attack stages associated with it

   - custom fields:

- intrusionDetailLink: a URL link that will go straight to the intrusion in the UI
- intrusionName: the name of the intrusion
- affectedHosts: number of affected hosts in the intrusion
- nrMalware: number of distinct malware in the intrusion

2.2.4 LEEF Format

A message in LEEF log format is maily composed by a optional syslog header, a LEEF header and a collection of attributes, either for a predefined or custom-defined set, describing the event.

The structure of syslog + LEEF headers remains the same for all types of trigger and is in the form "<date> <origin host> LEEF:<LEEF version>|<vendor>|<product>|<version>|<event id>":

- date: date of the notification generation in "MMMM dd HH:mm:ss" format
- origin host: source of the SIEM notification
- LEEF version: version of the LEEF format, currently "1.0"
- vendor: name of the vendor (i.e., "Lastline")
- product: name of the product (e.g., "Enterprise")
- version: version of the application sending the syslog message, currently "7.6"
- event_id: unique identifier of the reported event type. List of values for each event:
  - Appliance status events: "appliance-status"
  - Audit events: "audit-event" (available from format version 7.5)
  - Mail events:
    - "email-attachment"
    - "email-url" (available from format version 7.5)
    - "email-message" (available from format version 9.1)
  - Network events:
    - "dga-activity-domain"
    - "dga-activity-pattern"
    - "dns-resolution"
    - "file-download"
    - "network-connection"
    - "profile-match"
    - "signature-match"
    - "sinkhole-resolution"
    - "suspicious-url"
  - Intrusion events: "intrusion-event" (available from format version 8.1)

The event's attributes contained in the SIEM message depend on the type of event:

1. Appliance trigger fields

- predefined fields:
  - devTime: timestamp of the event as reported by the appliance
  - devTimeFormat: format of the devTime (MMM dd yyyy HH:mm:ss z)
  - deviceExternalId: unique identifier of the interested appliance
  - sev: severity, integer ranging from 0 to 10, reflects the importance of the event
  - cat: category, name of the component that sent the message. Possible values are listed in table 2.
  - src: ip address of the appliance

- custom fields:
  - deviceStatusLink: link to the status page of this appliance
  - deviceFacility: detailed name of the component that sent the message. Possible values are listed in table 2.
  - impact: impact of this event, ranging from 0-100 (message event only)
  - deviceType: the type of the appliance
  - msgIdentifier: identifier of the appliance message (message event only). Possible values are listed in table 2.
  - msg: the actual message being sent by the component (message event only)
  - dvchost: fully qualified domain name of the appliance

2. Audit trigger fields (this fields are available only from format version 7.3)

- predefined fields:
  - desc: extended description of the audit action
  - devTime: timestamp of the event
  - devTimeFormat: format of the devTime (MMM dd yyyy HH:mm:ss z)
  - deviceExternalId: unique identifier of the manager appliance (on-premise only)
  - sev: severity, integer ranging from 0 to 10, reflects the importance of the action
  - cat: category of the audit action, currently one of:
    - registration: account/customer/license related actions
    - configuration: appliance related actions
  - src: ip address of the user that performed this action
  - usrName: user that performed this action
  - accountName: customer to which the action refers

- custom fields:
  - impact: impact of this action, ranging from 0-100
  - externalId: identifier of the audit event
  - AffectedEntityType: type of the object affected by this action (e.g., "license", "account", "appliance")
  - AffectedEntityID: identifier of the object affected by this action (e.g., the license key, name of the account, uuid of the appliance)
  - eventDetailLink: link to details about this action on the user website
  - AuditActionType:type of the audit action, some of the possible values are described in table 1 (available from format version 7.5)
  - ConfiguredSoftwareVersion: version of the software that has been reconfigured (appliance_upgraded events only)

3. Network trigger fields: from format version 7.5, when configuring a notification it will possible to include information about pcaps related to a network event (LEEF format only). If multiple pcaps are available for a single event, multiple notifications for the same network event will be sent (with different pcap information).

   - predefined fields:
     - desc: description of the event (e.g., Suspicious DNS Resolution)
     - devTime: timestamp of the event
     - devTimeFormat: format of the devTime (MMM dd yyyy HH:mm:ss z)
     - deviceExternalId: obfuscated identifier of the appliance
     - src: source ip address of the event
     - dst: destination ip address of the event
     - proto: transport layer protocol used by the event
     - sev: severity, integer ranging from 0 to 10, reflects the importance of the event
     - cat: class of the detected malware
     - usrName: string representation of the list of users that were logged on at the time of the event
     - srcMAC: source mac address of the event

   - custom fields:
     - cnt: number of occurrences of this event
     - act: action taken in response to this event
     - externalId: identifier of the event
     - impact: impact of this event, ranging from 0-100
     - malware: name of the detected malware
     - detectionId: obfuscated string representing the concatenation of threat, activity and detector id
     - EventDetailLink: link to details about this event on the user website (available from format version 7.5)
     - dhost: destination hostname of the event (malicious file download only)
     - ResolvedDomain: resolved destination domain
     - EventUrl: URL of the network event, in case of a file download this will be the URL the file was downloaded from, otherwise it will be the URL directly associated with the network event (this field is available only from format version 7.2)
     - reason: name of the source (if this particular event is due to a hit on custom intelligence)
     - msg: comment on the intel entry (if this particular event is due to a hit on custom intelligence)
     - fsize: size of the malicious file (malicious file download only)
     - fname: name of the malicious file (malicious file download only)
     - fileHash: MD5 hash of the malicious file (malicious file download only)
     - fileType: type of the malicious file (malicious file download only)
     - fileCategory: category of the malicious file (malicious file download only)
     - fileSHA1: SHA-1 hash of the malicious file (malicious file download only)
     - FileDetailLink: link to details about the malicious file on the user website (malicious file download only)
     - IncidentId: identifier of the incident related to this event (this field is available only from format version 7.2)
     - IncidentImpact: impact of the incident related to this event (this field is available only from format version 7.2)
     - IncidentMalware: name of the malware related to the incident (this field is available only from format version 7.2)
     - IncidentClass: name of the malware family related to the incident (this field is available only from format version 7.2)
     - URLDetailLink: link to details about the supicious URL

   - pcap fields (available form version 7.5):

- pcapId: identifier of the pcap related to this event
- pcapStartTime: start time of the pcap
- pcapSrcIp: source IPV4 address of the pcap
- pcapSrcPort: source port of the pcap
- pcapDstIp: destination IPV4 address of the pcap
- pcapDstPort: destination port of the pcap
- pcapUrls: list of URLs associated with this pcap
- pcapHosts: list of contacted hostnames from the pcap
- pcapInBytes: number of bytes received
- pcapOutBytes: number of bytes sent
- pcapThreats: list of threats involved in this pcap
- pcapProtocols: list of protocols
- pcapSuccessfulConnections: number of successful connections from the pcap
- pcapFailedConnections: number of failed connections from the pcap
- pcapBody: base64 encoded, raw binary content of the traffic capture (might be truncated if too long)

4. Mail trigger fields

- predefined fields:
  - desc: description of the event (i.e., "Suspicious Email Attachment"")
  - devTime: timestamp of the event
  - devTimeFormat: format of the devTime (MMM dd yyyy HH:mm:ss z)
  - sev: severity, integer ranging from 0 to 10, reflects the importance of the event
  - deviceExternalId: obfuscated identifier of the appliance
  - usrName: recipients of the email message
  - cat: threat class of the mail message (mail-message type only, available from format 9.1)

- custom fields:
  - act: action taken in response to this event some of the possible values are described in table 3 (available from format version 7.6)
  - impact: impact of this event, ranging from 0-100
  - emailSubject: subject of the email message
  - messageID: identifier of the email message
  - Sender: sender of the email message
  - fsize: size of the malicious attachment (malicious attachment only)
  - fname: name of the malicious attachment (malicious attachment only)
  - fileHash: MD5 hash of the malicious attachment (malicious attachment only)
  - fileType: type of the malicious attachment (malicious attachment only)
  - fileCategory: category of the malicious attachment (malicious attachment only)
  - fileSHA1: SHA-1 hash of the malicious attachment (malicious attachment only)
  - FileDetailLink: link to details about the malicious attachment on the user website (malicious attachment only)
  - mailUrl: malicious URL found in the mail message (malicious URL only) (available from format version 7.5)
  - mailUrlHash: MD5 hash of the malicious URL (malicious URL only) (available from format version 7.5)
  - EventDetailLink:link to details about this event on the user website
  - malware: name of the threat detected
  - detectors: names of the detectors that flagged the email message

5. Test trigger fields

   - predefined fields:
     - desc: description of the event (i.e., "User triggered test event")
     - devTime: timestamp of the event
     - devTimeFormat: format of the devTime (MMM dd yyyy HH:mm:ss z)
     - impact: impact of this event, currently 10 for tests
     - externalId: unique identifier for the test

   - custom fields:
     - notification_config_id: unique identifier for the notification configuration

6. Intrusion trigger fields

   - predefined fields:
     - desc: detailed information about the intrusion event (e.g., "Correlated 3 incidents into an intrusion")
     - devTime: timestamp of the event
     - devTimeFormat: format of the devTime (MMM dd yyyy HH:mm:ss z)
     - deviceExternalId: obfuscated identifier of the appliance
     - sev: severity, integer ranging from 0 to 10, always 10
     - src: a sequence of each host with the threats and attack stages associated
     - url: A URL that links to the intrusion details page for this intrusion in the Lastline Portal.

   - custom fields:
     - externalId: unique identifier of the intrusion
     - intrusionName: the name of the intrusion
     - nrMalware: number of distinct malware in the intrusion
     - affectedHosts: number of affected hosts in the intrusion
     - msg: detailed information about the intrusion event (e.g., "Correlated 3 incidents into an intrusion")
     - reason: the reason behind the intrusion event
     - correlationRule: the correlation rule that caused the event, if any
     - mostAdvancedAttackStage: the most advanced attack stage
     - impact: the impact of the intrusion (only available from format 9.1)

The '^' (caret) and '|' (pipe) characters should be avoided in LEEF format notifications, for they could be interpreted as the default delimiters and cause parsing issues. To prevent this, '^' and '|' are encoded as '\x5E' and '\x7C' respectively in our SIEM notifications.

3 Configuration

To enable the Manager to send Syslog Integration, the appropriate configuration must be set in the user-portal. This paragraph will explain how.

3.1 Configuration of the Syslog Integration on the Manager

On the web interface of the Manager, go to Admin → Integration → Syslog.

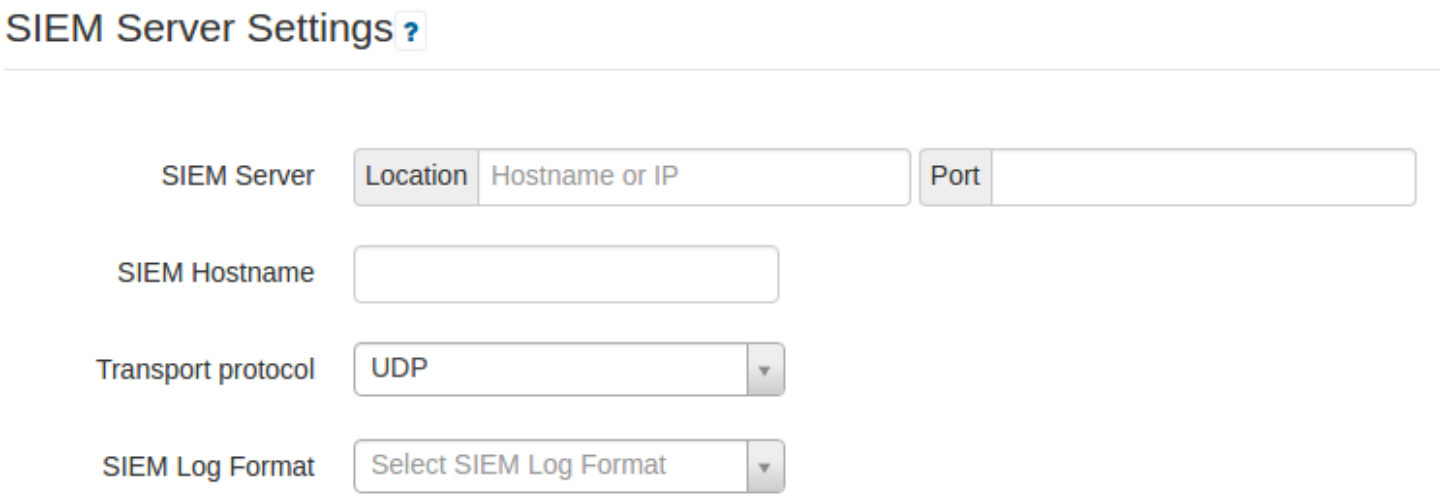
Click on the "+" button on the right side to enter the Syslog notification creation screen.

Syslog Notification common settings

On the upper part of the screen are the standard notification settings:

- Appliance: select the license of the appliance that will trigger the notification
- Sensor: select the sensor on a given license that will trigger the notification
- Daily Limit: daily limit to the number of notifications that can be sent ("0" is equivalent to no limit)
- Timezone: timezone to be used to determine the daily limit
- Enable/Disable Notification: click to enable/disable the notification

Then proceed to configure the "SIEM Server Settings" section:



Syslog Notification special settings

- SIEM Server:
  - Location: hostname or IP address the SIEM notification will be sent to
  - Port: port on which the SIEM syslog message will be sent

- SIEM Hostname: hostname that will show up in the prefix of the syslog message (i.e. "12-12-12 01:23:24 {SIEM Hostname} siem_message")
- SIEM Log Format: supported standard log format to be used for the syslog message (e.g., CEF or LEEF)
- Transport Protocol: The layer 4 network transport protocol to use. This can either be UDP or TCP (defaults to UDP). (Available from format version 7.10)
- Include pcap: Whether to include pcap information inside the notification for network events Pcaps can only be included for "LEEF" SIEM notifications. (Available from version 7.5)

3.2 Testing Syslog Integration

In order to make sure that the Syslog Integration have been correctly configured, appropriately configure rsyslog on the server that will receive the SIEM notifications, generate a request that will trigger one of the configured events, for example "curl test.lastline.com", and check if the request is correctly received on the destination server.
Both in case of success and failure in sending the SIEM notification an entry will be displayed in Appliances → Logs → Monitoring Logs under "Notification Delivery Service" Component and "SIEM Server Status" Type, reporting the details about the notification delivery.

3.3 Notifications examples

The guide will now show a few examples of Syslog notifications for each trigger category.

3.3.1 Test event notifications

Example of notification triggered for testing.

CEF format:

```
Aug 18 14:26:20 test1 CEF:0|Lastline|Enterprise|7.3|test-event|User triggered test event|1|cn1=10 cn1Label=impact cn2=37 cn2Label=notification_config_id devTime=Dec 12 2012 00:00:00 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z externalId=3dc144bdb3434b1abf7a465de3f57948
```

LEEF format:

```
Aug 18 14:26:20 test2 LEEF:1.0|Lastline|Enterprise|7.3|test-event|desc=User triggered test event devTime=Dec 12 2012 00:00:00 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z impact=10 notification_config_id=37 externalId=3dc144bdb3434b1abf7a465de3f57948
```

3.3.2 Mail event notifications

Example of notification after the detection of a malicious mail attachment.

CEF format:

```
Aug 18 14:26:20 test1 CEF: 0|Lastline|Enterprise|7.3|email-attachment|Suspicious Email Attachment|10|cn1=100 cn1Label=impact cs1=Test cs1Label=EmailSubject cs2=b89c9140637e49219d464b8f90eab8f7 cs2Label=MessageID cs3=Pdf cs3Label=fileCategory cs4=e1a1dcfefa8c96723d5f7816f0e991a0a01b5f0a cs4Label=fileSHA1 cs5=https://user.enterprise.lastline.local/malscape/#/task/d4ed2a4fcc454e82adc57d7d304b7fe3 cs5Label=FileDetailLink cs6=https://user.enterprise.lastline.local/mail/message#/3287884757/3459119816/9552?mail_time=2016-03-21 cs6Label=EventDetailLink deviceExternalId=3053322414:602745899 duser=<test@example.com> end=Aug 18 2015 14:26:20 UTC fileHash=5e2eceec69c9ef5435298abc1d10624b fileType=PDF document fname=5e2eceec69c9ef5435298abc1d10624b fsize=5984 start=Aug 18 2015 14:26:20 UTC suser=fake@example.com
```

LEEF format:

```
Aug 18 14:26:20 test2 LEEF: 1.0|Lastline|Enterprise|7.3|email-attachment|
EventDetailLink=https://user.enterprise.lastline.local/mail/message#/3287884757/3459119816/9552?mail_time=2016-03-21 FileDetailLink=https://user.enterprise.lastline.local/malscape/#/task/d4ed2a4fcc454e82adc57d7d304b7fe3 Sender=fake@example.com desc=Suspicious Email Attachment devTime=Aug 18 2015 14:26:20 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=3053322414:602745899 emailSubject=Test fileCategory=Pdf fileHash=5e2eceec69c9ef5435298abc1d10624b fileSHA1=e1a1dcfefa8c96723d5f7816f0e991a0a01b5f0a fileType=PDF document fname=5e2eceec69c9ef5435298abc1d10624b fsize=5984 impact=100 messageID=b89c9140637e49219d464b8f90eab8f7 sev=10 usrName=<test@example.com>
```

Example of notification after the detection of a malicious URL in a mail message (available from format version 7.5).

CEF format:

```
Nov 25 13:53:13 testhost CEF:0|Lastline|Enterprise|7.3|email-url|Suspicious Email Url|9|cn1=99 cn1Label=impact cs1=TEST EMAIL! cs1Label=EmailSubject cs2=e45t4751945e49219d464b8p43maw9r4 cs2Label=MessageID cs3=http://www.evil.fake cs3Label=mailUrl cs4=2be456f055282b7dc6d6b0f002a52dad cs4Label=mailUrlHash deviceExternalId=3287884757:3459119816 duser=<test@example.com> end=Nov 25 2015 13:53:13 UTC start=Nov 25 2015 13:53:13 UTC suser=fake@example.com
```

LEEF format:

```
Nov 25 13:53:13 testhost LEEF:1.0|Lastline|Enterprise|7.3|email-url|ApplianceName=sensor01 Sender=fake@example.com desc=Suspicious Email Url devTime=Nov 25 2015 13:53:13 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=3287884757:3459119816 emailSubject=TEST EMAIL! impact=99 mailUrl=http://www.evil.fake mailUrlHash=2be456f055282b7dc6d6b0f002a52dad messageID=e45t4751945e49219d464b8p43maw9r4 sev=9 usrName=<test@example.com>
```

Example of notification after the detection of a malicious mail message (available from format version 9.1).

CEF format:

```
Sep 09 23:32:33 testhost CEF:0|Lastline|Enterprise|9.1|email-message|Suspicious Email Message|8|act=LOG cat=drive-by/Mebroot cn1=80 cn1Label=impact cs1=TEST EMAIL! cs1Label=EmailSubject cs2=e45t4751945e49219d464b8p43maw9r4 cs2Label=MessageID cs3=https://do.no.connect/portal#/mail/message/3287884757/3459119816/9359?date=2019-09-09 cs3Label=EventDetailLink deviceExternalId=3287884757:3459119816 duser=<test@example.com> end=Sep 09 2019 23:32:33 UTC start=Sep 09 2019 23:32:33 UTC suser=fake@example.com
```

LEEF format:

```
Sep 09 23:32:33 testhost LEEF:1.0|Lastline|Enterprise|9.1|email-message|ApplianceName=sensor01 EventDetailLink=https://do.no.connect/portal#/mail/message/3287884757/3459119816/9360?date=2019-09-09 Sender=test@example.com act=LOG cat=drive-by desc=Suspicious Email Message detectors=email_anomaly:spam_domain, email_anomaly:spam_ip devTime=Sep 09 2019 23:41:12 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=3287884757:3459119816 emailSubject=TEST EMAIL! impact=80 malware=Mebroot messageID=a=unique=message_id sev=8 usrName=test@lastline.com
```

3.3.3 Appliance event notifications

Example of notification reporting that an appliance is online.

CEF format:

```
Aug 18 14:22:17 test1 CEF: 0|Lastline|Enterprise|7.3|appliance-status|Appliance Status|1|cat=Online cs1=SENSOR cs1Label=deviceType cs2=https://user.enterprise.lastline.local/appliance#/config/status/0284f6fcf42f4e859499f00bc00c19a7 cs2Label=deviceStatusLink deviceExternalId=0284f6fcf42f4e859499f00bc00c19a7 dvc=192.168.1.52 dvchost=lastline-sensor.lastline.local end=Aug 18 2015 14:22:17 UTC rt=Aug 18 2015 14:22:17 UTC start=Aug 18 2015 14:22:17 UTC
```

LEEF format:

```
Aug 18 14:22:17 test2 LEEF: 1.0|Lastline|Enterprise|7.3|appliance-status|cat=Online devTime=Aug 18 2015 14:22:17 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=0284f6fcf42f4e859499f00bc00c19a7 deviceStatusLink=https://user.enterprise.lastline.local/appliance#/config/status/0284f6fcf42f4e859499f00bc00c19a7 deviceType=SENSOR dvchost=lastline-sensor.lastline.local sev=1 src=192.168.1.52
```

Example of notification reporting that an appliance is offline.

CEF format:

```
Aug 18 15:30:46 test1 CEF: 0|Lastline|Enterprise|7.3|appliance-status|Appliance Status|4|cat=Offline cs1=SENSOR cs1Label=deviceType cs2=https://user.enterprise.lastline.local/appliance#/config/status/0284f6fcf42f4e859499f00bc00c19a7 cs2Label=deviceStatusLink deviceExternalId=0284f6fcf42f4e859499f00bc00c19a7 dvc=192.168.1.52 dvchost=lastline-sensor.lastline.local end=Aug 18 2015 15:30:46 UTC rt=Aug 18 2015 14:30:46 UTC start=Aug 18 2015 15:30:46 UTC
```

LEEF format:

```
Aug 18 15:30:46 test2 LEEF: 1.0|Lastline|Enterprise|7.3|appliance-status|cat=Offline devTime=Aug 18 2015 14:30:46 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=0284f6fcf42f4e859499f00bc00c19a7 deviceStatusLink=https://user.enterprise.lastline.local/appliance#/config/status/0284f6fcf42f4e859499f00bc00c19a7 deviceType=SENSOR dvchost=lastline-sensor.lastline.local sev=4 src=192.168.1.52
```

Example of notification reporting the successful upload of email metadata.

CEF format:

```
Aug 18 14:23:14 test1 CEF: 0|Lastline|Enterprise|7.3|appliance-status|Appliance Status|1|cat=Email Analysis Service cn1=10 cn1Label=impact cs1=SENSOR cs1Label=deviceType cs2=https://user.enterprise.lastline.local/appliance#/config/status/0284f6fcf42f4e859499f00bc00c19a7 cs2Label=deviceStatusLink cs3=llmail.shareduploader.upload cs3Label=msgIdentifier deviceExternalId=0284f6fcf42f4e859499f00bc00c19a7 deviceFacility=Email metadata uploader dvc=192.168.1.52 dvchost=lastline-sensor.lastline.local end=Aug 18 2015 14:21:18 UTC msg=Successful upload of email metadata rt=Aug 18 2015 14:21:18 UTC start=Aug 18 2015 14:21:18 UTC
```

LEEF format:

```
Aug 18 14:23:14 test2 LEEF: 1.0|Lastline|Enterprise|7.3|appliance-status|cat=Email Analysis Service devTime=Aug 18 2015 14:21:18 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=0284f6fcf42f4e859499f00bc00c19a7 deviceFacility=Email metadata uploader deviceStatusLink=https://user.enterprise.lastline.local/appliance#/config/status/0284f6fcf42f4e859499f00bc00c19a7 deviceType=SENSOR dvchost=lastline-sensor.lastline.local impact=10 msg=Successful upload of email metadata msgIdentifier=llmail.shareduploader.upload sev=1 src=192.168.1.52
```

3.3.4 Audit event notification

Example of notification triggered by the creation of a license.

CEF format:

Nov 25 12:24:59 testhost CEF:0|Lastline|Enterprise|7.3|audit-event|New license generated|1|cat=registration cn1=10 cn1Label=impact cs1=license cs1Label=AffectedEntityType cs2=AXYAAXYAAXYAAXYAAXYA cs2Label=AffectedEntityID cs3=https://user.enterprise.lastline.local/settings#/audit/a/2015-11-24/2015-11-26?audit_event_id%3d15 cs3Label=EventDetailLink cs4=license_created cs4Label=AuditActionType duser=test@fake.bet externalId=15 src=192.168.0.1 start=Nov 25 2015 12:24:59 UTC suser=test@fake.bet

LEEF format:

Nov 25 12:24:59 testhost LEEF:1.0|Lastline|Enterprise|7.3|audit-event|AffectedEntityID=AXYAAXYAAXYAAXYAAXYA AffectedEntityType=license AuditActionType=license_created accountName=test@fake.bet cat=registration desc=New license generated devTime=Nov 25 2015 12:24:59 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z eventDetailLink=https://user.enterprise.lastline.local/settings#/audit/a/2015-11-24/2015-11-26?audit_event_id%3d15 externalId=15 impact=10 sev=1 src=192.168.0.1 usrName=test@fake.bet

3.3.5 Network event notifications

Example of notification triggered by the detection of a malicious file download.

CEF format:

Aug 18 14:29:53 test1 CEF: 0|Lastline|Enterprise|7.3|file-download|Suspicious File Download|10|act=LOG cat=Malicious File Download/Malicious Document Download cn1=100 cn1Label=impact cn2=12 cn2Label=incidentId cn3=100 cn3Label=incidentImpact cnt=1 cs1=2535ec71:30fbe7df:e52cff2b cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/3053322414/602745899/2?event_time%3d2015-08-18 cs2Label=EventDetailLink cs3=http://127.0.0.2/5e2eceec69c9ef5435298abc1d10624b.pdf cs3Label=EventUrl cs4=Pdf cs4Label=fileCategory cs5=e1a1dcfefa8c96723d5f7816f0e991a0a01b5f0a cs5Label=fileSHA1 cs6=https://user.enterprise.lastline.local/malscape/#/task/d4ed2a4fcc454e82adc57d7d304b7fe3 cs6Label=FileDetailLink deviceExternalId=3053322414:602745899 dhost=127.0.0.2 dpt=80 dst=127.0.0.2 end=Aug 18 2015 14:27:56 UTC externalId=2 fileHash=5e2eceec69c9ef5435298abc1d10624b fileType=PDF document fname=/5e2eceec69c9ef5435298abc1d10624b.pdf fsize=5984 proto=TCP src=127.0.0.1 start=Aug 18 2015 14:27:56 UTC

LEEF format:

```
Aug 18 14:29:53 test2 LEEF: 1.0|Lastline|Enterprise|7.3|file-download|
EventDetailLink=https://user.enterprise.lastline.local/event#/3053322414/602745899/2?event_time%3d2015-08-18 EventUrl=http://127.0.0.2/5e2eceec69c9ef5435298abc1d10624b.pdf FileDetailLink=https://user.enterprise.lastline.local/malscape/#/task
act=LOG cat=Malicious File Download cnt=1 desc=Suspicious File Download detectionId=2535ec71:30fbe7df:e52cff2b devTime=Aug 18 2015 14:27:56 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=3053322414:602745899 dhost=127.0.0.2 dst=127.0.0.2 dstPort=80 externalId=2 fileCategory=Pdf fileHash=5e2eceec69c9ef5435298abc1d10624b fileSHA1=e1a1dcfefa8c96723d5f7816f0e991a0a01b5f0a fileType=PDF document fname=/5e2eceec69c9ef5435298abc1d10624b.pdf fsize=5984 impact=100 malware=Malicious Document Download proto=TCP sev=10 src=127.0.0.1 incidentId=12 incidentImpact=100 IncidentMalware=Malicious Document Download IncidentClass=Malicious File Download
```

Example of notification reporting the detection of a suspicious network connection.

CEF format:

```
Aug 18 14:34:30 test1 CEF: 0|Lastline|Enterprise|7.3|network-connection|Suspicious Network Connection|0|act=LOG cat=Lastline test/Lastline test cn1=1 cn1Label=impact cn2=13 cn2Label=incidentId cn3=1 cn3Label=incidentImpact cnt=1 cs1=fc900ff8:30fbe7df:30fbe7df cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/3053322414/602745899/3?event_time%3d2015-08-18 cs2Label=EventDetailLink cs3=http://test.lastline.com cs3Label=EventUrl deviceExternalId=3053322414:602745899 dhost=test.lastline.com dpt=80 dst=52.5.237.96 end=Aug 18 2015 14:32:27 UTC externalId=3 proto=TCP smac=08:00:27:00:c9:7a src=192.168.1.52 start=Aug 18 2015 14:32:27 UTC
```

LEEF format:

```
Aug 18 14:34:30 test2 LEEF: 1.0|Lastline|Enterprise|7.3|network-connection|
EventDetailLink=https://user.enterprise.lastline.local/event#/3053322414/602745899/3?event_time%3d2015-08-18
act=LOG cat=Lastline test cnt=1 desc=Suspicious Network Connection detectionId=fc900ff8:30fbe7df:30fbe7df devTime=Aug 18 2015 14:32:27 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=3053322414:602745899 dst=52.5.237.96 dstPort=80 externalId=3 impact=1 malware=Lastline test proto=TCP sev=0 src=192.168.1.52 srcMAC=08:00:27:00:c9:7a EventUrl=http://test.lastline.com incidentId=13 incidentImpact=1 IncidentMalware=Lastline test IncidentClass=Lastline test
```

Example of notification triggered by a suspicious dns resolution.

CEF format:

```
Aug 18 14:34:58 test1 CEF: 0|Lastline|Enterprise|7.3|dns-resolution|Suspicious DNS Resolution|0|act=LOG cat=Lastline test/Lastline test cn1=1 cn1Label=impact cn2=14 cn2Label=incidentId cn3=1 cn3Label=incidentImpact cnt=2 cs1=fc900ff8:30fbe7df:30fbe7df cs1Label=detectionId cs2=https://user.enterprise.lastline.local/event#/3053322414/602745899/4?event_time%3d2015-08-18 cs2Label=EventDetailLink cs3=test.lastline.com cs3Label=ResolvedDomain cs4=http://test.lastline.com cs4Label=EventUrl deviceExternalId=3053322414:602745899 dpt=53 dst=192.168.1.1 end=Aug 18 2015 14:32:27 UTC externalId=4 proto=UDP smac=08:00:27:00:c9:7a src=192.168.1.52 start=Aug 18 2015 14:32:27 UTC
```

LEEF format:

Aug 18 14:34:58 test2 LEEF: 1.0|Lastline|Enterprise|7.3|dns-resolution|
EventDetailLink=https://user.enterprise.lastline.local/event#/3053322414/602745899/4?event_time%3d2015-08-18
ResolvedDomain=test.lastline.com act=LOG cat=Lastline test cnt=2 desc=Suspicious DNS Resolution detectionId=fc900ff8:30fbe7df:30fbe7df devTime=Aug 18 2015 14:32:27 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=3053322414:602745899 dst=192.168.1.1 dstPort=53 externalId=4 impact=1 malware=Lastline test proto=UDP sev=0 src=192.168.1.52 srcMAC=08:00:27:00:c9:7a EventUrl=http://test.lastline.co incidentId=14 incidentImpact=1 IncidentMalware=Lastline test IncidentClass=Lastline test

Example of notification for a network event including information about the related pcap. (available from format version 7.5, pcap body truncated for brevity reasons)

Apr 22 13:41:30 testhost LEEF:1.0|Lastline|Enterprise|7.2|dns-resolution|ApplianceName=sensor01
EventDetailLink=https://user.enterprise.lastline.local/event#/3287884757/3459119816/1787?event_time=2012-
12-11 EventUrl=http://example.com act=LOG cat=Testing Class cnt=1 desc=Suspicious DNS Resolution detectionId=c90de0dd:d0051f96:d0051f96 devTime=Dec 11 2012 23:51:10 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z deviceExternalId=3287884757:3459119816 dst=10.0.0.1 dstPort=80 externalId=1787 impact=70 malware=Testing pcapDstIp=10.0.0.1 pcapDstPort=80 pcapBody=1MOyoQIABAAAAAAAAAAAAP//AAABAAAAI0ujQLi/BAA+AAAAPgAAAP7/
IAABAAAAAQAAAAgARQAAMA9BQACABpHrkf6g7UHQ5N8NLABQOK pcapFailedConnections=1
pcapHosts=www.lastline.com pcapId=868 pcapInBytes=1 pcapOutBytes=1 pcapProtocols=TCP pcapSrcIp=192.168.0.1
pcapSrcPort=23456 pcapStartTime=2012-12-11 23:51:10 pcapSuccessfulConnections=1 pcapThreats=User Threat
pcapUrls=http://example.com proto=TCP sev=7 src=192.168.0.1

3.3.6 Intrusion event notifications

Example of a notification triggered for an intrusion.

CEF format:

Jul 23 17:45:20 test1 CEF:0|Lastline|Enterprise|8.1|intrusion-event|Updated intrusion|10| cn1=1 cn1Label=affectedHosts
cs2=bad stuff cs2Label=intrusionName cat=Command and Control deviceExternalId=3287884757:3459119816 deviceFacility=C&C Rule dvc=1.2.3.4 end=Feb 01 2018 15:16:17 UTC externalId=0284f6fcf42f4e859499f00bc00c19a7
cs1=https://do.no.connect/portal#/campaigns/details/0284f6fcf42f4e859499f00bc00c19a7?customer
=mannimarcocs1Label=intrusionDetailLink cn2=1 cn2Label=nrMalware msg=Added detection information: hosts: 1.2.3.4; malware: Upatre Public IP Check reason=Detected Command&Control traffic indicating that 2 hosts are infected with malware Upatre Public IP Check start=Jan 07 2018 20:01:02 UTC devTime=Dec 12 2012 00:00:00 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z

LEEF format:

Jul 23 17:45:20 test2 LEEF:1.0|Lastline|Enterprise|8.1|intrusion-event|affectedHosts=1 correlationRule=C&C Rule desc=Updated intrusion deviceExternalId=3287884757:3459119816 externalId=0284f6fcf42f4e859499f00bc00c19a7 intrusionName=bad stuff nrMalware=1 mostAdvancedAttackStage=Command and Control msg=Added detection information: hosts: 1.2.3.4; malware: Upatre Public IP Check reason=Detected Command&Control traffic indicating that 2 hosts are infected with malware Upatre Public IP Check sev=10 src=1.2.3.4 impact=100 url=https://do.no.connect/portal#/campaigns/details/0284f6fcf42f4e859499f00bc00c19a7?customer=mannimarcodevTime=Dec 12 2012 00:00:00 UTC devTimeFormat=MMM dd yyyy HH:mm:ss z

cat	msgIdentifier	deviceFacility
Analysis	appliance_update.analysis.anonvpn	Traffic Routing
Analysis	appliance_update.analysis.lladoc	Document Analyzer
Analysis	appliance_update.analysis.llama	Windows Sandbox
Analysis	appliance_update.analysis.lldroid	Android Analyzer
Analysis	appliance_update.analysis.llweb	URL/PDF Sandbox
Analysis	appliance_update.analysis.processing	Processing
Database	appliance_update.db.server	Database Server
Disk Usage	sys.disk.usage	Disk Usage
Email Analysis	appliance_update.mail.llmail	Email Analysis Service
Email Analysis Service	llmail.receiver	Email receiver
Email Analysis Service	llmail.shardуploader.upload	Email metadata uploader
Email Analysis Service	llmail.smtpsender-dsn.message	SMTP bounce sender message status
Email Analysis Service	llmail.smtpsender-dsn.server	SMTP bounce sender server status
Email Analysis Service	llmail.smtpsender.message	SMTP sender message status
Email Analysis Service	llmail.smtpsender.server	SMTP sender server status
ICAP	appliance_update.icap.cicap	ICAP Server
IDS Service	llsnifflogmon.suricata.ruleparsing.customer	Customer Rule
Integrations	appliance_update.integration.session_tracker	Session Tracker Service
Integrations	appliance_update.integrations.notification-proxy_status	Notification Delivery Service
Integrations	appliance_update.integrations.session_tracker	Session Tracker Service
Management	appliance_update.mgmt.appliance_update	Lastline Update Service
Management	appliance_update.mgmt.lload	Load Monitoring Service
Management	appliance_update.mgmt.version	Version Update Service
Message Processing	appliance_update.mq.broker	Message Broker
Message Processing	appliance_update.mq.queue_workers	Message Processors
Monitoring	appliance_update.monitoring.llpsv	Sniffer Service
Monitoring	appliance_update.monitoring.suricata	IDS Service
Notification Delivery Service	notification.server.checkpoint	Checkpoint Server Status
Notification Delivery Service	notification.server.email	Email Server Status
Notification Delivery Service	notification.server.httppost	HTTP Server Status
Notification Delivery Service	notification.server.siem	SIEM Server Status
Notification Delivery Service	notification.server.tipping_point	TippingPoint SMS Server Status
Offline		
Online		
Queue Status	analyst_scheduler.status.capacity_percent	Analysis Queue - Load
Queue Status	analyst_scheduler.status.pickup_delay	Analysis Queue - Analysis Delay
Queue Status	analyst_scheduler.status.tasks_queued	Analysis Queue - Pending Tasks
Session Tracker Service	session-tracker.wmi_query	Session Tracker Query Status
System	appliance_update.action.configure	Configuration
System Status	appliance_update.appliance_clock	Appliance Clock
Threat Intelligence Replication	db.monitor_slave.io	Threat Intelligence Replication IO
Threat Intelligence Replication	db.monitor_slave.sql	Threat Intelligence Replication SQL
Traffic Routing	anonymity_provider.status	Traffic Routing Check
Windows Sandbox	analyst_daemon.llama.configuration	Sandbox Configuration Data

Table 2: Possible values for appliance trigger fields

action_name	description
BLOCK_EMAIL	The whole mail message was blocked
BLOCK_ATTACHMENT	The attachment contained in the mail message was blocked
BLOCK_URL	The URL contained in the mail message was blocked
WARN	A warning was issued about the content of the mail that triggered this mail event
LOG	The mail event was only logged
UNKNOWN	An unknown action was taken in response to this event

Table 3: Possible values for mail event action