

Lastline Enterprise HTTP POST notifications Integration

January 17, 2024

1 Introduction

This guide describes the integration of HTTP POST notifications into Lastline Enterprise.

The HTTP POST notifications Integration allows Lastline Enterprise to automatically send HTTP POST notifications to a specific URL when events that match some specified criteria are triggered.

In the next sections this guide will explain how to configure and use HTTP POST notifications.

2 Overview of the HTTP POST notifications Integration

2.1 Glossary

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

2.1.1 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.

2.1.2 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).

2.1.3 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)

2.1.4 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)

2.1.5 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.

2.1.6 Test trigger

Trigger category for testing events. A notification can be triggered from the UI to verify that the HTTP POST notifications Integration was successfully configured. (available from format version 7.17)

2.1.7 Intrusion trigger

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

2.2 Architecture

When using HTTP POST notifications Integration a Manager can be configured to send HTTP POST notifications automatically to a chosen URL whenever the configured events are triggered. The Manager can either send the notification directly to the specified URL, through a Sensor or it may be set to send it through the system configured proxy.

The content of the notifications differs depending on the event that has been triggered.

The guide will now list the fields that are included in the body of the request for every trigger type.

2.2.1 Appliance trigger fields

- `format_version`: version of the notification format, currently "8.1"
- `trigger_type`: type of the trigger (i.e., appliance checkin or appliance message)
- `timestamp`: timestamp of the event as reported by the appliance
- `appliance_uuid`: unique identifier of the interested appliance
- `appliance_type`: type of the interested appliance
- `impact`: impact of this event, ranging from 0-100
- `appliance_detail_link`: link to the status page of this appliance
- `appliance_attributes`:
 - `private_ip_address`
 - `public_ip_address`
 - `fully_qualified_domain_name`
- `special fields`:
 - `is_online` (checkin event only)
 - `last_checkin_timestamp` (checkin event only)
 - `source` (message event only). Source and key together provide an identifier of what is being reported. Possible values for `source.key` are listed in table 2.
 - `key` (message event only): Source and key together provide an identifier of what is being reported. Possible values for `source.key` are listed in table 2.
 - `component_name` (message event only): name of the component that sent the message. Possible values are listed in table 2.

- detail_name (message event only). Possible values are listed in table 2.
- message (message event only)

2.2.2 Audit trigger fields

(this fields are available only from format version 7.3)

- event_type: "audit-event" (available from format version 7.5)
- format_version: version of the notification format, currently "8.1"
- description: extended description of the action
- impact: impact of this action, ranging from 0-100
- timestamp: timestamp of the event
- account: account of the user that performed the logged action
- customer: customer to which the action refers
- source_ip: ip address of the user that performed this action
- audit_action type: type of the audit action, some of the possible values are described in table 1 (available from format version 7.5)
- audit_event_category: category of the audit action, currently one of:
 - registration: account/customer/license related actions
 - configuration: appliance related actions
- affected_entity_type: type of the object affected by this action (e.g., "license", "account", "appliance")
- affected_entity_id: identifier of the object affected by this action (e.g., the license key, name of the account, uuid of the appliance)
- audit_event_id: identifier of the audit event
- event_detail_link: a link to the details of this audit action on the user website
- device_id: unique identifier of the manager appliance (on-premise only)
- configured_software_version: version of the software that has been reconfigured (appliance_upgraded events only)

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

component_name	source.key	detail_name
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.sharduploader.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
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

2.2.3 Network trigger fields

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

- `format_version`: version of the notification format, currently "8.1"
- `description`: description of the event (e.g., Suspicious DNS Resolution)
- `impact`: impact of this event, ranging from 0-100
- `detection_type`: type of the detection (e.g., dns-resolution)
- `start_timestamp`: start timestamp of the event
- `end_timestamp`: end timestamp of the event
- `malware_class`: class of the detected malware
- `malware`: name of the detected malware
- `action`: action taken in response to this event
- `occurrences`: number of occurrences of this event
- `destination_port`: destination port of the event
- `event_id`: identifier of the event
- `source_ip`: source ip address of the event
- `destination_ip`: destination ip address of the event
- `source_mac`: source mac address of the event
- `transport_protocol`: transport layer protocol used by the event
- `destination_host`: destination hostname of the event
- `resolved_domain`: resolved destination domain
- `source_dns_domain`: hostname of the source
- `event_detail_link`: link to details about this event on the user website
- `detection_id`: obfuscated string representing the concatenation of threat, activity and detector id
- `device_id`: obfuscated identifier of the appliance
- `event_url`: 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
- incident information:
 - `incident_id`: identifier of the incident related to this event
 - `incident_impact`: impact of the incident related to this event
 - `incident_malware`: name of the malware involved in the incident
 - `incident_malware_class`: name of the malware family involved in the incident
- malicious file information:

- name
 - MD5 hash
 - SHA-1 hash
 - size
 - type
 - detail link: link to details about this malicious file on the user website
- suspicious url information:
 - url_detail_link: Link to details about the suspicious URL on the user website (this field is available only from format version 7.10)
 - logged users: list users that were logged on at the time of the event
 - custom intelligence fields:
 - last_modified: last modification time of this entry
 - source: name of the source
 - comment: comment on the intel entry
 - message (ids rules only): rule message
 - detection_id (ids rules only): string representing the concatenation of group rule and revision id
 - pcap fields: (available from format version 7.5)
 - pcap_id: identifier of the pcap related to this event
 - pcap_start_time: start time of the pcap
 - pcap_src_ip: source IPV4 address of the pcap
 - pcap_src_port: source port of the pcap
 - pcap_dst_ip: destination IPV4 address of the pcap
 - pcap_dst_port: destination port of the pcap
 - pcap_urls: list of URLs associated with this pcap
 - pcap_hosts: list of contacted hostnames from the pcap
 - pcap_in_bytes: number of bytes received
 - pcap_out_bytes: number of bytes sent
 - pcap_threats: list of threats involved in this pcap
 - pcap_protocols: list of protocols
 - pcap_successful_connections: number of successful connections from the pcap
 - pcap_failed_connections: number of failed connections from the pcap
 - pcap_body: base64 encoded, raw binary content of the traffic capture (might be truncated if too long)

2.2.4 Mail trigger fields

- `format_version`: version of the notification format, currently "8.1"
- `description`: description of the event (i.e., "Suspicious Email Attachment")
- `impact`: impact of this event, ranging from 0-100
- `detection_type`: type of the detection ("email-attachment", "email-message", "email-url")
- `timestamp`: timestamp of the event
- `sender`: sender of the email message
- `recipients`: recipients of the email message
- `subject`: subject of the mail message
- `device_id`: obfuscated identifier of the appliance
- `action`: action taken in response to this event, some of the possible values are described in table 3 (available from format version 7.6)
- malicious attachment information (malicious attachments only):
 - `name`
 - `MD5 hash`
 - `SHA-1 hash`
 - `size`
 - `type`
 - `detail link`: link to details about this attachment on the user website
- url information (email-url type only): (available from format version 7.5)
 - `mail_url`: url found in the mail message
 - `mail_url_md5`: MD5 hash of the url
- mail message information (mail-message type only): (available from format version 9.1)
 - `detectors`: detectors that flagged this piece of mail
 - `threat`: threat that was detected
 - `threat_class`: threat class of the detected threat
- `event_detail_link`: link to details about this event on the user website (available from format version 7.5)

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

2.2.5 Test trigger fields

(this fields are available only from format version 7.17)

- format_version: version of the notification format, currently "8.1"
- description: description of the event (i.e., "User triggered test event")
- impact: impact of this event, currently 10 for tests
- trigger_type: type of the trigger (i.e., "test-notification")
- timestamp: timestamp of the event
- test_uuid: unique identifier for the test
- notification_config_id: unique identifier for the notification configuration

2.2.6 Intrusion trigger fields

- correlation_rule: the correlation rule that caused the event
- description: short description of the event. (e.g., "Detected intrusion")
- device_id: obfuscated identifier of the appliance
- end_timestamp: end time of the event
- extended_description: detailed information about the intrusion event (e.g, "Correlated 3 incidents into an intrusion")
- format_version: version of the notification format, currently "8.1"
- hosts_affected: a sequence of each host with the threats and attack stages associated with it
- impact: the impact of the intrusion (only available from format 9.1)
- intrusion_details_link: A URL that links to the intrusion details page for this intrusion in the Lastline Portal.
- intrusion_name: the name of the intrusion
- intrusion_uuid: the unique identifier of the intrusion
- last_modified: last modification time of this entry
- most_advanced_stage: the most advanced attack stage
- nr_affected_hosts: number of affected hosts in the intrusion

- nr_malware: number of distinct malware in the intrusion
- reason: the reason behind the intrusion event
- start_timestamp: start timestamp of the event
- trigger_type: type of the trigger (i.e., "intrusion-event")

3 Requirements

- In order to be able to send HTTP POST notifications through an HTTPS proxy the system's HTTPS proxy in the form "proxy_address : port" must first be configured

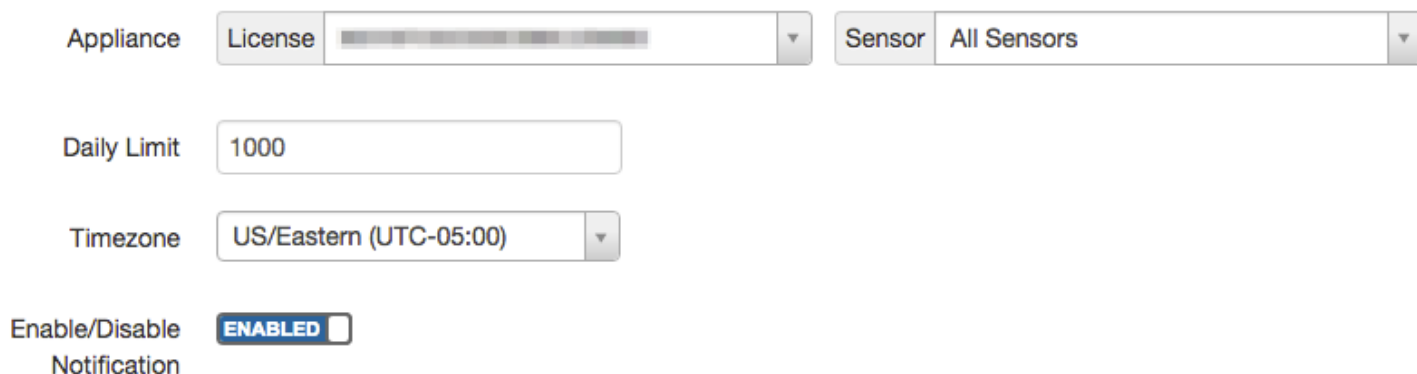
4 Configuration

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

4.1 Configuration of the HTTP POST notifications Integration on the Manager

On the web interface of the Manager, go to Admin → Integration → Generic HTTP Notification.

Click on the "+" button on the right side to enter the Generic HTTP Notification creation screen.



Appliance License Sensor All Sensors

Daily Limit

Timezone

Enable/Disable Notification ENABLED

HTTP POST 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

HTTP Post Settings [?](#)

Post URL Port Path

HTTP Proxy **DISABLED** [?](#)

Verify SSL Cert **DISABLED**

Post Body Format

HTTP POST Notification special settings

Then proceed to configure the "HTTP Post Settings" section:

- Post URL
 - Protocol: select either "HTTP" or "HTTPS" protocol to be used
 - Hostname or IP: insert the hostname or IP address of the destination server
 - Port: insert the TCP port on which the destination server is listening
 - Path: insert path section of the URL
- HTTP Proxy: enable this to proxy the requests through the system's configured proxy
- Verify SSL Cert: enable this to check the host's SSL certificate for HTTPS requests
- Post Body Format: select either JSON or XML as format for the request body
- Include pcap: Whether to include pcap information inside the notification for network events. (Available from version 7.5)

4.2 Testing HTTP POST notifications Integration

In order to make sure that the HTTP POST notifications have been correctly configured, 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 HTTP POST notification an entry will be displayed in Appliances → Logs → Monitoring Logs under "Notification Delivery Service" Component and "Httppost Server Status" Type, reporting the details about the notification delivery.

4.3 Notifications examples

The guide will now show a few examples of content of HTTP POST notifications for each trigger category.

4.3.1 Test event notifications

Example of a notification triggered for testing (available from format version 7.17).

```
"format_version": "8.1", "description": "User triggered test event", "impact": 10, "trigger_type": "test-notification", "timestamp": "2015-08-27 14:16:06+00:00", "test_uuid": "3dc144bdb3434b1abf7a465de3f57948", "notification_config_id": 37
```

4.3.2 Mail event notifications

Example of notification body after the detection of mail based on an attachment.

```
"impact": 100, "file_detail_link": "https://user.enterprise.lastline.local/malscape/#/task/613de0cc17534adbb0f046b88e1f70f7",  
"start_timestamp": "2015-08-27 14:16:06+00:00", "sender": "fake@example.com", "description": "Suspicious Email Attach-  
ment", "format_version": "7.3", "recipients": ["<test@example.com>"], "file_type": "Rich Text Format data, unknown version",  
"file_name": "f0b3f8277c884d4be2397bb05cd102f3", "file_sha1": "b4be2633ac9ca6ff6670d67473b042123a0a7644", "sub-  
ject": "Test", "file_md5": "f0b3f8277c884d4be2397bb05cd102f3", "detection_type": "email-attachment", "file_size":  
163699, "device_id": "3053322414:602745899", "end_timestamp": "2015-08-27 14:16:06+00:00", "event_detail_link":  
"https://user.enterprise.lastline.local/mail/message#/3287884757/3459119816/9561?mail_time=2016-03-21"
```

Example of notification body after the detection of mail based on a url (available from format version 7.5).

```
"end_timestamp": "2015-11-25 14:28:05+00:00", "impact": 99, "start_timestamp": "2015-11-25 14:28:05+00:00",  
"sender": "test@lastline.com", "description": "Suspicious Email Url", "format_version": "7.3", "recipients":  
["fake@lastline.com"], "mail_url_md5": "2be456f055282b7dc6d6b0f002a52dad", "detection_type": "email-url", "device_id":  
"3287884757:3459119816", "appliance_name": "sensor01", "mail_url": "http://www.evil.fake", "subject": "TEST EMAIL!",  
"event_detail_link": "https://user.enterprise.lastline.local/mail/message#/3287884757/3459119816/9561?mail_time=2016-  
03-21"
```

Example of notification body after the detection of mail based on a mail message characteristic (available from format version 9.1).

```
"end_timestamp": "2019-09-09 22:17:17+00:00", "impact": 80, "start_timestamp": "2019-09-09 22:17:17+00:00",  
"sender": "test@lastline.com", "description": "Suspicious Email Message", "format_version": "9.1", "re-  
cipients": ["fake@lastline.com"], "detectors": ["email_anomaly:spam_domain", "email_anomaly:spam_ip"],  
"threat": "Mebroot", "threat_class": "drive-by", "detection_type": "email-message", "device_id":  
"3287884757:3459119816", "appliance_name": "sensor01", "subject": "TEST EMAIL!", "event_detail_link":  
"https://user.enterprise.lastline.local/mail/message#/3287884757/3459119816/9359?date=2019-09-09"
```

4.3.3 Appliance event notifications

Example of notification reporting that an appliance is online.

```
"impact": 10,
"appliance_detail_link": "https://user.enterprise.lastline.local/appliance#/config/status/0284f6fcf42f4e859499f00bc00c19a7",
"format_version": "7.3", "appliance_type": "SENSOR", "trigger_type": "appliance-checkin", "timestamp": "2015-08-27 13:34:14", "appliance_fqdn": "lastline-sensor.lastline.local", "last_checkin_timestamp": "2015-08-27 13:34:14",
"is_online": true, "appliance_public_ip": "192.168.1.57", "appliance_private_ip": "192.168.1.57", "appliance_uuid": "0284f6fcf42f4e859499f00bc00c19a7"
```

Example of notification reporting the successful upload of email metadata.

```
"impact": 10, "detail_name": "Email metadata uploader", "appliance_detail_link": "https://user.enterprise.lastline.local/appliance#/config/status/0284f6fcf42f4e859499f00bc00c19a7", "format_version": "7.3", "appliance_type": "SENSOR", "trigger_type": "appliance-message", "timestamp": "2015-08-27 13:46:36", "source": "lmail", "appliance_uuid": "0284f6fcf42f4e859499f00bc00c19a7", "key": "sharduploader.upload", "appliance_fqdn": "lastline-sensor.lastline.local", "appliance_public_ip": "192.168.1.57", "appliance_private_ip": "192.168.1.57", "message": "Successful upload of email metadata", "component_name": "Email Analysis Service"
```

4.3.4 Audit event notifications

Example of notification reporting that the software version of an appliance has been upgraded.

```
"affected_entity_id": "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa", "customer": "test@fake.bet", "account": "fake@test.bet",
"description": "The software version of the appliance has been upgraded", "format_version": "7.3", "configured_software_version": "2.2.2", "impact": 40, "timestamp": "2015-11-25 14:25:45+00:00", "source_ip": "192.168.0.1", "event_type": "audit-event", "audit_action_type": "appliance_upgraded", "event_detail_link": "https://user.enterprise.lastline.local/settings#/audit/a/2015-11-24/2015-11-26?audit_event_id=17", "affected_entity_type": "appliance", "audit_event_id": 17, "audit_event_category": "configuration"
```

4.3.5 Network event notifications

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

```
"file_detail_link": "https://user.enterprise.lastline.local/malscape#/task/6ad71b9ddc554d1eac73ce27f55e2abb", "file_type": "PDF document", "file_name": "/5e2eceed69c9ef5435298abc1d10624b.pdf", "file_size": 5984, "detection_type": "file-download", "occurrences": 1, "detection_id": "2535ec71:30f7e7df:e52cff2b", "end_timestamp": "2015-08-27 13:46:13+00:00", "transport_protocol": "TCP", "malware": "Malicious Document Download", "event_id": 9, "src_ip": "127.0.0.1", "event_detail_link": "https://user.enterprise.lastline.local/event#/3053322414/602745899/9?event_time=2015-08-27", "impact": 100, "description": "Suspicious File Download", "format_version": "7.3", "file_md5": "5e2eceed69c9ef5435298abc1d10624b", "http_host": "127.0.0.2", "device_id": "3053322414:602745899", "event_url": "http://127.0.0.2/5e2eceed69c9ef5435298abc1d10624b.pdf", "incident_id": 12, "incident_impact": 100, "incident_malware": "Malicious Document Download", "incident_malware_class": "Malicious File Download", "start_timestamp": "2015-08-27 13:46:13+00:00", "malware_class": "Malicious File Download", "file_sha1": "e1a1dcfefa8c96723d5f7816f0e991a0a01b5f0a", "dst_port": 80, "action": "LOG", "dst_ip": "127.0.0.2"
```

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

```
"impact": 1, "transport_protocol": "TCP", "malware": "Lastline test", "description": "Suspicious Network Connection", "format_version": "7.3", "event_id": 8, "dst_port": 80, "start_timestamp": "2015-08-27 13:38:44+00:00", "dst_host": "test.lastline.com", "src_ip": "192.168.1.57", "detection_type": "network-connection", "malware_class": "Lastline test", "occurrences": 1, "event_detail_link": "https://user.enterprise.lastline.local/event#/3053322414/602745899/8?event_time=2015-08-27", "detection_id": "fc900ff8:30fbe7df:30fbe7df", "action": "LOG", "dst_ip": "52.5.237.96", "device_id": "3053322414:602745899", "event_url": "http://test.lastline.com", "incident_id": 13, "incident_impact": 1, "incident_malware": "Lastline test", "incident_malware_class": "Lastline test", "src_mac": "08:00:27:00:c9:7a", "end_timestamp": "2015-08-27 13:38:44+00:00"
```

Example of notification triggered by a suspicious dns resolution.

```
"impact": 1, "transport_protocol": "UDP", "malware": "Lastline test", "resolved_domain": "test.lastline.com", "description": "Suspicious DNS Resolution", "format_version": "7.3", "event_id": 7, "dst_port": 53, "start_timestamp": "2015-08-27 13:38:44+00:00", "src_ip": "192.168.1.57", "detection_type": "dns-resolution", "malware_class": "Lastline test", "occurrences": 2, "event_detail_link": "https://user.enterprise.lastline.local/event#/3053322414/602745899/7?event_time=2015-08-27", "detection_id": "fc900ff8:30fbe7df:30fbe7df", "action": "LOG", "dst_ip": "192.168.1.1", "device_id": "3053322414:602745899", "event_url": "http://test.lastline.com", "incident_id": 14, "incident_impact": 1, "incident_malware": "Lastline test", "incident_malware_class": "Lastline test", "src_mac": "08:00:27:00:c9:7a", "end_timestamp": "2015-08-27 13:38:44+00:00"
```

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

```
"event_url": "http://example.com", "detection_type": "dns-resolution", "occurrences": 1, "detection_id": "c90de0dd:d0051f96:d0051f96", "appliance_name": "sensor01", "impact": 70, "malware": "Test Threat", "src_dns_domain": "", "format_version": "7.2", "event_id": 1785, "src_ip": "192.168.0.1", "event_detail_link": "https://do.no.connect/event#/3287884757/3459119816/1785?event_time=2012-12-12", "end_timestamp": "2012-12-12 00:20:00+00:00", "transport_protocol": "TCP", "description": "Suspicious DNS Resolution", "dst_ip": "10.0.0.1", "device_id": "3287884757:3459119816", "start_timestamp": "2012-12-12 00:00:00+00:00", "malware_class": "Testing Threat Class", "dst_port": 80, "action": "LOG", "pcap_id": 866, "pcap_src_ip": "192.168.0.1", "pcap_threats": ["UserDefinedThreat"], "pcap_dst_port": 80, "pcap_failed_connections": 1, "pcap_in_bytes": 1, "pcap_start_time": "2012-12-12 00:00:00", "pcap_src_port": 23456, "pcap_protocols": ["TCP"], "pcap_urls": ["http://example.com"], "pcap_hosts": ["www.lastline.com"], "pcap_out_bytes": 1, "pcap_dst_ip": "10.0.0.1", "pcap_successful_connections": 1, "pcap_body": "1MOyoQIABAAAAAAAAAAAAAP//AAABAAAAI0ujQLi/BAA+AAAAPgAAAP7/IAABAAAAAQAAAAgARQAAMA9BQACABpHrkf6g7UHQ5N8NLABQOK",
```

4.3.6 Breach event notifications

Example of a notification triggered by a breach event (available from format version 8.3).

```
"hosts_affected": [ "host": "1.2.3.4", "attack_stages": ["Command and Control"], "malware": ["Upatre Public IP Check"] ], "correlation_rule": "C&C Rule", "device_id": "3287884757:3459119816", "device_id": "3287884757:3459119816", "end_timestamp": "2018-02-01 15:16:17", "format_version": "8.1", "impact": 90, "intrusion_details_link": "https://do.no.connect/portal#/campaigns/details/d5ec0e2e01cb49d993a0c4d7dbee968c?customer=mannimarco@oblivion.bet", "intrusion_name": "intrusion", "intrusion_uuid": "d5ec0e2e01cb49d993a0c4d7dbee968c", "last_modified": "2018-01-12 03:15:20", "most_advanced_stage": "Command and Control", "nr_affected_hosts": 1, "nr_malware": 1, "reason": "Detected Command&Control traffic indicating that 2 hosts are infected with malware Upatre Public IP Check", "start_timestamp": "2018-01-07 20:01:02", "trigger_type": "intrusion-event", "extended_description": "Added detection information: hosts: 1.2.3.4; malware: Upatre Public IP Check"
```