



# SENDING DARKTRACE ALERTS TO SPLUNK

Threat Visualizer v5.2

## SENDING DARKTRACE ALERTS TO SPLUNK

Threat Visualizer v5.2

|  |    |
|--|----|
| Darktrace Splunk App for Alerts                            | 3  |
| Prerequisites for the Splunk App                           | 4  |
| Configuring the Darktrace Splunk App for Splunk Enterprise | 5  |
| Configuring the Darktrace Splunk App for Splunk Cloud      | 7  |
| Splunk Alert Filters and Optional Settings                 | 9  |
| Darktrace Alert Splunk CIM Mappings                        | 12 |
| Darktrace Splunk Alert JSON Examples                       | 16 |



# DARKTRACE SPLUNK APP FOR ALERTS

## Introduction

Darktrace provides a fundamentally unique approach to cyber defense. With a detailed understanding of what is normal within the business, Darktrace's Self Learning AI can identify and contain emerging threats that have bypassed traditional defenses and are active within the network. For security teams who wish to leverage this learning to enhance the value of their existing security stack, the Threat Visualizer offers multiple ways to integrate.

The Darktrace Splunk app brings the power of Darktrace self learning to Splunk - insights from Darktrace's AI can be correlated against alerts from internal threat intelligence tools and other elements of your organization's security stack. The custom Workflow Integration data format allows model breach alerts, system status and AI Analyst incidents to be populated within the connected Splunk instance. Alert data is Splunk CIM compatible for enhanced integration across logs.

## Visualization



The Darktrace Splunk app enhances the Splunk user interface by populating it with real-time threat alerts and events from your Darktrace environment. The app provides multiple dashboards for quick review of high priority model breaches, AI Analyst insights and system status alerts.

The Latest Activity dashboard highlights model breach alerts in the last 7 days which can be easily filtered by timeframe, score, and model. Likewise, the Trending page highlights the performance of models for the last 2 weeks, displaying high-risk devices and high-frequency risky behaviors seen.

The Darktrace Cyber AI Analyst investigates, analyzes and reports upon threats seen within your Darktrace environment; the AI Analyst dashboard allows these AI powered insights to be leveraged and investigated within the Splunk interface. System status information is also available on a dedicated page so that operators stay informed of system health, changes in monitored traffic, and any errors experienced by Darktrace/Apps, Darktrace/Cloud, and Darktrace/Zero Trust modules, or virtual sensors.

Interacting with any of the panels will filter the detailed table below by the panel query - for example, selecting a "Top Device" on the AI Analyst dashboard will return only incident events relevant to that device. Each alert links to detailed reports in the Darktrace Threat Visualizer, allowing for deep analysis of emerging vulnerabilities and early-stage threats.

---

## PREREQUISITES FOR THE SPLUNK APP

### Prerequisites

- A Darktrace master instance running the most recent software version (minimum v5.1).
- A Fully Qualified Domain Name (FQDN) must be configured for the Darktrace instance for links to be included in external alerts. This can be found on the "Settings" tab of the Darktrace System Config page, under "System".
- A pre-existing Splunk Enterprise or Splunk Cloud instance.
- A Splunk ID which can be provided to your Darktrace representative to permit access to the app (see below).

### Splunk Environment

The Darktrace app for Splunk requires a pre-existing Splunk instance - both Splunk Enterprise and Splunk Cloud are supported. Please follow the appropriate installation steps for our Splunk instance type.

Splunk Enterprise can be downloaded directly from Splunk at <http://www.splunk.com/download>. For more information about installing and running Splunk Enterprise and system requirements, see the relevant [Splunk installation documentation](#).

### Supplying a Splunk ID

Providing your Splunk ID will allow Darktrace to pre-approve your account to download the Darktrace Splunk app from Splunkbase.

### How to Find your Splunk ID

1. Log into Splunkbase and go to '**Support and Services**' at the top-right corner, where your username is displayed.
2. Choose '**Support Portal**' and navigate to '**My Profile**'
3. Locate the Splunk ID listed under '**Screen Name**'
4. Supply this ID to your Darktrace representative prior to download.

# CONFIGURING THE DARKTRACE SPLUNK APP FOR SPLUNK ENTERPRISE

## Install the App for Splunk Enterprise

First, download the Darktrace app from [Splunkbase](#). If you do not have permission to download the app, please contact your Darktrace representative or a member of Darktrace Support.

Then, install the app via method 1 or 2 below.

### Method 1 - Install the Darktrace App within Splunk Enterprise

1. Log into Splunk Enterprise.
2. On the Apps menu, click **Manage Apps**.
3. Click **Install app from file**.
4. In the **Upload app window**, click **Choose File**. Select the TAR file you just downloaded, and then click **Open**.
5. Click **Upload**.
6. Click **Restart Splunk**, and then confirm that you want to restart.

### Method 2 - Install the Darktrace App directly into Splunk Enterprise

1. Move the downloaded file into the `$SPLUNK_HOME/etc/apps` directory.
2. Extract the app using a tool like `tar` (on Unix-based systems) or WinZip (on Windows).
3. Restart Splunk.

After you install the Splunk app, you will find it on Splunk Home.

## Configure the Splunk App to Receive Data

Upon installing the app, a TCP-listening port must be set up for direct interaction with the Darktrace Appliance.

*Other input methods will not be described here, please refer to Splunk documentation on alternative ingestion methods.*

1. Log in to your Splunk instance.
2. Click **Add Data** either on the main page, or under the settings heading in the toolbar at the top-right corner of the screen.
3. Click **Monitor**.
4. Select **TCP/UDP** from the list. Ensure TCP is selected in the configuration window and enter the desired port number.
5. If you wish to accept data from only a single Darktrace instance through this port, enter the IP address of the instance in the **Only Accept Connection From** field and click **Next**.
6. On the **Structured** tab, set the **Source type** to `darktrace`.
7. Set **App Context** to **Darktrace**.  
Click **Review** and confirm the settings are correct.
8. Click **Submit** to set the new TCP listening port.

## Darktrace Configuration

The Darktrace instance must now be configured to send alert data to the Splunk instance.

1. Within the Threat Visualizer, navigate to the **System Config** page (**Main menu > Admin**).  
From the left-side menu, select **Modules** and choose **Splunk** from the available **Workflow Integrations**.
2. A configuration window will open.  
Select the relevant form of Splunk output format - here, Syslog JSON - and click "**New**" to reveal the configuration settings.
3. In the **Server** field, enter IP address or hostname of the Splunk instance.
4. In the **Server Port** field, set the port number defined above in step 4 of "Configure the Splunk App to Receive Data".  
Ensure that the port selected is allowed by any intermediary firewalls.
5. Turn on **Show Advanced Options**.  
In the first section, turn on **Send Alerts Using TCP**.
6. Turn on **Send AI Analyst Alerts** and configure alerting thresholds for AI analyst events.  
Configure any optional filters and settings as described in *Optional Filters and Settings*, or leave the default options selected.  
Alerts will only be sent once the master **Send Alerts** toggle is turned on (Step 11.)
7. Turn on **Send Model Breach Alerts** and configure alerting thresholds for model breaches.  
Configure any optional filters and settings as described in *Optional Filters and Settings*, or leave the default options selected.  
Alerts will only be sent once the master **Send Alerts** toggle is turned on (Step 11.)
8. Turn on **Send System Status Alerts** and configure alerting thresholds for System Status Alerts.  
Configure any optional filters and settings as described in *Optional Filters and Settings*, or leave the default options selected.  
Alerts will only be sent once the master **Send Alerts** toggle is turned on (Step 11.)
9. Click **Add** to save the configuration and observe a confirmation message.
10. Scroll to the top of the entry and click **Verify alert settings** to send a test alert to Splunk.  
If the alert has been received successfully, it should appear in the Darktrace "Latest Activity" dashboard as a *Critical Severity* alert.
11. Finally, turn on **Send Alerts** and save changes.

# CONFIGURING THE DARKTRACE SPLUNK APP FOR SPLUNK CLOUD

## Install the App for Splunk Cloud

The app can be acquired and installed from within the Splunk Cloud user interface.

1. Log into your Splunk Cloud instance.
2. On the Apps menu, click on '**Find More Apps**'. This should take you to a '**Browse More Apps**' page.
3. Find the '**Darktrace App for Splunk**' App and click on '**Install**'.

After you install the Splunk app, you will find it on Splunk Home.

## Configure a HEC to Receive Darktrace Data

The process to create a HEC is described in the Splunk Cloud documentation [Configure HTTP Event Collector on Splunk Cloud Platform](#). The process is repeated here for reference.

1. Log into your Splunk Cloud instance. From the menu bar, click **Settings** > **Add Data**.
2. Click **Monitor**, under "Or get data in with the following methods".
3. Select **HTTP Event Collector** from the list.
4. In the **Name** field, enter a name for the token - for example, **Darktrace** .  
In the **Source name override** field, enter **darktrace**  
Add an optional description and click "Next".
5. Under "Input Settings", set the **Source Type** to **darktrace** .
6. Click **Review** and confirm the settings are correct.  
Click **Submit**.
7. You should now see "Token has been created successfully". Copy the contents of the **Token Value** field.  
This value must be inserted into the Darktrace System Config page, so do not close this tab.

## Darktrace Configuration

The Darktrace instance must now be configured to send alert data to the Splunk instance.

1. Within the Threat Visualizer, navigate to the **System Config** page (**Main menu** > **Admin**).  
From the left-side menu, select **Modules** and choose **Splunk** from the available **Workflow Integrations**.
2. A configuration window will open.  
Select the relevant form of Splunk output format - here, **HTTPS JSON** - and click "**New**" to reveal the configuration settings.
3. In the **Splunk Cloud Platform Hostname** field, enter hostname of the Splunk Cloud instance. For example, **example.splunkcloud.com** .
4. In the **HTTP Event Collector Token** field, enter the token generated in Splunk Cloud during the configuration above ("Configure a HEC to Receive Darktrace Data", step 7.)
5. Turn on **Show Advanced Options**.

6. Turn on **Send AI Analyst Alerts** and configure alerting thresholds for AI analyst events.  
  
Configure any optional filters and settings as described in *Optional Filters and Settings*, or leave the default options selected.  
  
Alerts will only be sent once the master **Send Alerts** toggle is turned on (Step 11.)
7. Turn on **Send Model Breach Alerts** and configure alerting thresholds for model breaches.  
  
Configure any optional filters and settings as described in *Optional Filters and Settings*, or leave the default options selected.  
  
Alerts will only be sent once the master **Send Alerts** toggle is turned on (Step 11.)
8. Turn on **Send System Status Alerts** and configure alerting thresholds for System Status Alerts.  
  
Configure any optional filters and settings as described in *Optional Filters and Settings*, or leave the default options selected.  
  
Alerts will only be sent once the master **Send Alerts** toggle is turned on (Step 11.)
9. Click **Add** to save the configuration and observe a confirmation message.
10. Scroll to the top of the entry and click **Verify alert settings** to send a test alert to Splunk.  
  
If the alert has been received successfully, it should appear in the Darktrace "Latest Activity" dashboard as a *Critical Severity* alert.
11. Finally, turn on **Send Alerts** and save changes.




## SPLUNK ALERT FILTERS AND OPTIONAL SETTINGS

Filters control whether alerts are sent or suppressed. An alert **must pass through all relevant filters** to be created by the Splunk integration. Not all criteria are applicable to all alert types - this is indicated in the *Applies To* column of the subsequent table.

Some filters and settings may not appear unless "send alerts" for the relevant alert type has been turned on.

### Available Filters

An alert **must meet all filter criteria** that are relevant to it. For example, a model breach must meet all thresholds, regular expressions and device restrictions applied.

If the settings fields appear to be read-only, it means that they are configured globally. Global Settings can be accessed by clicking the  **Config** icon to the right of **Workflow Integrations** on the **System Config** page, and changes can be made to individual modules by turning on **Enable Modular Alert Thresholds**.

Obfuscation (**Restricted View Alerts**) can also be configured for AI Analyst and model breach alerts from the global settings.

| FIELD NAME                              | APPLIES TO          | DEFAULT              | DESCRIPTION   |
|---|---------------------|----------------------|---|
| AI Analyst Behavior Filter              | AI Analyst Alerts   | Critical             | Behavior categories are high level filters that allow an operator to focus in on specific levels of severity or behavior. There are four categories: Critical, Suspicious, Compliance and Informational. Select the categories to filter alerts to. |
| Minimum AI Analyst Incident Event Score | AI Analyst Alerts   | 0                    | Restricts incident events sent as external alerts to those with an individual event score above the threshold.  |
| Minimum AI Analyst Incident Score       | AI Analyst Alerts   | 20                   | Incident events are part of a larger incident. Restricts incident events sent as external alerts to those with an overall incident score above the threshold. Incident scores are expected to use the full range of scores from 0-100.              |
| Model Breach Behavior Filter            | Model Breach Alerts | Critical, Suspicious | Behavior categories are high level filters that allow an operator to focus in on specific levels of severity or behavior. There are four categories: Critical, Suspicious, Compliance and Informational. Select the categories to filter alerts to. |
| Minimum Breach Score <sup>1</sup>       | Model Breach Alerts | 50                   | Enter a value to restrict the sending of alerts to those with a Breach Score that exceeds that value.   |
| Minimum Breach Priority <sup>1</sup>    | Model Breach Alerts | 0                    | Enter a value to restrict the sending of alerts to those with a Breach priority that exceeds that value (0-5). "Enable Modular Alert Thresholds" must be turned on in the Global Alert Config.  |
| Model Expression <sup>1</sup>           | Model Breach Alerts | N/A                  | Enter a regular expression to restrict the sending of alerts to those with model names (and folder) that match the regular expression. "Enable Modular Alert Thresholds" must be turned on in the Global Alert Config.                              |
| Model Tags Expression                   | Model Breach Alerts | N/A                  | Enter a regular expression restrict the sending of alerts to models with tags matching the expression.  |
|   |                     | N/A                  |   |

| FIELD NAME                     | APPLIES TO           | DEFAULT | DESCRIPTION   |
|--------------------------------|----------------------|---------|---|
| Device IP Addresses            | Model Breach Alerts  |         | Enter a comma separated list of IP addresses, and/or CIDR IP range(s) to restrict the sending of alerts to only those alerts concerning a device with one of the listed IP addresses. |
| Device Tags Expression         | Model Breach Alerts  | N/A     | Enter a regular expression restrict the sending of alerts to those for devices with tags matching the expression.   |
| Minimum System Status Priority | System Status Alerts | High    | Choose a priority level. Darktrace will only send System Status Alerts of the chosen priority level or above.   |

<sup>1</sup> Setting controlled by the global alert thresholds.

## Available Settings

Settings control the type and format of alerts sent.

### Alert Settings

| FIELD NAME                         | APPLIES TO           | DEFAULT | DESCRIPTION  |
|------------------------------------|----------------------|---------|--|
| Send AI Analyst Alerts             | AI Analyst Alerts    | On      | Turn on to send AI Analyst alerts.   |
| Send AI Analyst Alerts Immediately | AI Analyst Alerts    | On      | Turn on to send AI Analyst alerts as they occur and filter by score. Turn off to send a curated list of the most interesting AI Analyst Incidents every hour (legacy). |
| Send Model Breach Alerts           | Model Breach Alerts  | On      | Turn on to send Model Breach alerts.   |
| Send System Status Alerts          | System Status Alerts | On      | Turn on to send System Status alerts.  |
| Send Resolved System Status Alerts | System Status Alerts | On      | By default, alerts are sent to notify when a System Status issue is resolved. Turn off to only send alerts when issues arise.  |

### Additional Settings - Syslog JSON Only

| FIELD NAME            | APPLIES TO | DESCRIPTION  |
|-----------------------|------------|--|
| Send Alerts Using TCP | All alerts | Turn on to send alerts over TCP. TCP allows for a longer message and additional fields, such as destination hostname (dhost). Turn off to send alerts over UDP |
| Timezone              | All alerts | This setting alters the timestamp displayed in the Splunk alert to reflect a different timezone  |
| Use TLS               | All alerts | Turn on to send TCP traffic with TLS encryption. Requires "Send Alerts Using TCP": On.   |

---

| FIELD NAME                          | APPLIES TO | DESCRIPTION  |
|-------------------------------------|------------|--|
| TLS Verify Certificate              | All alerts | Turn on to ensure that the server certificate is signed by a trusted root certificate authority. Requires "Send Alerts Using TCP": On, "Use TLS": On.                                    |
| TLS Server Certificate Fingerprints | All alerts | Turn on to ensure syslog will only be sent to TLS servers that present certificates with fingerprints in this comma separated list. Requires "Send Alerts Using TCP": On, "Use TLS": On. |

## DARKTRACE ALERT SPLUNK CIM MAPPINGS

The Darktrace Splunk integration utilizes a custom JSON output format for Model Breach, AI Analyst and System Status alerts. Each alert type can be enabled separately if desired.

The format is Splunk CIM compatible and field mappings are listed below. Examples for each alert type are available in *Darktrace Alert Splunk JSON Examples*.

### Splunk CIM Mappings

#### Model Breaches

| CIM FIELD       | DARKTRACE MODEL BREACH JSON FIELD  |
|-----------------|--|
| src_user        | device.credentials   |
| user            | device.credentials   |
| action          | model.actions.antigena.action  |
| reason          | triggeredComponents{}.metric.label   |
| dvc             | host   |
| dest_host       | triggeredComponents{}.triggeredFilters{}.trigger.value (when triggeredComponents{}.triggeredFilters{}.filterType is 'Connection hostname')                                       |
| dest_ip         | triggeredComponents{}.triggeredFilters{}.trigger.value (when triggeredComponents{}.triggeredFilters{}.filterType is 'Destination IP')  |
| dest_port       | triggeredComponents{}.triggeredFilters{}.trigger.value (when triggeredComponents{}.triggeredFilters{}.filterType is 'Destination port')  |
| dest            | triggeredComponents{}.triggeredFilters{}.trigger.value (when triggeredComponents{}.triggeredFilters{}.filterType is 'Connection hostname' or 'Internal destination device name') |
| file_hash       | triggeredComponents{}.triggeredFilters{}.trigger.value (when triggeredComponents{}.triggeredFilters{}.filterType is 'MD5 file hash' or 'SHA1 file hash' or 'SHA256 file hash')   |
| id              | pbid   |
| vendor_severity | score >= 75 "Critical", 75 > score >= 50 "High", 50 > score >= 25 "Medium", score < 25 "Low"   |
| severity        | score >= 75 "Critical", 75 > score >= 50 "High", 50 > score >= 25 "Medium", score < 25 "Low"   |
| severity_id     | model.priority   |
| src             | device.hostname  |
| src_host        | device.hostname  |
| src_ip          | device.ip  |
| signature       | model.name   |
| subject         | model.name   |
| category        | model.name   |
| signature_id    | pbid   |

---

| CIM FIELD          | DARKTRACE MODEL BREACH JSON FIELD                                       |
|--------------------|---|
| body               | <code>model.description</code>  |
| description        | <code>model.description</code>  |
| url                | <code>breachUrl</code>  |
| tag=alert          | <i>Always applied</i>   |
| tag=attack         | <i>Always applied</i>   |
| tag=dlp & incident | <code>model.tags{} =AP: Egress</code>                                   |
| tag=malware        | <code>model.tags{} =“AP: Exploit” OR model.tags{}=“AP: C2 Comms”</code> |
| tag=authentication | <code>model.name =“User::*”</code>                                      |

## AI Analyst Incident Events

| CIM FIELD          | DARKTRACE AI ANALYST JSON FIELD                                 |
|--------------------|---|
| score              | aiaScore  |
| id                 | uuid  |
| vendor_severity    | score >= 90 "High", 90 > score >= 70 "Medium", score < 70 "Low" |
| severity           | score >= 90 "High", 90 > score >= 70 "Medium", score < 70 "Low" |
| src                | breachDevices{}.hostname  |
| src_host           | breachDevices{}.hostname  |
| src_ip             | breachDevices{}.ip  |
| signature          | title   |
| subject            | title   |
| category           | title   |
| signature_id       | summariser  |
| body               | summary   |
| description        | summary   |
| tag=alert          | <i>Always applied</i>   |
| tag=attack         | attackPhases{} =1   |
| tag=malware        | attackPhases{} =2   |
| tag=dlp & incident | attackPhases =6   |
| tag=authentication | attackPhases =3   |

## System Status Alerts

| CIM FIELD       | DARKTRACE SYSTEM STATUS JSON FIELD   |
|-----------------|--|
| vendor_severity | <code>priority &gt;= 80 "Critical", 80 &gt; priority &gt;= 60 "High", 60 &gt; priority &gt;= 40 "Medium", 40 &gt; priority &gt;= 20 "Low", priority &lt; 20 "Informational"</code> |
| severity        | <code>priority &gt;= 80 "Critical", 80 &gt; priority &gt;= 60 "High", 60 &gt; priority &gt;= 40 "Medium", 40 &gt; priority &gt;= 20 "Low", priority &lt; 20 "Informational"</code> |
| src             | <code>hostname</code>  |
| src_host        | <code>hostname</code>  |
| src_ip          | <code>ip_address</code>  |
| signature       | <code>alert_name</code>  |
| subject         | <code>alert_name</code>  |
| category        | <code>alert_name</code>  |
| signature_id    | <code>name</code>  |
| body            | <code>message</code>   |
| description     | <code>message</code>   |
| tag=alert       | <i>Always applied</i>  |

---

## **DARKTRACE SPLUNK ALERT JSON EXAMPLES**

The Darktrace Splunk integration utilizes a custom JSON output format for Model Breach, AI Analyst and System Status alerts. Each alert type can be enabled separately if desired.

Examples for each alert type are included below.



## Model Breaches

```

{
  "dest": "example.me",
  "model": {
    "name": "Device::Suspicious Domain",
    "pid": 330,
    "phid": 13733,
    "uuid": "80010119-6d7f-0000-0305-5e0000000294",
    "description": "A device is connecting to a rare external domain that is not commonly
visited within the network, with a TLD commonly associated with malicious activities.\\n\\
\nAction: Investigate the domain being visited and review the other connections being made
by the device around the breach time.",
    "priority": 0,
    "tags": [
      "AP: C2 Comms",
      "AP: Tooling"
    ]
  },
  "device": {
    "did": 5292,
    "quarantine": 1633971221000,
    "ip": "10.140.15.89",
    "ips": [
      {
        "ip": "10.140.15.89",
        "timems": 1633968000000,
        "time": "2021-10-11 16:00:00",
        "sid": 82
      }
    ],
    "sid": 82,
    "hostname": "workstation-local-82",
    "firstSeen": 1581426410000,
    "lastSeen": 1633971302000,
    "typename": "desktop",
    "typeLabel": "Desktop",
    "tags": [
      {
        "tid": 73,
        "expiry": 0,
        "thid": 78,
        "name": "Example Tag",
        "restricted": false,
        "data": {
          "auto": false,
          "color": 134,
          "description": "Example Tag",
          "visibility": "Public"
        }
      },
      "isReferenced": false
    ],
    ...
  ]
},
"triggeredComponents": [
  {
    "time": 1633971408000,
    "cbid": 10053187,
    "cid": 17413,
    "chid": 26905,
    "size": 1,
    "threshold": 0,
    "interval": 3600,
    "metric": {
      "mlid": 1,

```

continued...

```
    "name": "externalconnections",
    "label": "External Connections"
  },
  "triggeredFilters": [
    ...
    {
      "cfid": 160081,
      "id": "D",
      "filterType": "Connection hostname",
      "arguments": {
        "value": "^(?:.*\\.)?[\\w-]{4,}\\.[\\w]+$"
      },
      "comparatorType": "matches regular expression",
      "trigger": {
        "value": "example.me"
      }
    },
    {
      "cfid": 160087,
      "id": "J",
      "filterType": "Destination port",
      "arguments": {
        "value": 25
      },
      "comparatorType": "!=",
      "trigger": {
        "value": "80"
      }
    }
  ],
  ...
]
},
"breachUrl": "https://example-darktrace-instance.com/#modelbreach/1234",
"pbid": 1234,
"score": 0.284,
"commentCount": 0,
"creationTime": 1633971412000,
"time": 1633971409000
}
```

*Example is abbreviated*

## AI Analyst Incident Events

```

{
  "summariser": "SaasHijackSummary",
  "acknowledged": false,
  "pinned": false,
  "attackPhases": [
    3
  ],
  "title": "Possible Hijack of GSuite Account",
  "id": "58d0434a-5c38-42e2-b9ae-b479cb2ee53b",
  "children": [
    "58d0434a-5c38-42e2-b9ae-b479cb2ee53b"
  ],
  "category": "critical",
  "currentGroup": "g233a28e2-ed9f-4004-a70f-cdee45539742",
  "groupCategory": "critical",
  "groupScore": 89.97840255597085,
  "groupPreviousGroups": [],
  "activityId": "da39a3ee",
  "groupingIds": [
    "74b53963"
  ],
  "groupByActivity": false,
  "userTriggered": false,
  "externalTriggered": false,
  "aiaScore": 68,
  "summary": "The SaaS actor sofia.martinez@holdingsinc.com was observed making suspicious requests over a configured GSuite service from the IP 172.217.169.36...",
  "periods": [
    {
      "start": 1634506746000,
      "end": 1634506948000
    }
  ],
  "breachDevices": [
    {
      "identifier": "SaaS::GSuite: sofia.martinez@holdingsinc.com",
      "hostname": "SaaS::GSuite: sofia.martinez@holdingsinc.com",
      "ip": null,
      "mac": null,
      "subnet": null,
      "did": 16592,
      "sid": -9
    }
  ],
  "relatedBreaches": [
    {
      "modelName": "SaaS / Admin / Global Administrator Added",
      "pbid": 8960106,
      "threatScore": 59,
      "timestamp": 1634506915000
    }
  ],
  "details": [
    [
      {
        "header": "SaaS User Details",
        "contents": [
          {
            "key": "SaaS account",
            "type": "device",
            "values": [
              {

```

continued...

```
        "identifier": "SaaS::GSuite: sofia.martinez@holdingsinc.com",
        "hostname": "SaaS::GSuite: sofia.martinez@holdingsinc.com",
        "ip": null,
        "mac": null,
        "subnet": null,
        "did": 16592,
        "sid": -9
    }
  ]
},
{
  "key": "Actor",
  "type": "string",
  "values": [
    "sofia.martinez@holdingsinc.com"
  ]
}
]
},
[
  {
    "header": "Agent Carrying out Suspicious Activity",
    "contents": [
      {
        "key": "Source IP",
        "type": "externalHost",
        "values": [
          {
            "hostname": "93.93.133.164",
            "ip": "93.93.133.164"
          }
        ]
      },
      {
        "key": "ASN",
        "type": "string",
        "values": [
          "AS44684 Mythic Beasts Ltd"
        ]
      },
      {
        "key": "Country",
        "type": "string",
        "values": [
          "United Kingdom"
        ]
      }
    ]
  },
  {
    "header": "Summary of Activity",
    "contents": [
      {
        "key": "Time",
        "type": "timestampRange",
        "values": [
          {
            "start": 1634506746000,
            "end": 1634506948000
          }
        ]
      }
    ]
  },
],
```

continued...

```
    {
      "key": "Suspicious properties",
      "type": "string",
      "values": [
        "Unusual time for activity",
        "Configuration changes made"
      ]
    }
  ]
},
{
  "header": "Activity Details",
  "contents": [
    {
      "key": "Event",
      "type": "string",
      "values": [
        "Authorize"
      ]
    },
    {
      "key": "Number of events",
      "type": "integer",
      "values": [
        1
      ]
    },
    {
      "key": "Resource name",
      "type": "string",
      "values": [
        "Google Chrome"
      ]
    },
    {
      "key": "Event",
      "type": "string",
      "values": [
        "ChangeLastName"
      ]
    },
    {
      "key": "Number of events",
      "type": "integer",
      "values": [
        1
      ]
    },
    {
      "key": "Destination resource name",
      "type": "string",
      "values": [
        "birch3"
      ]
    },
    {
      "key": "Resource name",
      "type": "string",
      "values": [
        "sofia.martinez@holdingsinc.com"
      ]
    }
  ]
}
```

continued...

```
    "key": "Event",
    "type": "string",
    "values": [
      "PasswordEdit"
    ]
  },
  {
    "key": "Number of events",
    "type": "integer",
    "values": [
      1
    ]
  }
]
}
],
"url": "https://example-darktrace-instance.com/saas#aiincident/58d0434a-5c38-42e2-b9ae-
b479cb2ee53b"
}
```

## System Status Alerts

```
{
  "hostname": "dt-1234-01",
  "ip_address": "10.12.14.2",
  "child_id": null,
  "name": "high-unidirectional-traffic-10-0-18-0/24",
  "priority": 53,
  "priority_level": "medium",
  "alert_name": "High Unidirectional Traffic",
  "status": "Active",
  "message": "Unidirectional Traffic on subnet 10.0.18.0/24 is high (65.0%). This means that
Darktrace may experience issues tracking devices on your network.\n\nIf you have any issues,
please open a ticket using the following link. https://customerportal.darktrace.com/ticket/
create",
  "last_updated": 1634720568.856285,
  "last_updated_status": 1634720568.856285,
  "acknowledge_timeout": null,
  "uuid": "2be53c13-16c2-4c0f-99c0-15b714a05503",
  "url": "https://example-darktrace-instance.com/sysstatus?
alert=2be53c13-16c2-4c0f-99c0-15b714a05503"
}
```

