Generating ServiceNow Incidents with Forcepoint ONE

Forcepoint

Table of Contents

Overview

While Forcepoint ONE has impressive logging and analysis capabilities, it is often necessary to make use of external tools such as Security Information and Event Management (SIEM) external logging systems and Ticket Management Systems (TMS). This guide covers the latter case, in which we will use Proxy and API events and/or alert conditions detected by Forcepoint ONE to create incident cases within ServiceNow, a very popular cloud-based TMS.

Methodology

Generally, there are two methods by which Forcepoint ONE can provide event data to external systems:

1. By pulling logs via our REST API log export capabilities
2. By sending emails to external systems, using the Forcepoint ONE Group Email Notification feature, which can be applied to Proxy and API policies within Forcepoint ONE

In either case, the result will be that Proxy/API events detected by Forcepoint ONE will generate new incidents within ServiceNow. A discussion follows on both methodologies, but this guide will focus on the email method as an example.

REST API Log Export
The first method results in a fully externalized solution, as we are just providing raw logs to an authenticated external host that pulls them via API. ServiceNow can support this capability directly in its support of “Outbound REST Web Service.” ServiceNow would periodically poll our API (by incrementally adjusting the “startdate” query parameter and inclusion of the “nextpagetoken”) and parse any resulting responses into new incidents.

The benefit of using this method is in its responsiveness, as the email-based systems may incur transport-related delays, as well as the fact that log information is delivered in JSON or CSV format, which may be easier for ServiceNow to parse than an email body.

Email
In the second method, Forcepoint ONE sends emails to ServiceNow using either ServiceNow’s **Flow Manager** > **Inbound Email Flows** or **System Policy** > **Email** > **Inbound Actions** to process received emails and parse them into new incidents. The Forcepoint ONE administrator would need to:

- Create a local user within a Forcepoint ONE supported tenant domain, and define its email address to that of the ServiceNow provided email address
- Add that user to a group defined on Forcepoint ONE
- Create a Group Email Notification with the information needed by a new ServiceNow incident and add the appropriate group to it
- Apply the Group Email Notification to Proxy or API policy actions within Forcepoint ONE applications

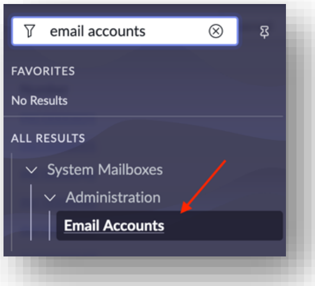
Specifications

In this example, we will be configuring a ServiceNow developer account to receive Group Notification emails and parse them using **System Policy** > **Email** > **Inbound Actions** to create new incident tickets within ServiceNow.

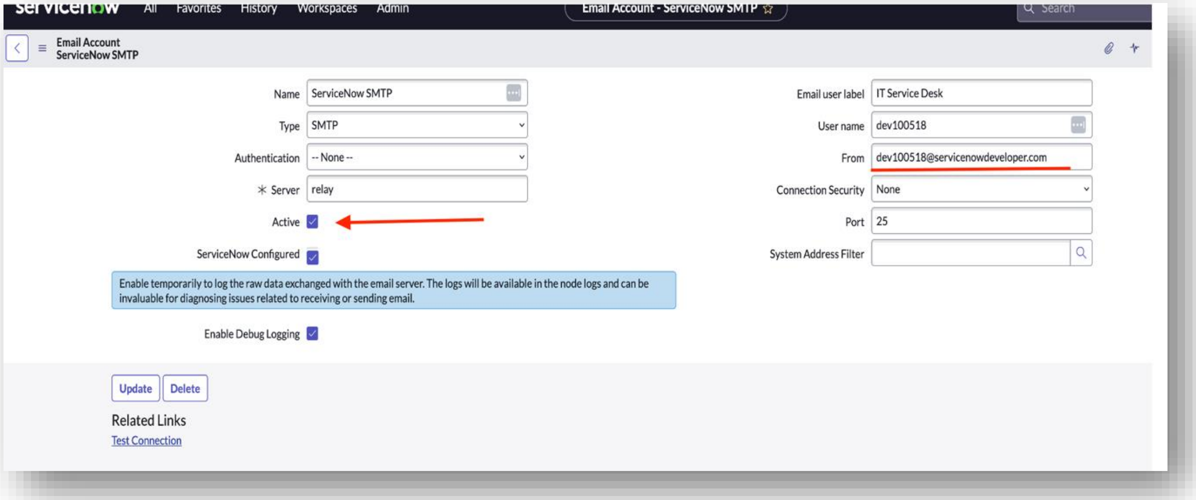
ServiceNow Configuration

The steps involved for the ServiceNow configuration are as follows:

1. Set the ServiceNow SMTP service to active (it is not active by default)
   a) Go to **All** and in the search box type "Email Accounts"



   b) Click **New**
   c) Check the **Active** checkbox
   d) Copy the "from" email address as this is the email address Forcepoint ONE will send group notifications to

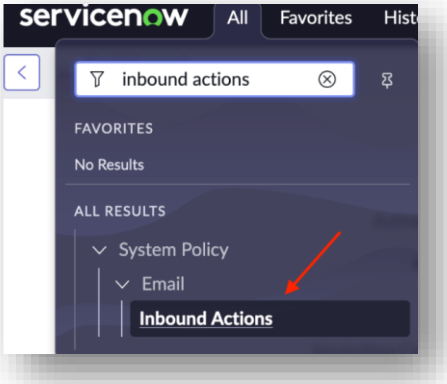


Name	ServiceNow SMTP	Email user label	IT Service Desk
Type	SMTP	User name	dev100518
Authentication	-- None --	From	dev100518@servicenowdeveloper.com
* Server	relay	Connection Security	None
Active	☑	Port	25
ServiceNow Configured	☑	System Address Filter	

Enable temporarily to log the raw data exchanged with the email server. The logs will be available in the node logs and can be invaluable for diagnosing issues related to receiving or sending email.

Enable Debug Logging ☑

2. Configure ServiceNow to parse inbound email messages from Forcepoint ONE to create new incident tickets; go to **All** in the search box and type “Inbound Actions” and create a new action



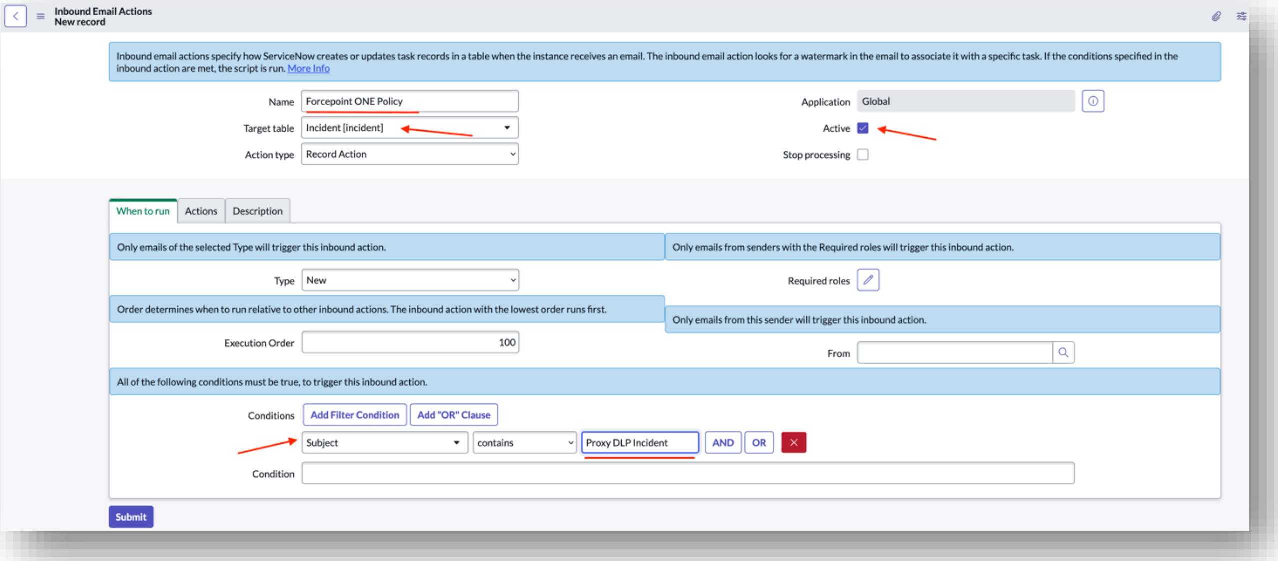
a) Give it a Name – this example uses “Create Incident - Forcepoint ONE Policy”

b) Set the **Target** table to “Incident (Incident)”

c) Check the **Active** checkbox

d) Configure the **Conditions** to match emails sent by Forcepoint ONE – this example uses the email “Subject” and matches if it is a “Proxy DLP Incident”

- Note this email subject must match the Global Notification subject field configured in Forcepoint ONE



Inbound Email Actions
New record

Inbound email actions specify how ServiceNow creates or updates task records in a table when the instance receives an email. The inbound email action looks for a watermark in the email to associate it with a specific task. If the conditions specified in the inbound action are met, the script is run. More Info

Name: Forcepoint ONE Policy
Target table: Incident [incident]
Action type: Record Action
Application: Global
Active: ☑
Stop processing: □

Only emails of the selected Type will trigger this inbound action.

Type: New

Only emails from senders with the Required roles will trigger this inbound action.

Required roles

Order determines when to run relative to other inbound actions. The inbound action with the lowest order runs first.

Execution Order: 100

Only emails from this sender will trigger this inbound action.

From

All of the following conditions must be true, to trigger this inbound action.

Conditions: Add Filter Condition | Add "OR" Clause

Subject | contains | Proxy DLP Incident | AND | OR

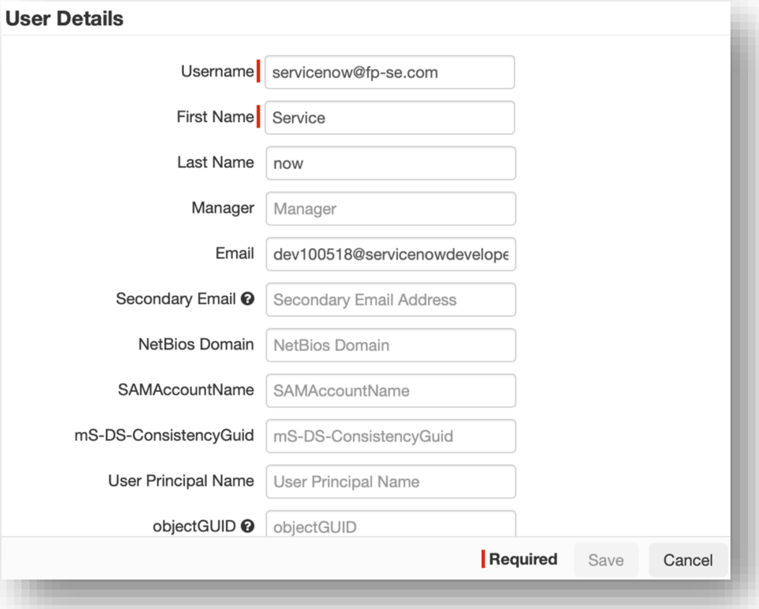
Condition

Received emails matching this inbound action policy will create a new ServiceNow Incident ticket.

Forcepoint ONE Configuration

Note that this section will use the author's trial Tenant "fp-se.com" within examples and illustrations. The steps involved in the Forcepoint ONE configuration are as follows:

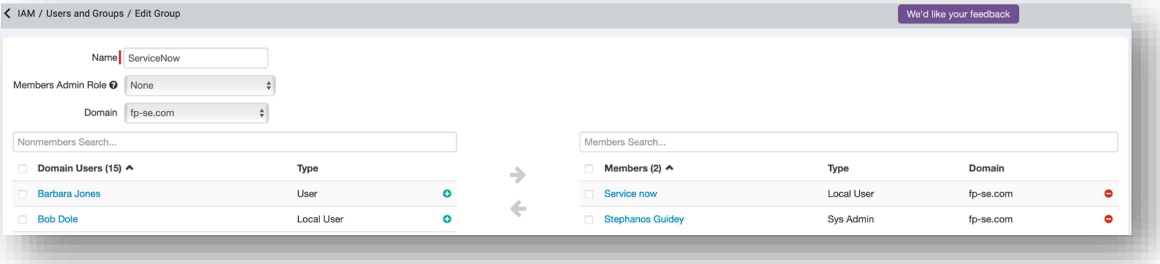
1. Go to **IAM** > **Users and Groups** and create a new local User for use by the ServiceNow email address
   a) In this example, the User "servicenow@fp-se.com" was created to support the "dev100518@servicenowdevelopers.com" email address



User Details

Username	servicenow@fp-se.com
First Name	Service
Last Name	now
Manager	Manager
Email	dev100518@servicenowdevelope
Secondary Email	Secondary Email Address
NetBios Domain	NetBios Domain
SAMAccountName	SAMAccountName
mS-DS-ConsistencyGuid	mS-DS-ConsistencyGuid
User Principal Name	User Principal Name
objectGUID	objectGUID

2. Add a new group and add the new user to this group. This new group will be used when creating Group Notification
   a) In this example, the group "ServiceNow" was created and the "servicenow@curveballnetworks.com" user was added to it



Name	ServiceNow
Members Admin Role	None
Domain	fp-se.com

Domain Users (15)	Type
Barbara Jones	User
Bob Dole	Local User

Members (2)	Type	Domain
Service now	Local User	fp-se.com
Stephanos Guidey	Sys Admin	fp-se.com

3. **Go to Protect** > **Notifications** > **Group Emails** and press **New Group Email**
   a) Add a **Notification Name.** In this example "Proxy DLP Incident" is used
   b) Under **Mail to** Groups, add the new group you previously created. In this example it's "ServiceNow"
   c) Add a value for **From Name**. In this example "Forcepoint ONE Admin" is used

d) Configure the **Email Subject** to match the value that the ServiceNow **System All** > **Inbound Actions** rule you create will match on for creating a new incident ticket. In this example the value is “Policy DLP Incident”

e) Configure an appropriate **Email Body**. In this example we use the following:

Forcepoint ONE has detected a proxy DLP violation, with the following details:

Transaction ID: [TRANSACTION_ID]

Timestamp: [TIMESTAMP]

Username: [EMAIL_ADDRESS] ([FIRST_NAME] [LAST_NAME])

Location: [LOCATION]

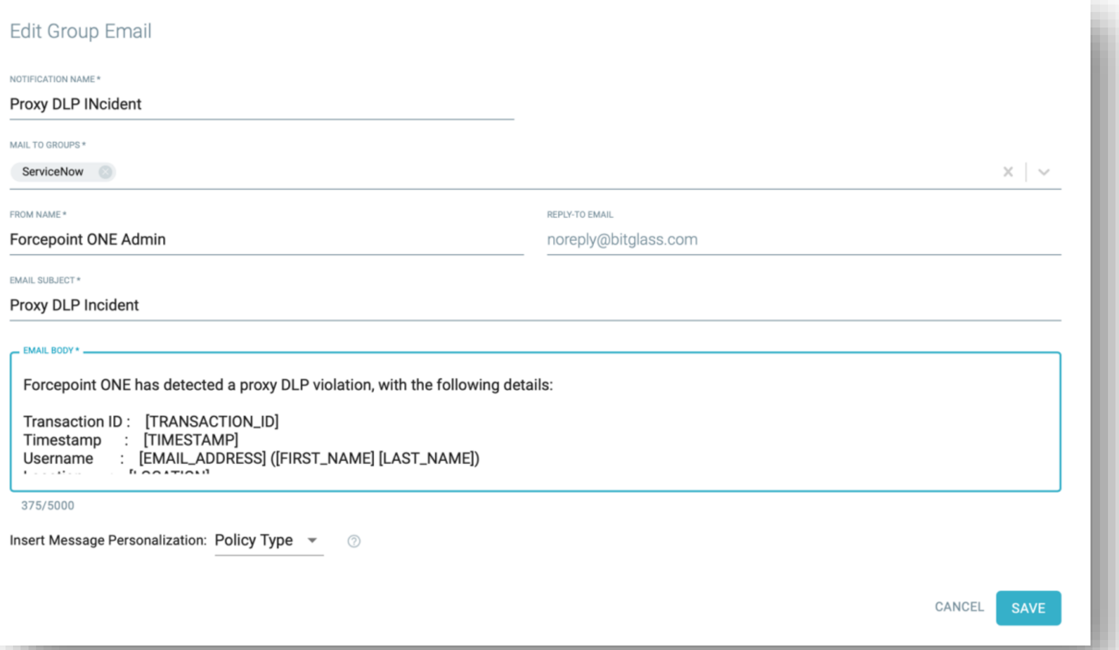
IP Address: [IP_ADDRESS]

Application: [APPLICATION]

File Name: [FILE_NAME]

Direction: [DIRECTION]

f) Note that this body makes use of variables provided by Forcepoint ONE and can be adjusted to suit ServiceNow parsing rules



Edit Group Email

NOTIFICATION NAME *
Proxy DLP INcident

MAIL TO GROUPS *
ServiceNow

FROM NAME *
Forcepoint ONE Admin

REPLY-TO EMAIL
noreply@bitglass.com

EMAIL SUBJECT *
Proxy DLP Incident

EMAIL BODY *

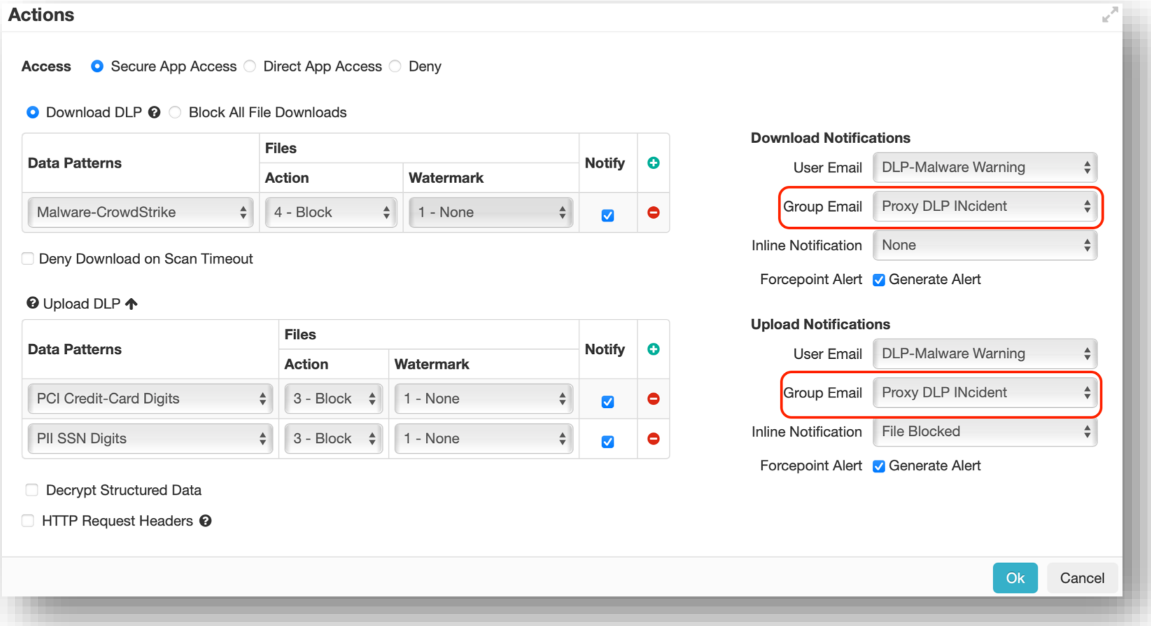
Forcepoint ONE has detected a proxy DLP violation, with the following details:

Transaction ID : [TRANSACTION_ID]
Timestamp : [TIMESTAMP]
Username : [EMAIL_ADDRESS] ([FIRST_NAME] [LAST_NAME])

375/5000

Insert Message Personalization: Policy Type

4. Go to **Protect** > **Policies** and add the new Group Email Notification to application policies as needed
   a) For Proxy policies the Group Email Notification is added to the policy action:



Actions

Access ● Secure App Access ○ Direct App Access ○ Deny

● Download DLP ○ Block All File Downloads

Data Patterns	Files		Notify
	Action	Watermark	
Malware-CrowdStrike	4 - Block	1 - None	☑

□ Deny Download on Scan Timeout

Upload DLP

Data Patterns	Files		Notify
	Action	Watermark	
PCI Credit-Card Digits	3 - Block	1 - None	☑
PII SSN Digits	3 - Block	1 - None	☑

□ Decrypt Structured Data

□ HTTP Request Headers

Download Notifications

User Email	DLP-Malware Warning
Group Email	Proxy DLP INcident
Inline Notification	None
Forcepoint Alert	☑ Generate Alert

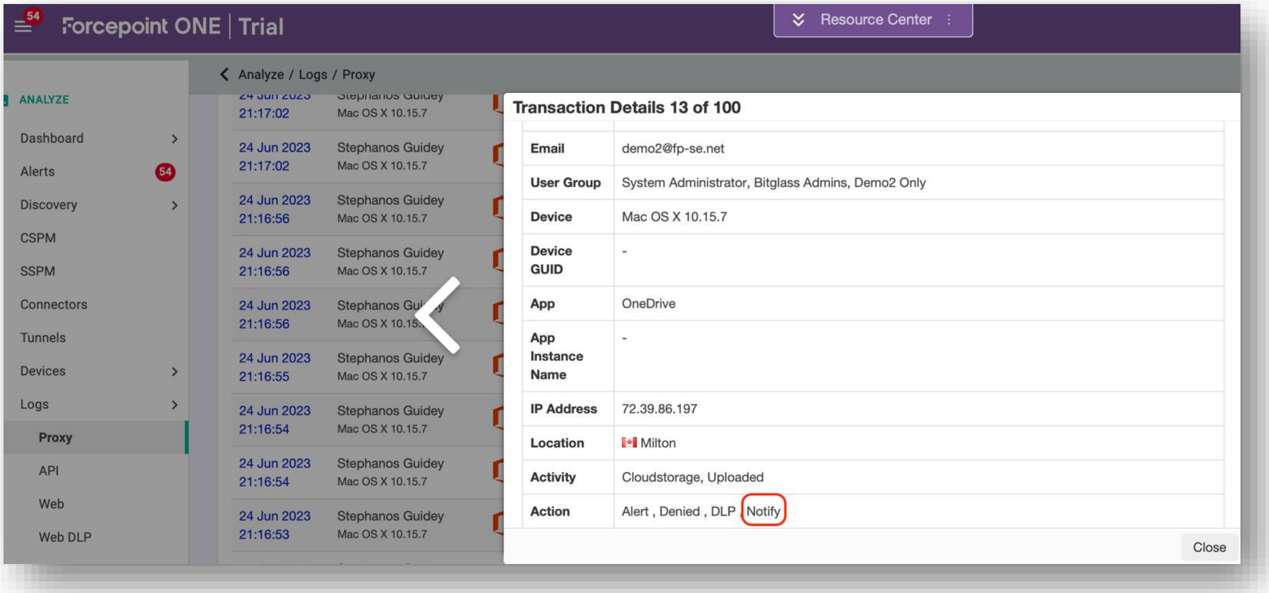
Upload Notifications

User Email	DLP-Malware Warning
Group Email	Proxy DLP INcident
Inline Notification	File Blocked
Forcepoint Alert	☑ Generate Alert

At this point DLP events detected by Forcepoint ONE will issue a Group Email Notification email to the ServiceNow email address, which will in turn be processed by ServiceNow to create new Incident tickets.

Solution At Work

To verify the solution, generate a DLP event that will trigger a Group Email Notification from Forcepoint ONE. Check the log at **Analyze** > **Logs** > **Proxy/API** to ensure the event generated a notification.

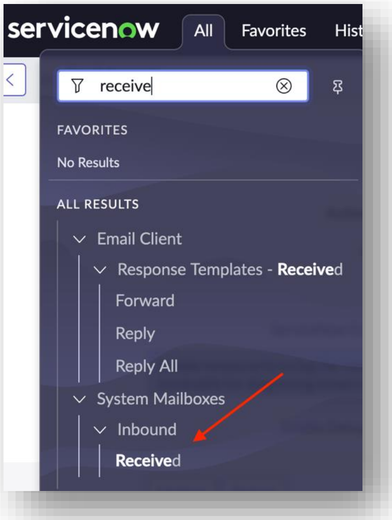


24 Jun 2023 21:17:02 Stephanos Guidey Mac OS X 10.15.7
24 Jun 2023 21:17:02 Stephanos Guidey Mac OS X 10.15.7
24 Jun 2023 21:16:56 Stephanos Guidey Mac OS X 10.15.7
24 Jun 2023 21:16:56 Stephanos Guidey Mac OS X 10.15.7
24 Jun 2023 21:16:56 Stephanos Guidey Mac OS X 10.15.7
24 Jun 2023 21:16:55 Stephanos Guidey Mac OS X 10.15.7
24 Jun 2023 21:16:54 Stephanos Guidey Mac OS X 10.15.7
24 Jun 2023 21:16:54 Stephanos Guidey Mac OS X 10.15.7
24 Jun 2023 21:16:53 Stephanos Guidey Mac OS X 10.15.7

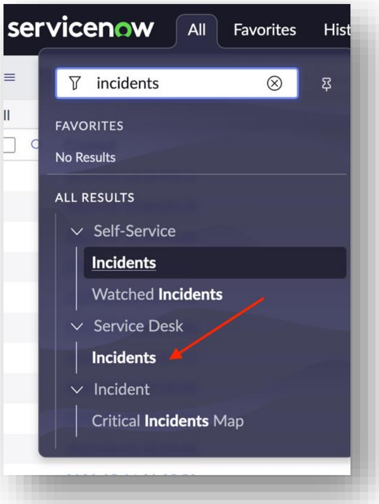
Transaction Details 13 of 100

Email	demo2@fp-se.net
User Group	System Administrator, Bitglass Admins, Demo2 Only
Device	Mac OS X 10.15.7
Device GUID	-
App	OneDrive
App Instance Name	-
IP Address	72.39.86.197
Location	Milton
Activity	Cloudstorage, Uploaded
Action	Alert , Denied , DLP Notify

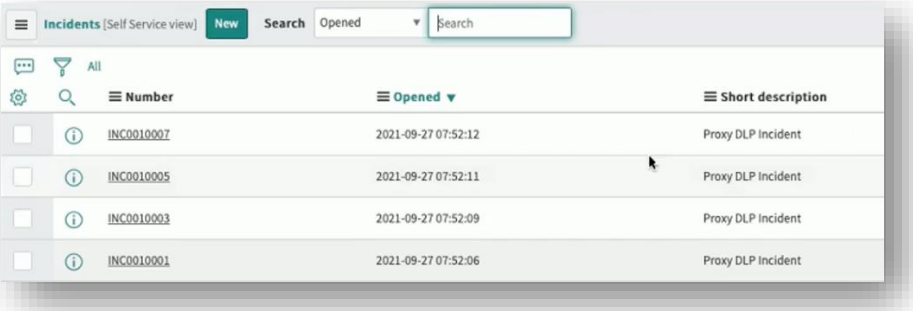
In ServiceNow, the received email will appear in **System Mailboxes** > **Inbound** > **Received**. Select the email and look at the Email Log tab near the bottom of the page.



It will indicate that the “Create Incident – Forcepoint ONE Policy” rule was processed and it created a new incident. In SerivceNow go to “Incident.” You will find a new incident created here.



Please note that the screenshot provided below might differ from the current interface, as they are based on a previous version of ServiceNow.



Number	Opened ▼	Short description
INC0010007	2021-09-27 07:52:12	Proxy DLP Incident
INC0010005	2021-09-27 07:52:11	Proxy DLP Incident
INC0010003	2021-09-27 07:52:09	Proxy DLP Incident
INC0010001	2021-09-27 07:52:06	Proxy DLP Incident

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.