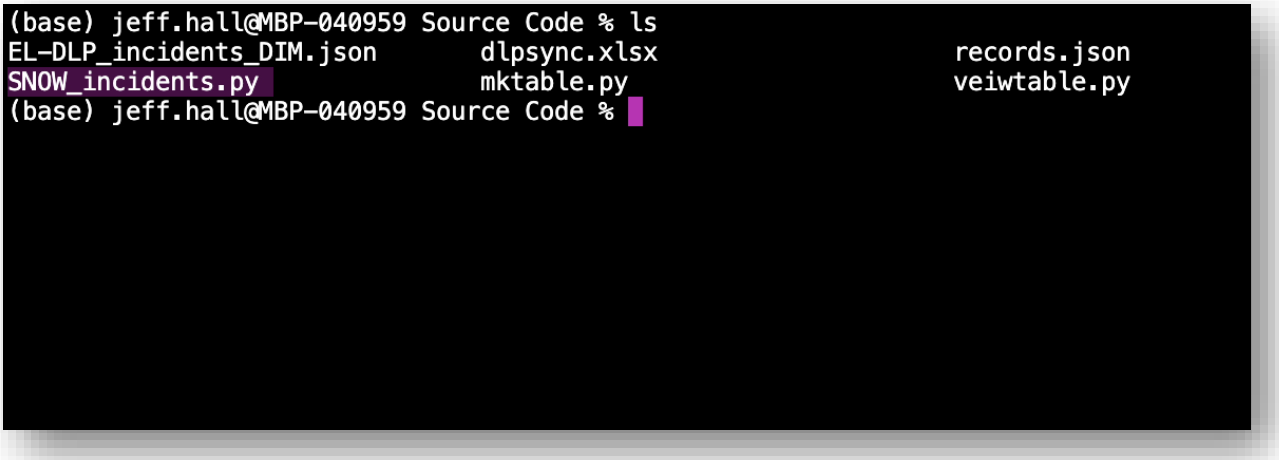
Forcepoint DLP API and Service Now Demo Script

Forcepoint

forcepoint.com

Forcepoint DLP API and ServiceNow Demo Script

1. Run the integreation script by going to the directory that contains the Pyhin script.



```
(base) jeff.hall@MBP-040959 Source Code % ls
EL-DLP_incidents_DIM.json       dlpsync.xlsx                        records.json
SNOW_incidents.py               mktable.py                          veiwtable.py
(base) jeff.hall@MBP-040959 Source Code % 
```

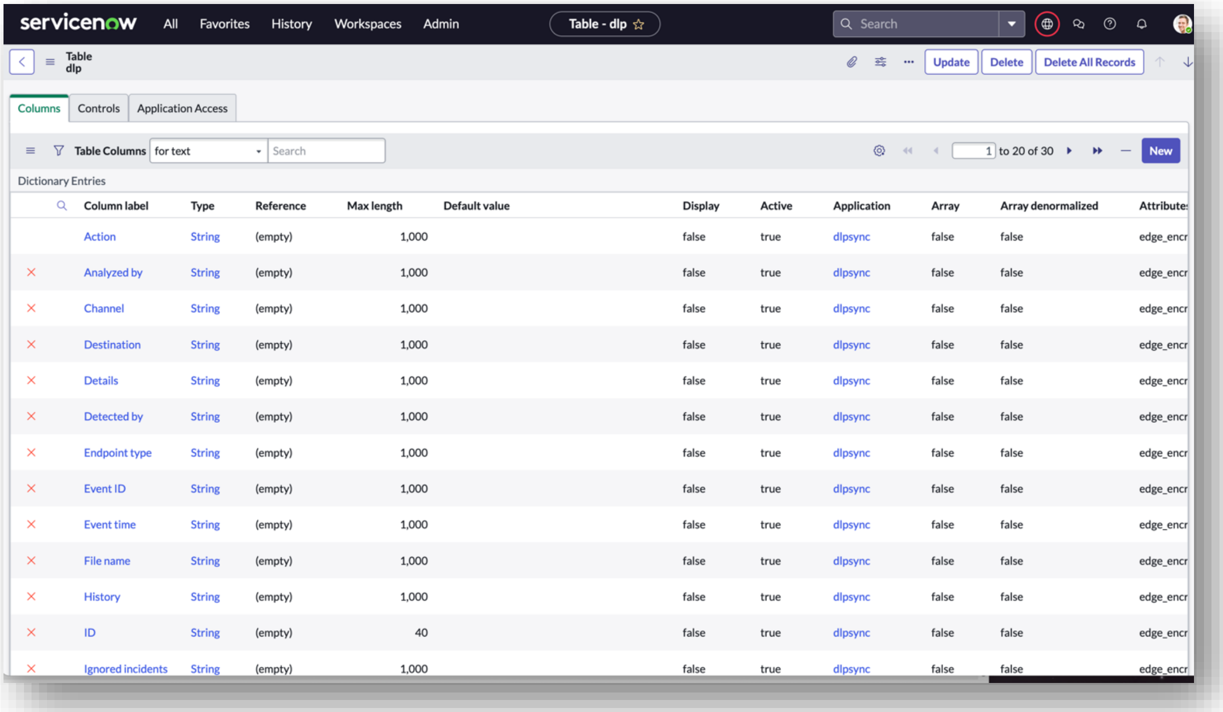
2. Modify the payload portion of the script to retrieve the data from the FSM that you want to send to ServiceNow.
    - payload = json.dumps({
    - type: INCIDENT
    - from_date: 08/06/2023 18:55:00
    - to_date: 10/06/2023 18:55:00
    - })
    - Refer to Forcepoint DLP REST API Guide for full syntax and required fields

3. Modify the ServiceNow section of the script to connect to your ServiceNow tenet.
    - Add ServiceNow details
    - service_now_instance = https://dev68380.service-now.com
    - service_now_user = admin
    - service_now_pass = '=CA9gk-2Vz/Nw'=
    - def create_service_now_incident(incident):
    - # Define the incident data
    - data = json.dumps({
    - short_description: DLP Incident + str(incident[id])
    - description: DLP Incident Details: + json.dumps(incident)
    - # add more fields as necessary
    - })

- # Send a POST request to the ServiceNow incidents API
- response = requests.post
- service_now_instance + /api/now/table/x_579165_dlpsync_dlp
- auth=(service_now_user, service_now_pass)
- headers={Content-Type: application/text}

4. Ensure that you have a ServiceNow table created with the following columns.

- id: integer
- severity: string
- action: string
- status: string
- login_name: string
- host_name: string
- task_name: string
- admin_name: string
- update_time: integer
- event_id: integer
- maximum_matches: integer
- transaction_size: integer
- analyzed_by: string
- ignored_incidents: boolean
- event_time: string
- incident_time: string
- channel: string
- policies: string
- partition_index: integer
- destination: string
- detected_by: string
- details: string
- released_incident: boolean
- endpoint_type: string
- classifier_name: string
- number_matches: integer
- policy_name: string
- rule_name: string

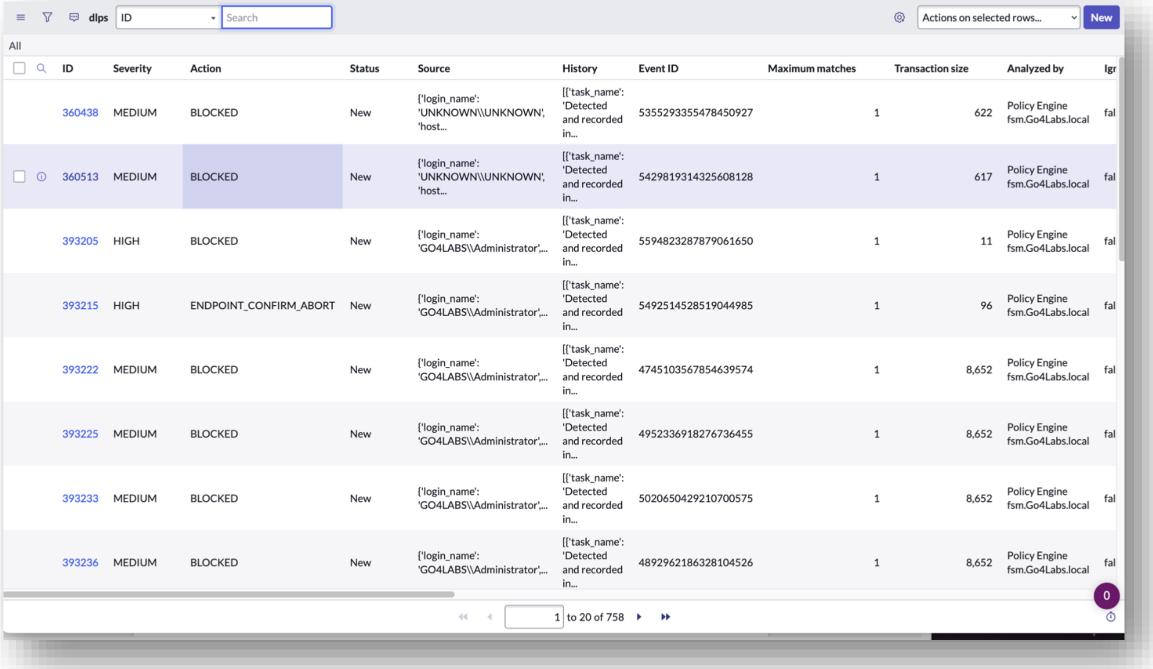


Dictionary Entries

	Column label	Type	Reference	Max length	Default value	Display	Active	Application	Array	Array denormalized	Attribute:
	Action	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	Analyzed by	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	Channel	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	Destination	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	Details	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	Detected by	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	Endpoint type	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	Event ID	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	Event time	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	File name	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	History	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr
×	ID	String	(empty)	40		false	true	dlpsync	false	false	edge_encr
×	Ignored incidents	String	(empty)	1,000		false	true	dlpsync	false	false	edge_encr

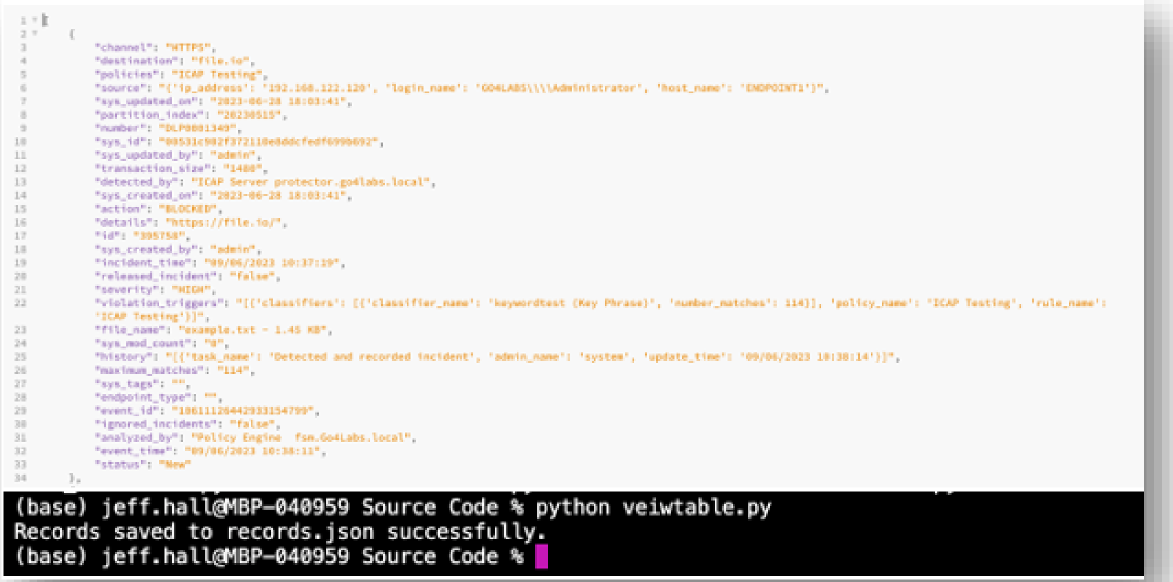
5. Once the script has been modified with the correct connection information, execute the script {python SNOW_incidents.py}

6. Once the script is finished, verify that the data has loaded to ServiceNow.



ID	Severity	Action	Status	Source	History	Event ID	Maximum matches	Transaction size	Analyzed by	Igr
360438	MEDIUM	BLOCKED	New	{'login_name': 'UNKNOWN\\UNKNOWN', 'host...	[{'task_name': 'Detected and recorded in...	5355293355478450927	1	622	Policy Engine fsm.Go4Labs.local	fal
360513	MEDIUM	BLOCKED	New	{'login_name': 'UNKNOWN\\UNKNOWN', 'host...	[{'task_name': 'Detected and recorded in...	5429819314325608128	1	617	Policy Engine fsm.Go4Labs.local	fal
393205	HIGH	BLOCKED	New	{'login_name': 'GO4LABS\\Administrator',...	[{'task_name': 'Detected and recorded in...	5594823287879061650	1	11	Policy Engine fsm.Go4Labs.local	fal
393215	HIGH	ENDPOINT_CONFIRM_ABORT	New	{'login_name': 'GO4LABS\\Administrator',...	[{'task_name': 'Detected and recorded in...	5492514528519044985	1	96	Policy Engine fsm.Go4Labs.local	fal
393222	MEDIUM	BLOCKED	New	{'login_name': 'GO4LABS\\Administrator',...	[{'task_name': 'Detected and recorded in...	4745103567854639574	1	8,652	Policy Engine fsm.Go4Labs.local	fal
393225	MEDIUM	BLOCKED	New	{'login_name': 'GO4LABS\\Administrator',...	[{'task_name': 'Detected and recorded in...	4952336918276736455	1	8,652	Policy Engine fsm.Go4Labs.local	fal
393233	MEDIUM	BLOCKED	New	{'login_name': 'GO4LABS\\Administrator',...	[{'task_name': 'Detected and recorded in...	5020650429210700575	1	8,652	Policy Engine fsm.Go4Labs.local	fal
393236	MEDIUM	BLOCKED	New	{'login_name': 'GO4LABS\\Administrator',...	[{'task_name': 'Detected and recorded in...	4892962186328104526	1	8,652	Policy Engine fsm.Go4Labs.local	fal

7. As a secondary validation you can execute the viewtable.py script to generate a json file to view the contents of the ServiceNow table.



```
[
    {
        "channel": "HTTPS",
        "destination": "file.io",
        "policies": "ICAP Testing",
        "source": "{'ip_address': '192.168.122.120', 'login_name': 'GO4LABS\\\\Administrator', 'host_name': 'ENDPOINT1'}",
        "sys_updated_on": "2023-06-28 18:03:41",
        "partition_index": "20230515",
        "number": "DLP0001349",
        "sys_id": "09531c902f372110e8ddcfedf6996692",
        "sys_updated_by": "admin",
        "transaction_size": "1480",
        "detected_by": "ICAP Server protector.go4labs.local",
        "sys_created_on": "2023-06-28 18:03:41",
        "action": "BLOCKED",
        "details": "https://file.io/",
        "id": "395758",
        "sys_created_by": "admin",
        "incident_time": "09/06/2023 10:37:19",
        "released_incident": "false",
        "severity": "HIGH",
        "violation_triggers": "[{'classifiers': [{'classifier_name': 'keywordtest (Key Phrase)', 'number_matches': 114}], 'policy_name': 'ICAP Testing', 'rule_name':
        'ICAP Testing'}]",
        "file_name": "example.txt - 1.45 KB",
        "sys_mod_count": "0",
        "history": "[{'task_name': 'Detected and recorded incident', 'admin_name': 'system', 'update_time': '09/06/2023 10:38:14'}]",
        "maximum_matches": "114",
        "sys_tags": "",
        "endpoint_type": "",
        "event_id": "1861112844293315479",
        "ignored_incidents": "false",
        "analyzed_by": "Policy Engine  fsm.Go4Labs.local",
        "event_time": "09/06/2023 10:38:11",
        "status": "New"
    },
```

```
(base) jeff.hall@MBP-040959 Source Code % python veiwtable.py
Records saved to records.json successfully.
(base) jeff.hall@MBP-040959 Source Code %
```

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.

[FP DLP API and SerivceNow Demo Script] 01Nov2023