

# ServiceNow Incident Creation Script

## Usage

This script is made to be used with Flowmon ADS version 10 and above. It can create an incident by ServiceNow REST API. The documentation of [Table API](#) is available online and we are using primarily to create the incident with filled in details from ADS event.

This script requires three informations. Server URL/IP address, and user name and password of someone who can create incidents. Those informations could be prefiled to the script itself

```

8  DEBUG=1
9  # IP/hostname of ServiceNow server
10 IP='dev121928.service-now.com'
11 API_USER='admin'
12 API_PASS='K4/t1FbuM$eL'
13 # ServiceNow endpoint
14 SNI="https://$IP/api/now/table/incident"

```

Or you can just use those three information as parametres for the script

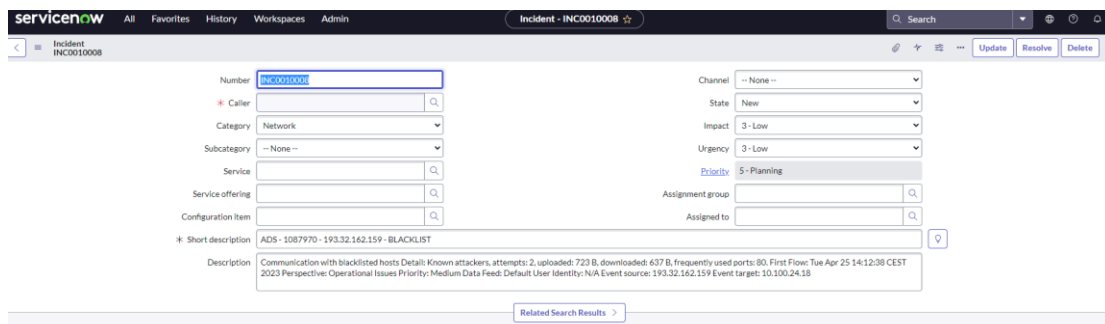
Script is using now a basic authentication as this is enough for this use case.

usage: sn-incident.sh <options>

Optional:

- srv IP / hostname of ServiceNow server
- user Username to be used for authentication
- pass Password for the user from the above

Once the script is run it would create an incident in ServiceNow instance which would look like



The screenshot shows the ServiceNow Incident form for Incident INC0010008. The form includes fields for Number (INC0010008), Caller, Category (Network), Subcategory, Service, Service offering, Configuration item, Channel (None), State (New), Impact (3 - Low), Urgency (3 - Low), Priority (5 - Planning), Assignment group, and Assigned to. The Short description is 'ADS - 1087970 - 193.32.162.159 - BLACKLIST'. The Description is 'Communication with blacklisted hosts Detail: Known attackers, attempts: 2, uploaded: 723 B, downloaded: 637 B, frequently used ports: 80, First Flow: Tue Apr 25 14:12:38 CEST 2023 Perspective: Operational Issues Priority: Medium Data Feed: Default User Identity: N/A Event source: 193.32.162.159 Event target: 10.106.24.18'.

Feel free to modify the data passed to your liking or set up various information in the ticket. This can be easily made if you use REST API Explorer. More details could be found also at this [external blog](#).

Details how to configure a custom script are at User Guide section [2.3.18](#)

## Details

I have used for the testing of this script [Non-production developer instance](#) offered by ServiceNow on release Tokyo. It's using the default username but of course it's recommended to have a separate user and probably use a different authentication mechanism but my aim here wasn't to learn how to configure and use ServiceNow. I wanted to provide a simple example script which can be used to create incidents in ServiceNow.