Progress

Flowmon ADS integration with ProLion CryptoSpike

Description of steps required to integrate Flowmon Anomaly Detection System (ADS) with ProLion CryptoSpike to identify and report threat actor movements on your network.

Introduction

Integrating Flowmon's network anomaly detection capabilities with ProLion CryptoSpike solution can promote early warning, detection, and remediation of various security issues.

Document Purpose

This document provides recommended settings used when integrating Flowmon ADS (Anomaly Detection System) and ProLion CryptoSpike.

Intended Audience

Anyone interested in leveraging Flowmon ADS to block storage users by ProLion CryptoSpike functionality.

Configure Progress Flowmon ADS

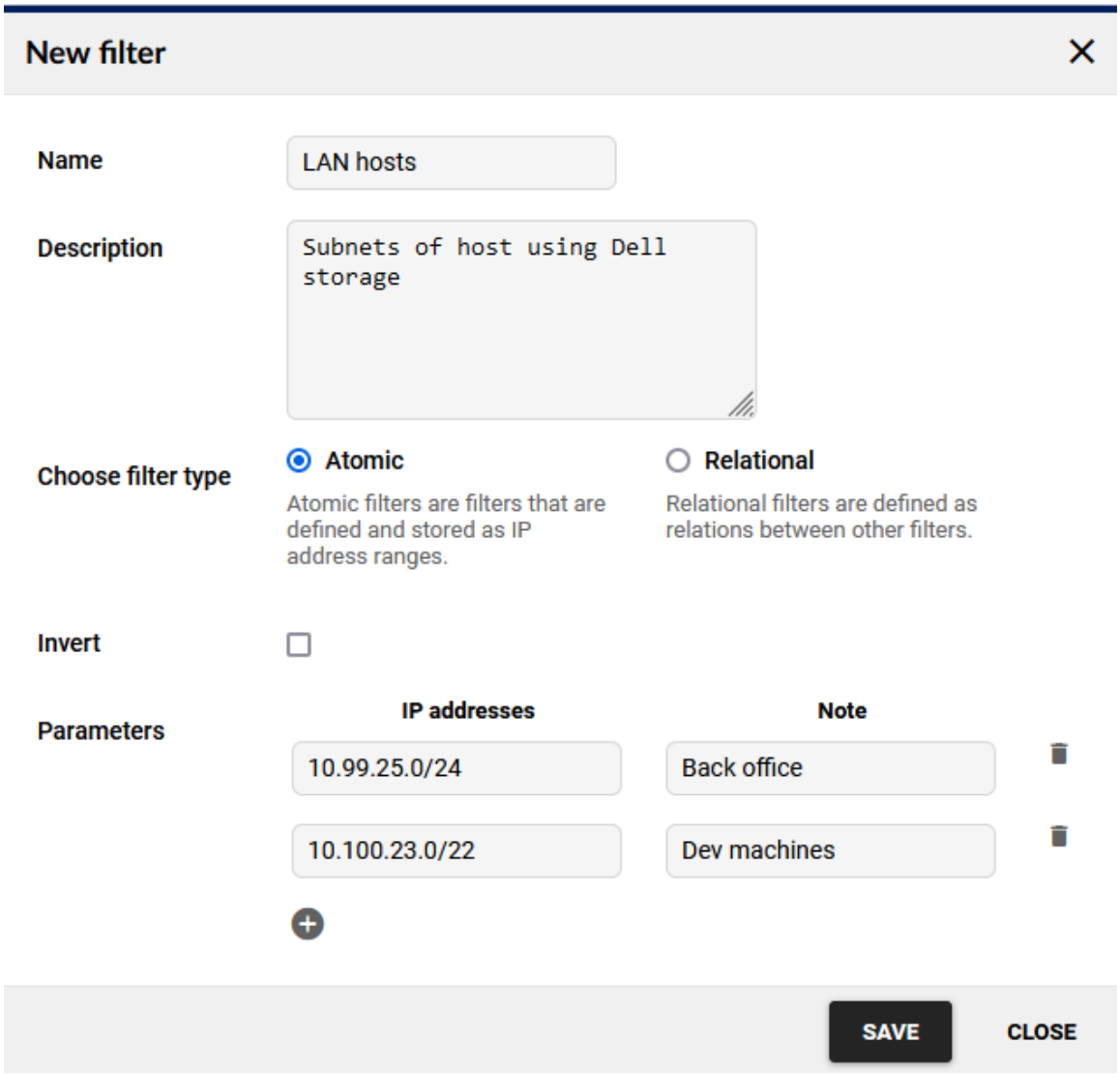
We assume that you have deployed Flowmon ADS and have configured data feeds to filter analyzed network traffic. For more details around Flowmon ADS deployment and configuration please visit the follow documentation page: Progress Flowmon Anomaly Detection System

To have the script working properly it needs to be able to find a user based either on User Identity information provided by Flowmon or identify specific user by IP address in the ProLion CryptoSpike. There we are looking at last 30 minutes of file activity and if there is a single match for the IP address we are going to block this user.

Create a Filter

We would use a filter for Perspective as we want to limit detections only to the hosts where the backup is running.

1. Within the ADS Module, go to **Settings > Processing > Filters**.
2. Click **+ NEW FILTER**.



EXAMPLE ONLY

a) Provide a **Name**.

b) Select **Atomic**.

c) Under **Parameters** add the networks that should be monitored for anomalies.

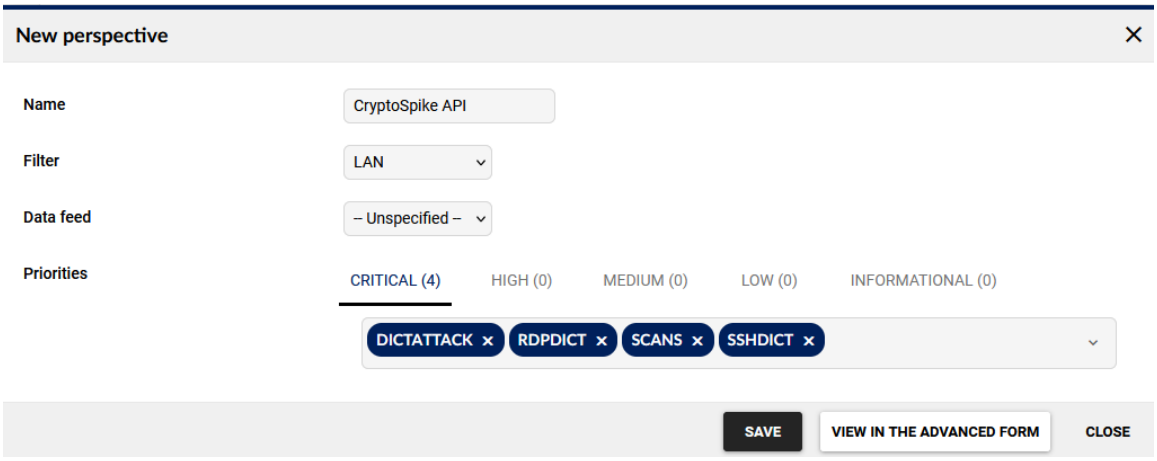
d) Click **SAVE**.

Create Perspective(s)

You can create one or more Perspectives to categorize anomalies on the network.

This document provides an example only. In production, you must identify what traffic your organization would like to enable alerts and triggers on.

1. Within the ADS module, go to Settings > Processing > Perspectives.
2. Click + NEW PERSPECTIVE.



EXAMPLE ONLY

a) Provide a Name.

b) Select the relevant Filter.

c) Select the relevant Data feed.

d) Select the priority (Critical, High, Medium, Low, and Informational) and add the relevant detection methods to each priority.

e) Click SAVE.

Create a Custom Script (API trigger)

In Flowmon ADS, custom scripts are used to automate actions when activities are needed based on the configured Perspective. Each custom script must be bound to exactly one Perspective. A script can be in the active or inactive state.

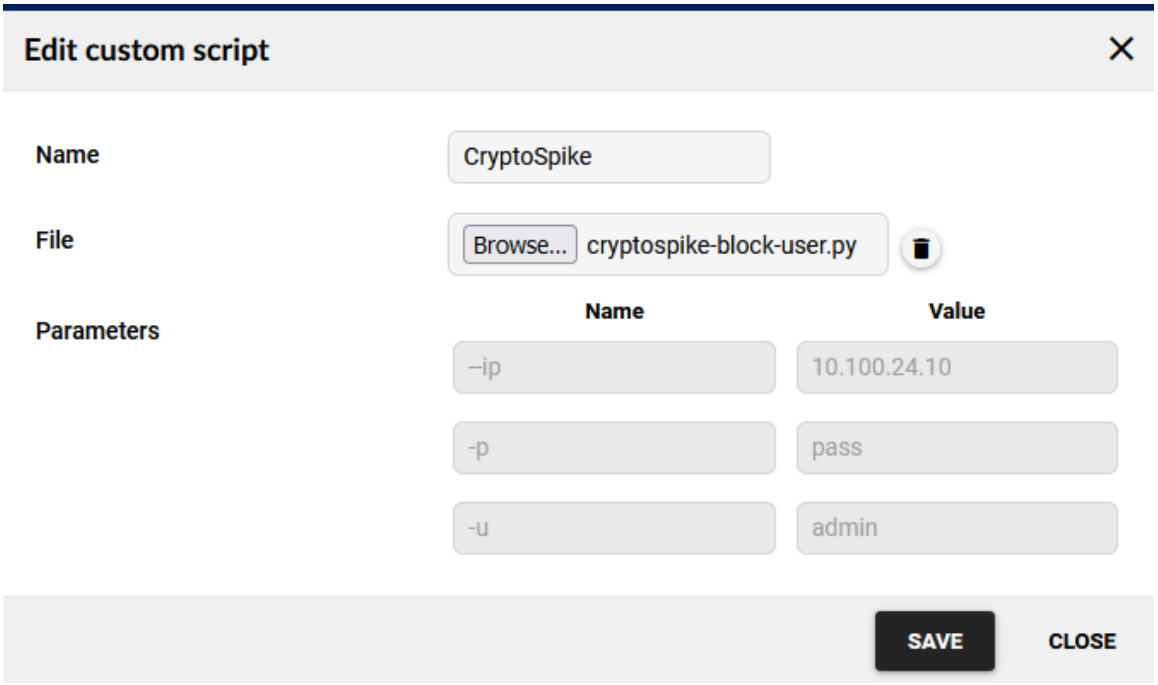
You can use the script provided by us which accepts the parameters for IP addresses/hostname and port if needed of ProLion CryptoSpike, username and password for authentication.

In case you don't want to have your password present in a clear form in Flowmon ADS user interface do not use the Parameters -u and -p and modify the code of the script lines 27 and 28 where is a default value with the correct values. That way it would be used what is in the script as a default value.

```
25  def parse_arguments():
26      parser = argparse.ArgumentParser(prog='cryptospike-block-user.py')
27      parser.add_argument("-u", "--username", action='store', type=str, help="Username to authenticate for the API call.", default='sysadm')
28      parser.add_argument("-p", "--password", action='store', type=str, help="Password for the user.", default='Inv3a-t3ch123')
29      parser.add_argument("-i", "--ip", action='store', type=str, help="IP address/hostname of the CryptoSpike", default='10.100.24.10')
30      arguments = vars(parser.parse_args())
31      return arguments
```

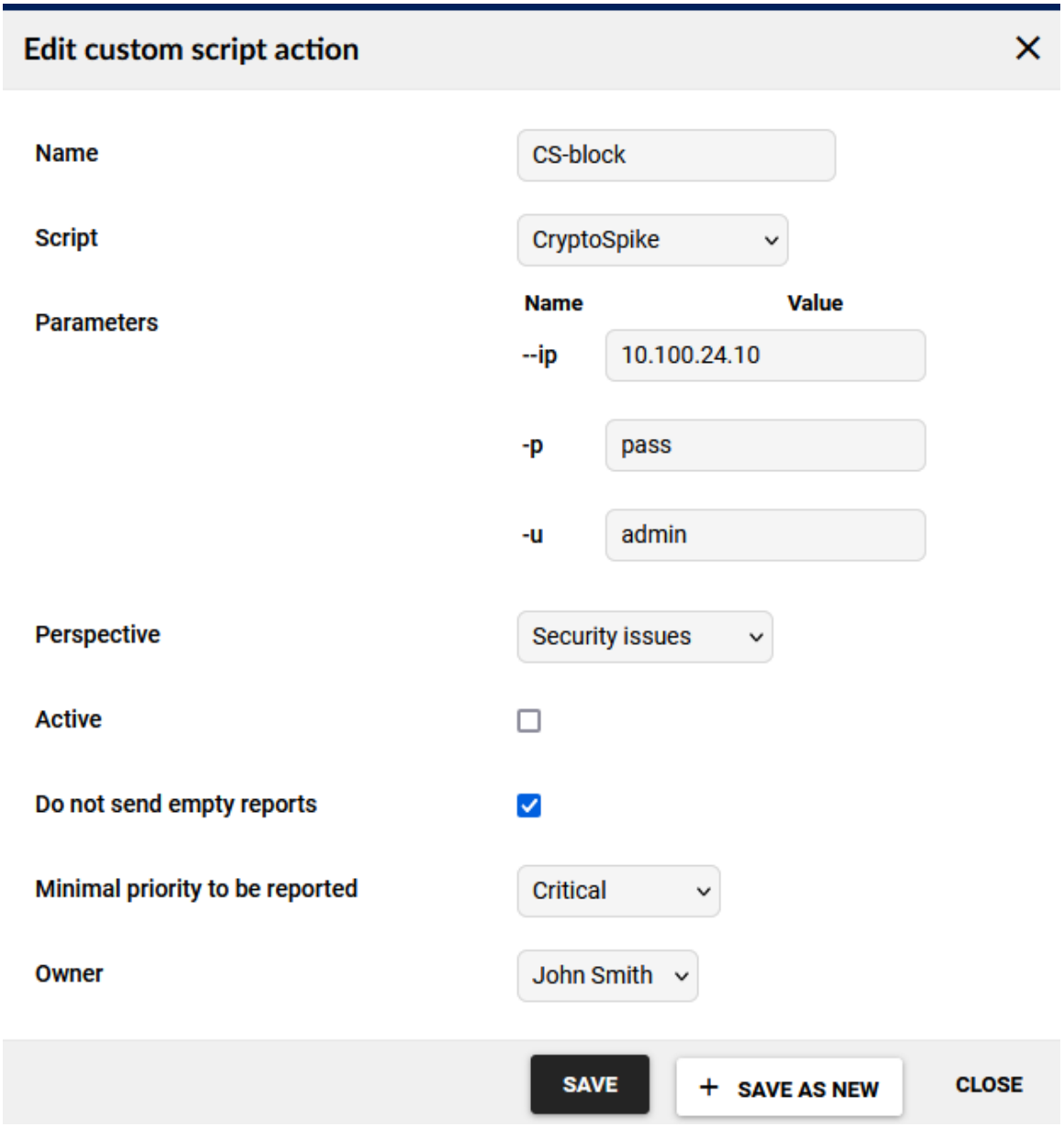
1. Within the ADS Module, go to **Settings > System Settings > Custom scripts**.
2. Click **+ NEW CUSTOM SCRIPT**.
3. Provide a **Name** for the script.

4. Under **File**, click **Choose file** and select the custom script to trigger Veeam Backup & Replication actions.



Click **SAVE**.

5. Within the ADS Module, go to **Settings > Processing > Custom scripts**.
6. Click **+ NEW CUSTOM SCRIPT ACTION**.
7. Provide a **Name** for the action.
8. Select the **Perspective**.
9. Tick the box to make the action **Active**.
10. Set the **Minimum priority to be reported**.
11. Click **SAVE**.



Perspective Methods

Methods outlined within the perspectives shown are recommendations and should be adjusted as relevant to your network access details. Progress Flowmon engineers are available to assist with determining which methods should be leveraged and we recommend the testing of triggers to ensure all is working as expected before enabling the actions taken by this script in production.

As a good starting point leveraging the methods: SCANS, RANDOMDOMAIN, BPATTERNS, DICTATTACK, SSHDICT, RDPDICT, and BLACKLIST (BotnetActivities, MalwareDomains and BotnetDomains) will provide detection of hosts that are carrying out anomalous actions.