EXHIBIT 5

Threat Intelligence Open API Setup Guide

Sky Advanced Threat Prevention (Sky ATP) provides the following APIs that can help you keep your network free of sophisticated malware and cyberattacks by using superior cloud-based protection:

Threat Intelligence API Overview

The Threat Intelligence open API allows you to program the Sky ATP Command and Control server (C&C) feeds to suit your requirements. You can perform the following operations using the threat intelligence API:

- Inject an IP, URL, or domain into a C&C feed with a threat level from 1 through 10. You can create up to 30 different custom C&C feeds.
  - An IP can be an IP address, IP range, or IP subnet.
  - Only IPv4 addresses are currently supported.
- Update the threat level of an IP, URL, or domain from 1 through 10.
- Delete a specific server in the feed or delete the entire feed.
- Retrieve the current status of an operation (processing) or errors (if any) from the feed processing engine.

The Threat Intelligence API supports a Swagger API specification in JSON format to allow programmatic access to it. For more information on the Swagger API specification, see https://threat-api.sky.junipersecurity.net/swagger.json.

NOTE: C&C regular feeds currently support only HTTP host URLs. For example, if you create www.example.com/example1/, it will check only www.example.com.

Blacklist and whitelist feeds (see below) support full URLs with Junos OS 15.1X49-D70 and later releases.

configure security policies to use the DAE within a security policy. When the DAE is updated, the changes automatically become part of the security policy. There is no need to update the policy manually. Note that this is an IP address-only feed. It does not support URLs or fully qualified domain names (FQDNs).

The IP filter APIs let you perform the following tasks:

- Remove IP addresses (in a .csv file) from an IP filter feed
- Add IP addresses (in a .csv file) to an IP filter feed.
- Remove a specific IP address from the IP filter feed.
- Add a specific IP address to the IP filter feed.
- Remove a specific IP filter feed.
- Get the processing status of a specific IP Filter feed.

The IP filter API supports a Swagger API specification in JSON format to allow programmatic access to it. For more information on the Swagger API specification, see https://api.sky.junipersecurity.net/swagger.json.

Configuration and Setup

To access the API, you must create an application token in the Sky ATP Web UI and use that token as the bearer token in the authorization header. See section "Configuration and Setup" on page 2 for more information on the creation of the token.

Example

In this example, targeted attacked are being performed against web servers in a DMZ while concealing their identities via Tor. Tor exit nodes move frequently and keeping an up-to-date list of all 1000+ exit nodes within a firewall policy is almost impossible. This can, however, be done easily using Sky ATP's APIs. For more information on this example, see Automating Cyber Threat Intelligence with Sky ATP.

Shown below is an example script that performs the following actions:

- Polls the official TorProject's exit-node list via cURL and extracts legitimate IP information via **grep**.
- Utilizes Sky ATP's open API to install and propagate third-party threat intelligence to all SRX Series devices in the network.
- Runs on an hourly basis via cron to ensure that the active Tor Relays are always being blocked.

```
#!/bin/bash

# Define Application Token (Paste in your value between the "")
APPToken="Your_Application_Token_Here"

# Define the name of the feed you wish to create
FeedName="Tor_Exit_Nodes"

#Define temporary file to store address list
```