

Tech brief

How to configure Phantom event forwarding from Splunk saved searches

Background

This document will outline in detail how to create the Splunk saved search and Phantom event forwarding rule necessary to feed Corelight's DNS investigation playbook on an automated basis. It assumes that you already have the [Phantom App for Splunk](#) installed and [connected to the Phantom instance](#) you want to feed.

Create Saved Search in Splunk

The specific search you'll want to use breaks down into several pieces:

- `index=corelight` - use the index where you're storing Corelight data
- `sourcetype=corelight_suricata_corelight` - log type for Suricata events, this should not be modified
- `alert.signature_id IN (<comma-separated list of signature IDs, see our Github>)` - Corelight is periodically updating the list, so be sure to come back for updates
- `earliest=-5m latest=now` - time window to match the interval at which events are sent into Phantom
- `| table uid ts` - extracts the two fields necessary for the playbook to run in a way that Phantom maps them properly

Combined together, the search would look like this (SID list trimmed for brevity):

```
index=corelight sourcetype=corelight_suricata_corelight alert.signagture_id IN
(2011409,2011410,2012171) earliest=-5m latest=now
```

The search should then be saved using the “Save As -> Report” drop down on the top right of the Splunk search and reporting interface; choose a name and an optional description, and select “No” for the “Time Range Picker” option in the save dialog.

Once the search report is saved, you’ll want to edit its permissions (which can be done directly from the Permissions hyperlink that appears on the confirmation screen), and ensure that the Phantom user has read permissions to the search, similar to the setup below:

Edit Permissions ✕

Report **MaliciousDNS**

Owner **admin**

App **search**

Display For Owner App All apps

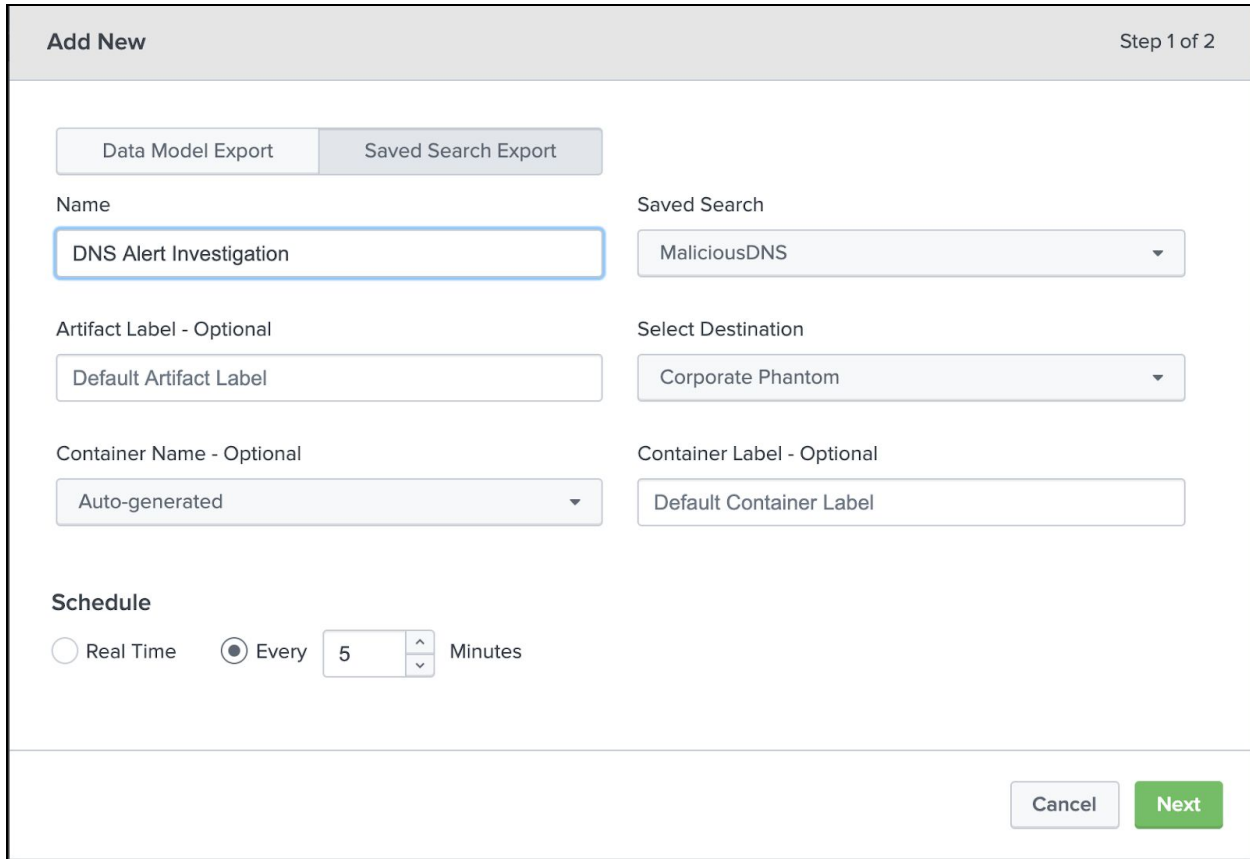
Run As Owner User

[Learn More](#)

	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
phantom	<input checked="" type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>
user_clone-demo	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Save

Upon opening the Phantom App for Splunk, the Event Forwarding tab is displayed by default. You'll want to click "Add New", which presents you first with a screen similar to this:



The name chosen on this screen will be used as a base for container event names in Phantom, if you use the default value of Auto-generated for the Container Name. You'll want to choose the name of the saved search done previously, and choose your configured Phantom instance in the destination field as well. We recommend Splunk's default polling interval of 5 minutes, which aligns to the time modifier in the query above.

One you click "Next", the second configuration window will appear, similar to this:

Add New
Step 2 of 2

Configuring [MaliciousDNS](#) on **Corporate Phantom**

Severity and Sensitivity Fields

Severity ?

Sensitivity ?

Unmapped Fields (2)

Group ?	Search Fields	CEF Fields	Contains
<input checked="" type="checkbox"/>	<input type="text" value="ts"/>	<input type="text" value="Choose the CEF field n..."/>	<input type="text" value="Select contains"/> <input type="button" value="-"/>
<input type="checkbox"/>	<input type="text" value="uid"/>	<input type="text" value="filter"/> <input type="button" value="Q"/> <ul style="list-style-type: none"> Add a non-standard field act app applicationProtocol baseEventCount 	<input type="text" value="Select contains"/> <input type="button" value="-"/> <input type="button" value="+"/> <input type="checkbox" value="Save mappings"/> ?

> Mapped Fields (0)

You'll need to first specify a severity and a sensitivity level. Next, you'll choose the "Add a non-standard field" from the CEF Fields dropdown menu, and input the names of the search fields in the CEF fields column (i.e. "ts" becomes "ts"). We recommend checking the "Group" box for the "ts" search field, as it will append the timestamp of the event to the container name, making it easier for analysts to distinguish between events of this type.

Once the mappings are complete, you can click "Save and Close". Matching events will now be forwarded automatically to Phantom on your specified time interval.