TECHNICAL BRIEF

proofpoint.

ET INTELLIGENCE SPLUNK TECHNICAL ADD-ON

The ET Intelligence Splunk Technology Add-On (ET TA) allows ET customers with Splunk deployments to enrich and search any log with ET Intelligence data. The ET TA provides two primary functions:

- Automatically downloads, installs, and updates the ET Intelligence reputation list into Splunk Enterprise, Splunk Cloud and Splunk Light.
- Provides additional Splunk macros, allowing you to build your own complex Splunk queries using ET and any other data or Splunk features.

This document explains how to leverage the ET TA to find suspicious activity in your network by enriching your enterprise security logs with ET Intelligence and then searching that data with ET Splunk macros.

IDENTIFYING SUSPICIOUS NETWORK ACTIVITY IN SPLUNK WITH ET INTELLIGENCE

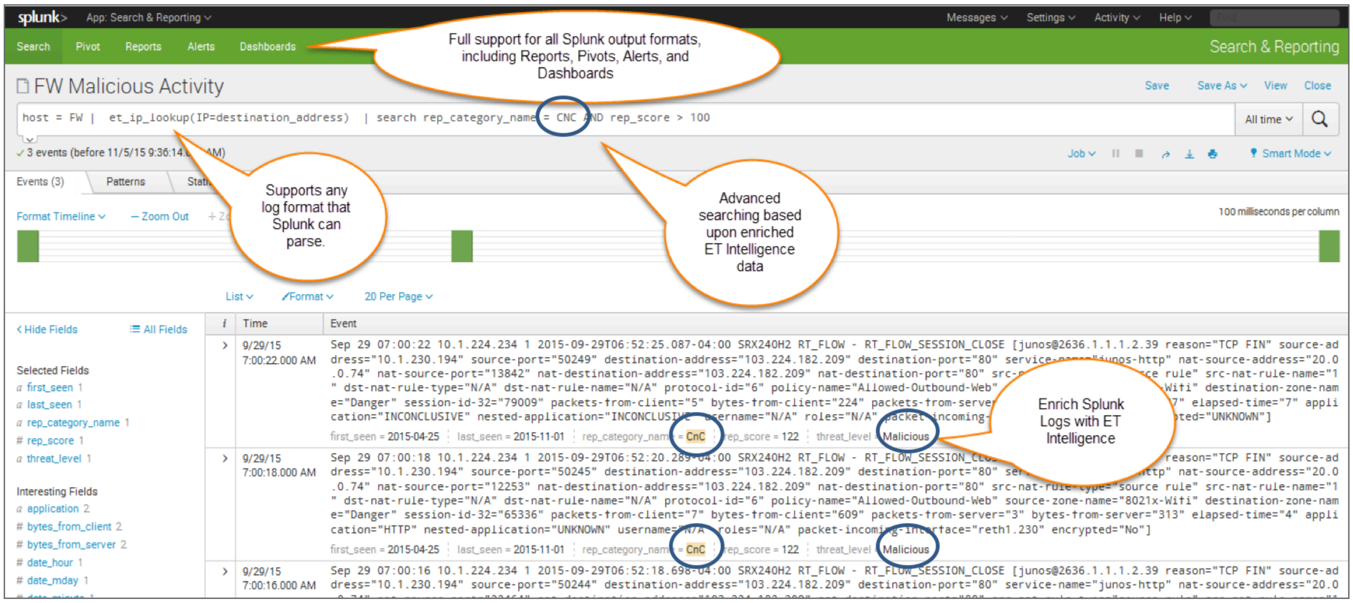
This first workflow explains how to find suspicious activity in your Splunk log database in a single query. We start by creating a query that defines the following information:

- Filter Input Data (Recommended)
- Select ET macro, and define field to match/enrich (Required)
- Filter output Data (Recommended)

In this example we will look to enrich our firewall logs with ET Intelligence. Normally, firewall logs contain information that pertains only to a specific connection, not any reputation or auxiliary information. A firewall does not normally raise any alerts if the traffic is permitted by policy. In this example, we are searching for logs whose destination are known to be involved in command-and-control (C&C) activity.

As shown in Figure 1, we have searched through our Splunk log database to enrich our logs in real time with ET Intelligence data, and searched to further find any firewall logs that matched the category C&C. We could then take this query and turn it into a Splunk dashboard, report, alert, or any other built-in feature.

Because the macro allows you to define what the IP field of your logs that you want to search, the ET TA can input logs from any log source; as long as Splunk can parse it, the ET TA can extract and enrich the data.



FW Malicious Activity

```
host = FW |  et_ip_lookup(IP=destination_address)  | search rep_category_name = CNC AND rep_score > 100
```

✓ 3 events (before 11/5/15 9:36:14. AM)

```
9/29/15          Sep 29 07:00:22 10.1.224.234 1 2015-09-29T06:52:25.087-04:00 SRX240H2 RT_FLOW - RT_FLOW_SESSION_CLOSE [junos@2636.1.1.1.2.39 reason="TCP FIN" source-ad
7:00:22.000 AM   dress="10.1.230.194" source-port="50249" destination-address="103.224.182.209" destination-port="80" service-    junos-http" nat-source-address="20.0
                 .0.74" nat-source-port="13842" nat-destination-address="103.224.182.209" nat-destination-port="80" src-             ce rule" src-nat-rule-name="1
                 " dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="Allowed-Outbound-Web"              Wifi" destination-zone-nam
                 e="Danger" session-id-32="79009" packets-from-client="5" bytes-from-client="224" packets-from-serve             7" elapsed-time="7" appli
                 cation="INCONCLUSIVE" nested-application="INCONCLUSI   ername="N/A" roles="N/A" packet incoming-              ted="UNKNOWN"]
                 first_seen = 2015-04-25 | last_seen = 2015-11-01 | rep_category_nam = CnC | rep_score = 122 | threat_level Malicious

9/29/15          Sep 29 07:00:18 10.1.224.234 1 2015-09-29T06:52:20.28  04:00 SRX240H2 RT_FLOW - RT_FLOW_SESSION_CL            reason="TCP FIN" source-ad
7:00:18.000 AM   dress="10.1.230.194" source-port="50245" destination-address="103.224.182.209" destination-port="80" se         ttp" nat-source-address="20.0
                 .0.74" nat-source-port="12253" nat-destination-address="103.224.182.209" nat-destination-port="80" src-nat-rule-type="source rule" src-nat-rule-name="1
                 " dst-nat-rule-type="N/A" dst-nat-rule-name="N/A" protocol-id="6" policy-name="Allowed-Outbound-Web" source-zone-name="8021x-Wifi" destination-zone-nam
                 e="Danger" session-id-32="65336" packets-from-client="7" bytes-from-client="609" packets-from-server="3" bytes-from-server="313" elapsed-time="4" appli
                 cation="HTTP" nested-application="UNKNOWN" username=N/A roles="N/A" packet-incoming-interface="reth1.230" encrypted="No"]
                 first_seen = 2015-04-25 | last_seen = 2015-11-01 | rep_category_nam = CnC | rep_score = 122 | threat_level Malicious

9/29/15          Sep 29 07:00:16 10.1.224.234 1 2015-09-29T06:52:18.698-04:00 SRX240H2 RT_FLOW - RT_FLOW_SESSION_CLOSE [junos@2636.1.1.1.2.39 reason="TCP FIN" source-ad
7:00:16.000 AM   dress="10.1.230.194" source-port="50244" destination-address="103.224.182.209" destination-port="80" service-name="junos-http" nat-source-address="20.0
```

Full support for all Splunk output formats, including Reports, Pivots, Alerts, and Dashboards

Supports any log format that Splunk can parse.

Advanced searching based upon enriched ET Intelligence data

Enrich Splunk Logs with ET Intelligence

Figure 1. Finding suspicious activity in network logs