Plixer splunk>

SOLUTION BRIEF

Scrutinizer and Splunk solution integration

In all organizations, catching security threats hidden within network traffic is vital to keeping the business running safely. When organizations grow and IT teams have to oversee a distributed network, however, collecting and correlating data becomes much more difficult.

Information may come from multiple geolocations, and using multiple layers of security makes the data correlation process more complicated. To compound the problem, your main data analysis system may not be optimized for gathering other types of data.

Splunk users have the option to use Scrutinizer alongside their solution, allowing for easier and faster data correlation with Plixer's integration application.

Splunk: log data aggregator

Splunk captures, indexes, and correlates real-time machine data in a searchable repository in which the user can generate graphs, reports, alerts, dashboards, and more. This includes application logs, filesystem audit logs, SCADA data, and web access logs. With this insight, IT teams have access to all user transactions, customer behavior, machine behavior, security threats, and fraudulent activity—leading to all-encompassing business intelligence.

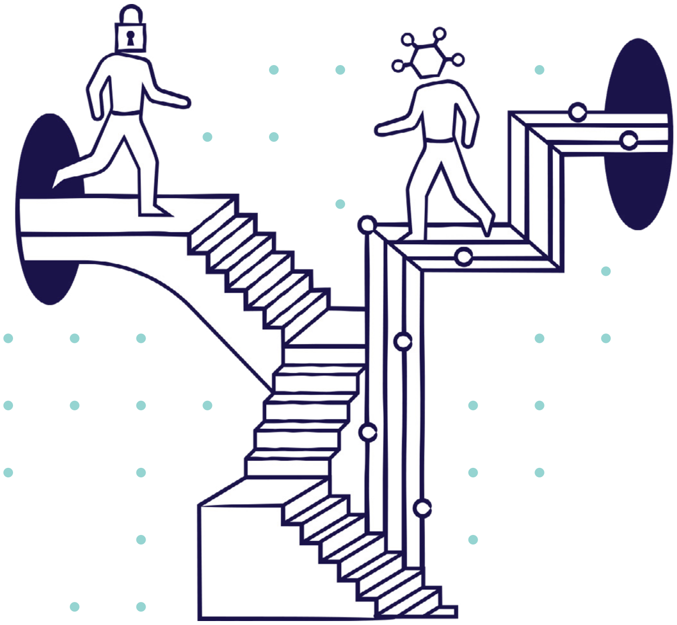
Scrutinizer: security & network intelligence platform

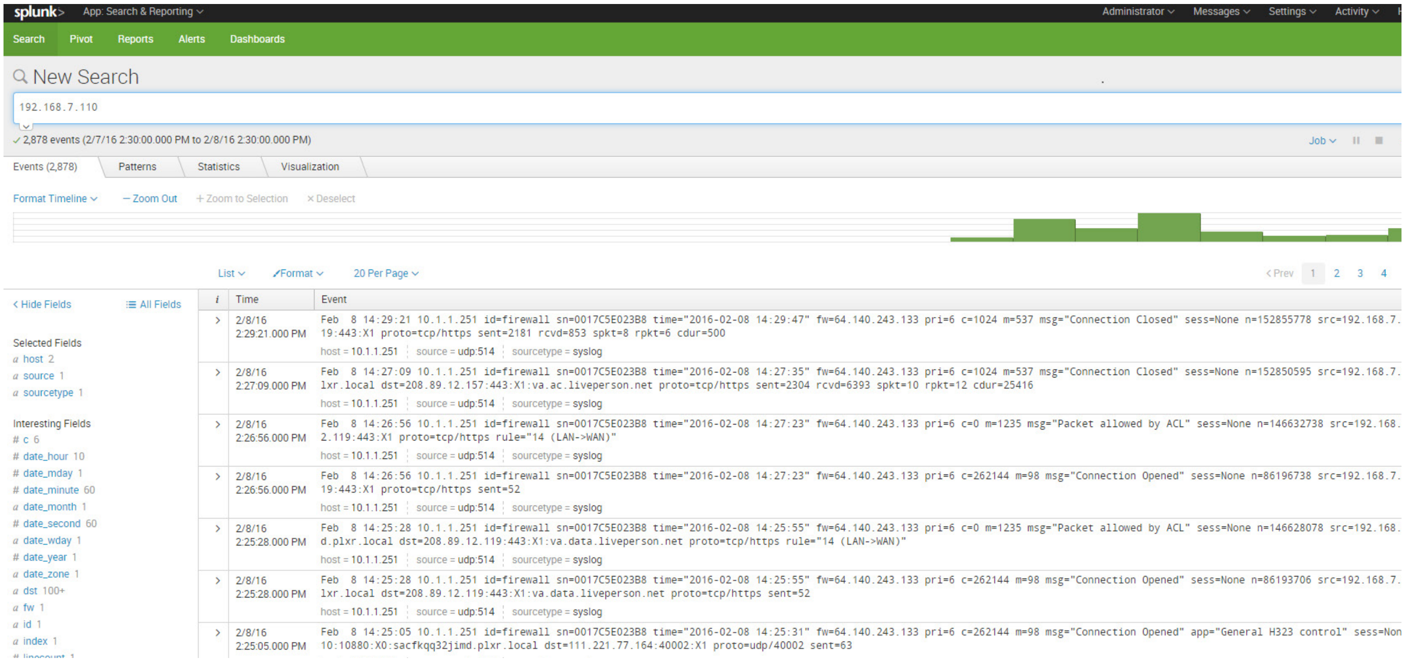
The Scrutinizer system collects and analyzes flows and metadata. Flow data is comparable to packet capture in richness of information, while being far more lightweight and scalable. As a result, Scrutinizer can store millions of flow and metadata records for decades, enabling IT teams to perform deep forensic investigations.

Save time, save money

Plixer has developed a plugin that enables Splunk users to access Scrutinizer from within the Splunk interface. Users can also access Splunk event data from within the Scrutinizer interface. A user can click on an IP address or hostname in Scrutinizer and tell the system to pass the data to Splunk. The timeframe and IP address are then passed in a URL string to Splunk for further investigation. Splunk will then display the events for the specified host and timeframe.

Splunk users who want more context around an event and who want to take advantage of powerful filtering with boolean expressions will find themselves often passing data from Splunk to Scrutinizer as well.





splunk> App: Search & Reporting

Administrator Messages Settings Activity

Search Pivot Reports Alerts Dashboards

New Search

192.168.7.110

✓ 2,878 events (2/7/16 2:30:00.000 PM to 2/8/16 2:30:00.000 PM)

Job

Events (2,878) | Patterns | Statistics | Visualization

Format Timeline — Zoom Out + Zoom to Selection × Deselect

List Format 20 Per Page

< Prev 1 2 3 4

< Hide Fields ☰ All Fields

Selected Fields
- a host 2
- a source 1
- a sourcetype 1

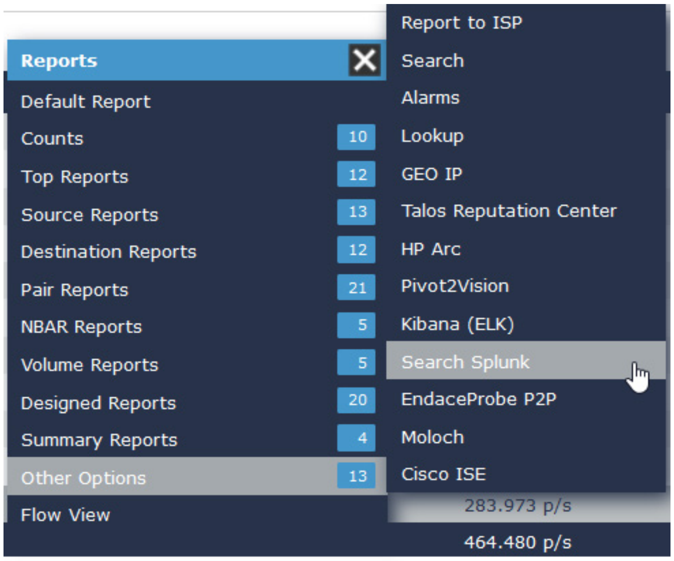
Interesting Fields
- # c 6
- # date_hour 10
- # date_mday 1
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 1
- # date_year 1
- a date_zone 1
- a dst 100+
- a fw 1
- a id 1
- a index 1
- # linecount 1

```
i  Time                Event
>  2/8/16              Feb  8 14:29:21 10.1.1.251 id=firewall sn=0017C5E023B8 time="2016-02-08 14:29:47" fw=64.140.243.133 pri=6 c=1024 m=537 msg="Connection Closed" sess=None n=152855778 src=192.168.7.
   2:29:21.000 PM      19:443:X1 proto=tcp/https sent=2181 rcvd=853 spkt=8 rpkt=6 cdur=500
                       host = 10.1.1.251   source = udp:514   sourcetype = syslog
>  2/8/16              Feb  8 14:27:09 10.1.1.251 id=firewall sn=0017C5E023B8 time="2016-02-08 14:27:35" fw=64.140.243.133 pri=6 c=1024 m=537 msg="Connection Closed" sess=None n=152850595 src=192.168.7.
   2:27:09.000 PM      lxr.local dst=208.89.12.157:443:X1:va.ac.liveperson.net proto=tcp/https sent=2304 rcvd=6393 spkt=10 rpkt=12 cdur=25416
                       host = 10.1.1.251   source = udp:514   sourcetype = syslog
>  2/8/16              Feb  8 14:26:56 10.1.1.251 id=firewall sn=0017C5E023B8 time="2016-02-08 14:27:23" fw=64.140.243.133 pri=6 c=0 m=1235 msg="Packet allowed by ACL" sess=None n=146632738 src=192.168.
   2:26:56.000 PM      2.119:443:X1 proto=tcp/https rule="14 (LAN->WAN)"
                       host = 10.1.1.251   source = udp:514   sourcetype = syslog
>  2/8/16              Feb  8 14:26:56 10.1.1.251 id=firewall sn=0017C5E023B8 time="2016-02-08 14:27:23" fw=64.140.243.133 pri=6 c=262144 m=98 msg="Connection Opened" sess=None n=86196738 src=192.168.7.
   2:26:56.000 PM      19:443:X1 proto=tcp/https sent=52
                       host = 10.1.1.251   source = udp:514   sourcetype = syslog
>  2/8/16              Feb  8 14:25:28 10.1.1.251 id=firewall sn=0017C5E023B8 time="2016-02-08 14:25:55" fw=64.140.243.133 pri=6 c=0 m=1235 msg="Packet allowed by ACL" sess=None n=146628078 src=192.168.
   2:25:28.000 PM      d.plxr.local dst=208.89.12.119:443:X1:va.data.liveperson.net proto=tcp/https rule="14 (LAN->WAN)"
                       host = 10.1.1.251   source = udp:514   sourcetype = syslog
>  2/8/16              Feb  8 14:25:28 10.1.1.251 id=firewall sn=0017C5E023B8 time="2016-02-08 14:25:55" fw=64.140.243.133 pri=6 c=262144 m=98 msg="Connection Opened" sess=None n=86193706 src=192.168.7.
   2:25:28.000 PM      lxr.local dst=208.89.12.119:443:X1:va.data.liveperson.net proto=tcp/https sent=52
                       host = 10.1.1.251   source = udp:514   sourcetype = syslog
>  2/8/16              Feb  8 14:25:05 10.1.1.251 id=firewall sn=0017C5E023B8 time="2016-02-08 14:25:31" fw=64.140.243.133 pri=6 c=262144 m=98 msg="Connection Opened" app="General H323 control" sess=Non
   2:25:05.000 PM      10:10880:X0:sacfkqq32jimd.plxr.local dst=111.221.77.164:40002:X1 proto=udp/40002 sent=63
```

Splunk users will save valuable time with this ease of correlation between Scrutinizer's network traffic analytics and Splunk log data. It also saves money for organizations because Scrutinizer is optimized for flow and metadata support and is capable of collecting and storing millions of records per second.

By implementing Scrutinizer as a complementary solution to Splunk, organizations can take advantage of a more mature, more scalable, and richer filtering and reporting interface at a lower price. Working together, Splunk and Scrutinizer provide richer context when solving problems.

This app can be downloaded from Plixer's website at plixer.com/splunk-integration.html.



©Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.