



CONNECTING
THE WORLD



Cybersecurity Monitoring

Brian Gilmore

IoT Advocacy and Evangelism

Splunk

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

The Security Journey



Market Trends



Demand for
Automation and
Adaptive
Response



Convergence
of IT and OT



Analytics and
Machine Learning
for Threat
Detection

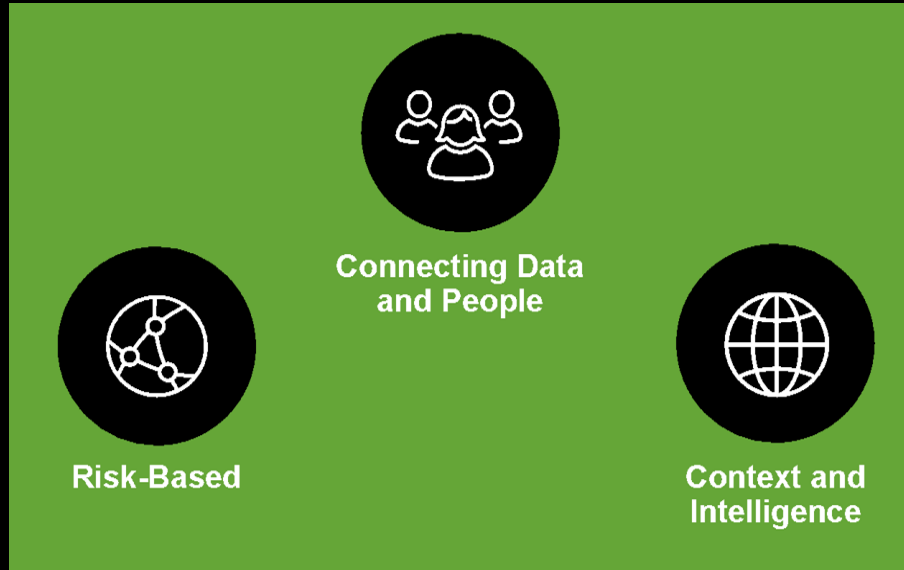


Security Strategy
Reliant on Data
Strategy



Shift From
Prevention to
Detection and
Response

Analytics-Driven Security



Security Relevance of All Data

All data is needed to detect and investigate advanced threats



Threat Intelligence



Email



Web



Desktops



Servers



DHCP/ DNS



CMDB



Hypervisor



Badges



Firewall



Authentication



Vulnerability
Scans



Custom Apps



Network
Flows



Storage



Mobile



Intrusion
Detection



Data Loss
Prevention



Anti-Malware



Physical
Sensors



Transaction
Records

Traditiona

SECURITY JOURNEY

Nerve center for security

Collaborative SOC

Establish security operations

Solve across multiple domains

Specific problem

Step 1: Specific Problem

Monitor Niagara Weblogs for Threats
(bonus: other cool insights!)

Three Easy Steps!

- Install Splunk
- Monitor your Niagara webserver logs
- Detect threats and realize new insights

Download Security Monitoring Solution

Splunk Enterprise (Free)

- www.splunk.com/downloads
- 60 day free trial with PERPETUALLY FREE option
- Thousands of free Splunk apps at www.splunkbase.com
 - IP Reputation App
 - Splunk Security Essentials
 - Splunk App for Web Analytics
- Fast install



Splunk Enterprise 7.0.3

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Windows

Linux

Mac OS

64-bit

Windows 8.1, and 10
Windows Server 2012, 2012 R2, and 2016

.msi

167.34 MB

Download Now

32-bit

Windows 8.1 and 10

.msi

149.5 MB

Download Now

[Release Notes](#) | [System Requirements](#) | [Older Releases](#) | [All Other Downloads](#)

Monitor Your Niagara Web Logs

- Configure the Niagara Web Server
- Configure Splunk to index the logs created by the web server

Configure the Niagara Web Server

- NCSA Logging Properties
- Set Enabled=True
- Retain Days is up to you
- Extended Format=True
- Log Cookies=True

The screenshot shows the 'Property Sheet' for 'JettyWebServer (Jetty Web Server)'. The 'NCSA Log' section is expanded, showing the following settings:

Property	Value	Range/Options
Server State	started	
Min Threads	4	[4 - 30]
Max Threads	30	[7 - max]
Thread Idle Timeout	000000h 05m 00s	[1sec - +inf]
NCSA Log	N C S A Request Log	
Enabled	false	
Retain Days	7	[1 - max]
Extended Format	true	
Log Cookies	false	
Log Time Zone	UTC (+0)	
Diagnostics Enabled	false	

Configure Splunk to Index the Weblogs

- Splunk Enterprise vs Universal Forwarding
- Continuously monitor the log file directories created by Niagara
- Indexing of files will occur in real-time each time a new line is written

The screenshot shows the Splunk web interface for configuring a new data source. The top navigation bar includes the Splunk logo, 'Apps', and user roles 'Administrator' and 'Messages'. The main heading is 'Add Data', followed by a progress bar with steps: 'Select Source' (active), 'Set Source Type', 'Input Settings', 'Review', and 'Done'. A green 'Next >' button is visible.

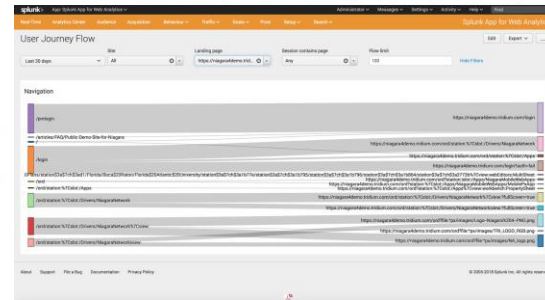
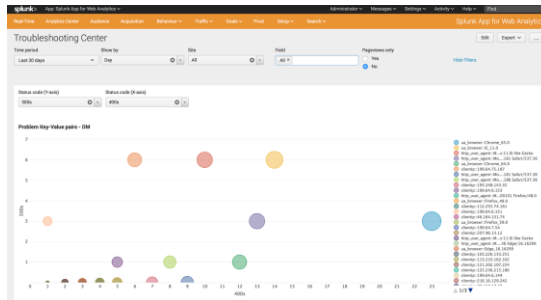
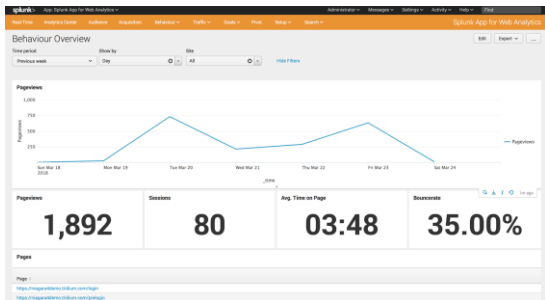
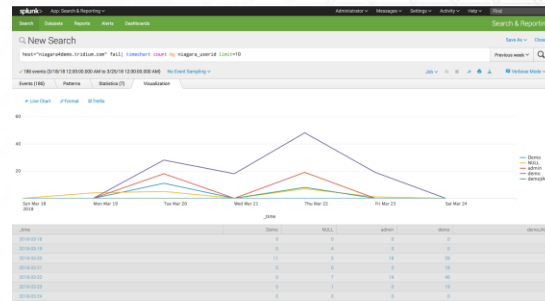
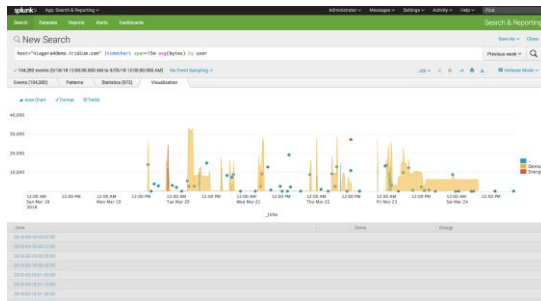
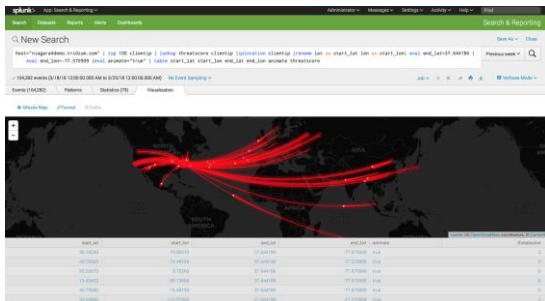
Under the 'Files & Directories' section, there are three options: 'HTTP Event Collector', 'TCP / UDP', and 'Scripts'. The 'Files & Directories' option is selected, showing a description: 'Upload a file, index a local file, or monitor an entire directory.' Below this, there are three sub-sections: 'HTTP Event Collector', 'TCP / UDP', and 'Scripts', each with a brief description.

The main configuration area for 'Files & Directories' includes a text input field for 'File or Directory' with the value 'c:\niagara\bin\logs\weblogs' and a 'Browse' button. Below this, there are two radio buttons: 'Continuously Monitor' (selected) and 'Index Once'. There are also input fields for 'Whitelist' and 'Blacklist'.

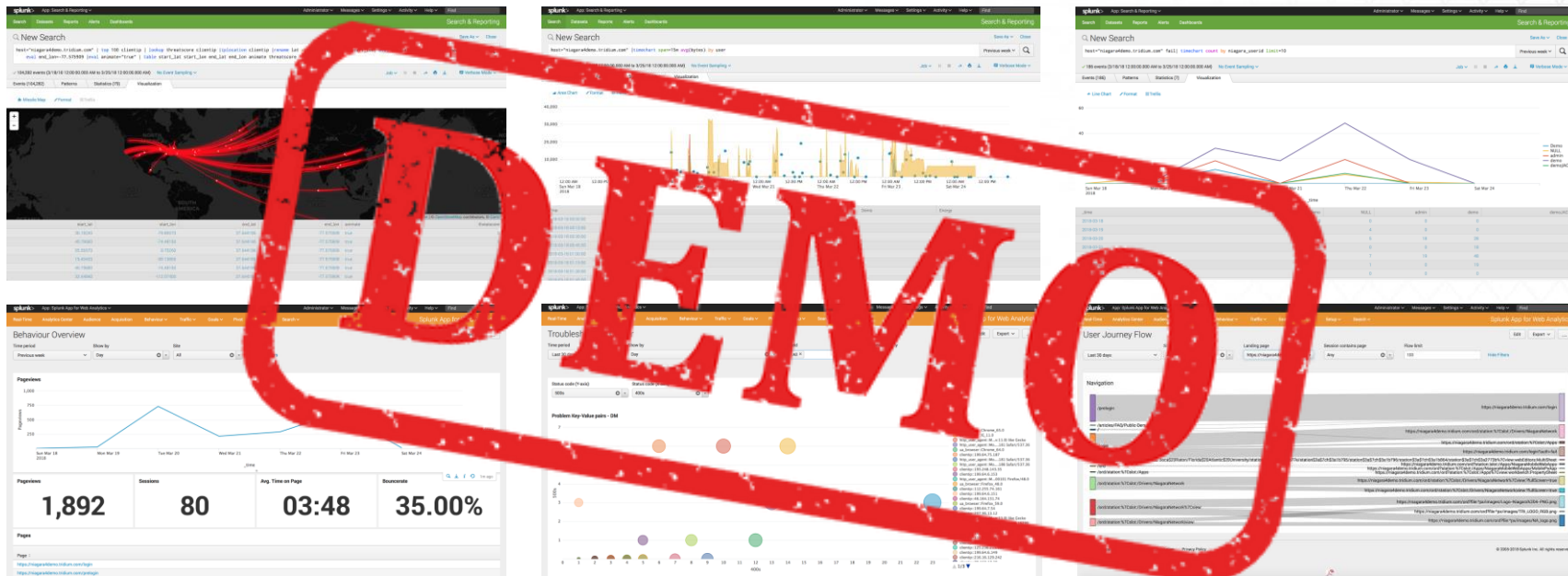
At the bottom, there is an 'FAQ' section with several questions and answers:

- > What kinds of files can Splunk index?
- > I can't access the file that I want to index. Why?
- > How do I get remote data onto my Splunk instance?
- > Can I monitor changes to files in addition to their content?
- > What is a source type?
- > How do I specify a whitelist or blacklist for a directory?

Detect Threats and Realize New Insights



Detect Threats and Realize New Insights



SECURITY JOURNEY

Nerve center for security

Collaborative SOC

Establish security operations

Solve across multiple domains

Specific problem

Tell Us What You Think!
<https://ponypoll.com/ns18splunksec>



Login with LinkedIn

NSIS-Splunk-Sec

splunk>PonyPoll

QUESTION 1
How would you rate this session?

Quality of content	☆ ☆ ☆ ☆ ☆	-
Relevance to my business	☆ ☆ ☆ ☆ ☆	-
Speaker's presentation skills	☆ ☆ ☆ ☆ ☆	-
Splunk Values: innovation, passion, disruption, openness, fun	☆ ☆ ☆ ☆ ☆	-

1 of 3

◀ Prev Next ▶

Keep in Touch!

Email: bgilmore@splunk.com

LinkedIn: [Linkedin.com/in/industrialdata](https://www.linkedin.com/in/industrialdata)

Twitter: @BrianMGilmore

Web: www.splunk.com/iot



Thank You!