CONNECTING
THE WORLD

Cybersecurity Monitoring

Brian Gilmore
IoT Advocacy and Evangelism
Splunk

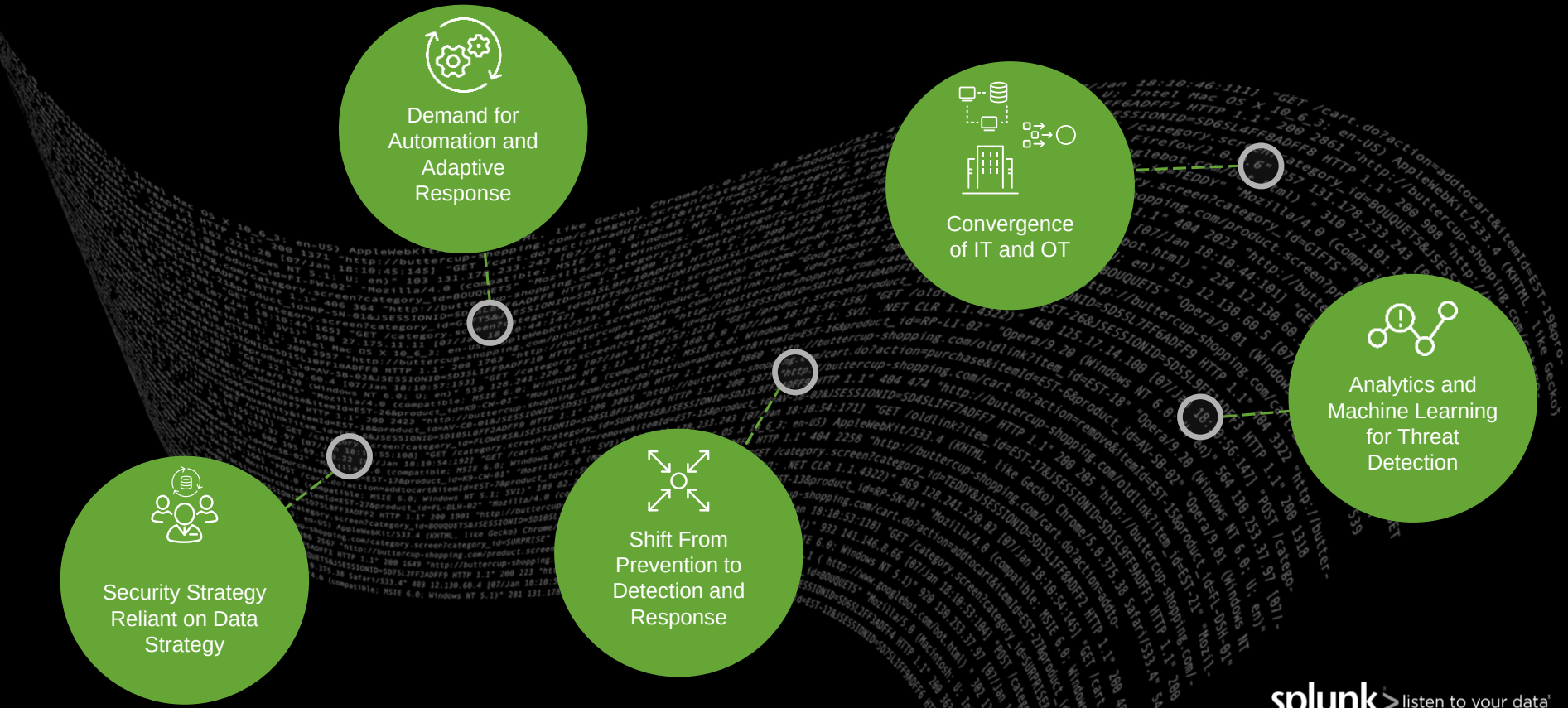
Forward-Looking Statements

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.

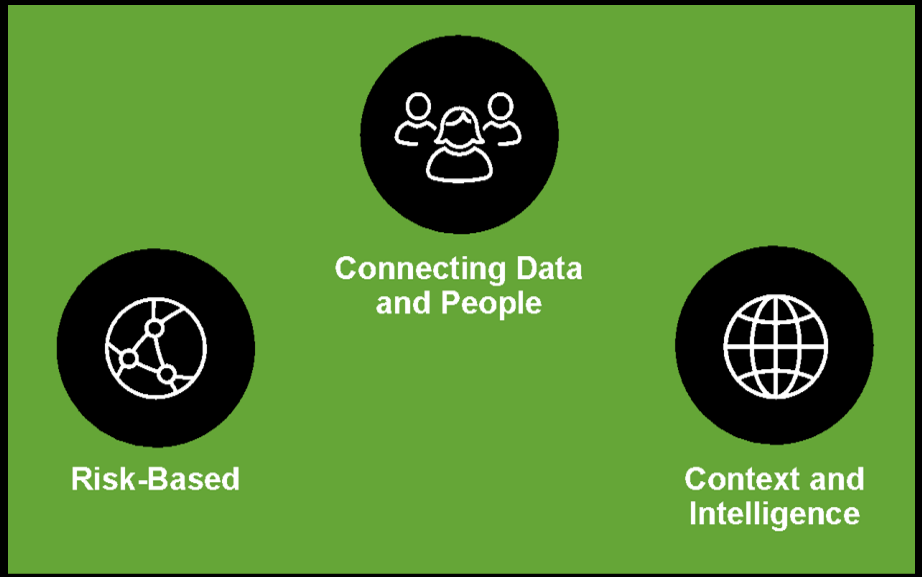
The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements 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.

The Security Journey

Market Trends



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

Traditiona


Hypervisor


Badges


Firewall


Authentication


Vulnerability Scans

Custom Apps


Network Flows


Storage


Mobile


Intrusion Detection


Data Loss Prevention


Anti-Malware


Physical Sensors


Transaction Records

splunk>

SECURITY JOURNEY

splunk> listen to your data

Step 1: Specific Problem

Monitor Niagara Weblogs for Threats

(bonus: other cool insights!)

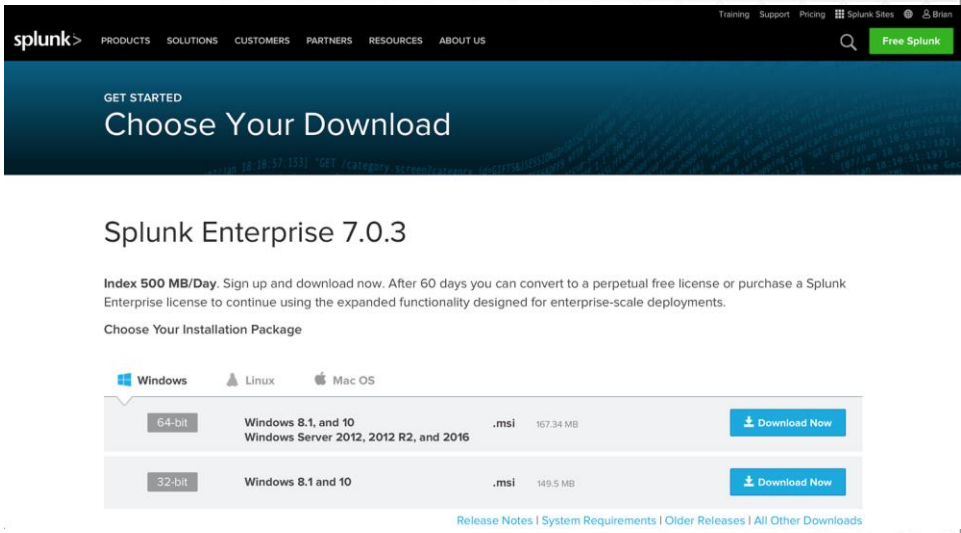
Three Easy Steps!

- 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

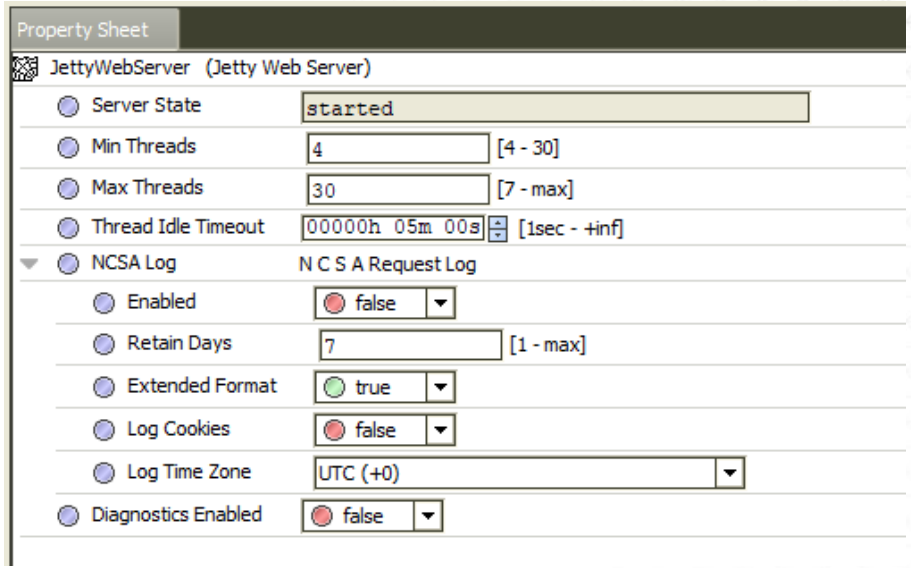


Monitor Your Niagara Web Logs

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

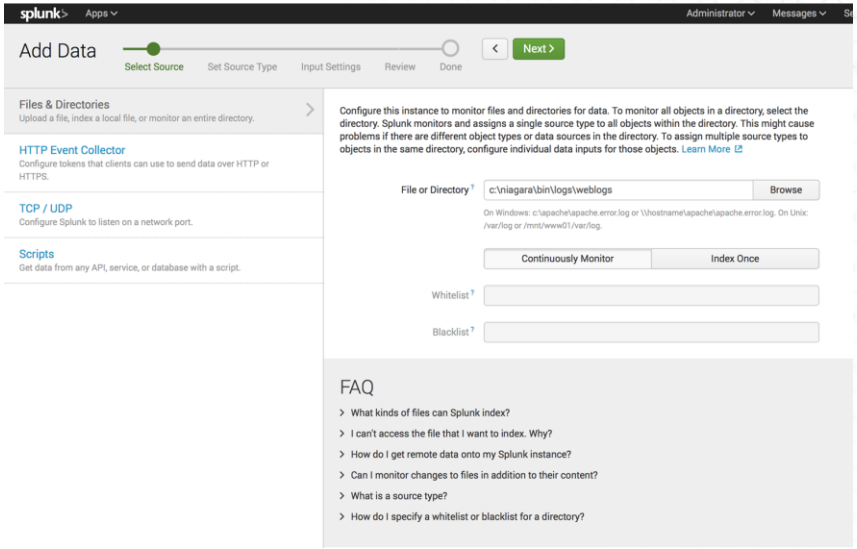
Configure the Niagara Web Server

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

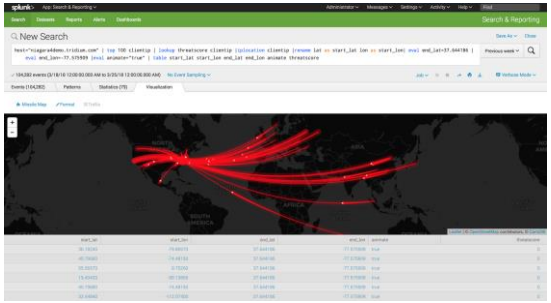


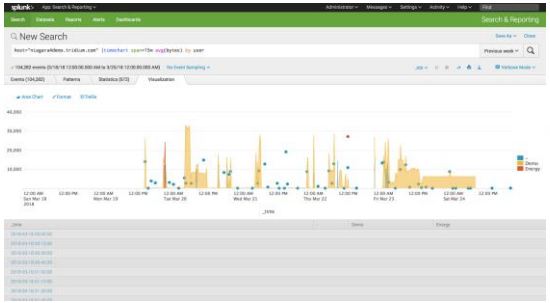
Configure Splunk to Index the Weblogs

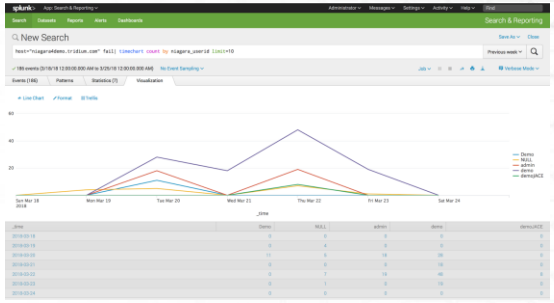
- Splunk Enterprise vs Universal Forwarding
- Continuously monitor the log file directories created by Niagara
- Indexing of files will occur in real-time each time a new line is written

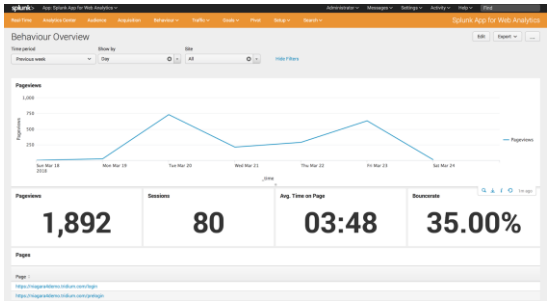


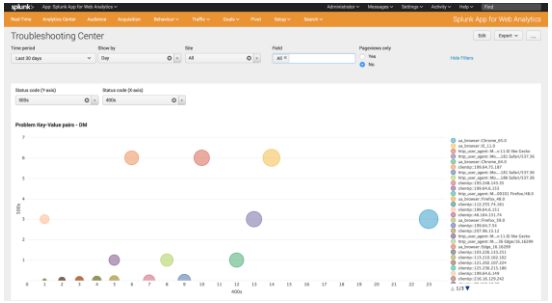
Detect Threats and Realize New Insights

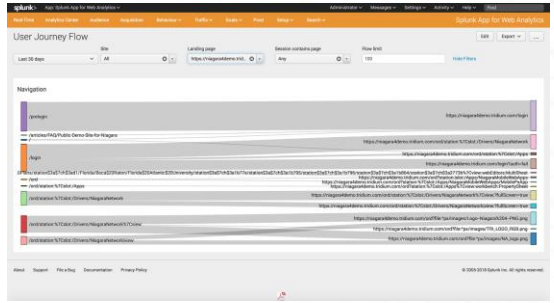




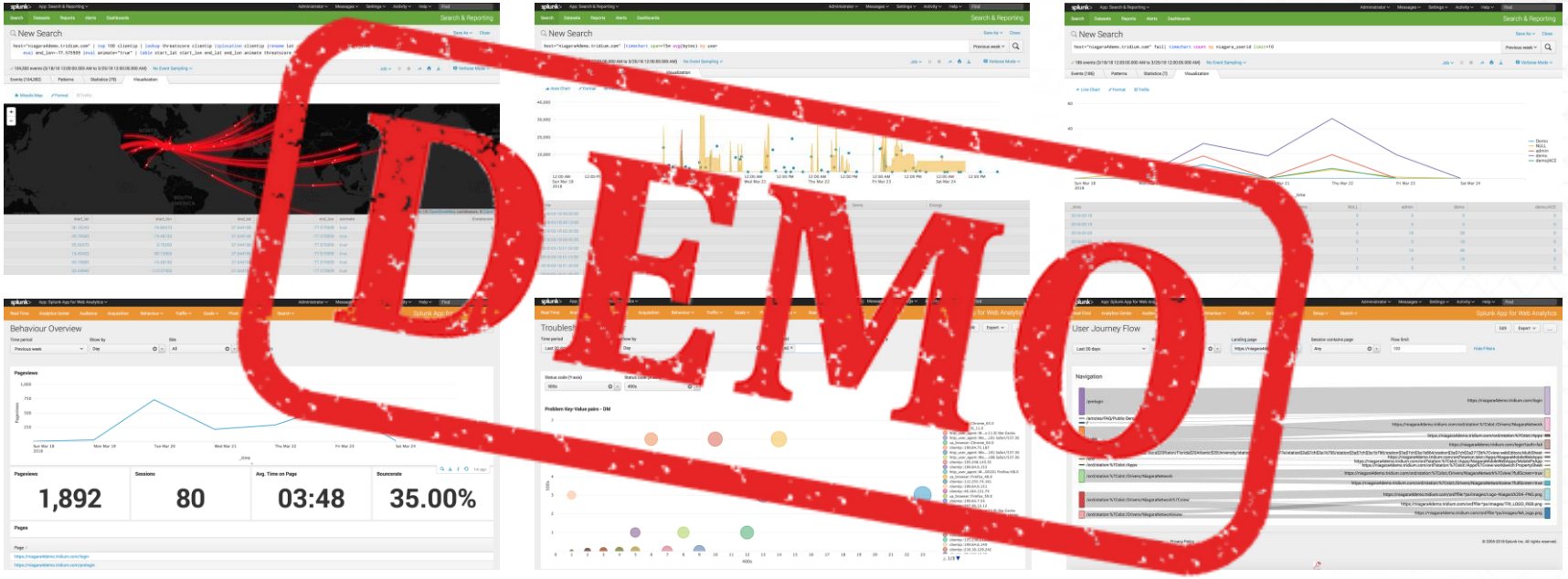








Detect Threats and Realize New Insights

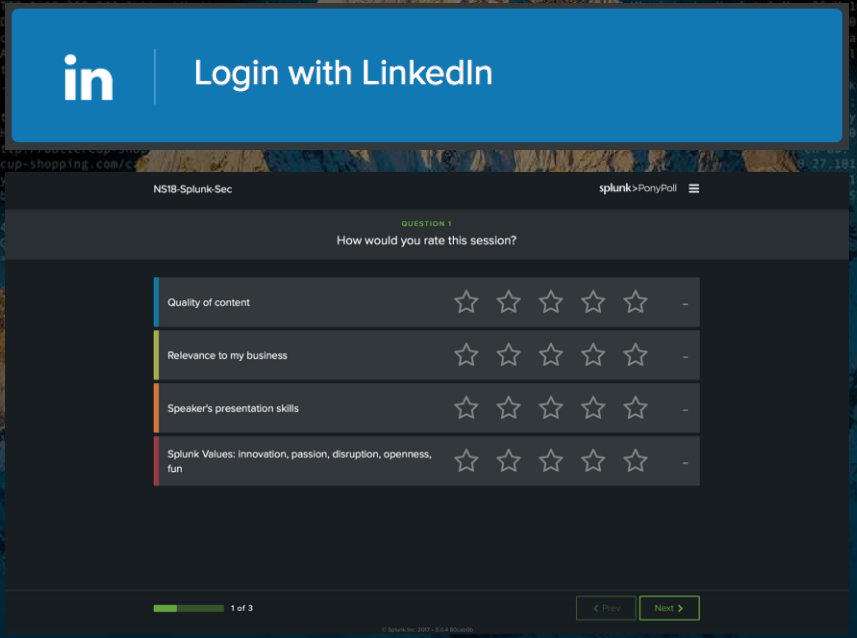


SECURITY JOURNEY

splunk> listen to your data

Tell Us What You Think!

https://ponypoll.com/ns18splunksec



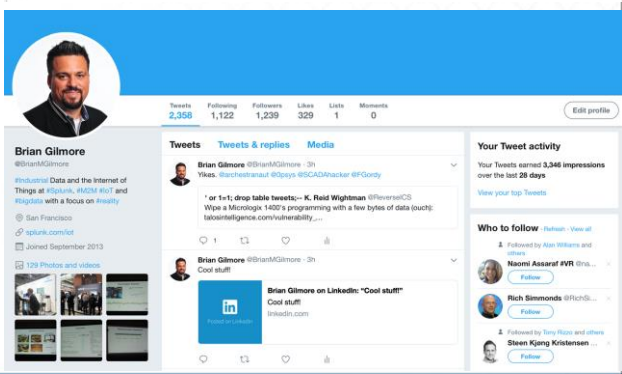
Keep in Touch!

Email: bgilmore@splunk.com

LinkedIn: Linkedin.com/in/industrialdata

Twitter: @BrianMGilmore

Web: www.splunk.com/iot



Thank You!