

Welcome



splunk> .conf2017

Data Wars: A New Hope for IT & Security Insights

Jade Catalano | Senior Product Marketing, Security
Robert Christian | Senior Sales Engineer
Sept. 25-28, 2017 | Washington, DC

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.

How we see ourselves



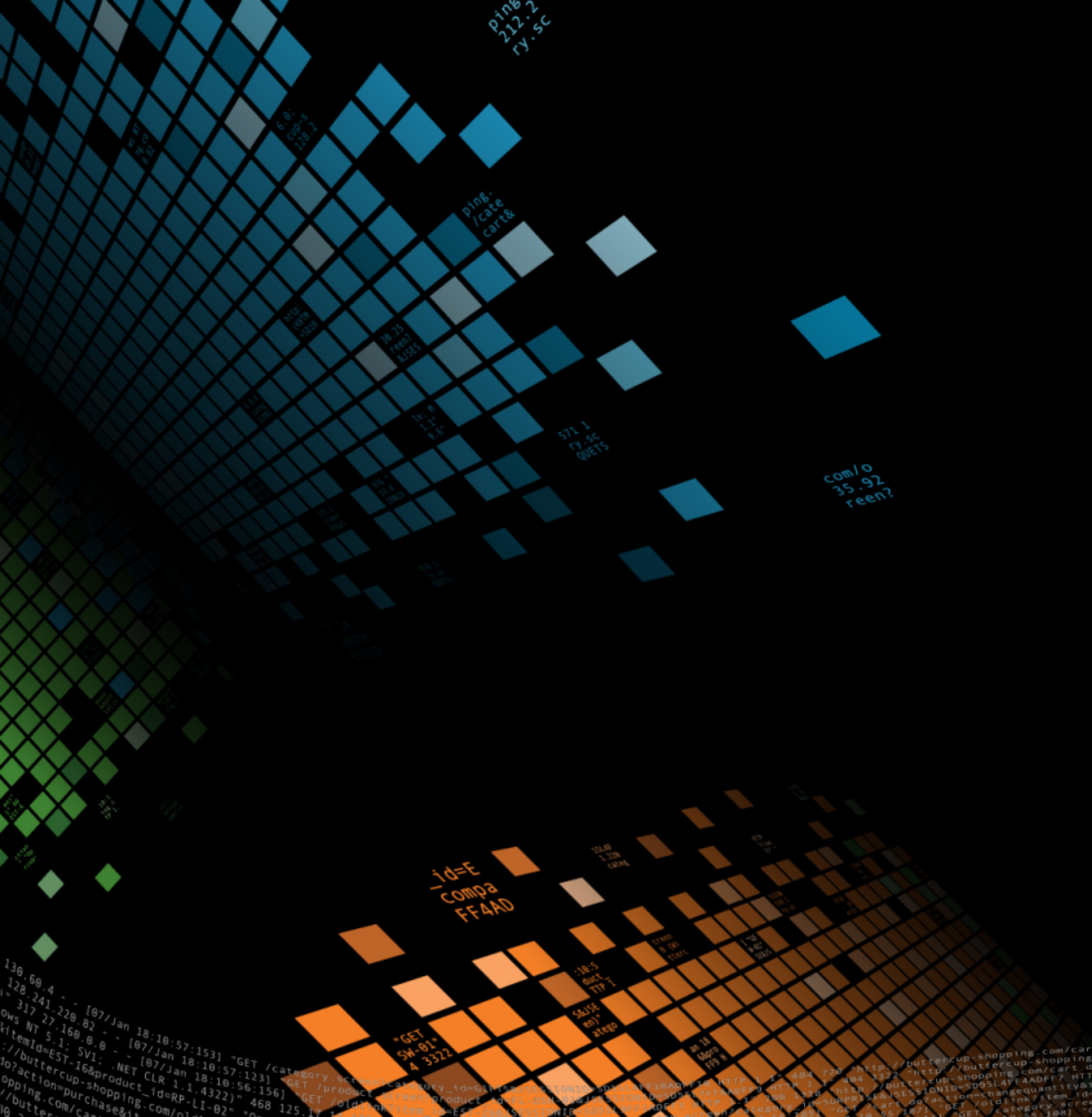
← Security Operations

IT Operations →



Objectives

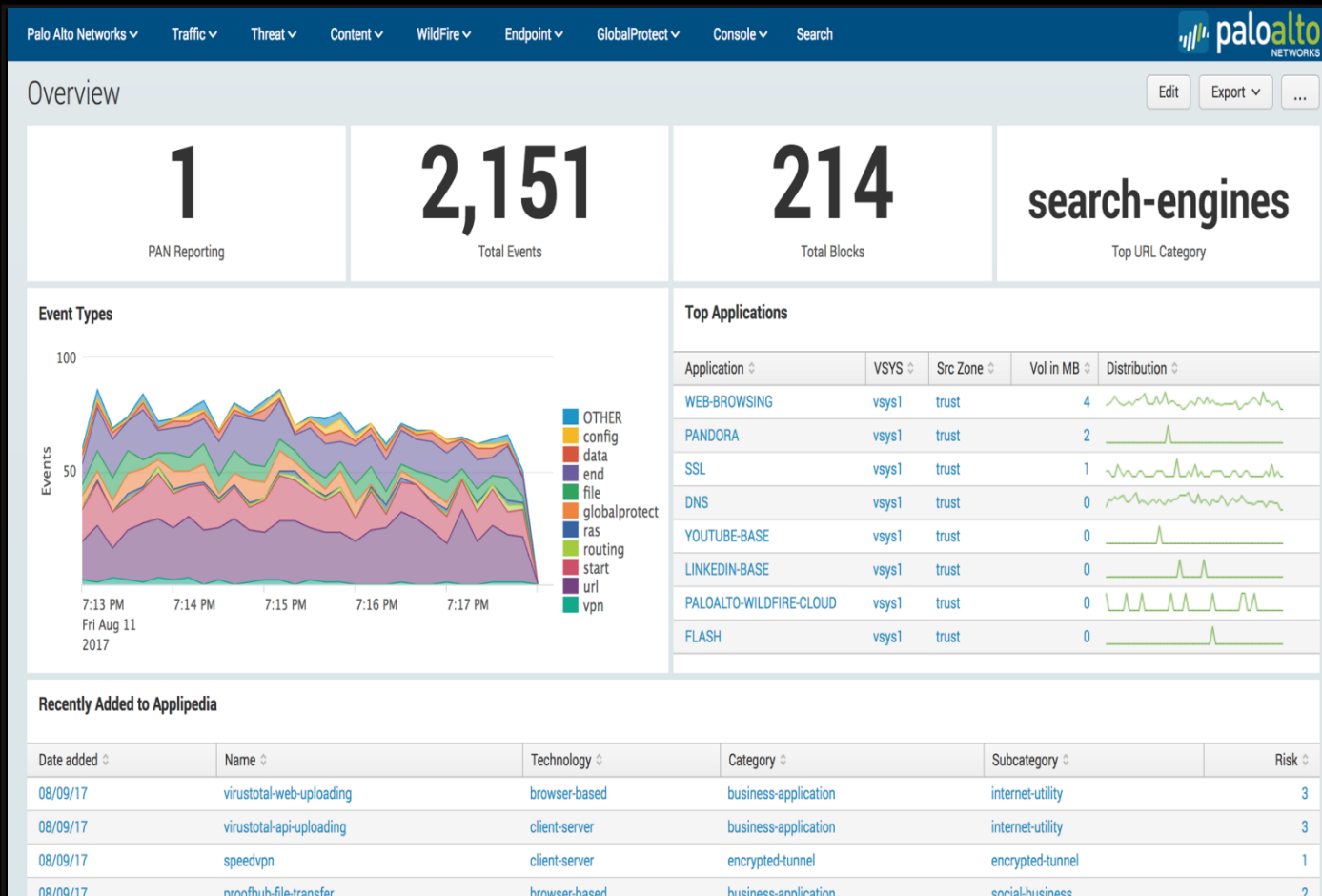
1. How to use Splunk for security investigations & IT troubleshooting
2. How to leverage the same data for different use cases
3. How to share IT & security insights with Splunk as a single pane of glass



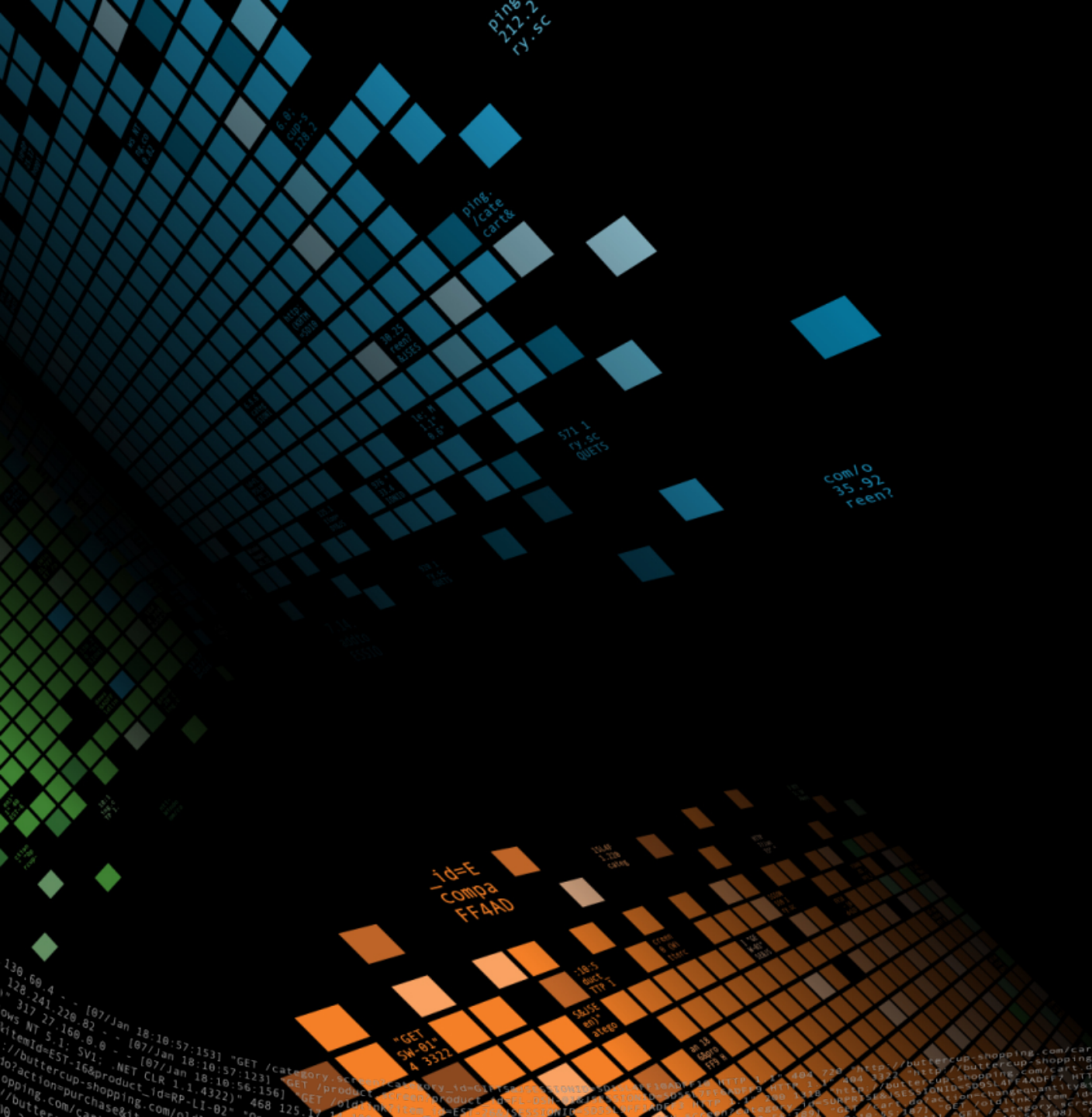
Security

Using Splunk to look at Firewall Data

Palo Alto Networks App for Splunk



- ▶ Demo
 - Traffic Data
 - Host
 - External
 - Internal



IT Operations

Section subtitle goes here

Using Splunk to Monitor Windows Infrastructure

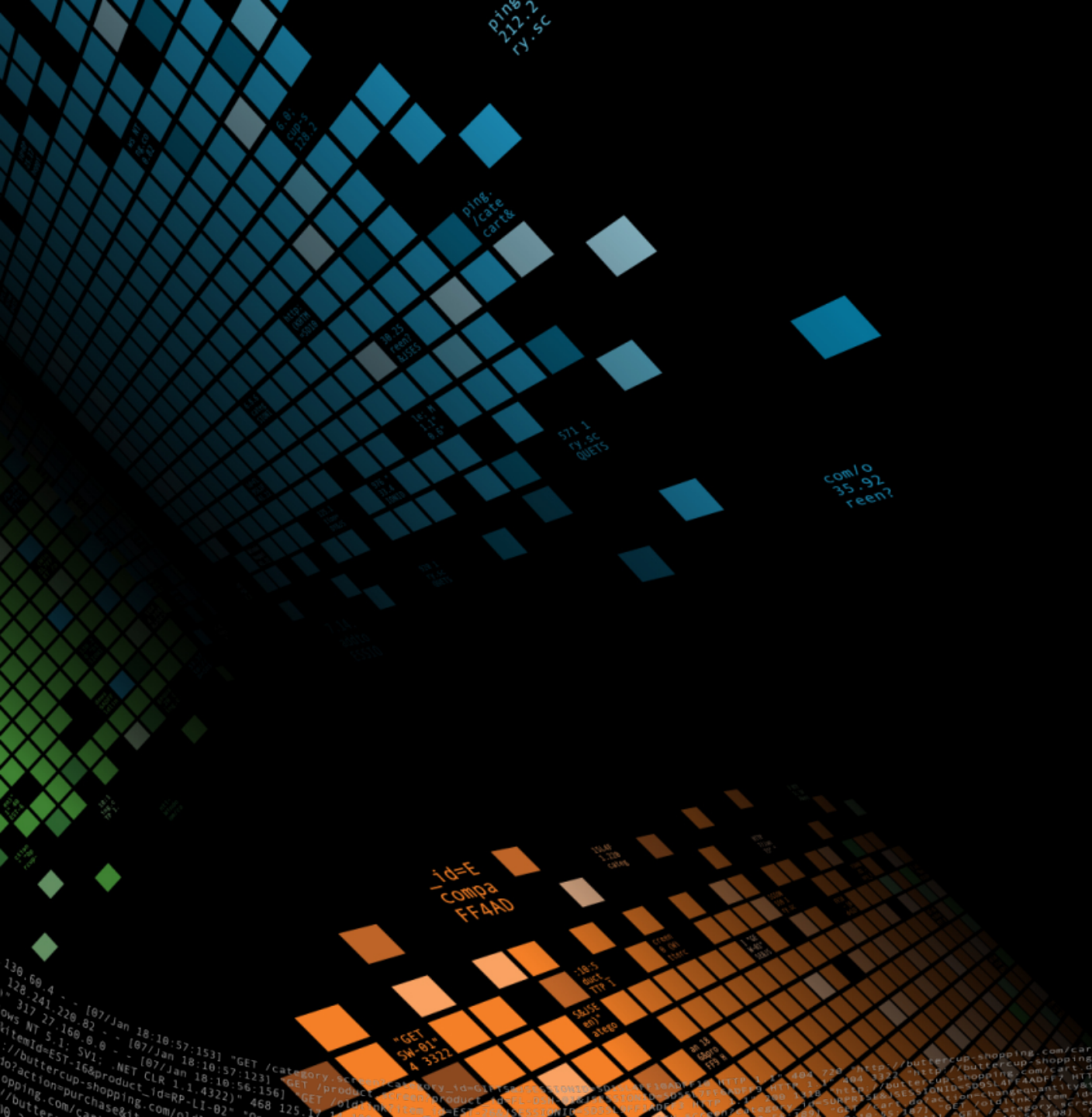
Splunk App for Windows Infrastructure

The screenshot displays the Splunk App for Windows Infrastructure interface. The main view is titled 'Anomalous Logons'. It features a navigation bar with 'Overview', 'Windows', 'Active Directory', 'Case Views', 'Search', and 'Tools and Settings'. The user is logged in as Robert Christian. The interface includes filters for Forest, Site, Domain, and Server, all set to 'All X'. A time range of 'Last 15 minutes' is selected. The main content area is divided into two panels: 'Users logging in from more than one Site' and 'Logons from Multiple Workstations'. The first panel contains a table with columns for Username, Domain, and Sites. The second panel shows 'No results found'. Below these panels is a section for 'Attempted Access to Disabled or Expired Accounts' with a table listing usernames, domains, IP addresses, sites, counts, workstations, and site domains.

Username	Domain	Sites
Bypass Security	SEATTLE	Default First Site-Name Default Second Site-Name
caibh	SEATTLE	Default First Site-Name Default Second Site-Name
domingo	SEATTLE	Default First Site-Name Default Second Site-Name

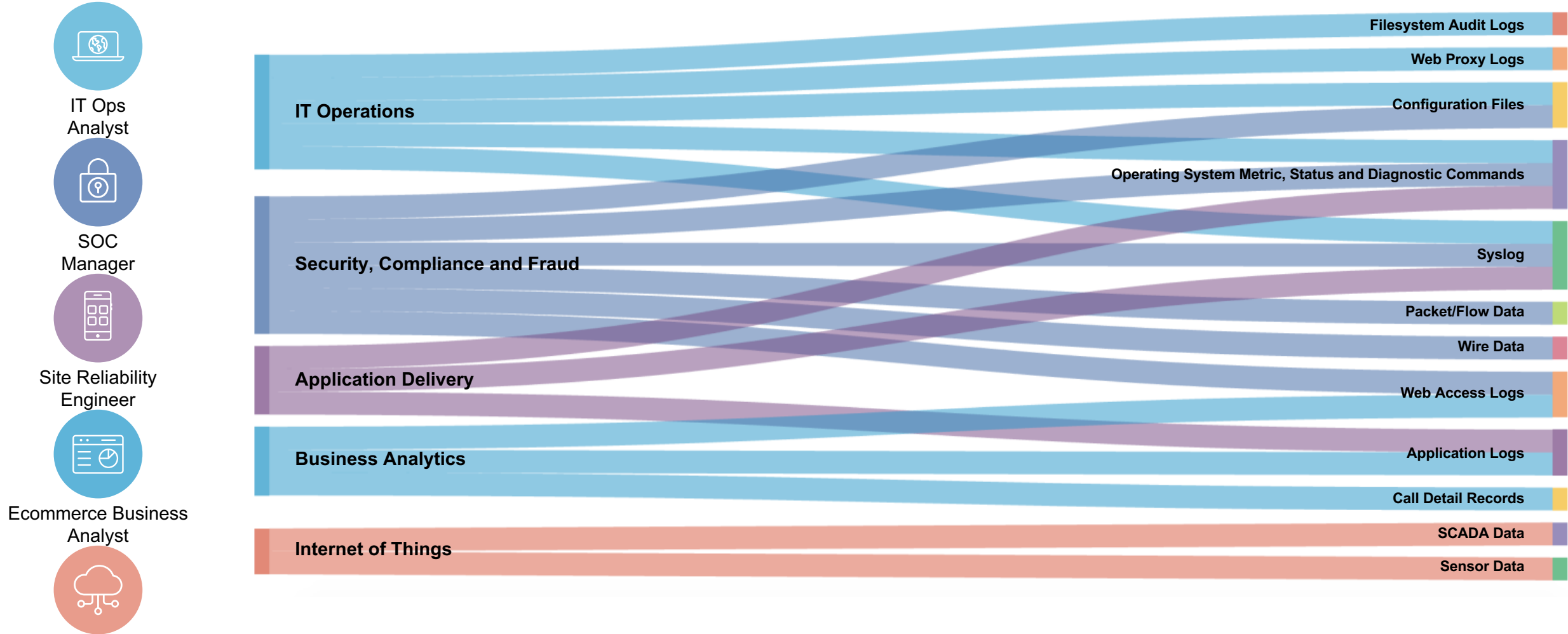
Username	Domain	IP Address	Site	count	Workstation	src_site_domain
Bypass Security	SEATTLE	172.16.80.191	Default Second Site-Name	1	SEATTLE:Bypass Security	SEATTLE
caibh	SEATTLE	172.16.80.24	Default Second Site-Name	1	SEATTLE:caibh	SEATTLE
domingo	SEATTLE	172.16.120.38	Default Second Site-Name	2	SEATTLE:domingo	SEATTLE
pete	SEATTLE	172.16.120.71	Default First Site-Name	1	SEATTLE:pete	SEATTLE
tevior	SEATTLE	172.16.120.84	Default First Site-Name	1	SEATTLE:tevior	SEATTLE

- ▶ Demo
 - Updates
 - Perfmon
 - Service availability



Joining Forces

Data Types Light Up Use Cases



IT Ops Analyst



SOC Manager



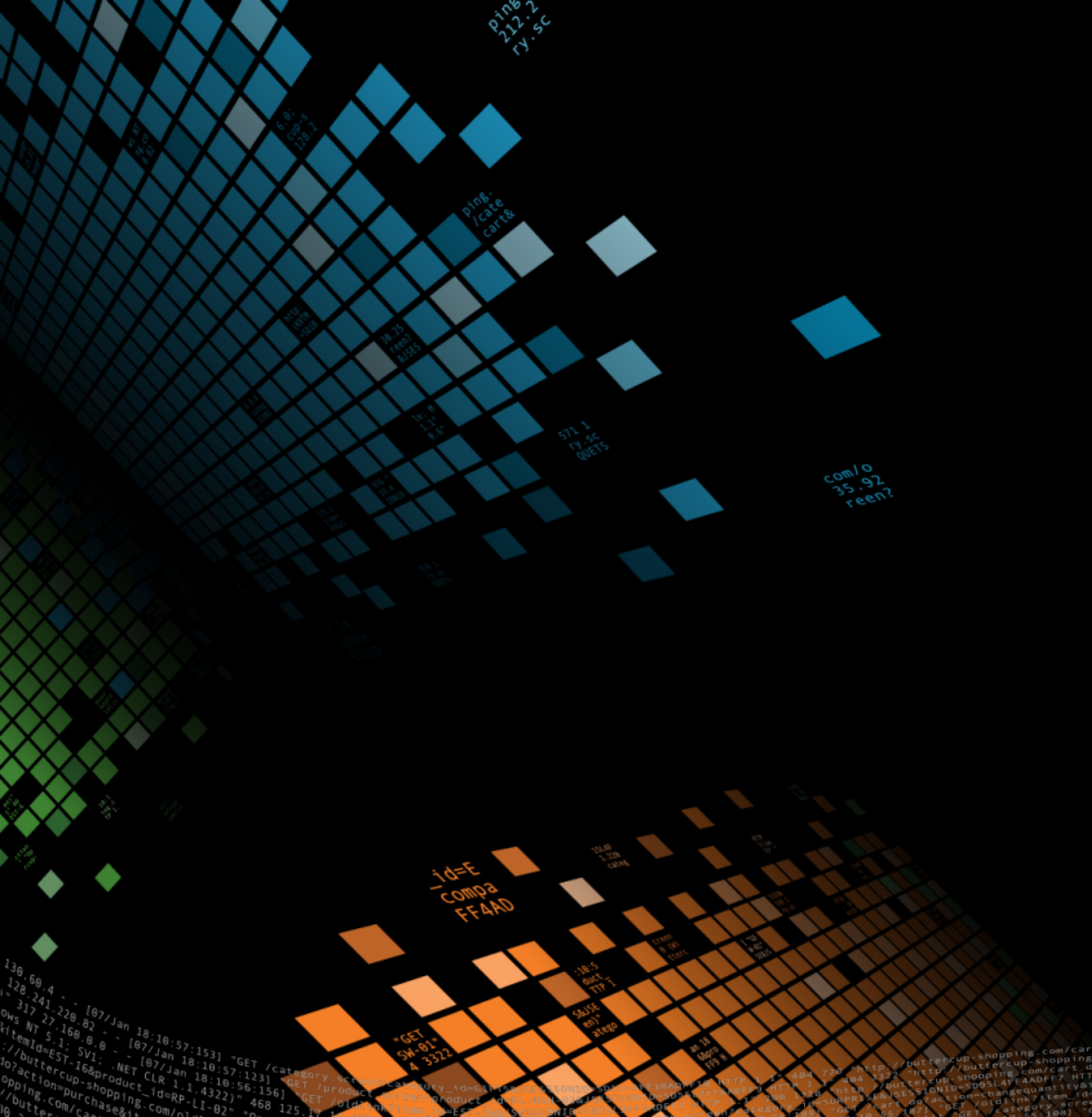
Site Reliability Engineer



Ecommerce Business Analyst



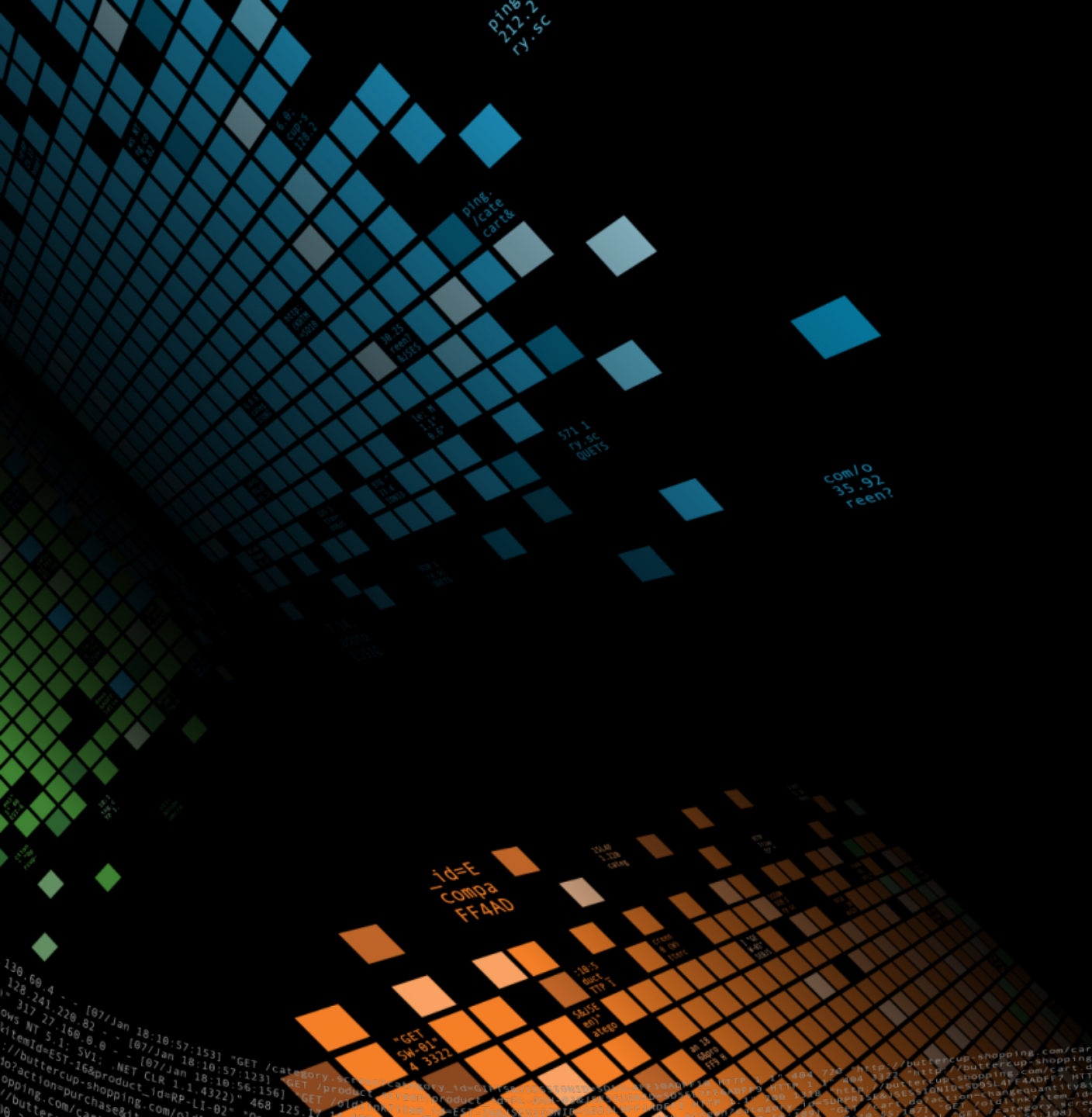
Manufacturing Engineer



Demo

End-to-End Visibility





Thank you!
