Machine Data Alchemy: Turning Digital Exhaust into Campus Gold

BA2766

Nitin Madhok - Executive Director Business Intelligence & Advanced Data Analytics | Clemson University

Matt Portnoy – Senior Sales Engineer | 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.

.conf19

splunk>

Matt Portnoy

Senior Systems Engineer | Splunk

Nitin Madhok

Executive Director Business Intelligence & Advanced Data Analytics | Clemson University

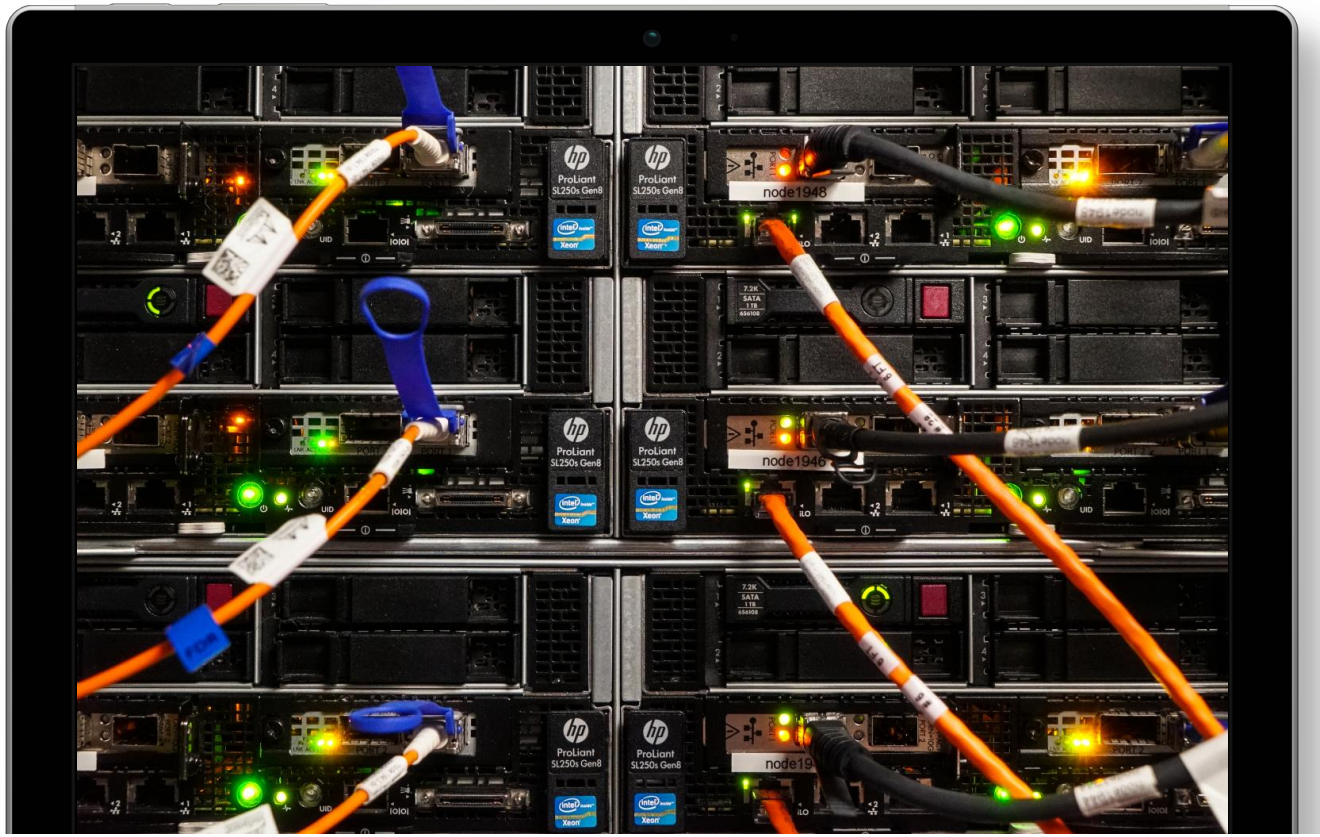
Clemson University

Second largest university by student population in South Carolina.

- 22,000 undergraduate and 5,000 graduate students
- 80 undergraduate majors and 110 graduate degree programs
- Current Division I Football National Champion, ranked #2 as of 10/10/2019. Twice in the last four years.

Some IT oriented numbers from 2018

One of the country's most selective public research (R1) universities



- 1.4 million unique network connections
- 37.6 petabytes hosted storage
- 8.9 million student print jobs
- 118.8 million Palmetto Cluster (HPC) compute hours
- Clemson's Palmetto Cluster exceeded 1 petaflop (1,000 teraflops) for the first time in late 2018, continuing its Top 5 rank in supercomputers at a United States public university

Some Challenges

- Little or no visibility of data in many areas, including operations, security, customer support
- Data is siloed so no cross group/department visibility
- Data being stored without being analyzed
- Data governance / Data access

Some Solutions

What was our journey?

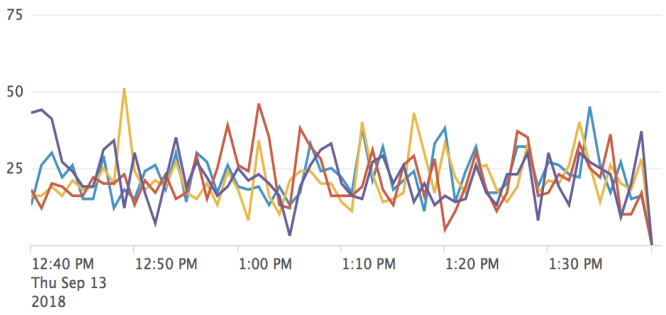
- What was implemented?
- Who was involved and what was the new process?
- Was the challenge met and achieve the desired outcome?

CCIT Support - Daily Stats

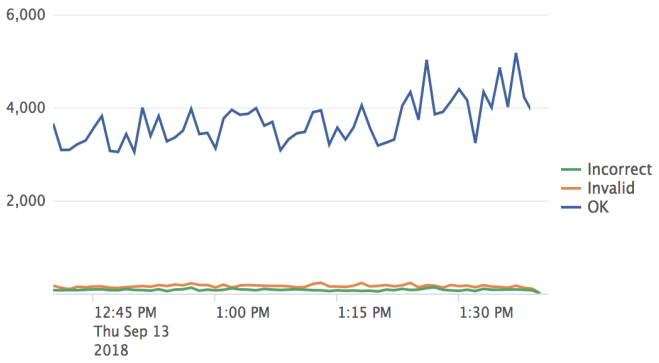
Export ...

Self-Service PW Resets	Lab Logins	Failed Drive Mappings	Folder Redirection Errors	Wi-Fi - Invalid User	Duo Enrollments	Duo Credits Used
19	54	0	0	0	7 → 0	3,267 ↘ -3,990

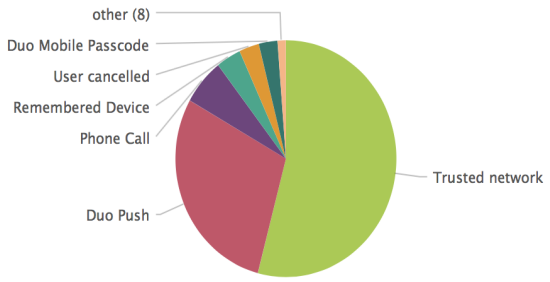
Shib Logins (60 min)



RADIUS Logins



Duo Auth Methods



Failed Shib Logins (60m)

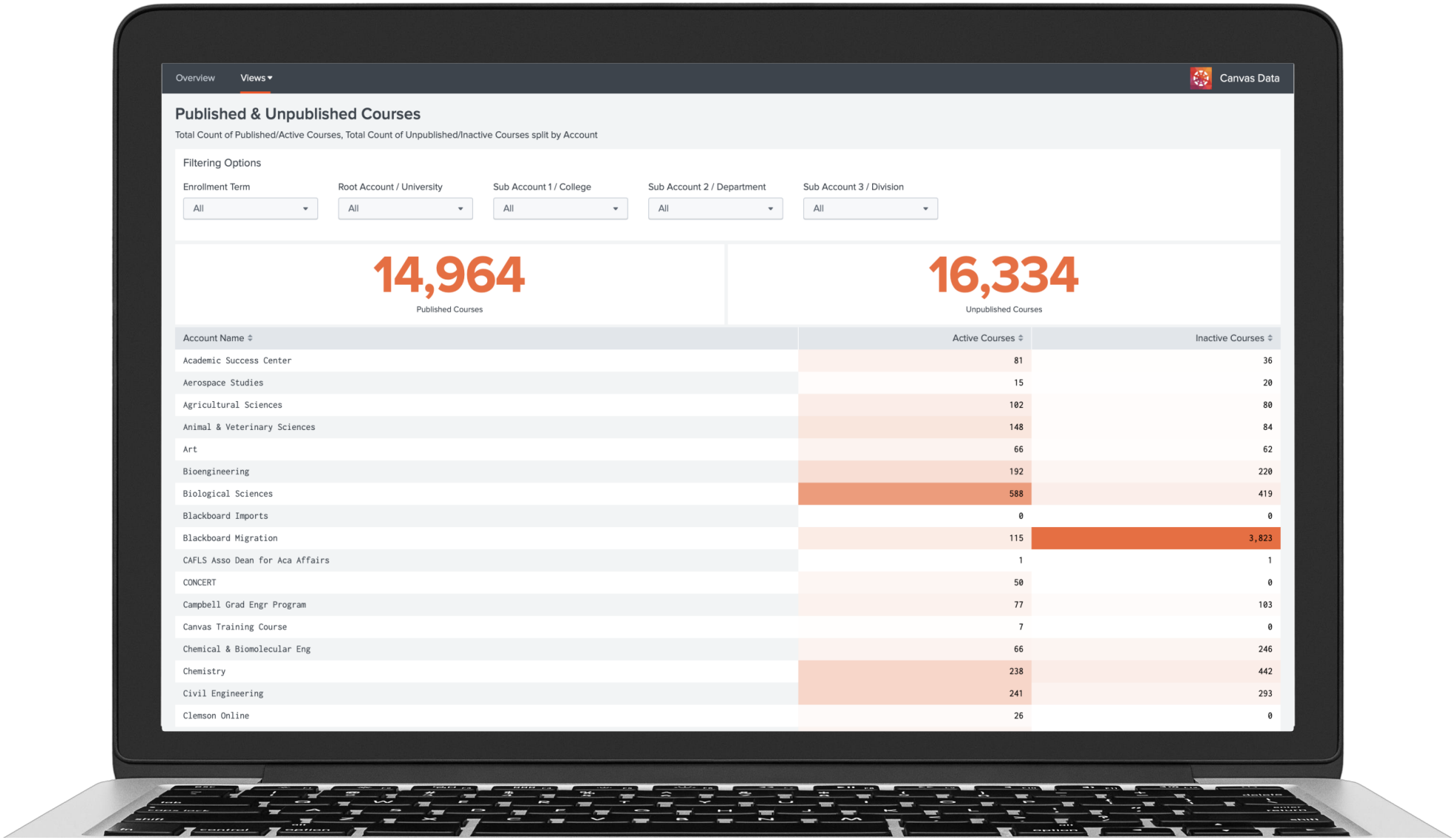
user	count	percent
s	6	4.000000
k	6	4.000000
v	5	3.333333
s	4	2.666667
k	4	2.666667
a	4	2.666667
f	3	2.000000
c	3	2.000000
c	3	2.000000
w	2	1.333333

Top Users with Failed Wi-Fi Logins (4 Hrs)

MAC Address	Username	Count
e4- -d8	k	10312
ec- -6e	a	792
d4- -94	p	669
90- -73	s	636
b4- -dc	b	596
40- -23	a	548
00- -85	t	537
cc- -43	m	527
0c- -2c	r	462
84- -4a	a	414

Top Telephony Users (7 Days)

username	count	percent
m	44	0.203018
a	44	0.203018
m	39	0.179947
m	37	0.170719
j	33	0.152263
c	33	0.152263
d	31	0.143035
s	30	0.138421
j	30	0.138421
s	28	0.129193



Overview Views Canvas Data

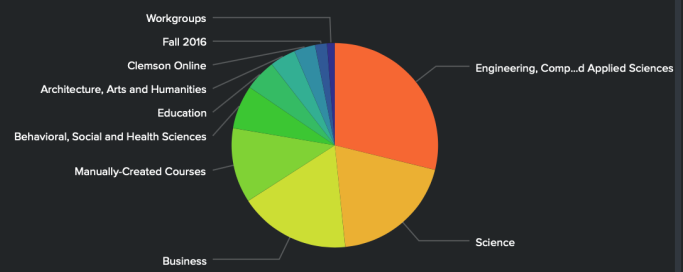
LTI Usage

Displays usage information for all LTI integrations/tools used within each college, department and course

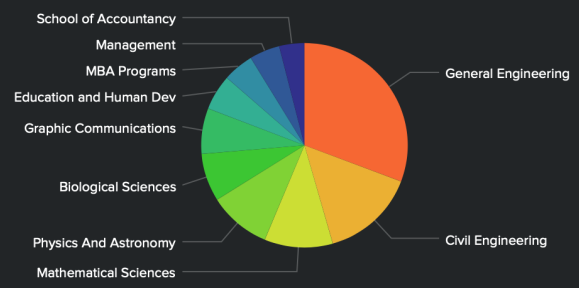
Filtering Options

Workflow State (Account): active
Root Account / University: All
Sub Account 1 / College: All
Sub Account 2 / Department: All
Sub Account 3 / Division: All
Enrollment Term: All
Workflow State (Course): All
Course Code/Name: All
LTI Integration/Tool: All

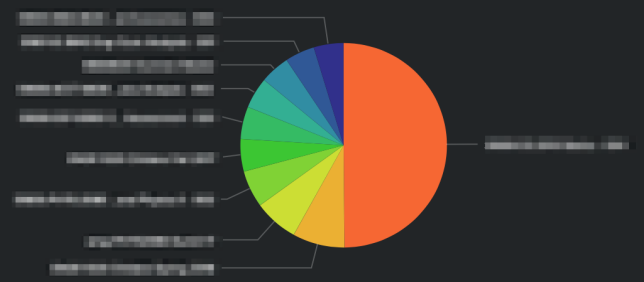
LTI Integration/Tool Usage by College (Top 10)



LTI Integration/Tool Usage by Department (Top 10)

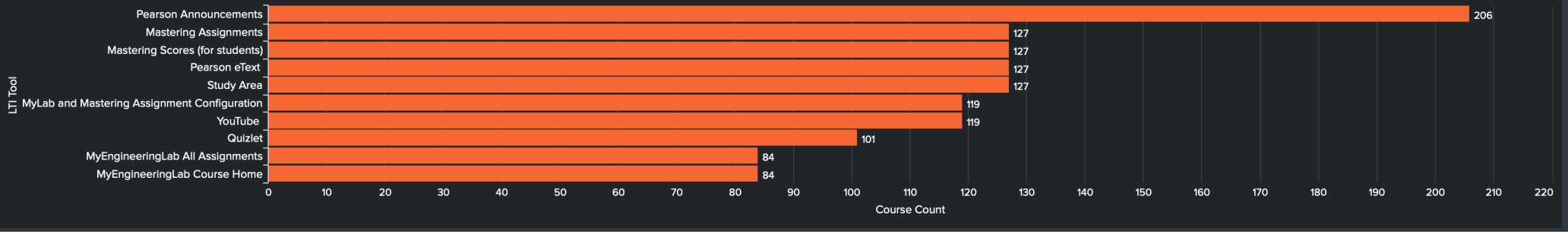


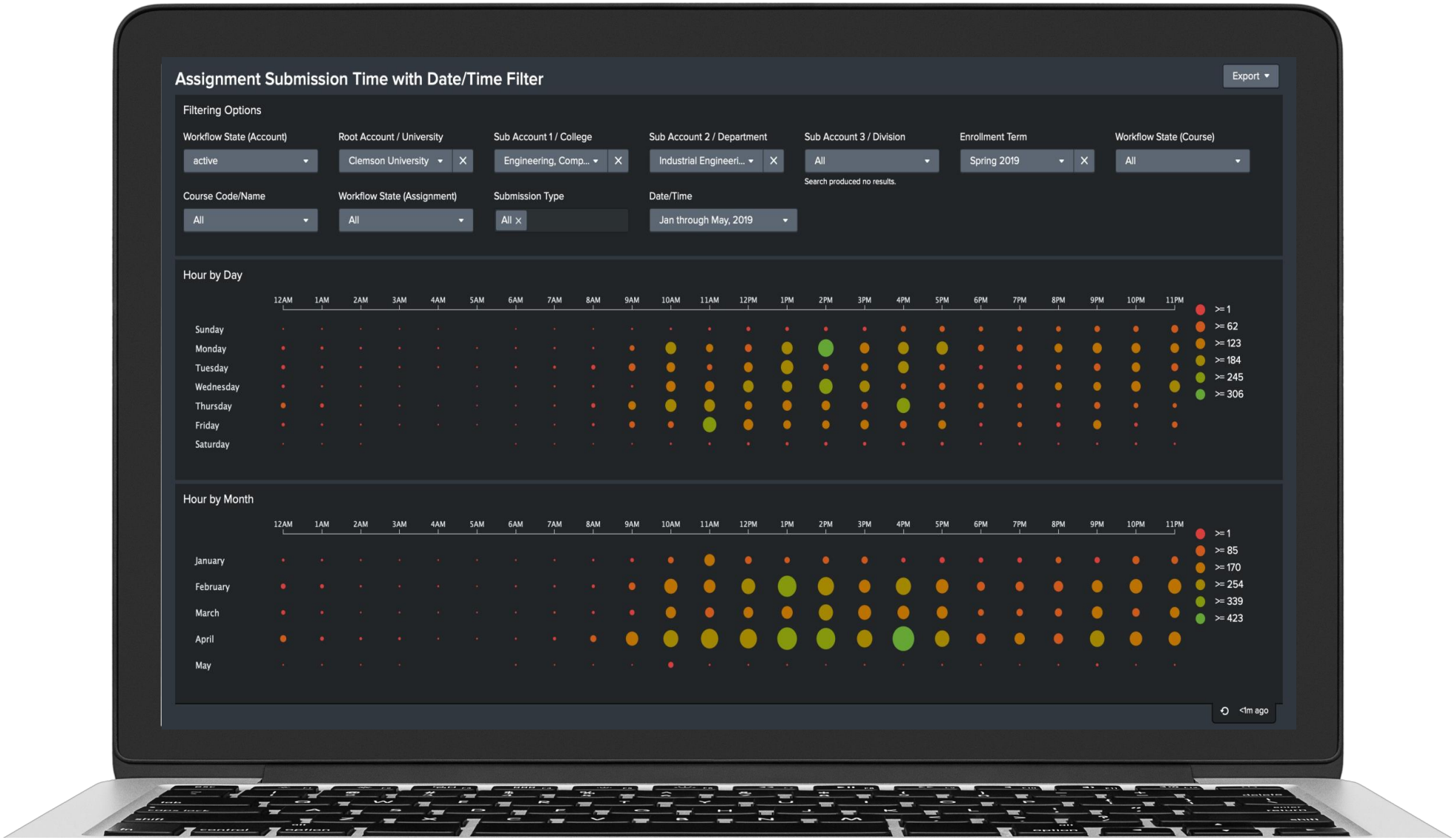
LTI Integration/Tool Usage by Course (Top 10)



LTI Integration/Tool Activations (Top 10)

Count represents number of courses utilizing the LTI integration/tool





Course Pageviews

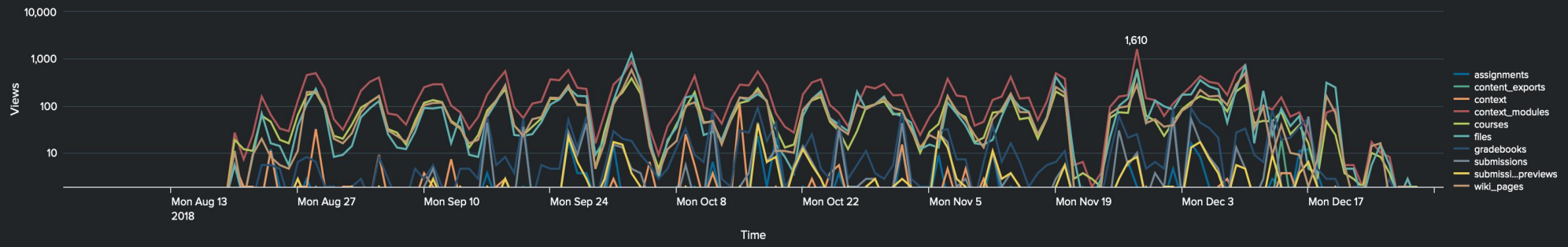
Displays the page views statistics for a selected course

Filtering Options

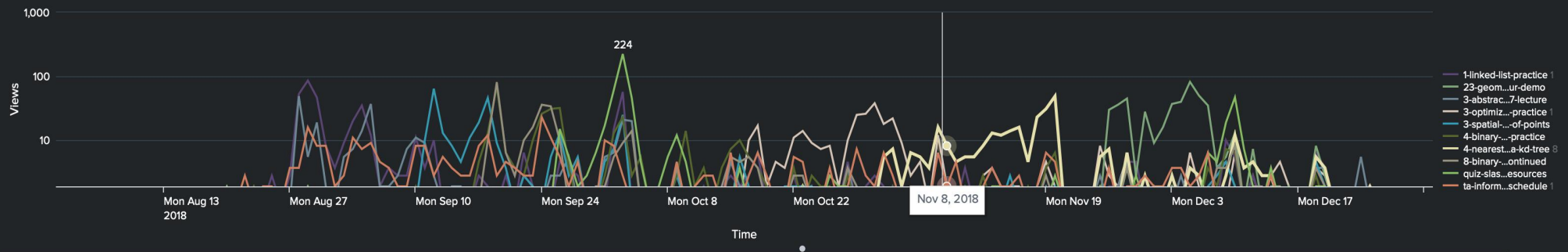
Workflow State (Account)	Root Account / University	Sub Account 1 / College	Sub Account 2 / Department	Sub Account 3 / Division	Enrollment Term	Workflow State (Course)
active	Clemson University	Engineering, Comp...	School of Computing	All	Fall 2018	All

Course Code/Name	Date/Time	Display Limit
[redacted]	Aug through Dec, 2018	Top 10

Course Pageviews



Wiki Page Views



6m ago

Threat Activity

Threat Group: All | Threat Category: All | Search: Threat Match Value | Last 24 hours | Submit | Hide Filters | Per-panel Filter

Edit

THREAT MATCHES	THREAT COLLECTIONS	THREAT CATEGORIES	THREAT SOURCES	THREAT ACTIVITY
Unique Count	Unique Count	Unique Count	Unique Count	Total Count
848 -13	5 0	5 0	13 -1	1.1k -15

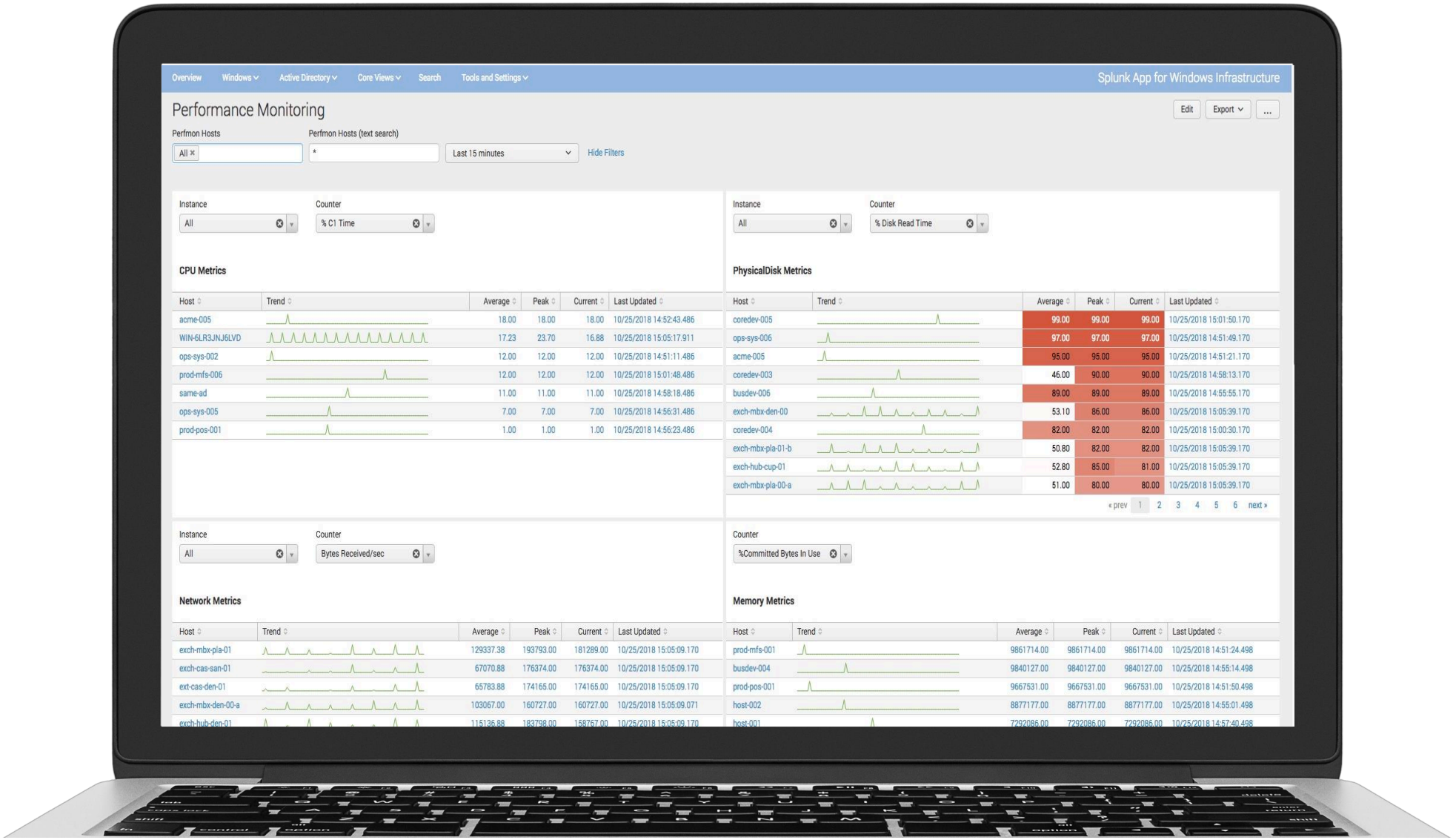
Threat Activity Over Time

Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		345	1049
file_intel	File Hash Matches File Name Matches Process Matches		24	39
certificate_intel	Certificate Common Name Matches Certificate Organization Matches Certificate Serial Matches		4	5

Most Active Threat Sources

source_id	source_path	source_type	count
emerging_threats_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv	csv	447
hijacked_ip_addresses	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/hijacked_ip_addresses.csv	csv	301
iblocklist_logmein	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	csv	283
mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_G_IOCs_No_OpenIOC.xml	stix	41
mandiant:package-190593d6-1861-4cfe-	/four/splunk/etc/apps/DA-ESS-	stix	5



Security Posture

Show Filters

Edit | Export | ...

Authentication Activity

Successes

869 ↗ 44

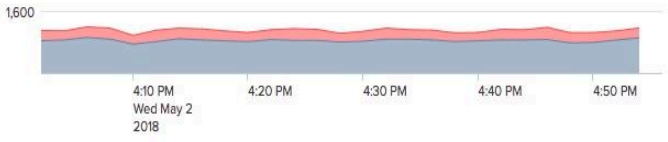
VS Last Hour

Failures

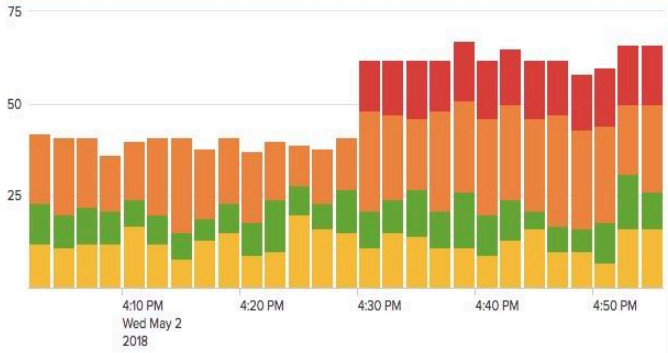
250 ↗ 10

VS Last hour

History



Notable Events



Network Activity

VPN Current Connections

5 → 0

vs Last Hour

Firewall Denies

808 → 0

vs Last Hour

Connection Capacity

Top Notable Events

Event	Severity	Frequency	count
SQL Injection Attack Detected	CRITICAL		200
Brute Force Access Behavior Detected	HIGH		168
High Volume of Traffic from High or Critical Host	HIGH		104
Insecure Or Cleartext Authentication	MEDIUM		98
High Number of Hosts Not Updating Malware Signatures	MEDIUM		97
Unroutable Host Activity	LOW		89
Expected Host Not Reporting	LOW		86
Anomalous Audit Trail Activity Detected	LOW		83
Recurring Malware Infection	HIGH		81
Excessive Failed Logins	HIGH		78

« prev 1 2 next »

Notable Events by Location

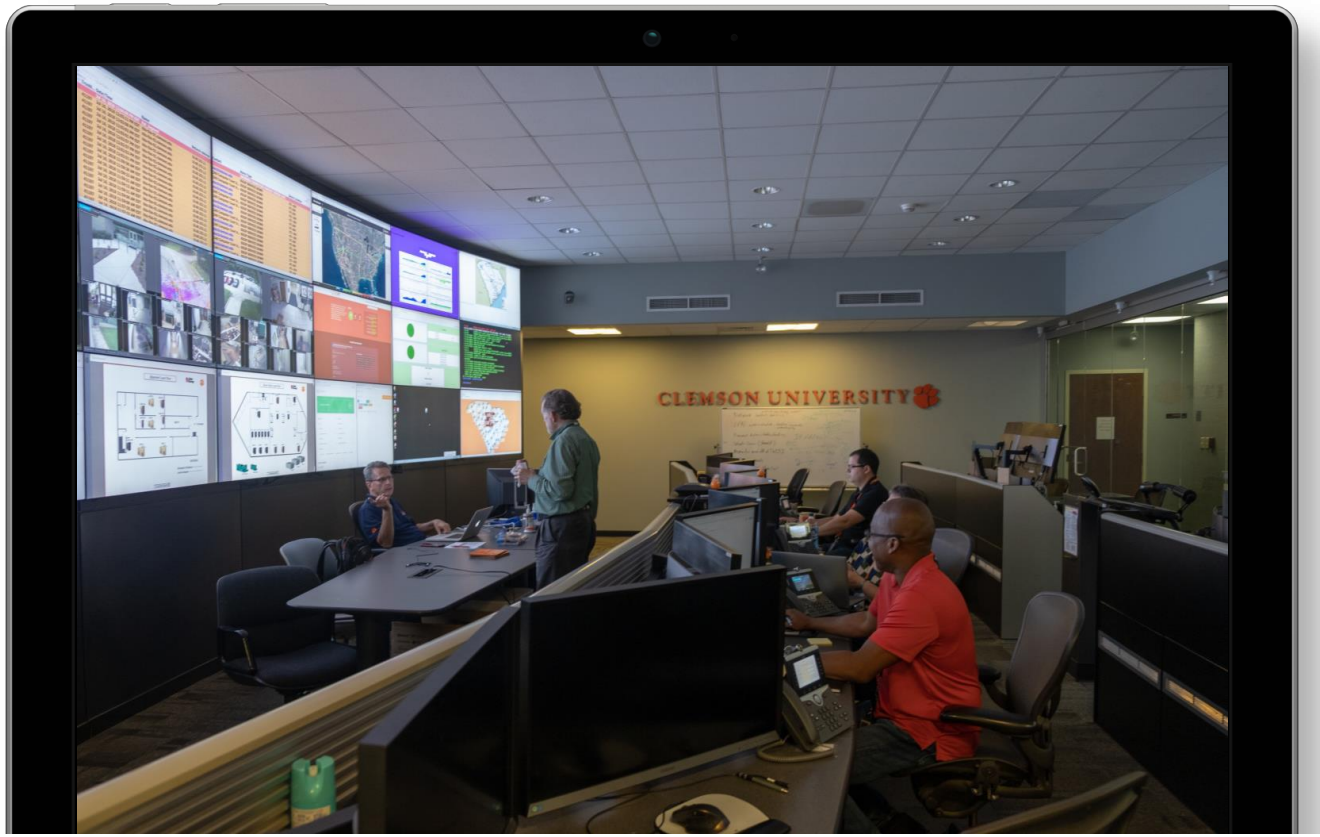
splunk> .conf19

Solutions Recap

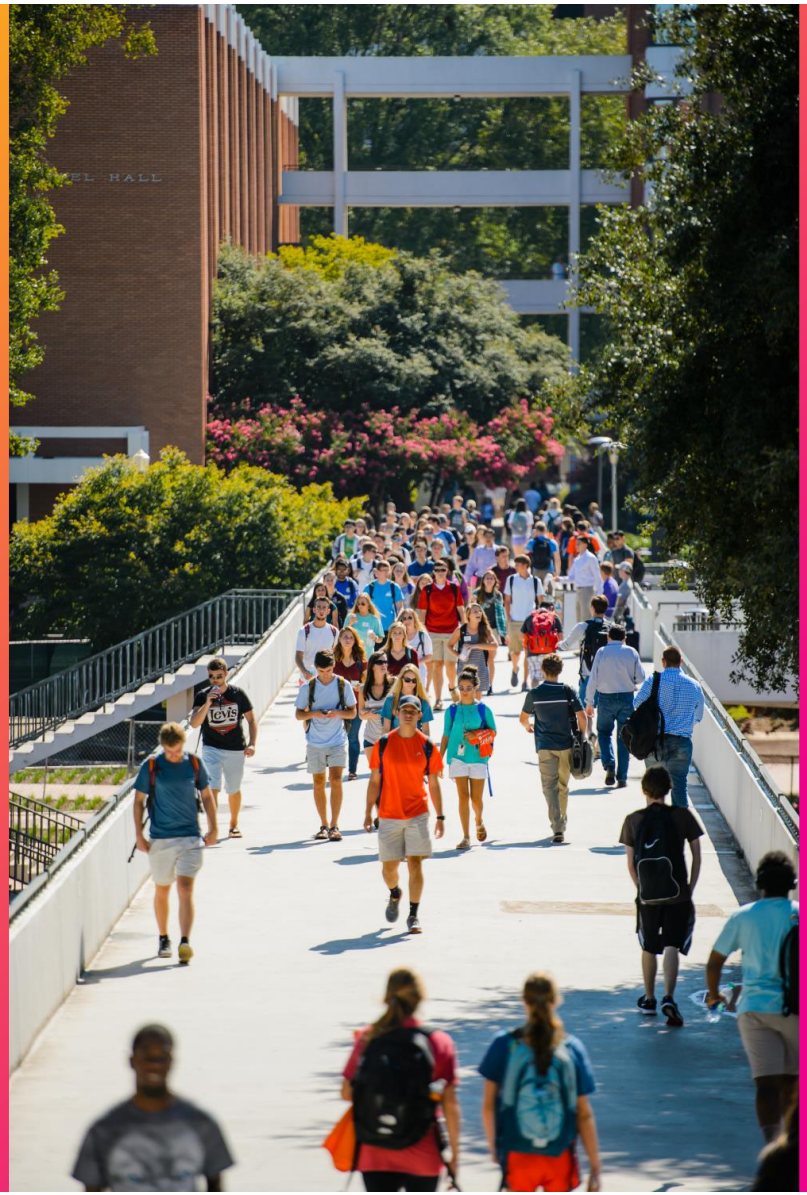
- Canvas
  - Insights into LMS activity and usage
- Security Operations
  - Flexible and proactive security posture
- Infrastructure Operations
  - Earlier warning for prevention
  - Faster root cause analysis
- Customer service
  - Increased visibility for more rapid resolutions

Outcomes

For these three use cases



- How did this support or enhance the mission?
- Cost savings or other benefits?
- Unanticipated benefit / side effects?



On the Horizon

What is next?

- Enhancing these solutions?
- Other areas of interest?

Key Takeaways

These outcomes are achievable!

1. Executive buy-in is critical to success.
2. Success also requires input from people who understand the data.
3. Data can be offered to more groups without providing them access to the core applications.

Q&A

Nitin Madhok - Executive Director Business Intelligence & Advanced Data Analytics | Clemson University

Matt Portnoy – Senior Sales Engineer | Splunk

.conf19

splunk>

splunk>

Thank You!