splunk> .conf2017

Taking Splunk inside the Classroom

Automated Grading with Splunk

Ryan O'Connor | Splunk Consultant, Adjunct Professor

September 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> .conf2017

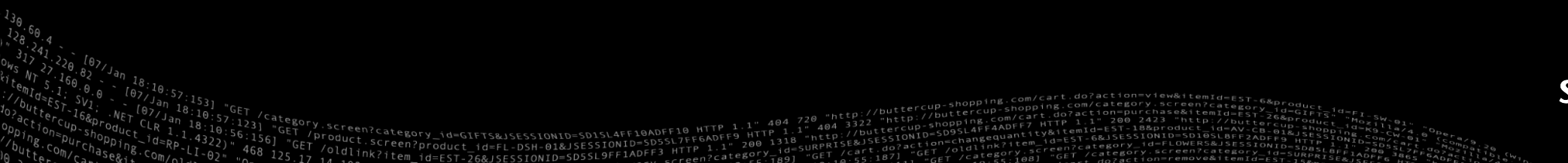
Who Am I?

- Adjunct Professor at the University of Connecticut (http://business.uconn.edu)
- Splunk & Security Consultant for Hurricane Labs (https://hurricanelabs.com/)
- Master's Degree in Business Analytics and Project Management from the University of Connecticut (http://msbapm.business.uconn.edu/)
- Splunk Certified Consultant II/Splunk Certified Sales Engineer III (https://www.splunk.com)

splunk> .conf2017

Why Am I Here?

- Solved a unique business problem in my role as a professor
- Share some experience I've had with Big Data inside the classroom
- Give you new ways to think about using Splunk
- Give you some strategies that might aid you in implementing business and security initiatives



splunk> .conf2017

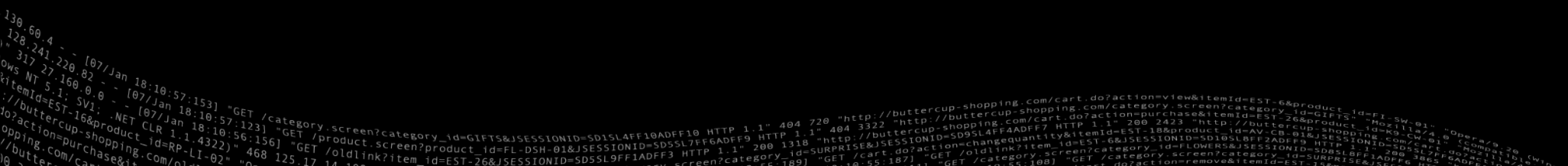
Business Problem

- Teach students about Big Data using emerging technologies
- Leverage Big Data Applications to provide valuable course content
- Ensure I taught the course in an efficient manner

splunk> .conf2017

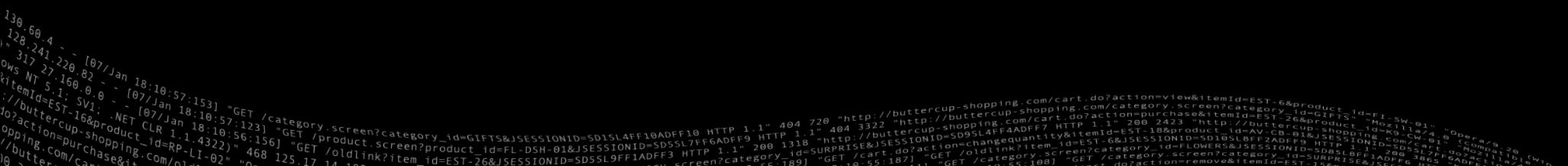
Questions I wanted to answer

- When did a student start the project?
- When was a student having technical trouble with the project?
- How long did it take for a student to complete the project?
- Do I need to modify or increase resources on these VM's?
- What can I do to improve the project next year?



Why Is This Problem Significant?

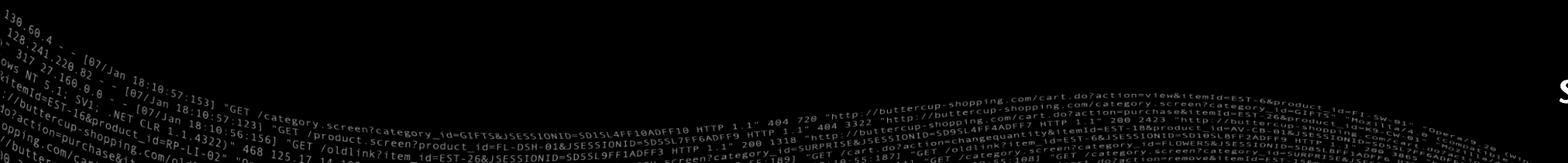
- For better or for worse, education in 2017 is a business problem
- Students are paying significant amounts of money for their education - they are going to want to get the most out of it
- For students to get more out of their courses, we need to spend less time with technology “overhead” and more time teaching
- In fast emerging fields like Big Data, departments that can teach concepts effectively and efficiently are more likely to be successful



splunk> .conf2017

Network Design and Applications

- The course that I am focusing on here is “Network Design and Applications”
- Previously taught by another professor
- The content was great, however it was dated - the syllabus was last updated 2 years prior to me teaching the class
- Professor left the University with no knowledge transfer



Example - “Password Project”

The “Network Design and Applications” course required a project simply titled the “Password Project”

Setbacks included:

- Undocumented project parameters
- “Institutional Knowledge”
- Fast approaching deadline

Important! - This course was closely being watched by department heads

Let's Start With Documentation

How was this project created?

SQL Query to get list of students	Generate Virtual Machine Names based on Student List	Create Folder for each user	Apply Required Permissions	Deploy Virtual Machines from Template	Customize Hostnames

Really great process by the IT Department at the UConn School of Business (HUGE Thank you to Christopher Zissis, Christopher Buckridge, and Chris Hewitt at UConn. Also to Rob Reed at Splunk for guidance on the course)

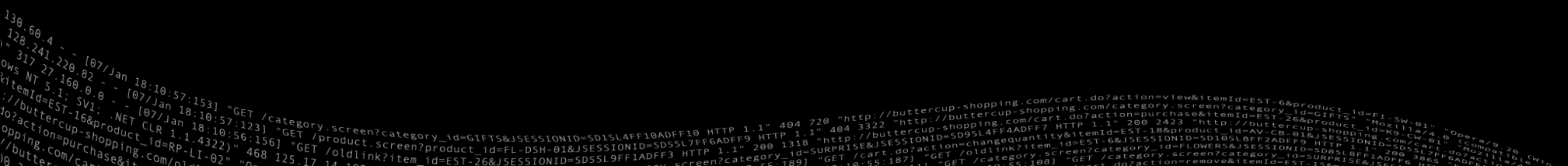
Process generated 2 VM's per student, totaling 72 VM's plus an additional File Server.

72 VM's were running with limited visibility into what was going on

splunk> .conf2017

How Can I Solve This Problem?

- Splunk!
- Splunk offers real-time analytics
- With schema-on-the-fly, Splunk can parse data quickly
- Splunk can store data for as long as I want



splunk> .conf2017

Inserting Splunk Into the Picture

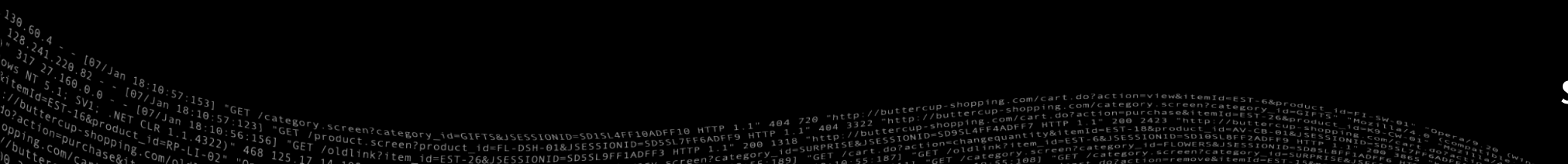
SQL Query to get list of students	Generate Virtual Machine Names based on Student List	Create Folder for each user	Apply Required Permissions	Deploy Virtual Machines from Template	Customize Hostnames

I was able to add Splunk into a VM Template by using the following instructions:

http://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Makeauniversalforwarderpartofahostimage

This simple process allowed me to install a forwarder on all 72 of the student VM's

Once that forwarder was installed, I could manage it using a Deployment Server to collect any data I needed



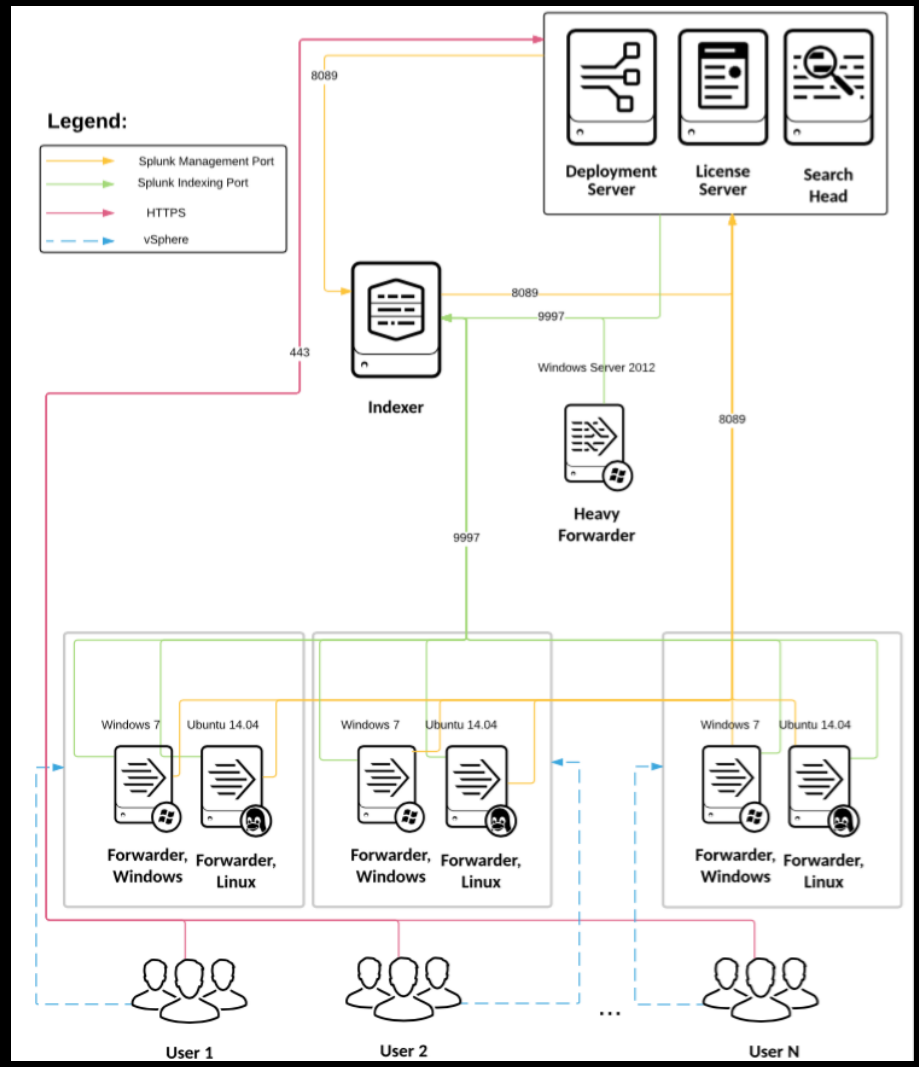
Documentation With Splunk

Splunk Infrastructure:

- 2 Ubuntu Servers

Student Systems:

- 36 Windows
- 36 Ubuntu
- 1 File Server



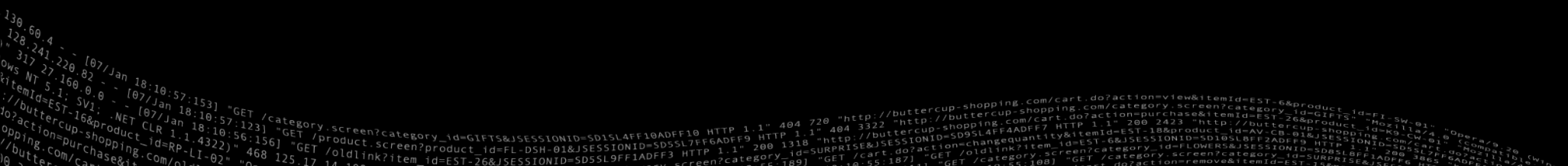
splunk> .conf2017

Collecting Data

How Did I Answer My Questions?

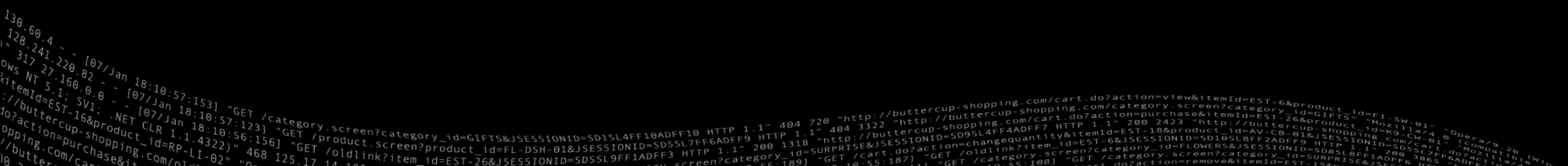
By collecting the following data from these machines I could begin to answer questions:

- Performance Data
- Security Logs
- Application Logs (ophcrack, windows process monitoring)
- User-generated data - custom file formats

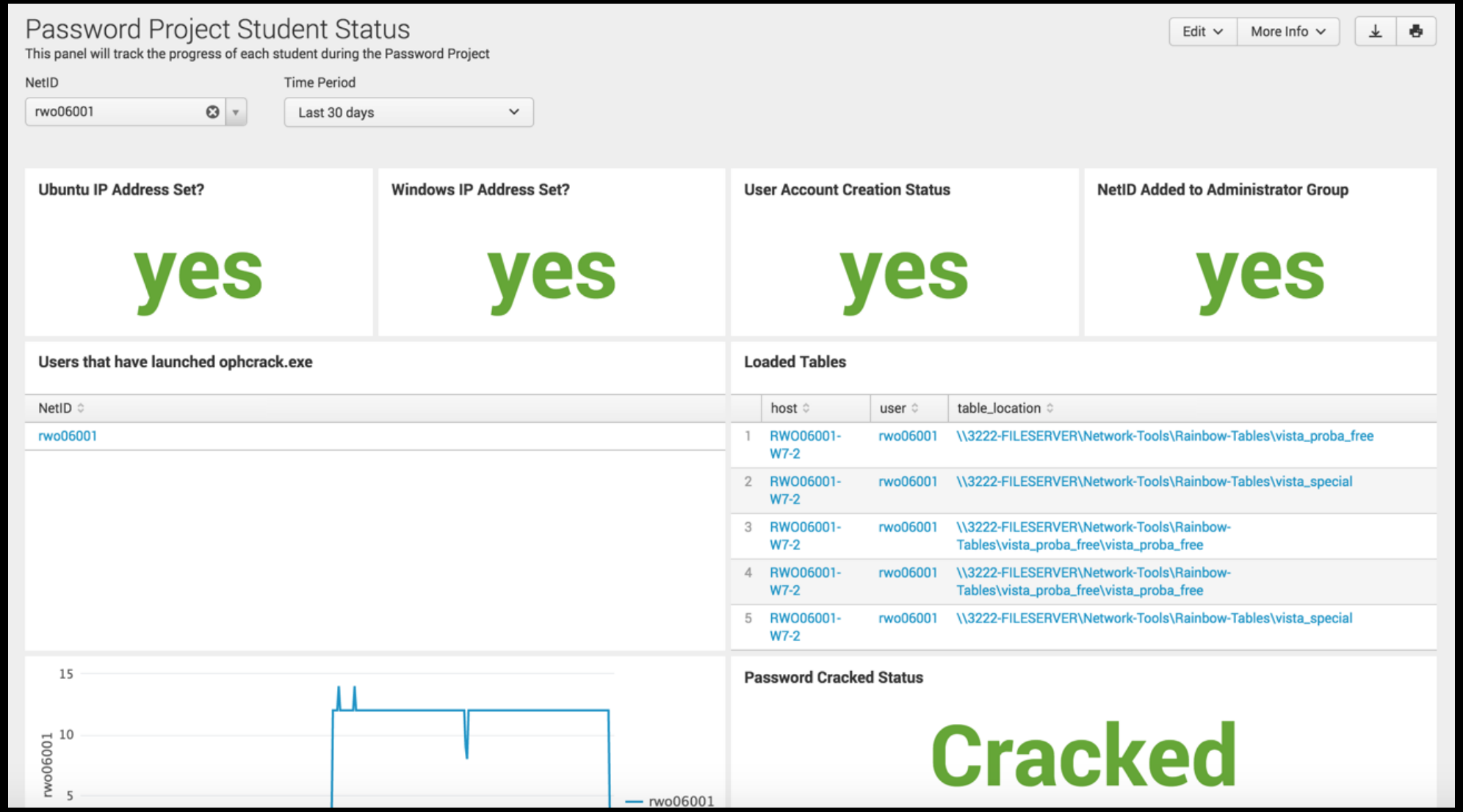


Creating a project that worked

- With Splunk in place, I was able to create a project that I felt made sense
- I was able to run through cracking a windows password a number of times and see what kind of logs were generated in Splunk
- With that data, I developed a project that not only taught students something, but could be parameterized and quantified with data

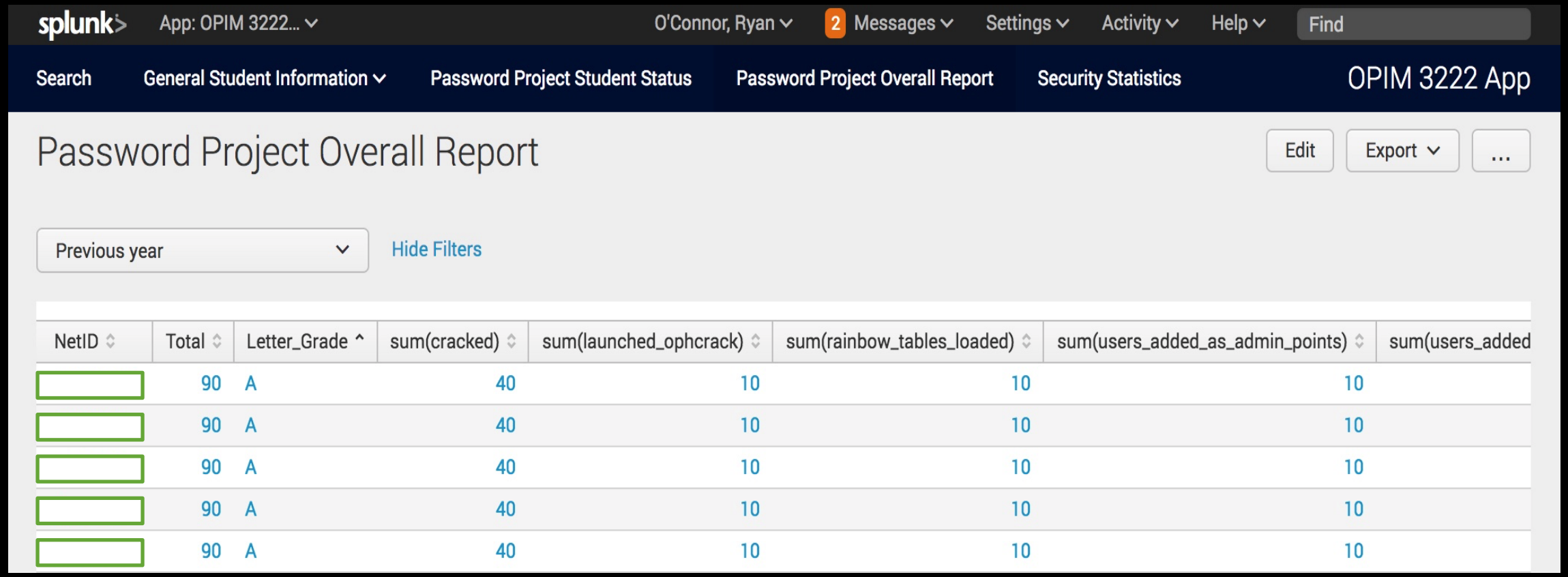


Building Dashboards



splunk> .conf2017

Automated Grading

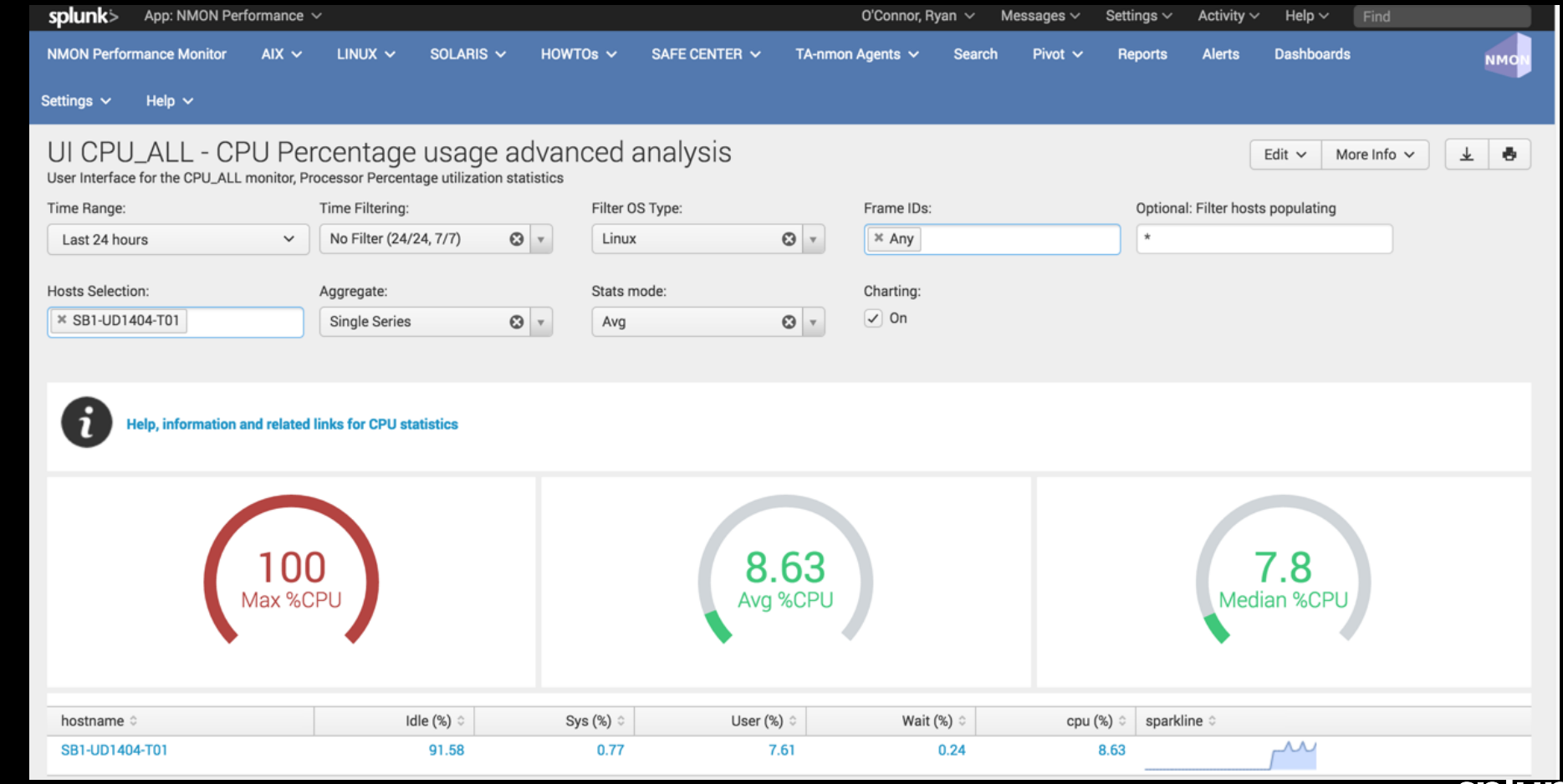


NetID	Total	Letter_Grade	sum(cracked)	sum(launched_ophcrack)	sum(rainbow_tables_loaded)	sum(users_added_as_admin_points)	sum(users_added
	90	A	40	10	10	10	
	90	A	40	10	10	10	
	90	A	40	10	10	10	
	90	A	40	10	10	10	
	90	A	40	10	10	10	

splunk> .conf2017

Monitor Performance Data

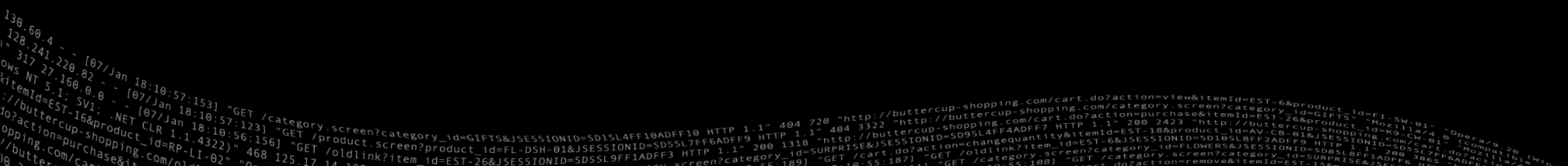
CPU Usage and other Performance Metrics can tell us if students are utilizing VM's



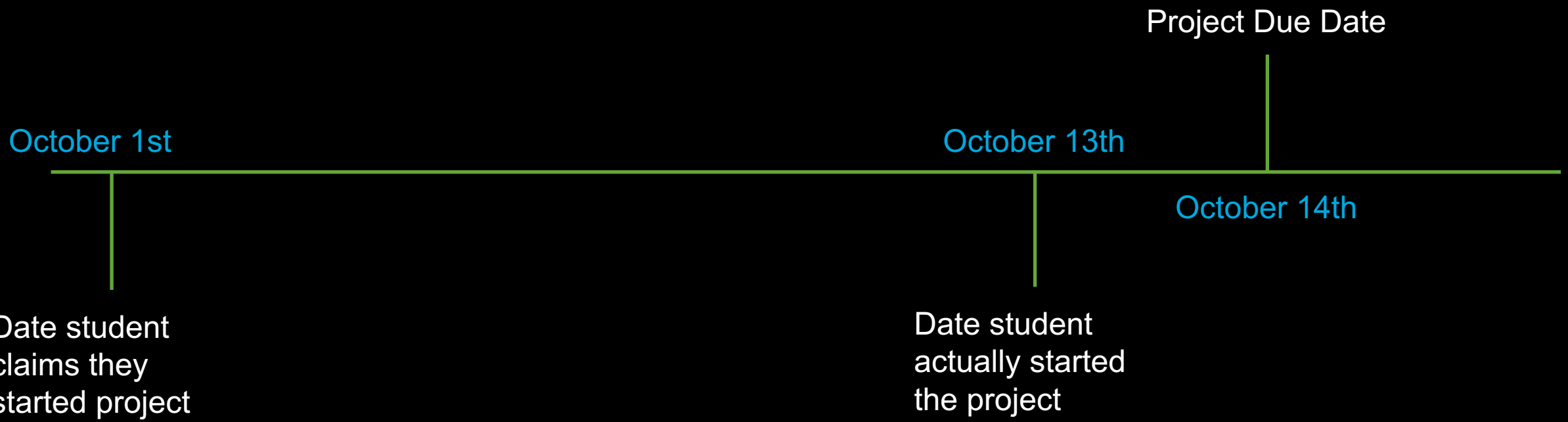
splunk> .conf2017

Questions I was able to answer

- When did a student start the project?
- When was a student having technical trouble with the project?
- How long did it take for a student to complete the project?
- Do I need to modify or increase resources on these VM's?
- What can I do to improve the project next year?

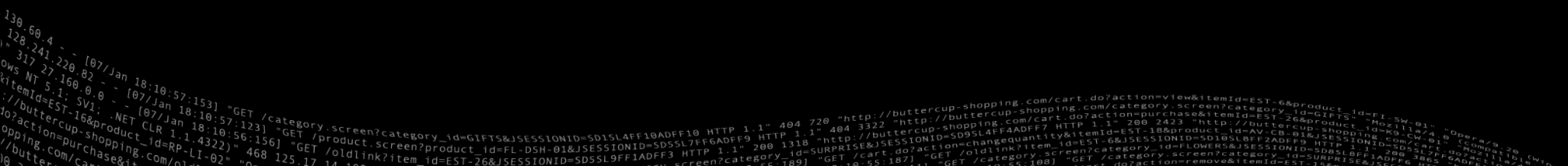


Example: Answering Questions



Thank You

Any Questions?



splunk> .conf2017