UBA Tunes Down the Volume at Shentel

John Decker | IT Security Analyst

Brian Kissick | IT Security Analyst

October 2018 | Version 1.8

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> .conf18

Agenda

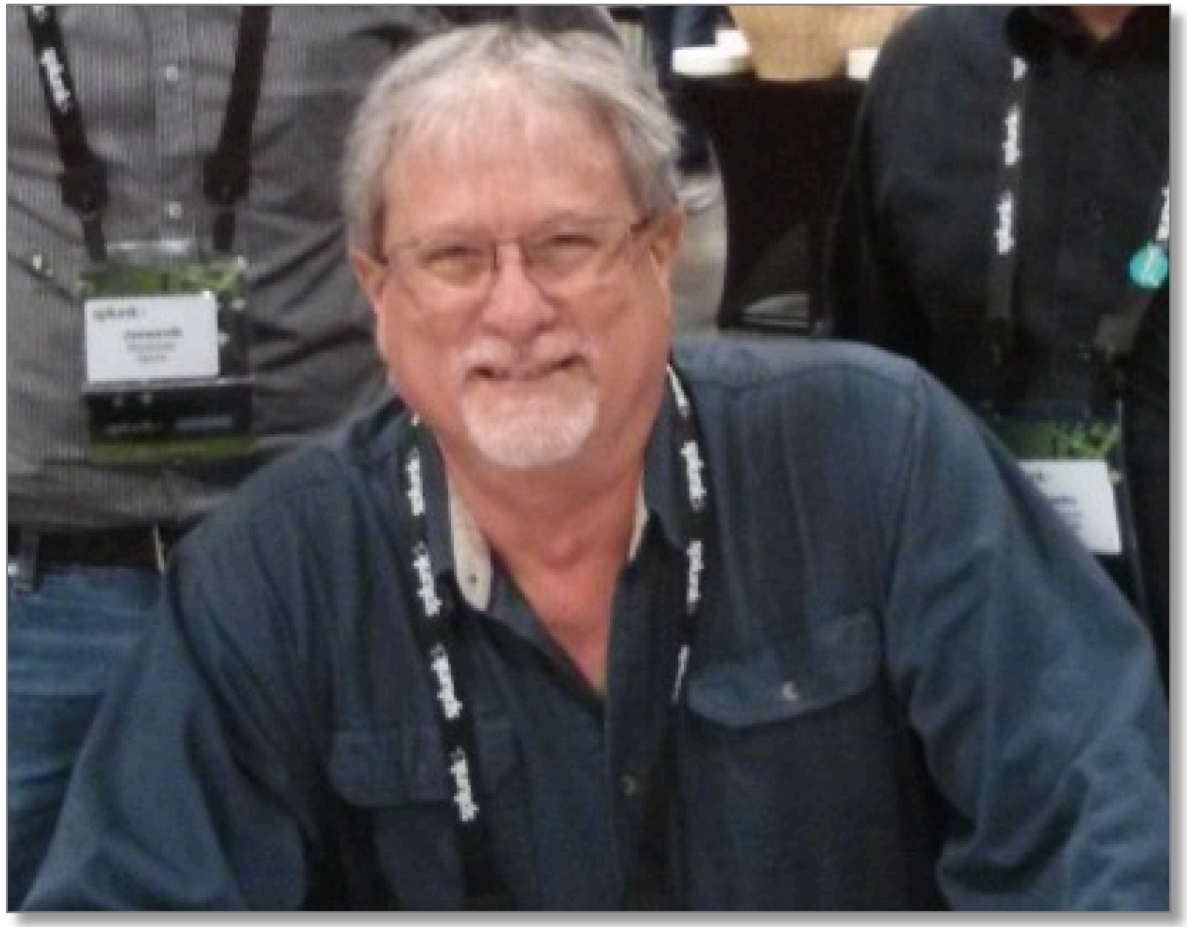
1. Speaker & Company Overview
2. Challenges
3. Initial Deployment
4. Where We Are Now
5. Next Steps

SHENTEL®
Always connected to you

John Decker

IT Security Analyst

- 20 Years in IT and IT Security
- 4.5 Years at Shentel
- Prior experience with Booz Allen, Virginia Beach Public Schools, and Regent University
- CISSP (and some other letters)
- BS in Information Security
- Love Playing my Guitars!



SHENTEL®
Always connected to you

Brian Kissick

IT Security Analyst

- 15 Years in IT/Security
- Over 15 Industry Standard Certifications
- B.S in Information Technology
- M.S in Information Security & Assurance
- I am a Gamer

splunk> .conf18

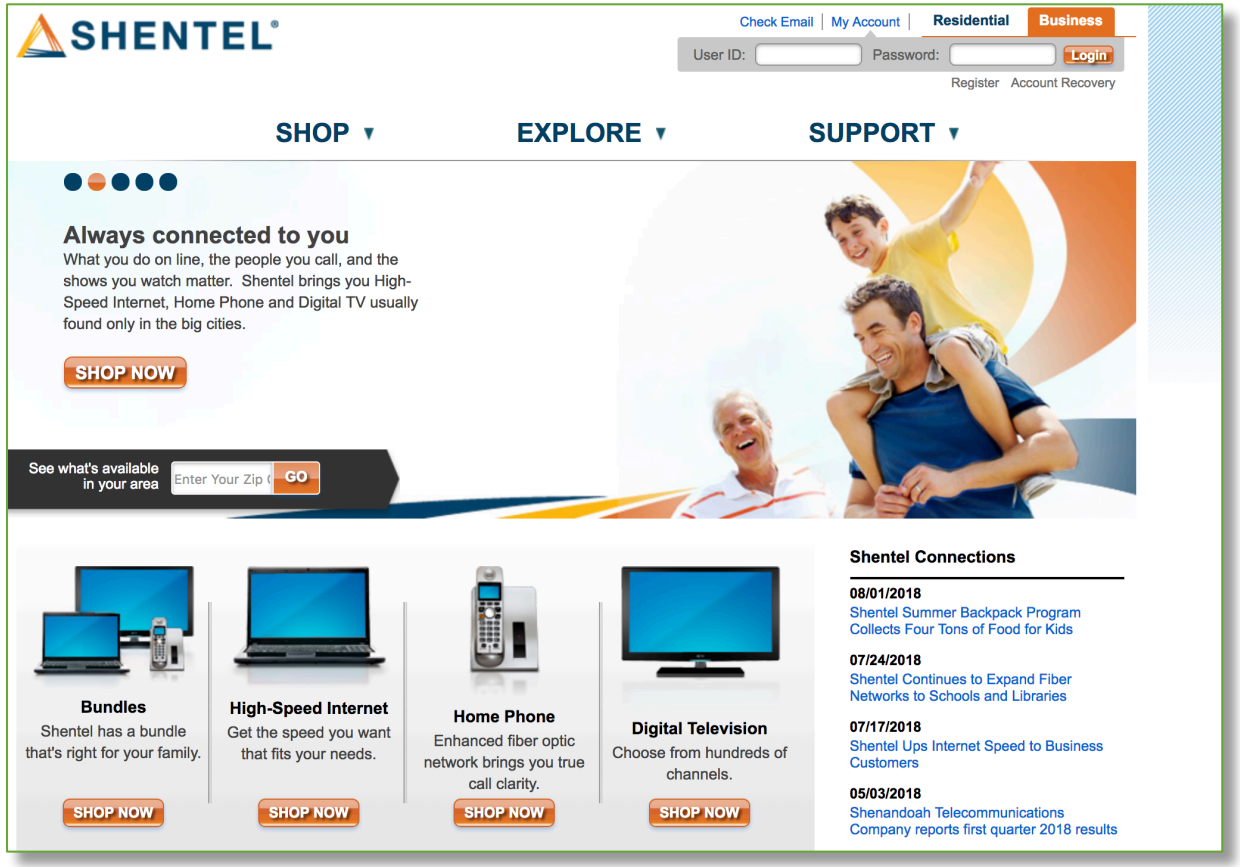
Shentel

Who We Are!

SHENTEL®
Always connected to you

https://www.shentel.com/

- Serving customers since 1902
- Provide
  - ***Advanced Broadband Services***
  - ***Digital TV***
  - ***Voice and High-Speed Internet***
  - ***Mobile Services*** *(through our affiliation with Sprint)*
- Virginia, West Virginia, Pennsylvania, & Maryland



In The Beginning…

In The Beginning!

Growth of an IT Security Dept.

- Make up of IT Security Department 5 Years Ago
  - Single IT Security Manager with Two Sub-Groups
  - Single IT Security Analyst
  - Two ID/Access Administrators (User onboarding, account management, etc.)

- IT Security Department Goals
  - Set up “net” of true alerts for quick response and remediation efforts
  - Provide accurate reporting to Shentel management
  - Install and configure existing security monitoring tools
  - Monitor all aspects of enterprise networking
  - Enable the IT Analysts to correlate anomalous activities and security events on Shentel networks
  - Enable Shentel staff to work in a safe cyber environment
  - Continue development of a robust cyber security program

Challenges to Growth

The Raw Materials

- 1700+ Users
- 300 Mixed Server Platforms
- 1700+ Workstations
- Network devices and printers
- No solid event communications across enterprise applications
- IT Security Staffing – not enough
- A Fantastic and Growing Company!

The Cyber Security Clue Hammers

Realities and Realizations

- No Solution to Monitor All Device Types
- No Centralized Log Storage Capability
  - No provisioning for sending collected data
  - No ability to store long term event
- “SIEM by Spreadsheet”
- Tools – Single applications, no inter-tool correlation
  - Largely Agent based
  - Individual Consoles
  - Proprietary databases
  - Based solely on Windows based operating systems

The Cyber Security Clue Hammers cont'd

- Humanly impossible to correlate all the data
- Log reviews by spreadsheets and multiple consoles is very inefficient and very time consuming
- Emailed Alerts Fatigue from multiple tools
- Did I Mention Spreadsheets Analysis?

Quick Poll!
Get some hands raised!

How ‘Bout YOU??!!

- Who can relate to the torrents of user related events pouring in for your review?
- Who can’t sleep at night ‘cuz you think of all the events you have in your logs that you didn’t get to analyze today?
- How many of you are capable of taking all of these user events and timelines and performing Probabilistic Suffix Tree algorithm calculations in your head? Hmmm…Really?

Directions

Event Analysis Solution Criteria

Which Product Would Meet Shentel Needs?

Centralized Access

Highly Configurable

Scalable

Multi-Platform

Manageable for Small Staff

There are many fine companies in the market with new detection capabilities and cutting edge technologies.

The decisions were tough!

Product Analysis

The Contenders

- LogRhythm, Qradar, Solarwinds LEM, Alien Vault, Splunk
- All excellent products but all did not meet Shentel needs:
  - Licensing models
  - Proprietary configurations
  - Use of devices or listeners
  - Young and visionary products

Finally – we found Splunk!

…AND…

Also found that the Splunk> Community Kicks Butt!!!!

Splunk> and User Behavior Analytics

The Start of Our Journey

splunk> .conf18

Why Splunk and UBA?

Swaying the Decision Criteria

- Text based, no special databases, log agnostic
- CIM and other regulatory compliance capabilities
- Machine Data Learning capabilities and accompanying data modeling
- Custom search development on our data
- Very configurable and expandable
- Long-term centralized storage with fast access
- UBA is Focused! Remember- UBA uses Machine Learning models on user related data! *(And - we can find out who was logging in from Cozumel!)*
- Large number of apps and add-ons with great documentation
- Willing and helpful community

Shentel's Splunk Experience

How We Implemented Splunk and UBA

Shentel decided on a slightly different path to achieve the desired security monitoring goals. At that time, sophisticated and successful phishing and ransomware attacks were making headline news. It was decided to protect and watch internal behaviors and user relationships using UBA before moving to Splunk Enterprise Security.

Splunk Enterprise → User Behavior Analytics → Splunk Enterprise Security

1 **2** **3**

Initial Impressions

Wow! Just Wow!

- Splunk opened up a whole new information world for Shentel's IT Security Dept.
- Inundated with data to the point of overload!
- Discovered everyday traffic and events we didn't know about!
- UF installations – quite a bit of initial work
- Stood up and configured new centralized syslog system. Experienced issues with some of the logging routes and filtering statements that send data to Splunk
- Little bit of a bumpy road installing and configuring UBA. Initially did not fully understand what data UBA needed to ingest or how to interpret its dashboard outputs
- The more we understood how Splunk and UBA worked, the more questions that we found asking ourselves about our network, data, and users – this is good and bad!

UBA – Lessons Learned and What You Need To Know

Just Some Friendly Advice!

- Know your data sources! Know how your data transverses your environment. It is surprising what you discover during this process!
  - e.g. We had issues connecting with Firewalls and Web Content Filtering system and getting it into UBA
- Know where your user data is, where your user data is collected, the connections to your user data
- Know how to get and expose your user account attributes
- If you install UBA prior to Enterprise Security – Realize you will still need to hop back and forth into Splunk Enterprise to run your own searches for individual data pieces and information.
- Have a high level understanding of what is normal for your different user groups or account types – this helps with tuning out the noise! Normal events may not be immediately recognizable when you first experience your new UBA installation.
- Collect data enhancements – DNS, DHCP

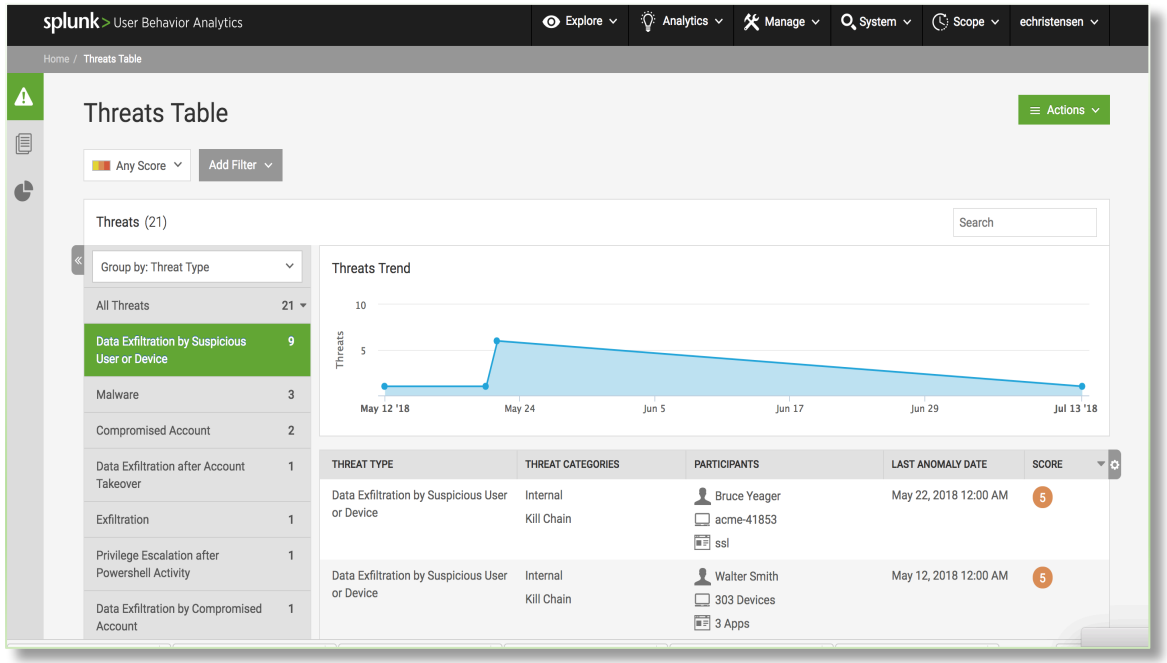
Let's Go Rabbit Hunting!

UBA Gotchas!

You are excited! You see data! You See Awesome Graphs and Spider Webs!

You need some more friendly advice:

- It is extremely easy to follow all kinds of new juicy events and anomalies – Don't go down the Rabbit Holes!
- We cannot stress enough the importance of knowing what is normal in your environment – not everything is evil! Take heart. We are still on that same journey.
- You also don't know what may not be there! Review your Active Directory, Server and Workstation Auditing settings to see what auditing is enabled. If auditing on your systems is not turned on, the data is not there.
- Read, Read, Read! Read the UBA docs and especially the headers and graph explanations in the UBA dashboards. There is a lot of great help in those explanations
- Be patient. UBA data models build and get better as time goes by. It is easy to jump to conclusions that something in UBA is broken early into a new UBA installation.
- Consider training for your UBA users and realize that understanding what UBA is telling you and working in UBA takes some time.



Let's Turn Down Some Volume!

Did you put your Advertisement in My UBA?

Challenges in the Environment

- **Challenge 1 Web Traffic**
  - End Users behavior day to day can change.
  - Source data for Bad IP Lists can change.

- **Challenge 2 Advertisements**
  - Most Web Content Contains Advertisements.
  - Advertisements may contain Malicious content.
  - Advertisements that don’t contain Malicious content can still mimic those that do.

Investigating Challenge 1

Approach to the Challenge of Web Traffic Part 1

- Users behavior change, lets work through 3 possible reasons for an alert.
  1. This may be a result of ebbs in flows in workload for certain positions.
     - Users take on different assignments when people are out of the office or turn over occurs.
     - UBA will resolve this as you perform investigations and the system continues to learn.
  2. This may be a result of an malicious actor.
     - Look for signs of command and control activity, especially if IOC's spread to other devices in the environment.
  3. This may be a result of an insider threat.
     - Look for signs of data exfiltration and destruction, even if its is not attributed to the original actors account.

Recommendation:

Use Alerts in UBA as a reason to Threat Hunt, REMEMBER...

Every Decision You Make Helps The Platform Learn!

splunk> .conf18

Investigating Challenge 1

Approach to the Challenge of Web Traffic Part 2

- Why does source data for Bad IP's matter?
  - Legitimate websites are sometimes compromised and make a Bad IP List.
    - The website in question may not leave the list for several weeks or months, even after the initial reason is addressed.
    - This has the potential to skew ratings which can lead to false positives.
  - Malicious websites sometimes do not make a specific Bad List.
    - UBA can really shine even in the event that a specific site intelligence is not accurate but for the best results we need to provide reliable data..

Recommendation:

Evaluate free lists and paid for threat intelligence.
A good place to start is
https://isc.sans.edu/suspicious_domains.html

splunk> .conf18

Investigating Challenge 2

Solving the Challenge of Advertisements

- Who doesn't like Advertisements?
  - IT Security Does Not!!!
- Advertisements with Malicious Content
  - Beacon out periodically.
  - May install crypto miners or other unwanted data.
  - May direct users to unwanted or unsafe websites.
- Advertisements with Non Malicious Content
  - Beacon out periodically.
  - May gather data from end users.
  - May direct users to unwanted sites.

Investigating Challenge 2

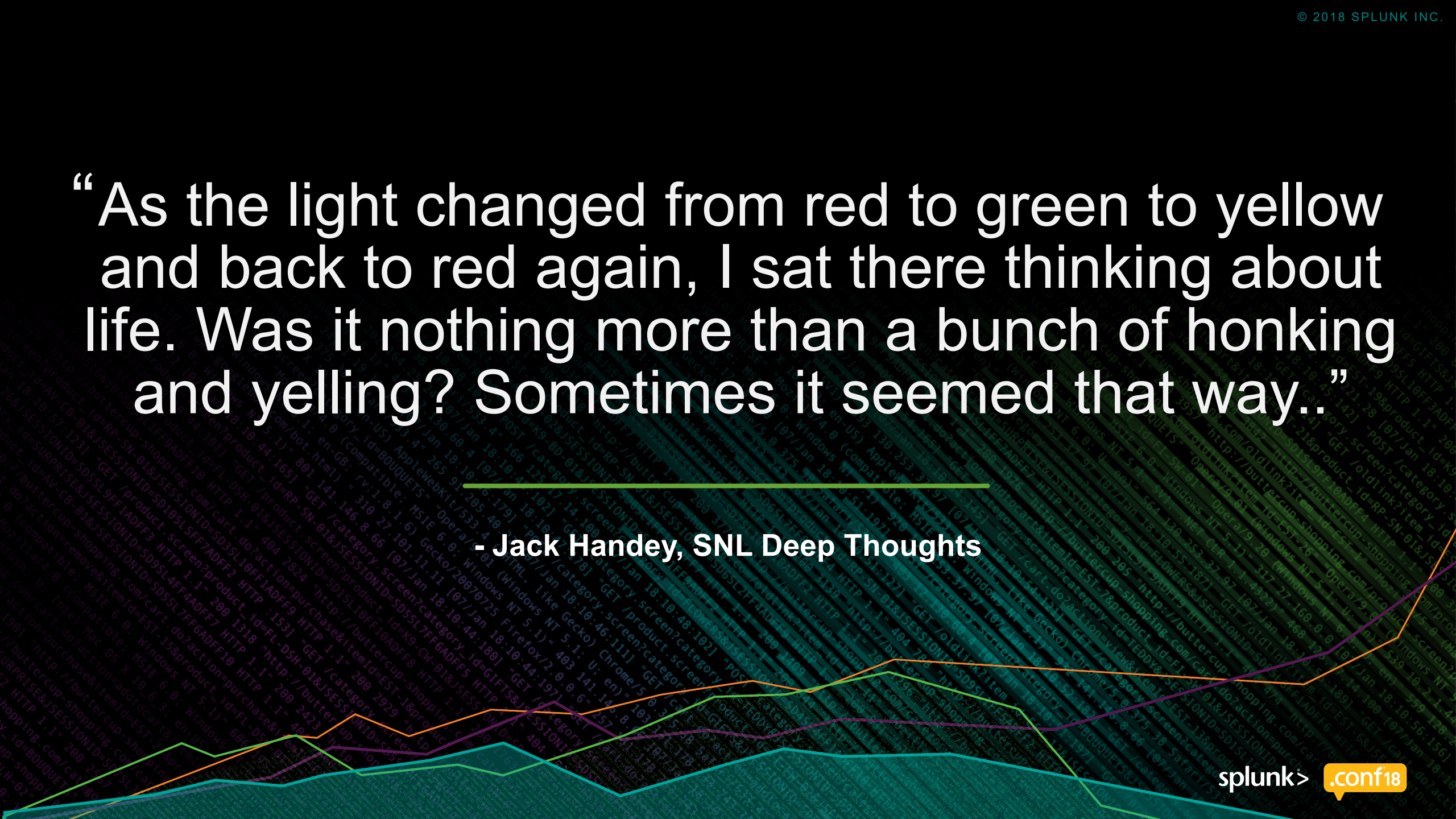
Solution to Advertisements

- **Recommendation:** Block All Advertisements!

- Couldn't that break something?
  - Maybe…
  - Test and work through the problems to find out.
  - The benefits outweigh the risks.
  - You are helping UBA provide more actionable results.
  - You are making your computing environment more secure.

"As the light changed from red to green to yellow and back to red again, I sat there thinking about life. Was it nothing more than a bunch of honking and yelling? Sometimes it seemed that way.."

- Jack Handey, SNL Deep Thoughts



Thank You

Don't forget to rate this session in the .conf18 mobile app