Threat Hunting and Anomaly Detection with Splunk UBA

Tom Smit | Staff SE
smitty@splunk.com

October 2018

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

Who is This guy?

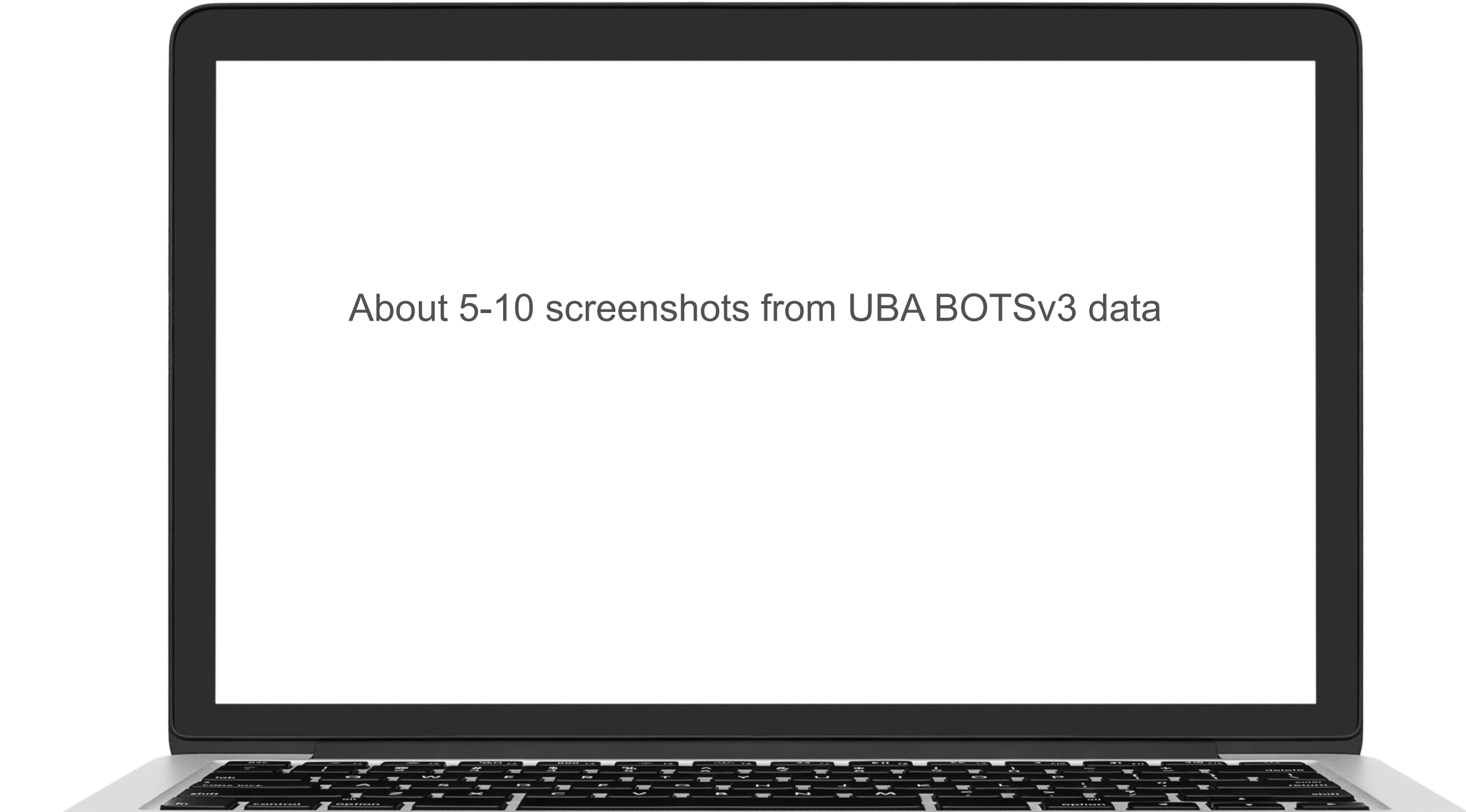
Tom Smit

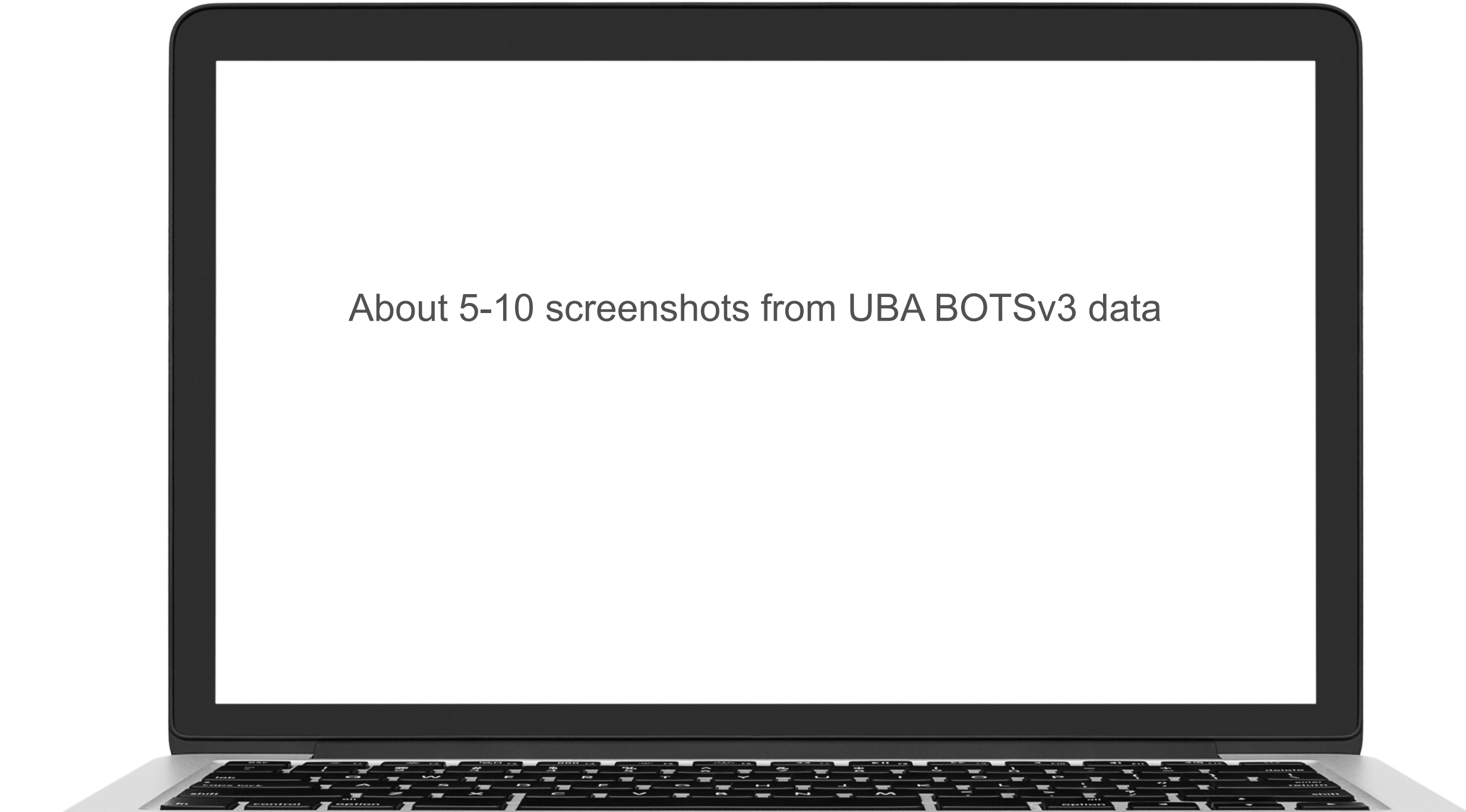
smitty@splunk.com
Staff Sales Engineer

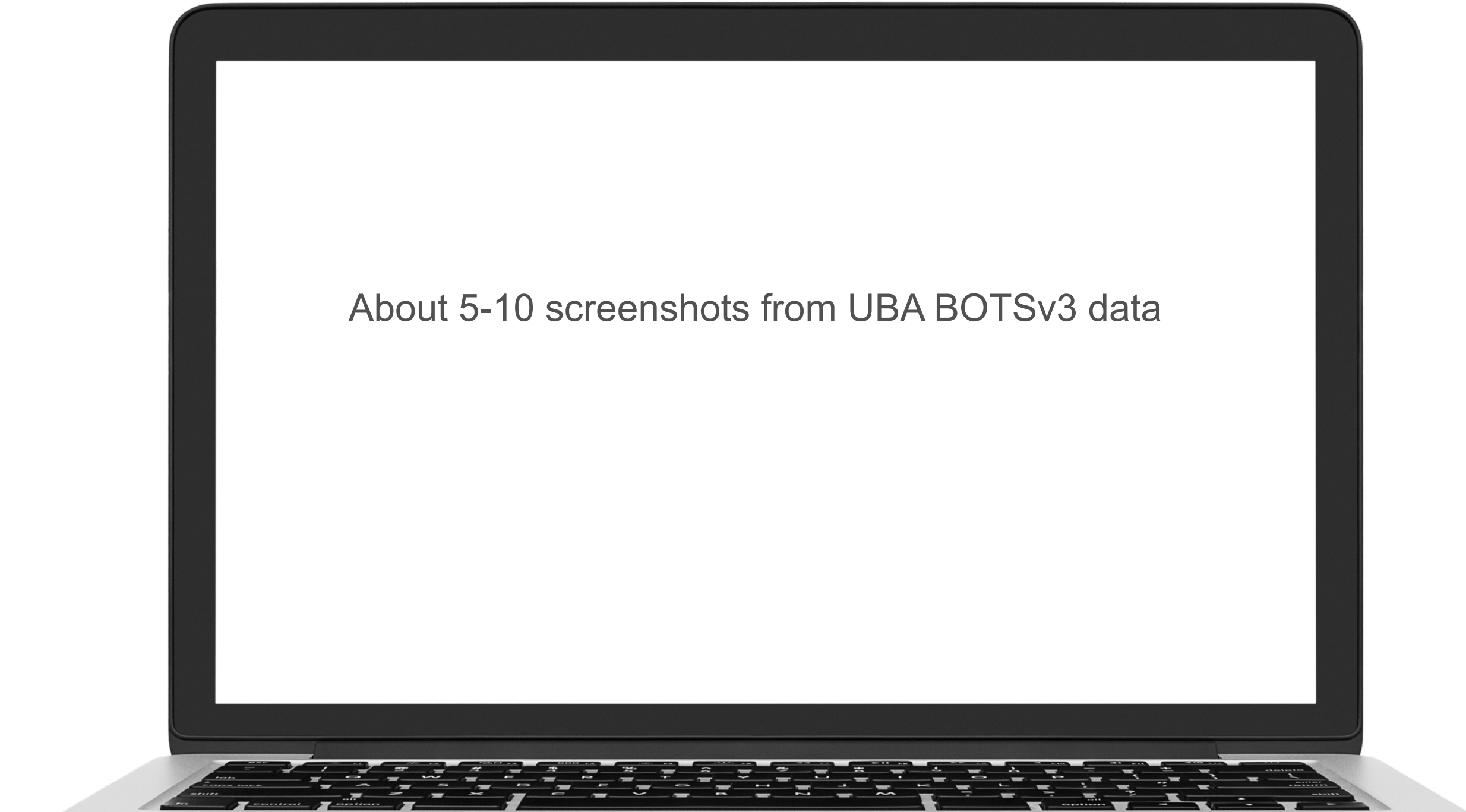
- Working at Splunk for almost 4 years
- Security and UBA SME
- Previous life at Core Security, Mimecast, and Symantec

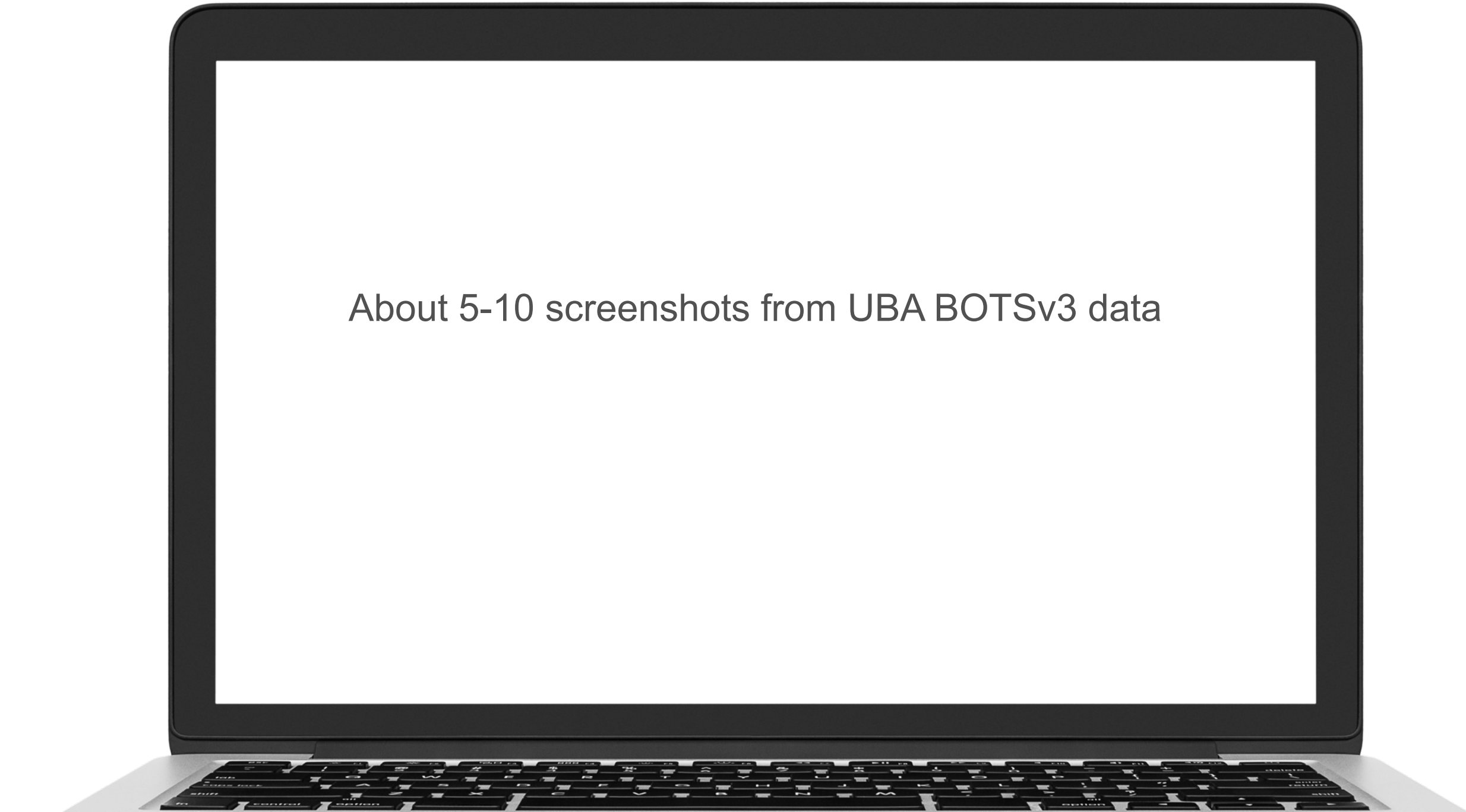
Threat Hunting and Anomaly Detection

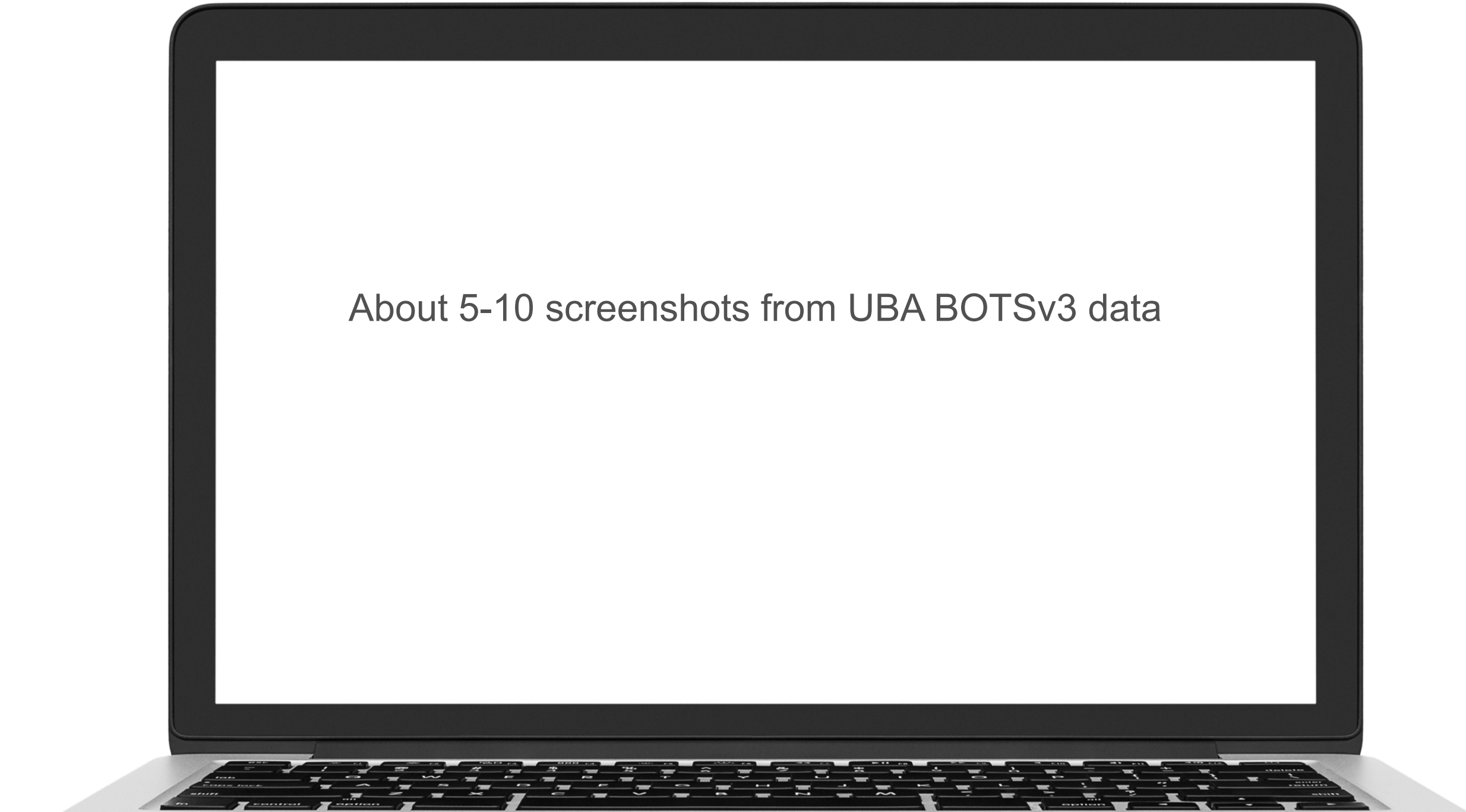
splunk> .conf18

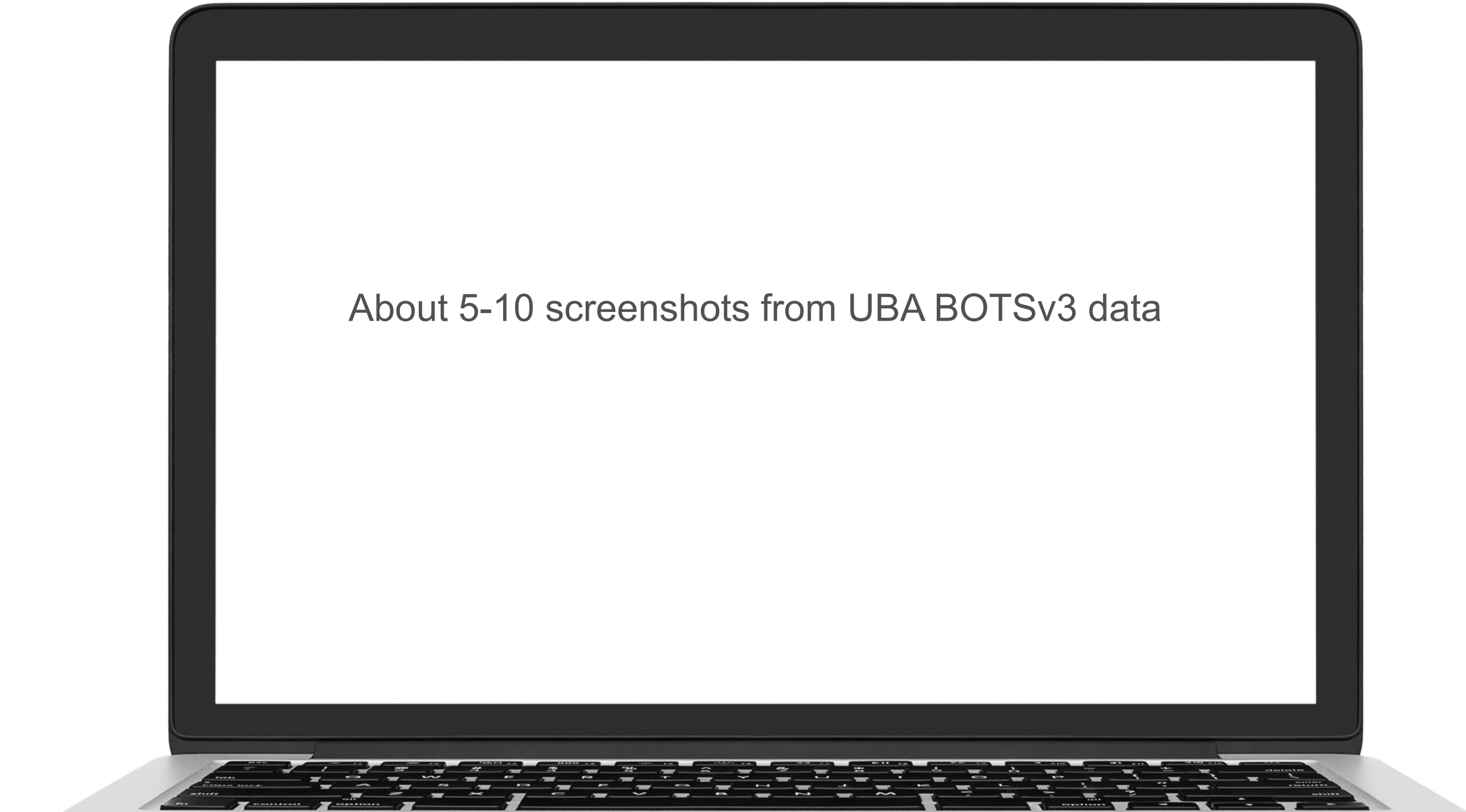


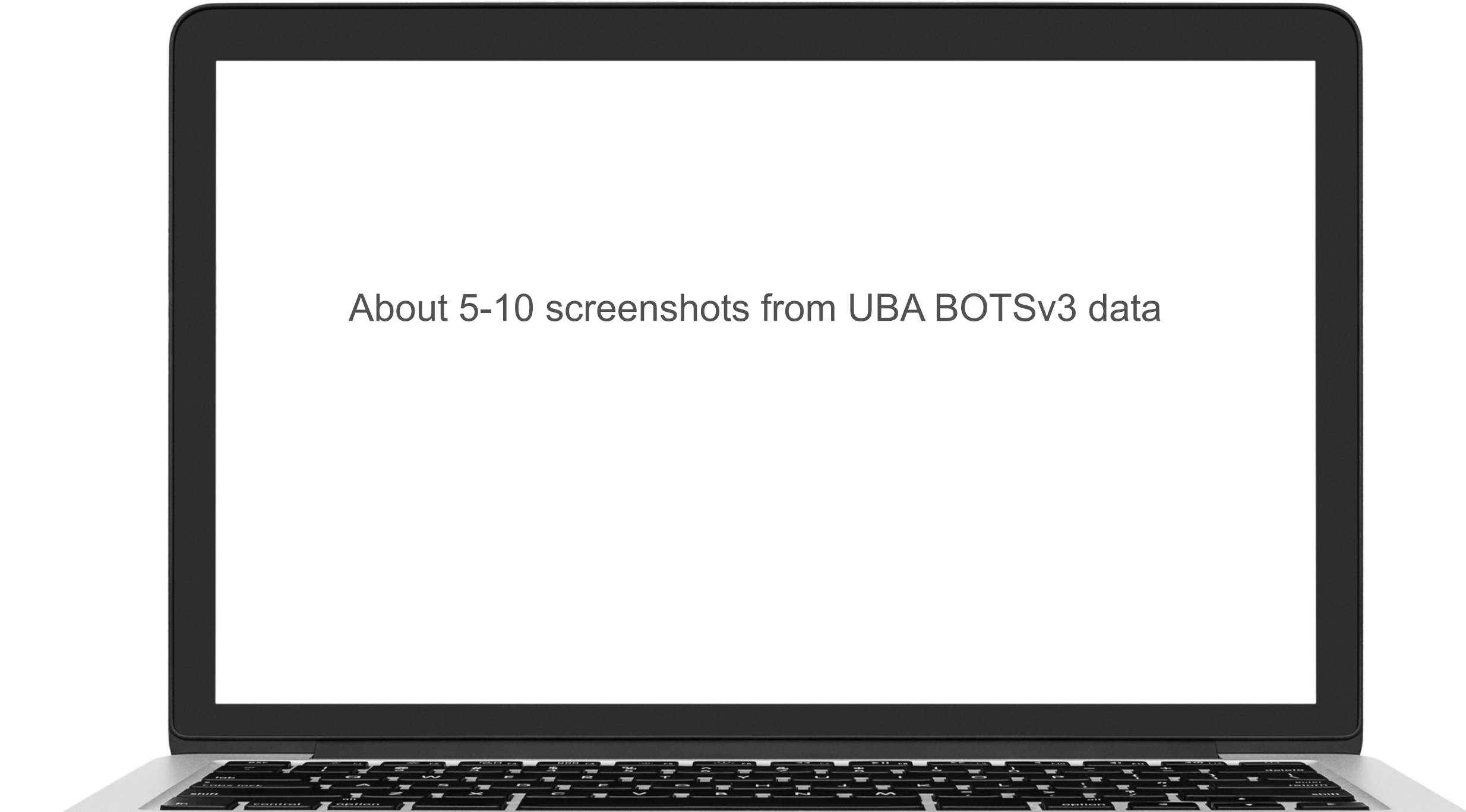










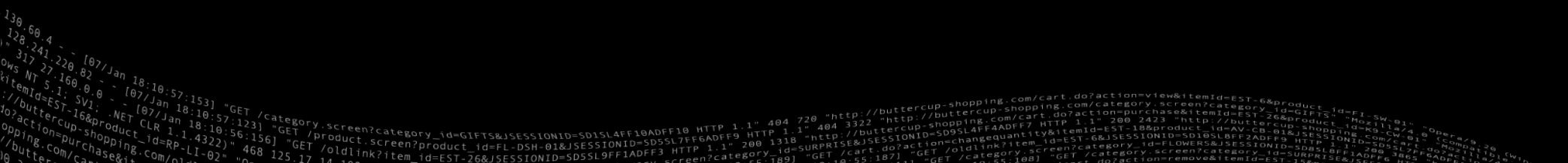


Best and Worst Practices

To do and *not* to do!

Quick Agenda

- Each Section Here
  - First Slide: Bad things we've seen in the field
  - Subsequent Slides: How to combat those things
- Pre-Requisites and Configuration
- Data Onboarding
- Usage and Integrations



Pre-Requisites and Configuration

Keep your arms and hands inside the tram at all times

Worst Practices

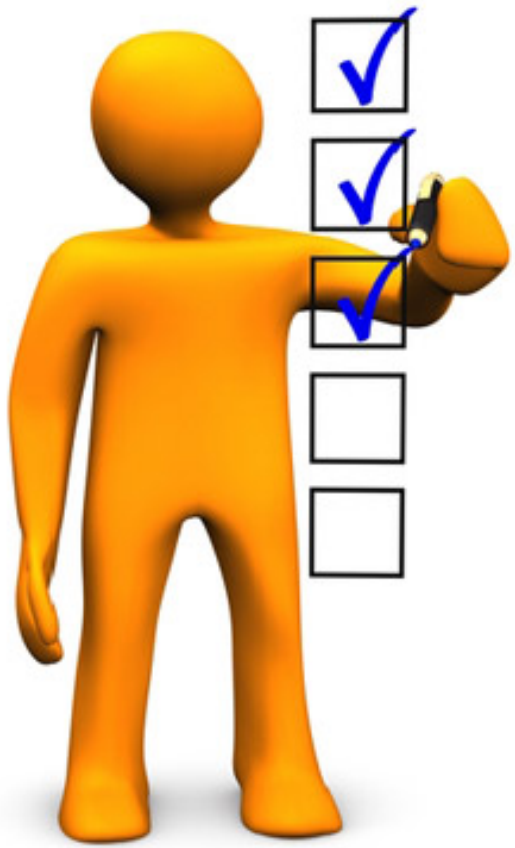
Break all the things!

- Undersize your environment
  - Decrease logging to meet sizing
- Block port 80/443
- Change file system permissions on the OVA/AMI
- Install custom kernels on Red Hat
- Block real time search
- Tinker!

Best Practices

Meet all the pre-requisites

- Real time required (recommend indexed real time)
- DNS/DHCP, Windows Security Logs, Proxy, and Firewall required
- Asset information
- IOPS at 800+
- Network ports open
- Use cases well defined
- For more information: http://docs.splunk.com/Documentation/UBA/4.1.2/Install/Requirements



Best Practices

Sizing and Configuration

Size of cluster	Max events per second capacity	Number of accounts	Number of devices
1	4K	up to 50K	up to 100K
3	12K	up to 50K	up to 200K
5	20K	up to 200K	up to 300K
7	28K	up to 350K	up to 500K
10	40K-45K	up to 350K	up to 500K
20	75K-80K	up to 750K	up to 1 Million

- Sizing exercise with you Splunk SME to verify data load
- 16 Core/64 RAM is set – throwing 96 cores at it will not affect data processing
- 50 GB/1 TB drives are required – SSD preferred
- AMI and OVA are available

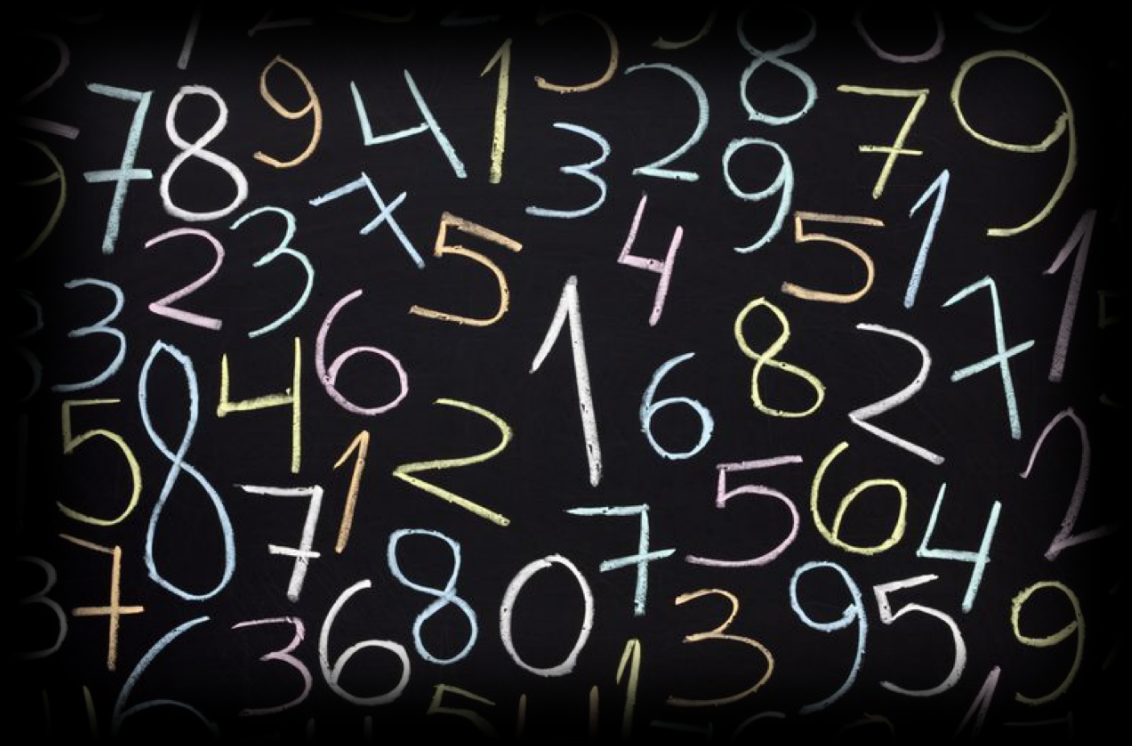
Data Onboarding

Let’s get rolling already

splunk> .conf18

Worst Practices

Data Onboarding

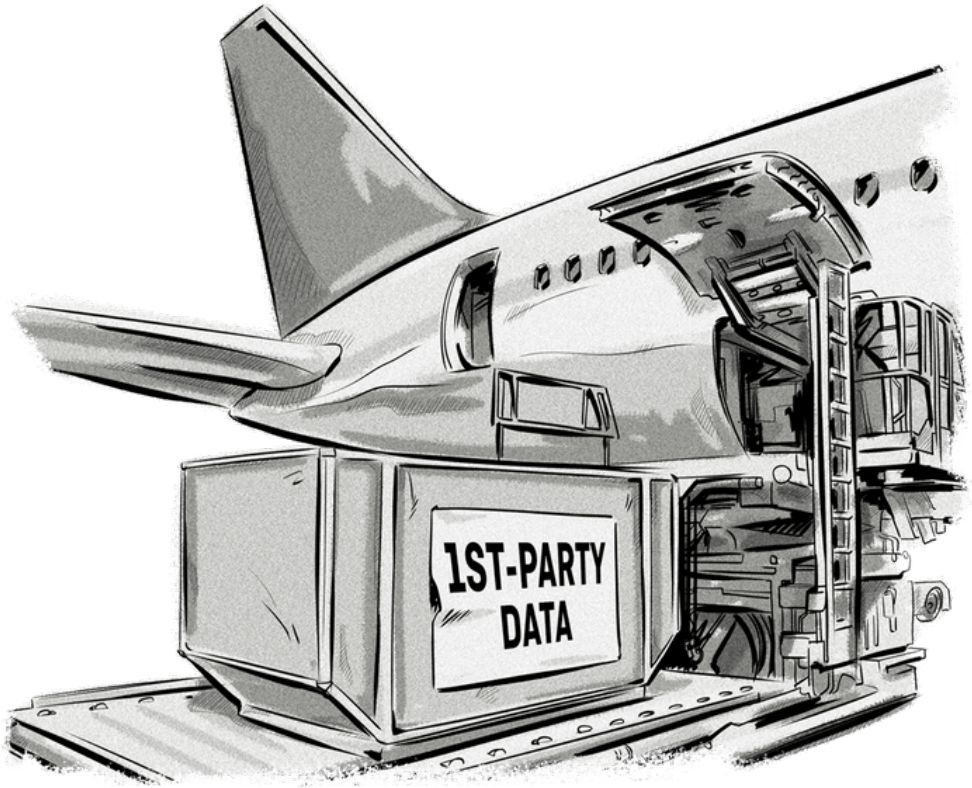


- Cut back on data to meet sizing/data requirements
- Logging only blocked traffic
- Proxy logging with audit information (bytes in/out)
- Ignoring bursts of data or inconsistencies in sizing
- Using Technical Add-ons (TAs) that are not CIM compliant (or no TA at all)
- Logging any of the required data sources without all data
- Using Windows DNS without Stream
- Logging only specific users/groups

Best Practices

Data Onboarding

- Data should be CIM compliant
- All users' data should be onboarded
- Full DHCP and DNS (including queries and responses) should be in Splunk
- Take time to ensure HR data is correct before onboarding other data



Usage and Integrations

What does this button do?

Worst Practices

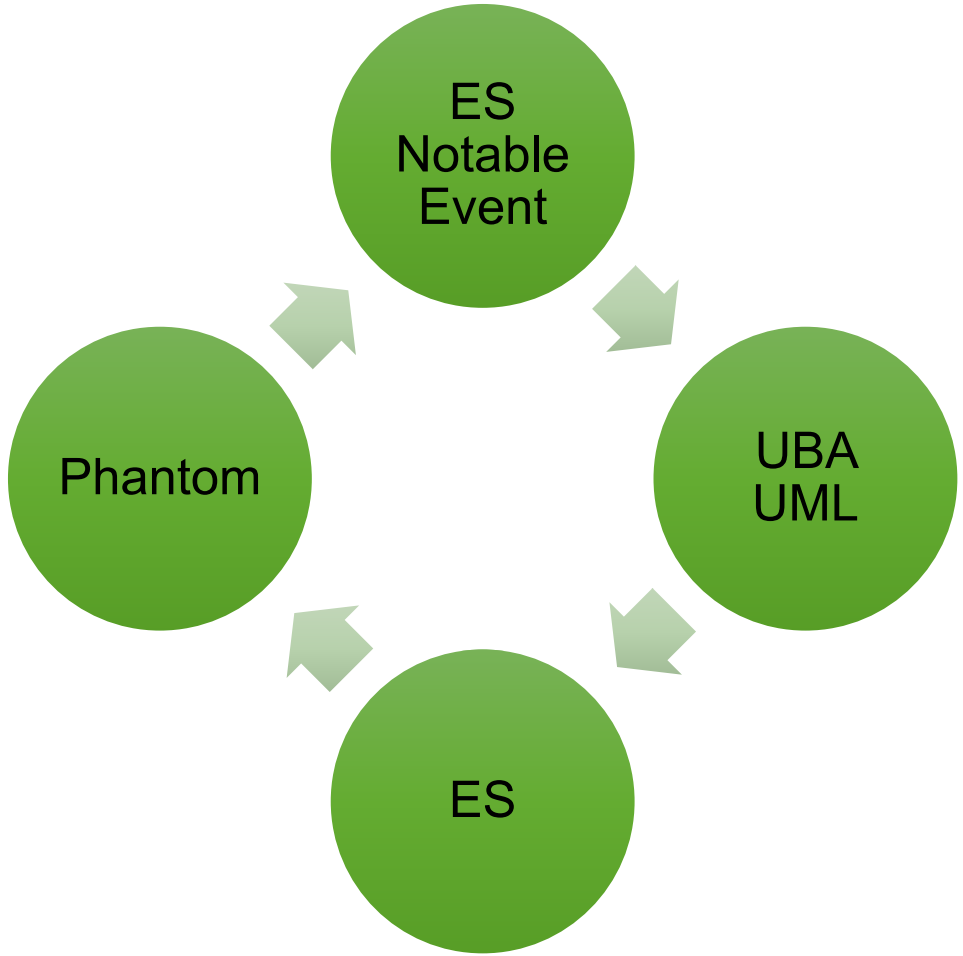
Usage and Integrations

- Trying to do everything inside of UBA
- Creating a bunch of basic correlation rules inside of UBA
- Trying to integrate everything in UBA that you already have integrated in Splunk
- Treat UBA as a stand alone platform in your environment

Best Practices

Usage and Integrations

- Pull in correlation notable events from ES
- Send anomalies back to ES and the ES risk framework – see Apger's risk deck for more!
- Send threats back to ES as notable events
- Reactions and responses to UBA data should be done through Splunk
- Take the online training!
- Follow the following methodology!

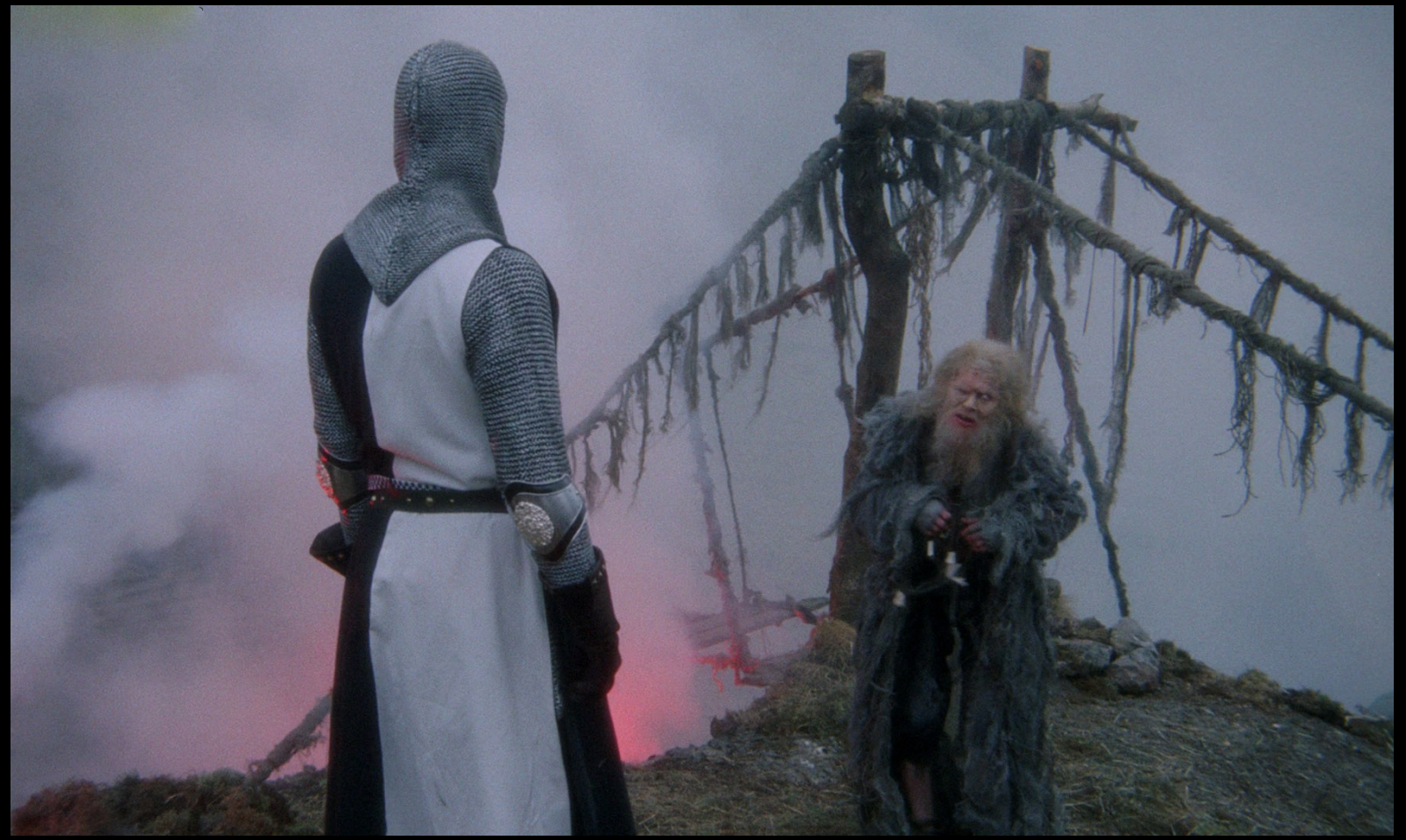


Where Do I Go from Here?

- Product Page: https://www.splunk.com/en_us/software/user-behavior-analytics.html
- UBA White Papers
  - https://www.splunk.com/pdfs/product-briefs/splunk-uba.pdf
  - https://www.splunk.com/pdfs/technical-briefs/using-splunk-uba-to-detect-cyber-attacks.pdf
  - https://www.splunk.com/pdfs/technical-briefs/using-splunk-uba-to-detect-insider-threats.pdf
- UBA Demo – reach out to your Splunk rep!
- UBA Test Drive – reach out to your Splunk rep!
- Coming soon!!!! – Threat Hunting on UBA Workshop (new year)

Ask Me Anything!

Well, not anything, it should be about Splunk or UBA



Thank You

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