splunk> .conf2017

FFIEC Cybersecurity Assessment Tool

Cybersecurity Controls & Incidence Mappings for Splunk Enterprise, Enterprise Security, User Behavior Analytics

Curtis Johnson | Senior Sales Engineer & Security SME

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

Agenda

- Part I: FFIEC CAT - Background, Overview, Maturity
  - What is it, and why you should you care
  - Cybersecurity Maturity according to the FFIEC
- Part II: FFIEC CAT – The Assessment
  - What does it look like, and how do you use it
- Part III: FFIEC CAT and Splunk
  - What Domains and controls does Splunk map to specifically
  - Explanation of Splunk Capabilities as they relate to the FFIEC CAT

“We have the proper controls, safeguards and procedures in place and have zero room for improvement.”

-No one ever

Did You Know?

Of the data compromised in reported financial breaches **71%** were **Credentials**, **12%** were **Payment**, and **9%** were **Personal**.

Source: 2017 Verizon Data Breach Investigation Report

Did You Know?

Denial of Service, **Web Application Attacks** and **Payment Card Skimming** represent **88%** of all security incidents within Financial Services.

Source: 2017 Verizon Data Breach Investigation Report

Part One: FFIEC CAT Background, Overview, Maturity

Assess Your Environment

splunk> .conf2017

Background

- Based on assessment that FFIEC members piloted in 2014
- Consistent with the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Provides a Measurable and Repeatable Process

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

FFIEC

Overview

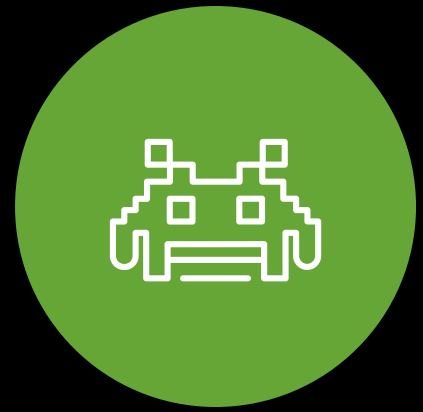
Determine Inherent Risk Profile

Technologies and Connection Types

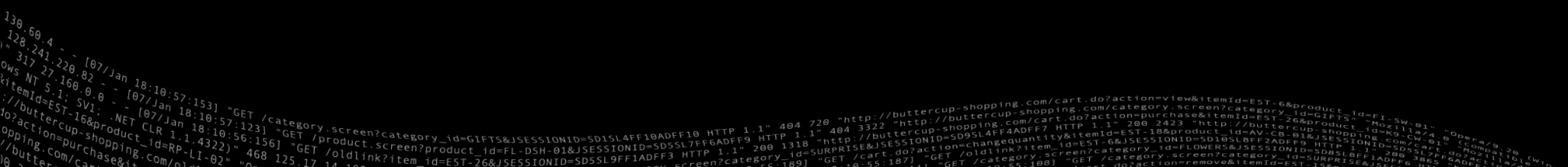
Delivery Channels

Online/Mobile Products and Technology Services

Organizational Characteristics



External Threats



splunk> .conf2017

Cybersecurity Maturity

Within each of the 5 Domains

Cyber Risk Management and Oversight

Cybersecurity Maturity

Within each of the 5 Domains

Threat Intelligence and Collaboration

Cybersecurity Maturity

Within each of the 5 Domains

Cybersecurity Controls

Cybersecurity Maturity

Within each of the 5 Domains

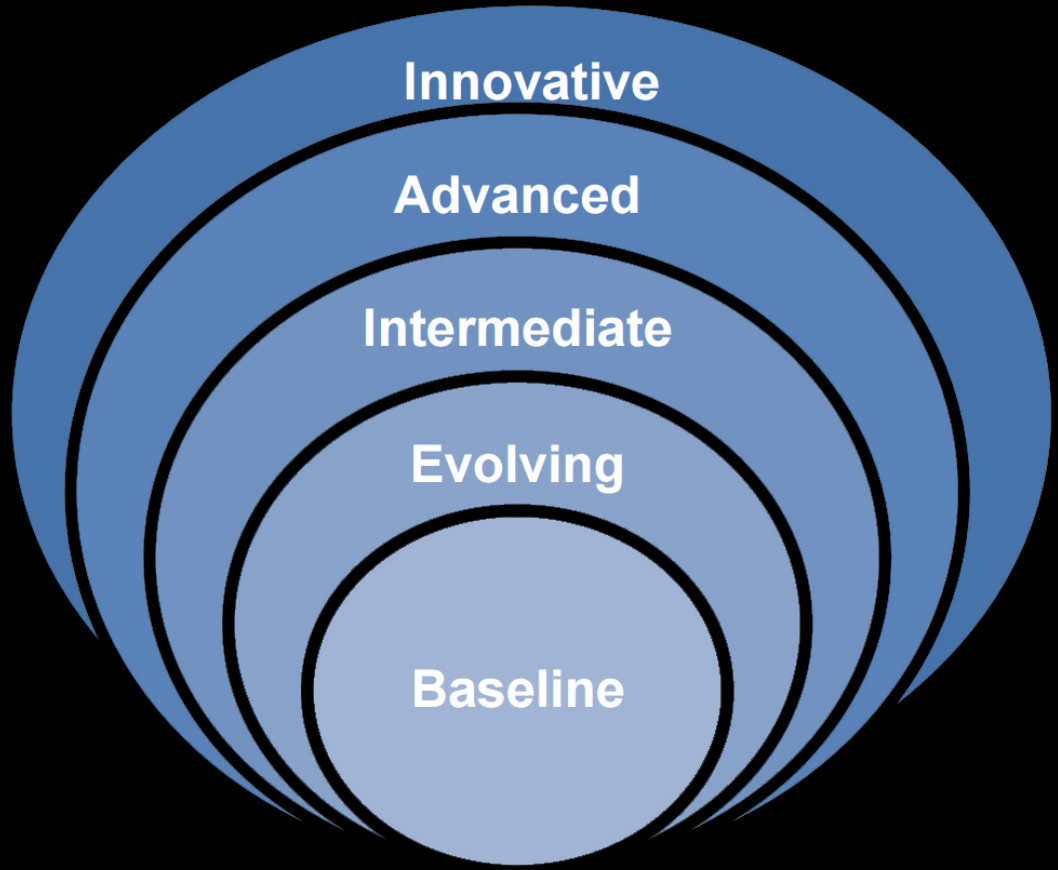
External Dependency Management

Cybersecurity Maturity

Within each of the 5 Domains

Cyber Incident Management and Resilience

Cybersecurity Maturity Levels

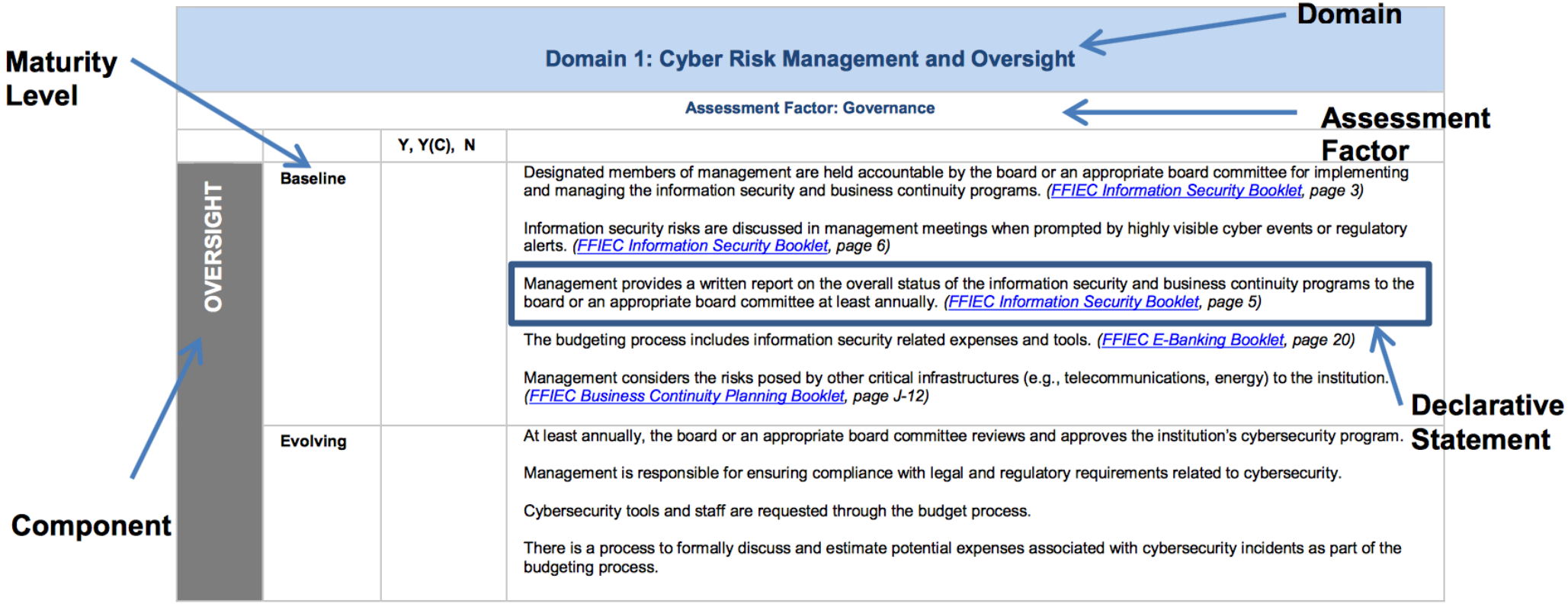


Part Deux: FFIEC CAT

The Assessment

splunk> .conf2017

Completing the Cybersecurity Maturity



Domain 1: Cyber Risk Management and Oversight			
	Assessment Factor: Governance		
		Y, Y(C), N	
OVERSIGHT	Baseline		Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. *(FFIEC Information Security Booklet, page 3)* Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. *(FFIEC Information Security Booklet, page 6)* Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. *(FFIEC Information Security Booklet, page 5)* The budgeting process includes information security related expenses and tools. *(FFIEC E-Banking Booklet, page 20)* Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. *(FFIEC Business Continuity Planning Booklet, page J-12)*
	Evolving		At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. Cybersecurity tools and staff are requested through the budget process. There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.

splunk> .conf2017

Part Tres: FFIEC CAT and Splunk = ❤️

How Splunk maps to the FFIEC CAT

splunk> .conf2017

Where do we fit?

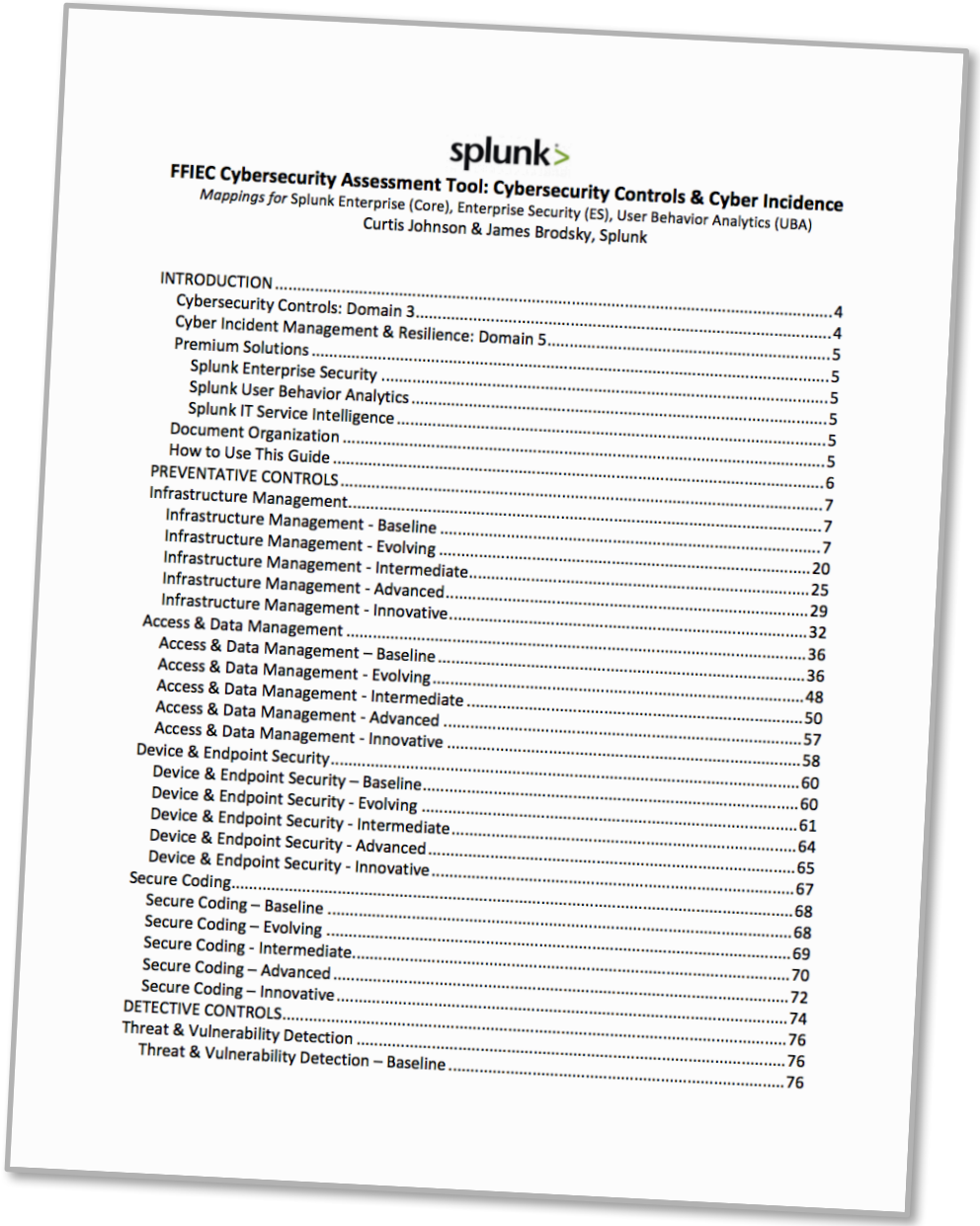
Cybersecurity Controls

Cyber Incident Management and Resilience

The Paper

Mappings for Splunk Enterprise (Core), Enterprise Security (ES), User Behavior Analytics (UBA)

- 160 Pages of Content
- Mappings to NIST CSF
- Track your FFIEC CAT Initiative
- http://bit.ly/2vxNpeC



splunk>

FFIEC Cybersecurity Assessment Tool: Cybersecurity Controls & Cyber Incidence

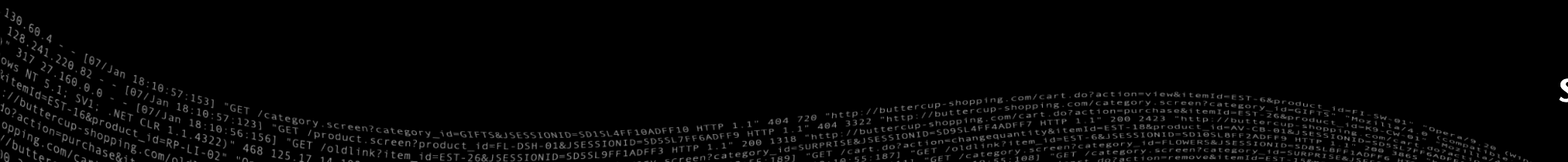
Mappings for Splunk Enterprise (Core), Enterprise Security (ES), User Behavior Analytics (UBA)

Curtis Johnson & James Brodsky, Splunk

splunk> .conf2017

Mapping Splunk Capability to the CAT

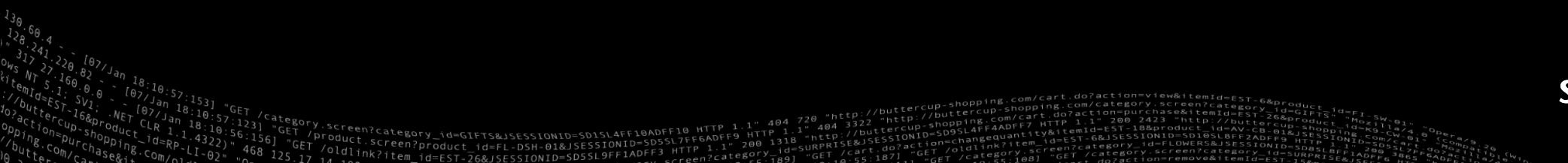
Execution: Splunk capabilities allow execution against this control. No third-party data sources are needed because Splunk can service this control entirely. Splunk then provides a central place to report on the efficacy of this control.



splunk> .conf2017

Mapping Splunk Capability to the CAT

Verification: Splunk does not perform this control directly but can ingest the data from data sources that support this control. Splunk then provides a central place to report on the efficacy of this control.



splunk> .conf2017

Mapping Splunk Capability to the CAT

Supporting: This generally applies to controls that are more process/policy or human oriented. Splunk may serve as an information input for the process so that the control can be met.

splunk> .conf2017

Mapping Splunk Capability to the CAT

Not Applicable: The control is entirely process/policy oriented, and there is no timestamped machine data output from the implementation of the control, therefore there is no clear role for Splunk.

How to Use this Mapping Guide

FFIEC Cybersecurity Assessment Tool Control	FFIEC Description	NIST Cybersecurity Framework Mapping	NIST Description	Implemented
D3.PC.Im.B.5	Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced.	PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained. (p. 26)	☐ YES ☐ NO

- **D3** – **Domain** (Domain 3)
- **PC** – **Assessment Factor** (Preventative Controls)
- **Im** – **Component** (Infrastructure Management)
- **B** – **Maturity Level** (Baseline)
- **5** – **Mapping Number** (5)

splunk> .conf2017

Mapping Example

Up to date antivirus and anti-malware tools are used.

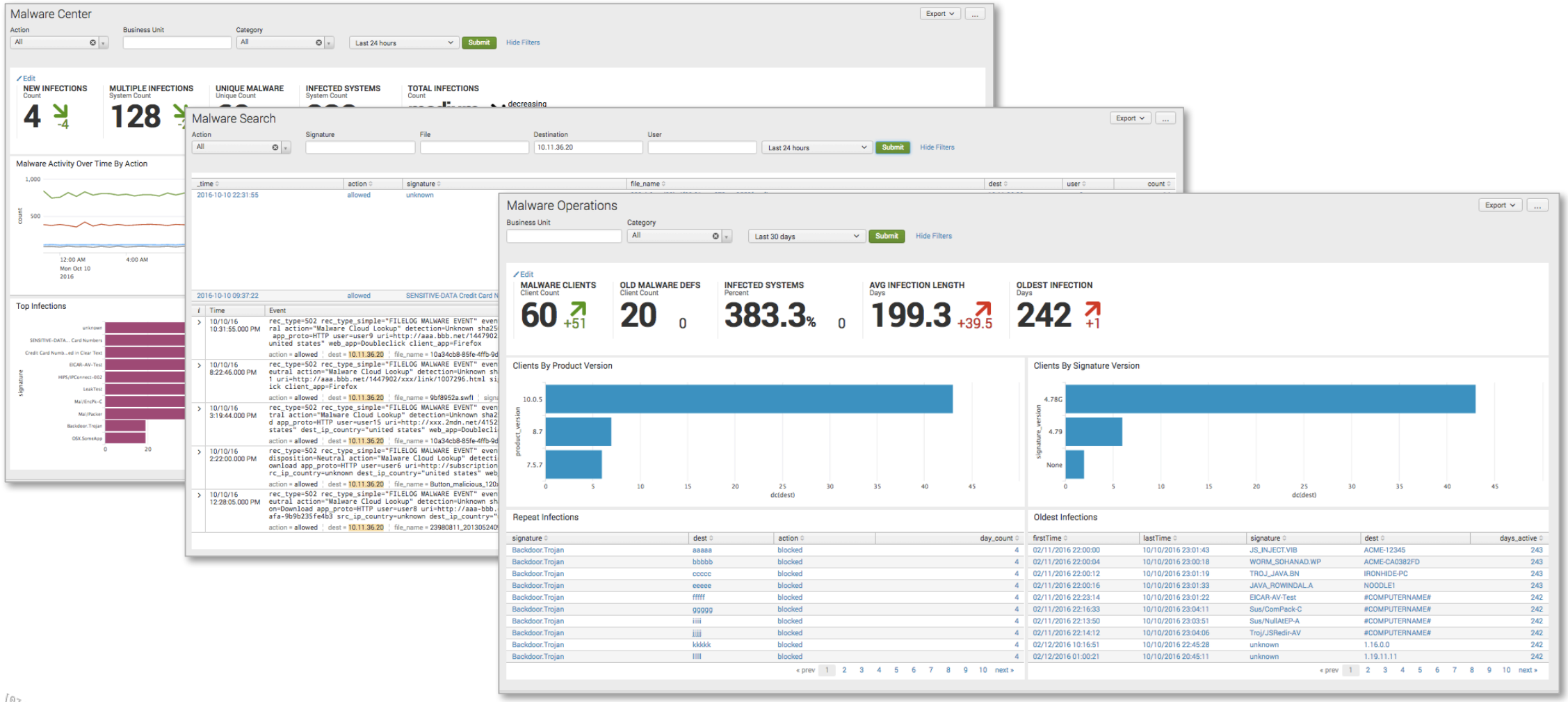
FFIEC Cybersecurity Assessment Tool Control	FFIEC Description	NIST Cybersecurity Framework Mapping	NIST Description	Implemented
D3.PC.Im.B.4	Up to date antivirus and anti-malware tools are used.	N/A	N/A	☐ YES ☐ NO

Splunk Role: ***Verification.*** Splunk ES provides the Malware Center, Malware Operations, and Malware Search dashboards and related reports and alerts. In particular, the Malware Operations dashboard allows for the tracking of systems that are failing malware updates. Data is on-boarded from common endpoint and malware solutions against the Malware data model.

splunk> .conf2017

Mapping Example

Up to date antivirus and anti-malware tools are used.



splunk> .conf2017

Mapping Example

Security controls are used for remote access to all administrative consoles.

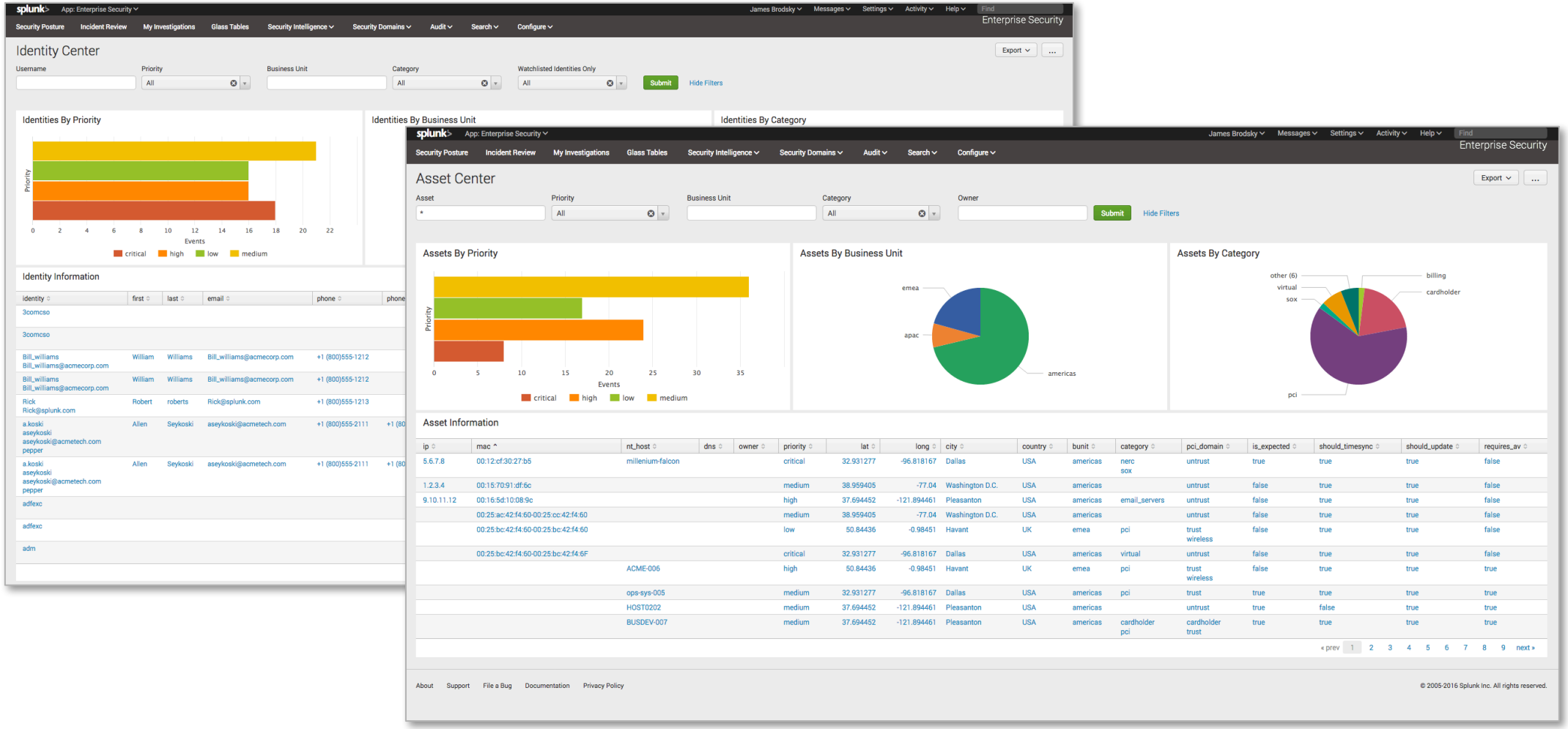
FFIEC Cybersecurity Assessment Tool Control	FFIEC Description	NIST Cybersecurity Framework Mapping	NIST Description	Implemented
D3.PC.Im.Int.2	Security controls are used for remote access to all administrative consoles, including restricted virtual systems.	**PR.AC-3**	Remote access is managed. (p. 23)	☐ YES ☐ NO

Splunk Role: ***Verification.*** Splunk can be used to monitor all accesses to all assets on the network. With the help of Identity Center and Asset Center, both built into Splunk Enterprise Security, it is simple to report on these accesses, using administrative credentials, against assets that are designated as providing admin consoles.

splunk> .conf2017

Mapping Example

Security controls are used for remote access to all administrative consoles.



splunk> .conf2017

Mapping Example

Proactively Identify High-Risk Behavior

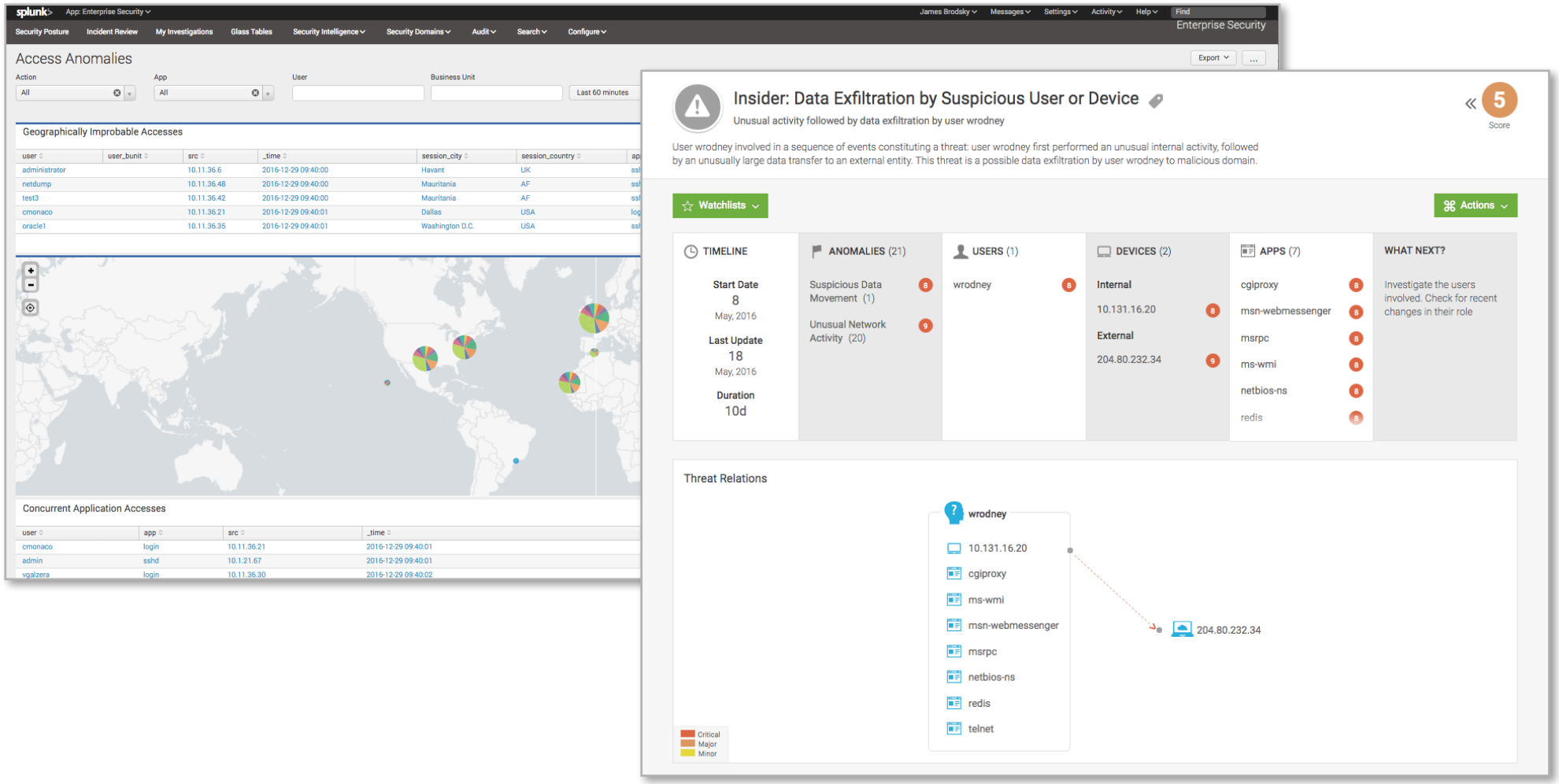
FFIEC Cybersecurity Assessment Tool Control	FFIEC Description	NIST Cybersecurity Framework Mapping	NIST Description	Implemented
D3.DC.Th.A.3	Automated tool(s) proactively identifies high-risk behavior signaling an employee who may pose an insider threat.	N/A	N/A	☐ YES ☐ NO

Splunk Role: ***Execution.*** Splunk Enterprise Security and Splunk UBA both provide ways of identifying high-risk insider behavior, and there are also statistical behavior-based searches that can be run in Splunk Enterprise to augment.

splunk> .conf2017

Mapping Example

Proactively Identify High-Risk Behavior



splunk> .conf2017

Key Takeaways

1. The FFIEC CAT and what it is
2. How the FFIEC CAT defines inherent risk and cybersecurity maturity
3. Where Splunk maps to the FFIEC CAT

Making Machine Data Accessible, Usable And Valuable To Everyone.

splunk> .conf2017

Thank You

Don't forget to rate this session in the .conf2017 mobile app