© 2017 SPLUNK INC.

splunk> .conf2017

Building a Threat-Based Cyber Team

Anthony Talamantes | Manager, Defensive Cyber Operations

Todd Kight | Lead Cyber Threat Analyst

Sep 26, 2017 | Washington, DC

© 2017 SPLUNK INC.

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, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2017 Splunk Inc. All rights reserved.

splunk> .conf2017

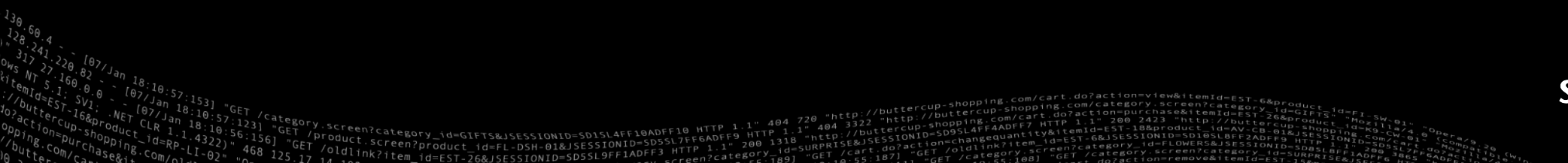
© 2017 SPLUNK INC.

Johns Hopkins University Applied Physics Lab

© 2017 SPLUNK INC.

Common Themes

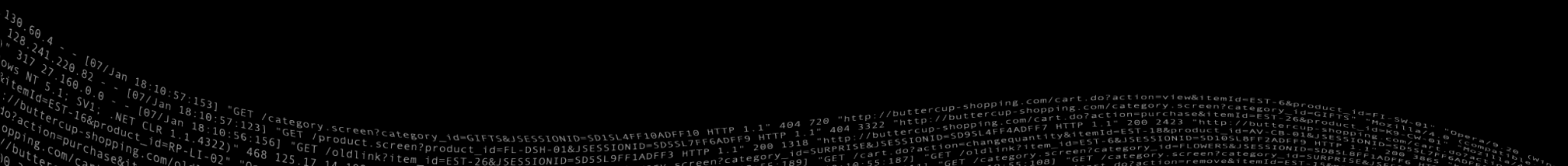
- Change in **Threat Landscape**
- The **Philosophy** of Security Posture vs. Capability Posture
- The value of making multi-faceted change in **Technology, People, and Process**
- Implementing new **Core competencies** including Research, Adaptive Red Team, DevOps, Analytics



© 2017 SPLUNK INC.

Cyber Attack 2009

- APT targeted JHUAPL
- 5 unique pieces of malware on disk
  - Backdoor, Password dumpers, Network exploration utility
- 13 accounts compromised
  - Domain Administrator
- Unclassified data exfiltrated
- Operational impact
  - 2 Weeks disconnected from the Internet



© 2017 SPLUNK INC.

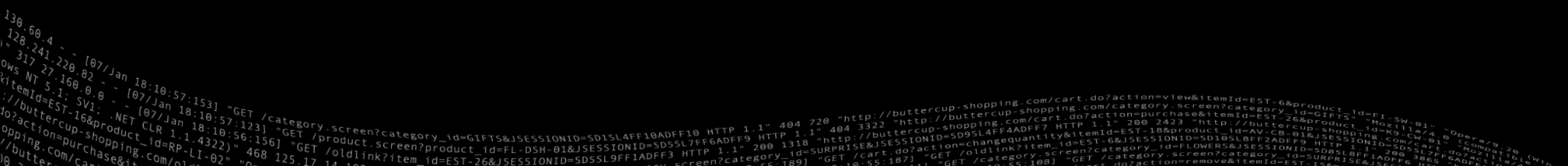
Build Resilient Security Infrastructure

- **Technology**
  - Legacy SIEM
  - Anti-Virus
  - IPS/IDS
  - Blackhole/Sinkhole
  - Sandboxes
  - Application Whitelisting

Security Posture

- **Philosophy**
  - Response
  - Signature based
  - Alert based
  - Mitigation focused
  - Tool focused
  - IOC focused
  - Limited data ingestion

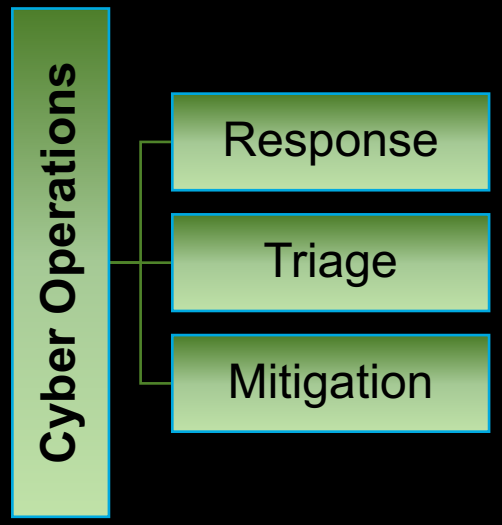
Capability Posture



splunk> .conf2017

© 2017 SPLUNK INC.

Cyber Maturity Evolution



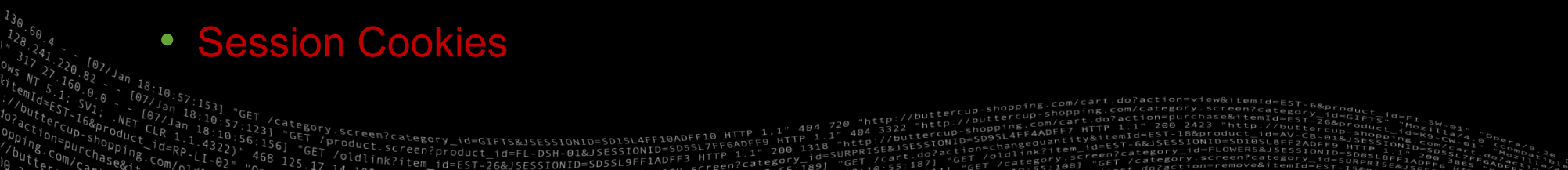
- **Philosophy Changing**
  - Use Cases
  - Behaviors
  - Visibility focused

Capability Posture

© 2017 SPLUNK INC.

Cyber Attack 2014

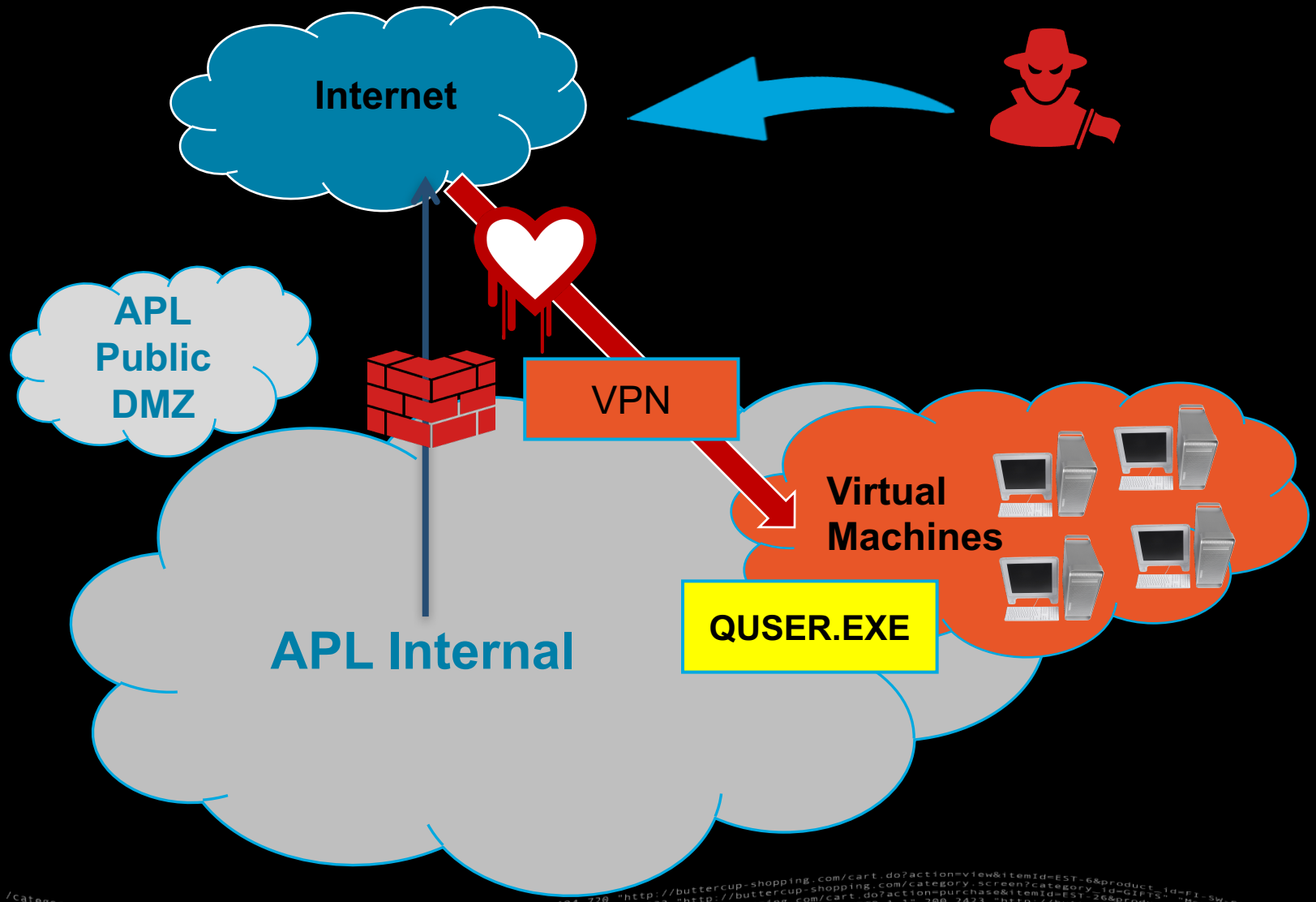
- Heartbleed
  - CVE-2014-0160 (Common Vulnerability & Exposures)
  - Publicly disclosed in April 2014
  - Vulnerability in the OpenSSL cryptography library
  - When it is exploited it leads to the leak of memory contents from the server to the client and from the client to the server
  - What is in memory?
    - Encryption keys
    - Usernames
    - Passwords
    - Session Keys
    - Session Cookies



splunk> .conf2017

© 2017 SPLUNK INC.

APL Unclassified Network



splunk> .conf2017

© 2017 SPLUNK INC.

The Landscape is Changing

Emergence of New Methodologies

splunk> .conf2017

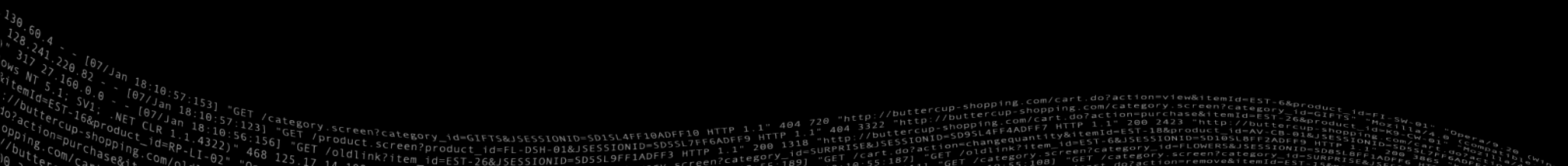
© 2017 SPLUNK INC.

Defense Partner – March IR Collaboration

- **Never Let a Good Incident Go to Waste**
  - Extensive use of commercial cloud and SSL
    - Command & Control
    - Exfiltration
    - Distributing malware
    - Constantly changed infrastructure
  - PowerShell
    - Reflective injection into memory
    - Lateral movement
    - Reconnaissance
  - Persistence
    - Windows Management Instrumentation (WMI)
    - Scheduled tasks
    - Registry (RunOnce)
  - Actor's actions on network – more agile than incident responders

Defenders had limited network visibility

Living off the Land

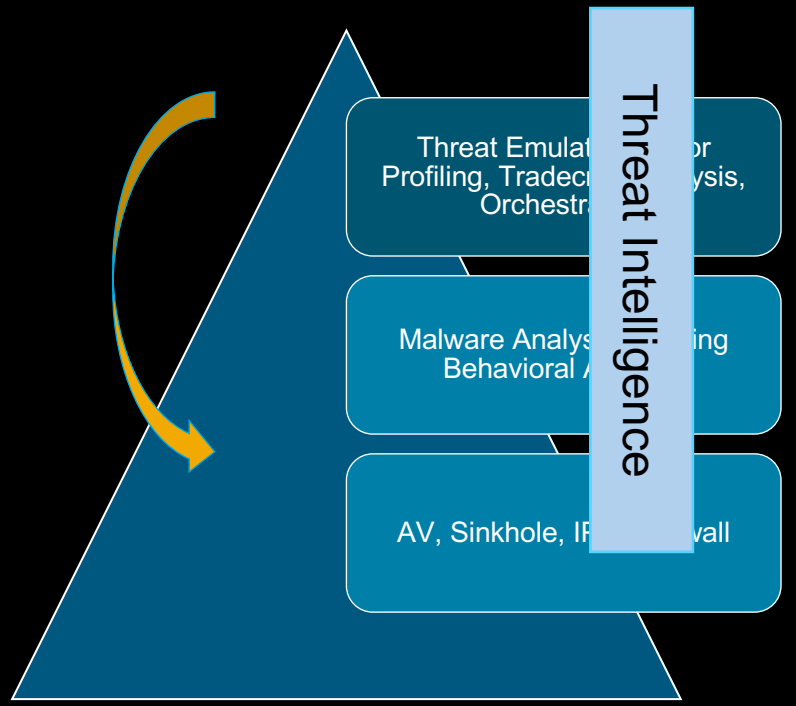


splunk> .conf2017

© 2017 SPLUNK INC.

Change in Philosophy

- Threat Focused Cyber Operations
  - Research and identify Threats targeting your organization
  - Target advanced tactics, techniques and procedures of adversary
  - Emulate threat in your environment
  - Develop hunting and analytics techniques
- Changes, Challenges & Culture
  - What is behavioral monitoring anyways?
  - Mitigation vs Detection
    - Not everything can be mitigated
    - Value in Visibility
  - What is Threat Intelligence?
    - More than indicators of compromise



splunk> .conf2017

© 2017 SPLUNK INC.

Defensive Cyber Operations Inception

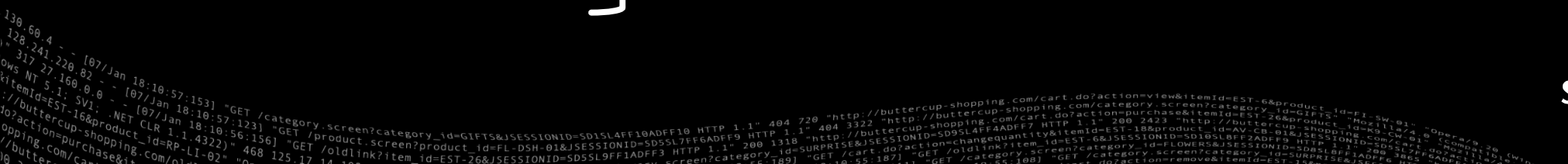
Philosophy

- Use Cases
- Data Analysis
- Behaviors
- Visibility based
- Agility
- Enrichment
- Automation
- Independence
- DevOps

Capability Posture

- **Technology**
  - Splunk
  - EDR
- **People**
  - New skillsets
  - New approach
- **Process**
  - Hunting
  - Agility

Vehicle For Change



splunk> .conf2017

© 2017 SPLUNK INC.

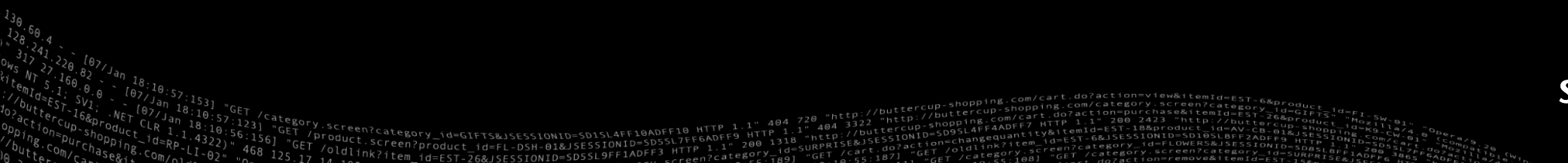
Change in Technology

Legacy SIEM implementation

- A few specialists creating content
- Very static and signature content
- Run scheduled reports for data analysis
- Only acquire logs that you need

Splunk

- All analysts creating content
- Dynamic & behavioral content
- Google like query language for agility
- More visibility means more data



splunk> .conf2017

© 2017 SPLUNK INC.

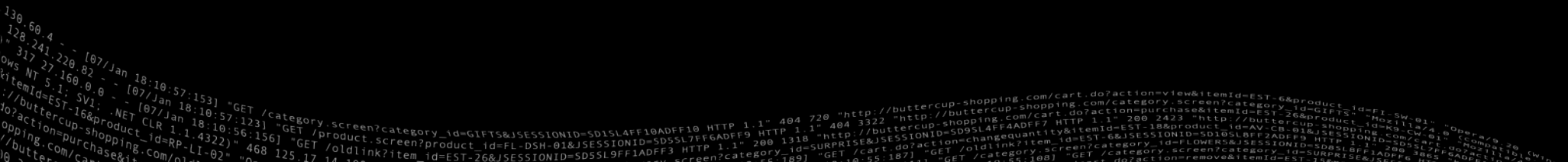
Change in People

Traditional Cyber Skillset

- Firewall Management
- IPS/IDS administrator
- Implementing rule/signature rulesets
- Strong network competencies
- Dead box forensics
- Implement mitigations

Adaptive Skillset

- Data manipulation capabilities
- OS internals
- Malware & memory analysis
- Strong research skills
- Collaborative teams
- Red Team skills
- Constant development of skills



splunk> .conf2017

© 2017 SPLUNK INC.

Change in Process

Analysts followed procedures

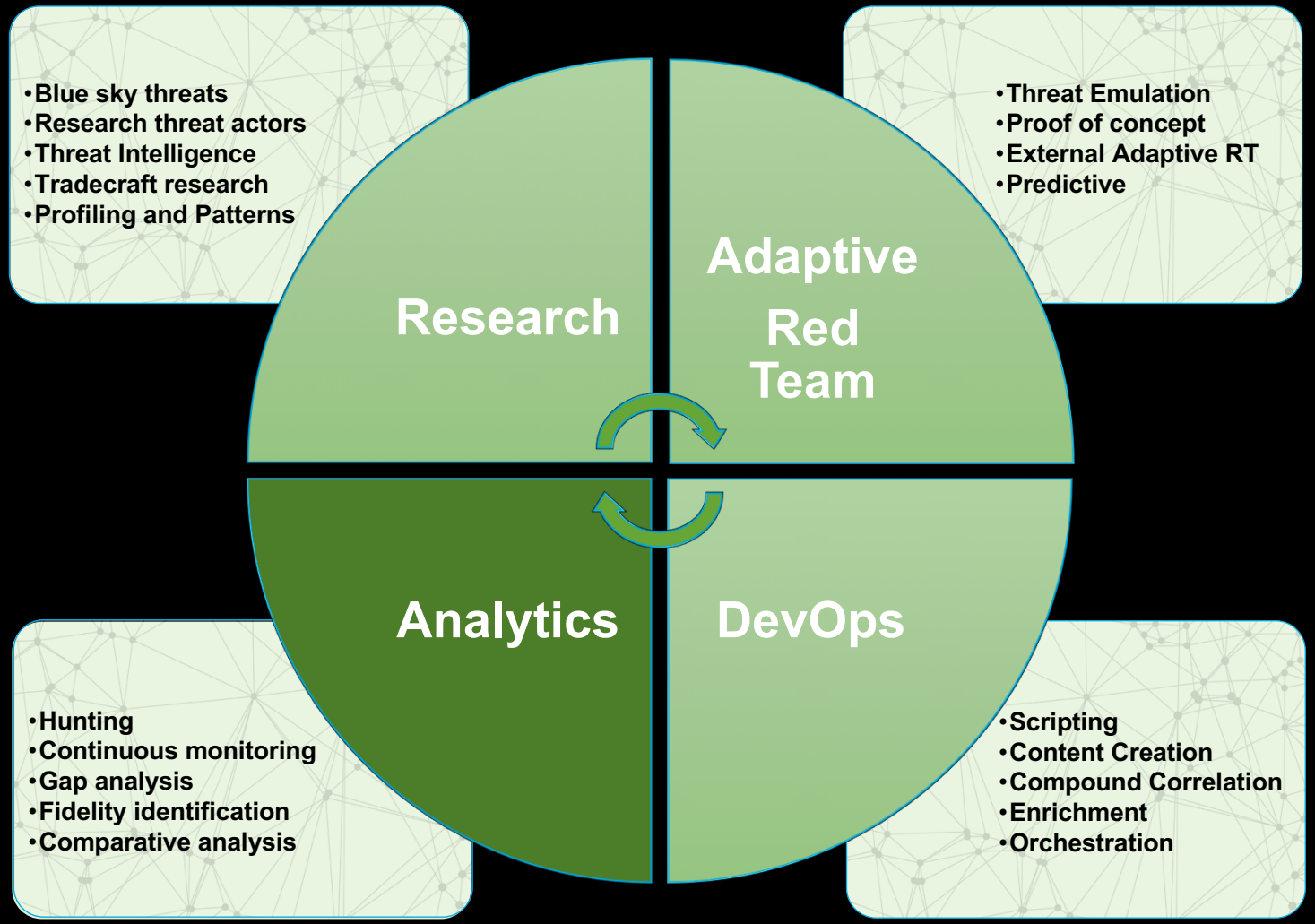
- Responded to alerts
- Followed playbooks
- Implemented mitigations

Analysts Performing Analysis

- Hunting for anomalies
- Researching threats
- Understanding adversary tradecraft
- Emulating threats
- Developing new analytics, content & alerts
- Understanding context

© 2017 SPLUNK INC.

Cyber Threat Team Construct



© 2017 SPLUNK INC.

Putting It All Together

splunk> .conf2017

© 2017 SPLUNK INC.

Research

What are the adversary's doing?

- **Blue sky threats**
  - What if…
  - Based on our environment and Threat Intel
  - LoE, ROI, Likelihood
- **Threat Intelligence**
  - Research threat actors
  - Tradecraft research
  - Emerging capabilities
- **Threat Models**
  - Behaviors
  - **Adversary profiling**


```
Invoke-WmiMethod -Class Win32_
'whoami', $null

Get-WmiObject -Class Win32_Net
```

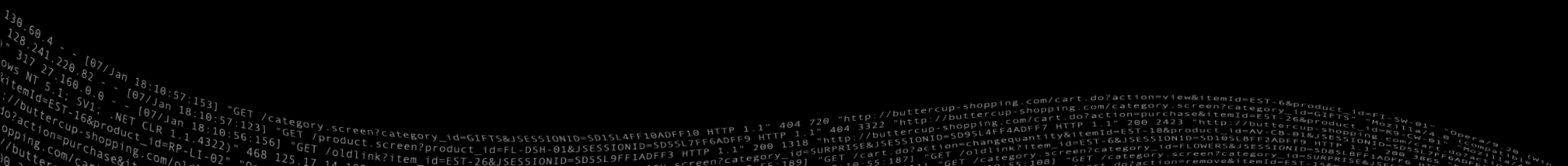
```
powershell.exe -NonInteractive -ExecutionPolicy Bypass -EncodedCommand
ZgB1AG4AYwB0AGkAbwBuACAAcABlAHIAZgBDAHIAKAAkAGMAcgBUAHIALAAgACQAZABhAHQ
```

splunk> .conf2017

© 2017 SPLUNK INC.

Adaptive Red Team

- **Proof of concept**
  - Predictive
  - Research driven
- **Threat Emulation**
  - Lateral movement
  - Privilege escalation
  - Persistence methodologies
  - Initial code execution
- **External Adaptive RT**
  - Comprehensive attack & response lifecycle



splunk> .conf2017

© 2017 SPLUNK INC.

DevOps

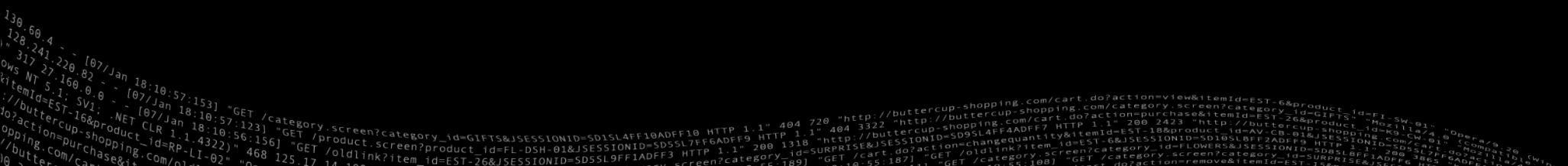
- **Scripting**
  - Forensic tool development
  - Data parsing
  - Orchestration
  - Enrichment
- **Application Development**
  - Threat Tracking System
  - REnigma
- **Content Creation**
  - Use Case Development
  - Compound Correlation
  - YARA development

splunk> .conf2017

© 2017 SPLUNK INC.

Analytics

- **Proactive Threat Hunting**
  - Process behaviors
  - Network behaviors
  - Account behaviors
- **Uniqueness/Rareness/Newness**
  - Email
  - FQDN
- **Gap analysis**
  - Visibility
  - Technology
  - People
- **Content review**
  - Threat scoring
  - Prioritization



splunk> .conf2017

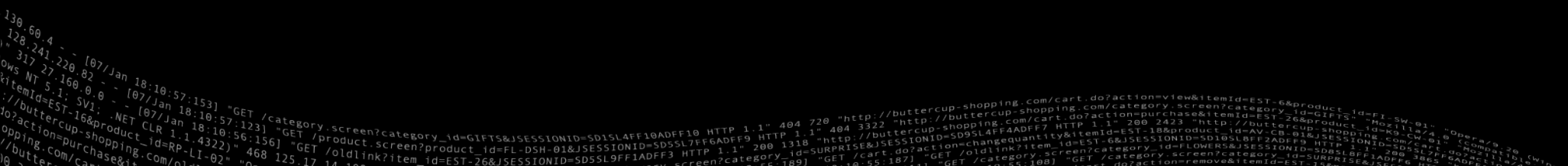
© 2017 SPLUNK INC.

Challenges & Wins

© 2017 SPLUNK INC.

Challenges

- Splunk Core is not a traditional SIEM
  - Uniqueness identifiers
  - Tagging events
- Expensive Live queries
- Sub-Search limitations
- An imperfect start is better than a perfect unimplemented plan
- Leverage existing talent in Cyber Operations
- Managing larger data sets – the cost of visibility
- Solving the same problems differently

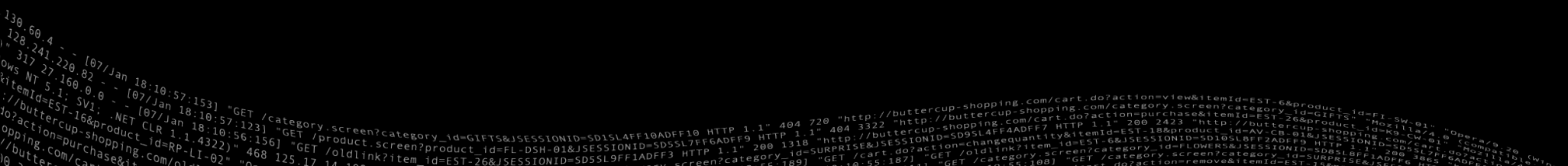


splunk> .conf2017

© 2017 SPLUNK INC.

Wins

- Leveled analyst playing field
- APT targeting
- DMZ Breach
- Red Team
- No formal Splunk training



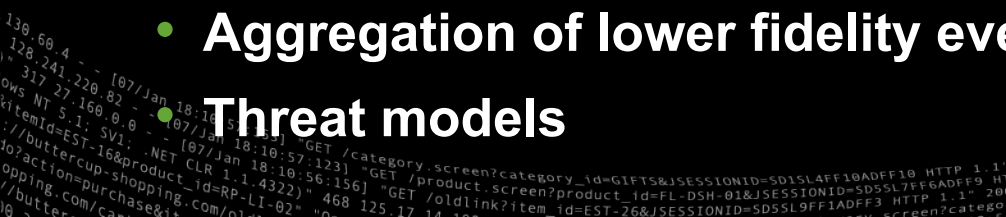
splunk> .conf2017

© 2017 SPLUNK INC.

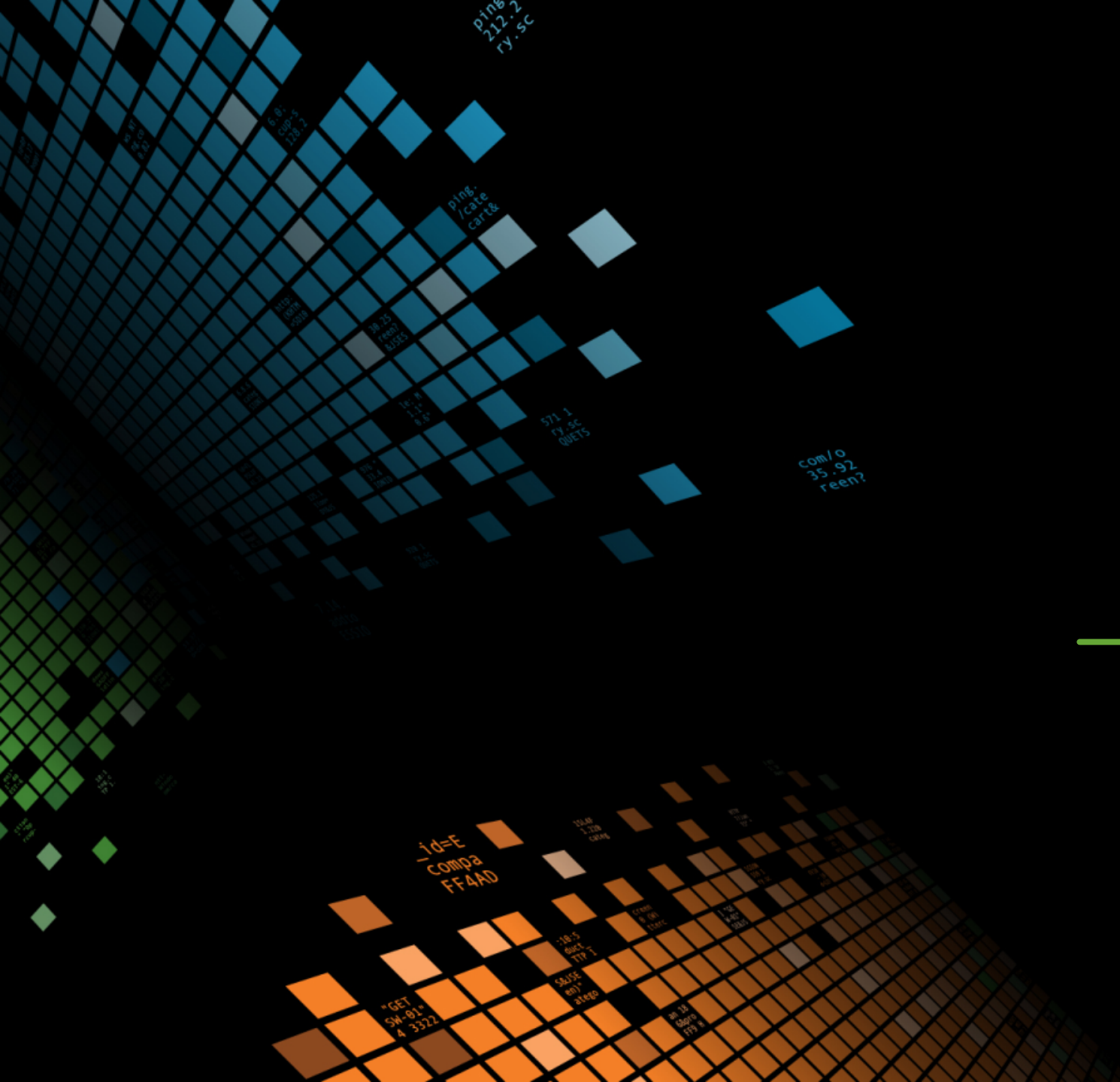
Adaptive Red Team Exercise

The Fruits of Our Labor

- Hits on existing custom developed content
- Anomalies associated with credential theft
  - Mimikatz
- RPC & SMB baseline drift
  - Lateral movement
  - AD Reconnaissance
- Privileged account usage
  - Uniqueness
  - Rareness
- Bubble-Up Analytics
  - Aggregation of lower fidelity events of interest
  - Threat models



© 2017 SPLUNK INC.



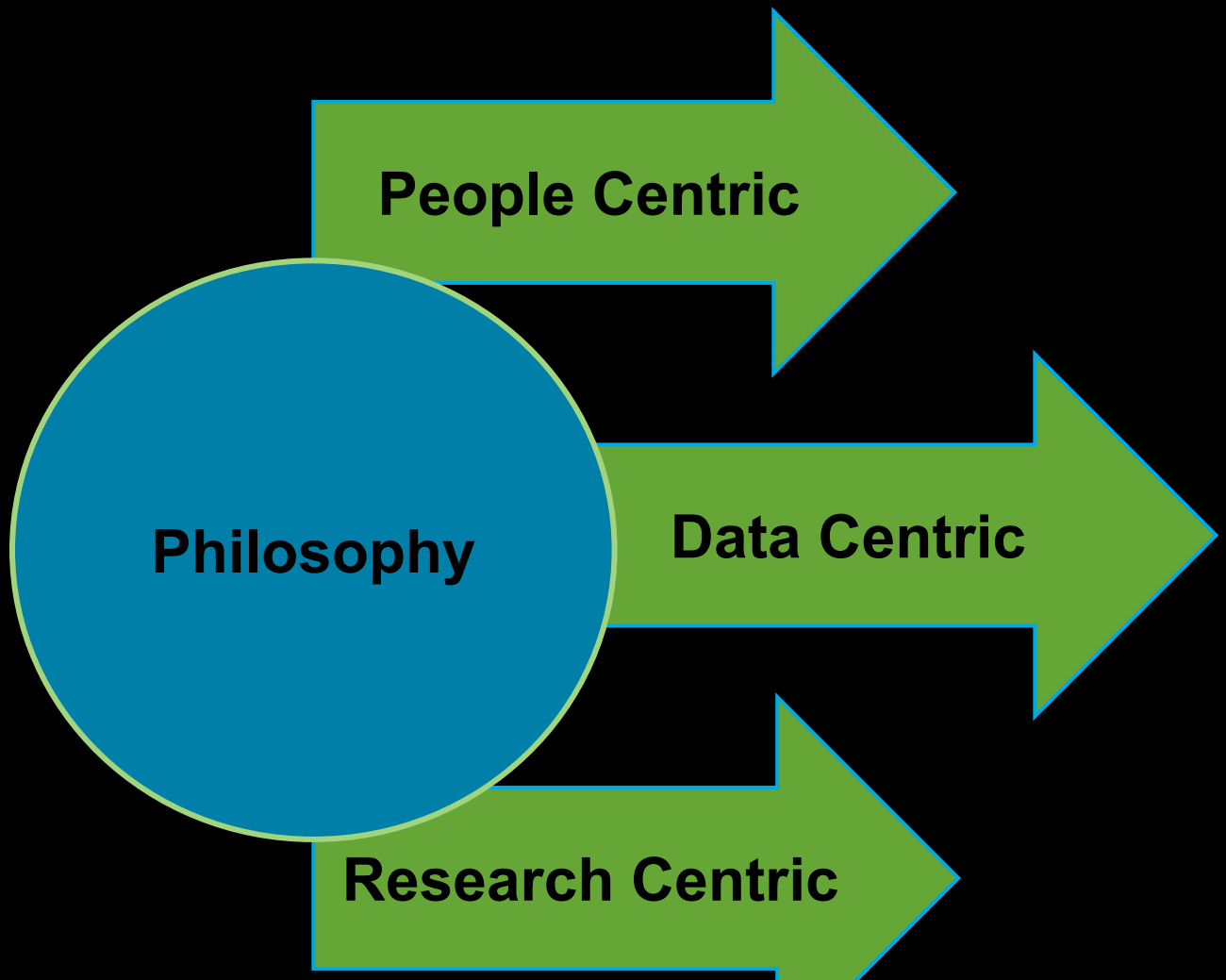
Summary

Key Takeaways

splunk> .conf2017

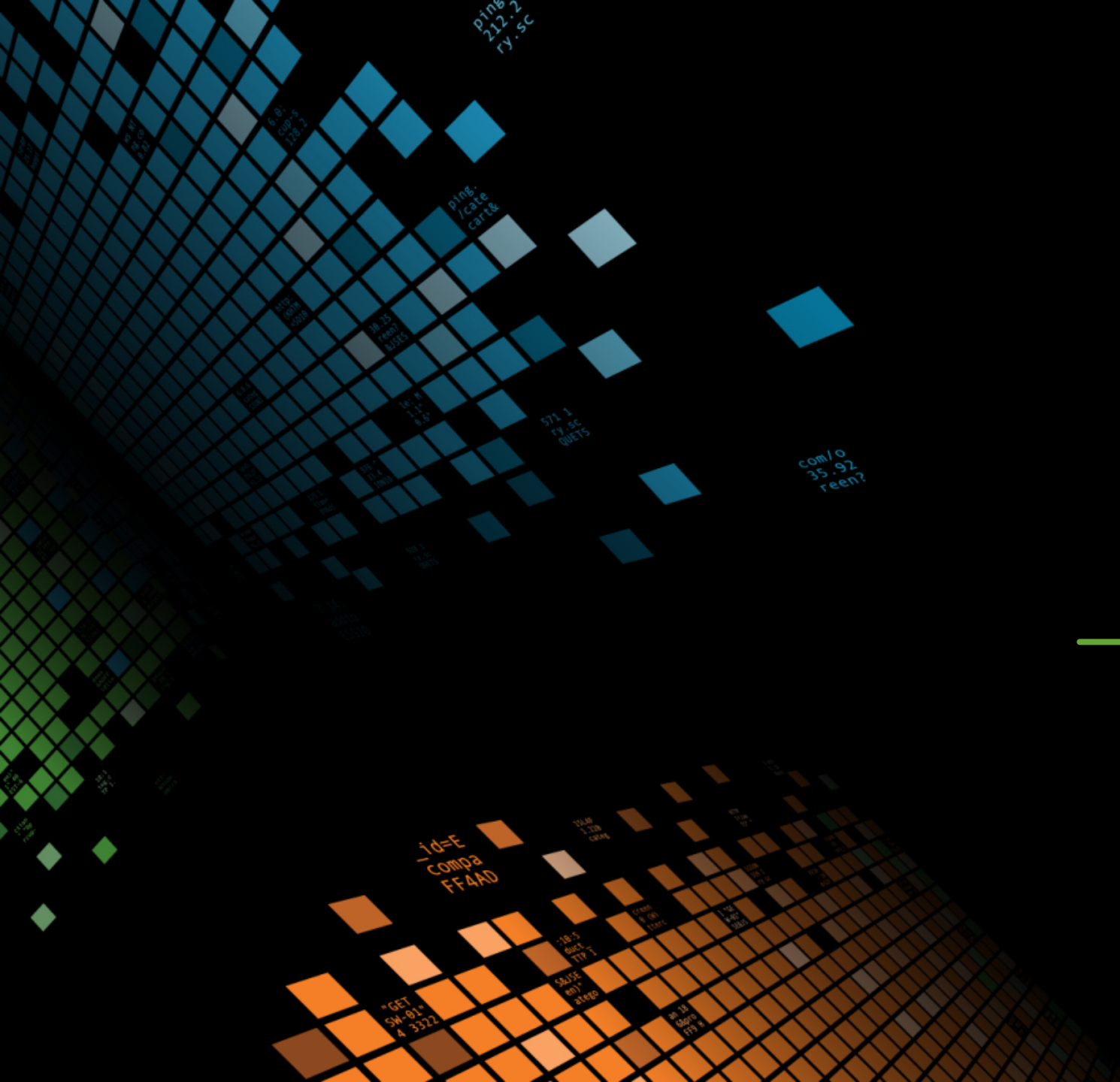
© 2017 SPLUNK INC.

Summary



splunk> .conf2017

© 2017 SPLUNK INC.



Questions

© 2017 SPLUNK INC.

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