© 2017 SPLUNK INC.

splunk> .conf2017

From Monitoring and Alerting to Ensuring Mission Readiness Through Improved Availability

Tunay Basar | Vice President & CIO – Pernix Consulting LLC

September 26th | Washington, DC

© 2017 SPLUNK INC.

Tunay Basar & Pernix

Brief Introduction

- An economically disadvantaged and Veteran-owned small business
- Specializes in cyber security, software engineering & integration
- Pernix Consulting's Core Competencies:
  - Software Engineering, Data Analytics, Enterprise Business Process Management, Project Management, Employee Resource Management
- Tunay Basar, CIO and Co-Founder of Pernix, with over 20 years in the IT industry providing software and cyber security solutions.
- DUNS Number: 966841947 , Cage Code: 74PQ1
- Customers:
  - Department of State, Department of Treasury, Department of Navy

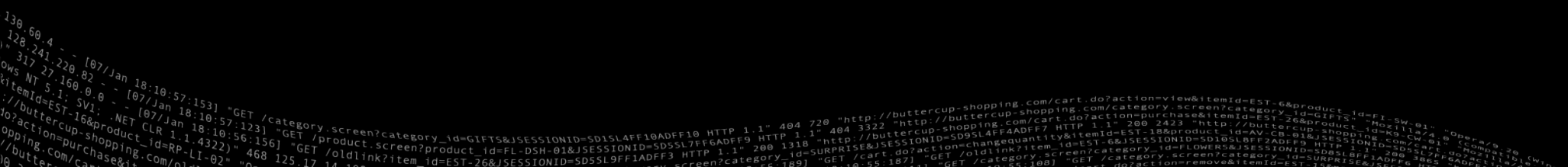
splunk> .conf2017

© 2017 SPLUNK INC.

Our Customer: Diplomatic Security

IT Operations – Mission Critical Systems

- Support of Mission critical systems and applications
- Global user base and 24x7 operation
- Performance and availability is absolutely essential
- End-to-end visibility critical to get to root cause fast
- Number of resources and time it takes to resolve issues



splunk> .conf2017

© 2017 SPLUNK INC.

Our Customer: Diplomatic Security

The Challenge

200+

200+ VM & Physical Servers

70+

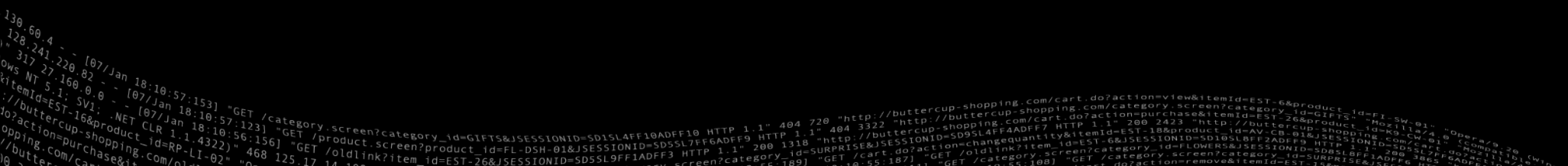
Critical Applications

99.9%

System Availability

300+

Systems requiring FISMA Compliance



splunk> .conf2017

© 2017 SPLUNK INC.

The Approach

© 2017 SPLUNK INC.

Requirements & Actions

- Critical Application Monitoring
  - Began with highly critical applications at first
  - Alerts designed to inform Ops when applications encounter issues
- VM & Hardware Monitoring
  - Collecting data from 200+ VMs and physical servers
  - High level dashboards to watch over the health of the systems
  - Detailed dashboards provide the tools for Ops to troubleshoot issues
  - Alerts & Reports help inform Operations of critical issues
- New Challenges
  - Our customers challenges us with new requests daily
  - We have yet to say “we can’t provide that”, as long as we have the data

splunk> .conf2017

© 2017 SPLUNK INC.

Alerts and Reports

© 2017 SPLUNK INC.

Notifications

Getting the right data to the right individuals

1. Alerts are used to inform operation center of critical issues by email
2. Emails contain detail about the issue in hand
3. Operation center is equipped with detailed dashboards to further troubleshoot issues

© 2017 SPLUNK INC.

High Level Dashboard

Summary of Systems

hostname	Description	Severe	Warning	Metrics
[redacted]		1 metrics needing immediate attention.	0 metrics needing attention soon.	memory
[redacted]		0 metrics needing immediate attention.	2 metrics needing attention soon.	C: memory
[redacted]		0 metrics needing immediate attention.	1 metrics needing attention soon.	C:
[redacted]		0 metrics needing immediate attention.	1 metrics needing attention soon.	C:
[redacted]		0 metrics needing immediate attention.	1 metrics needing attention soon.	C:
[redacted]		0 metrics needing immediate attention.	1 metrics needing attention soon.	C:
[redacted]		0 metrics needing immediate attention.	1 metrics needing attention soon.	C:
[redacted]		0 metrics needing immediate attention.	1 metrics needing attention soon.	memory
[redacted]		0 metrics needing immediate attention.	1 metrics needing attention soon.	C:
[redacted]		0 metrics needing immediate attention.	1 metrics needing attention soon.	C:

« prev 1 2 3 4 5 6 7 8 9 10 next »

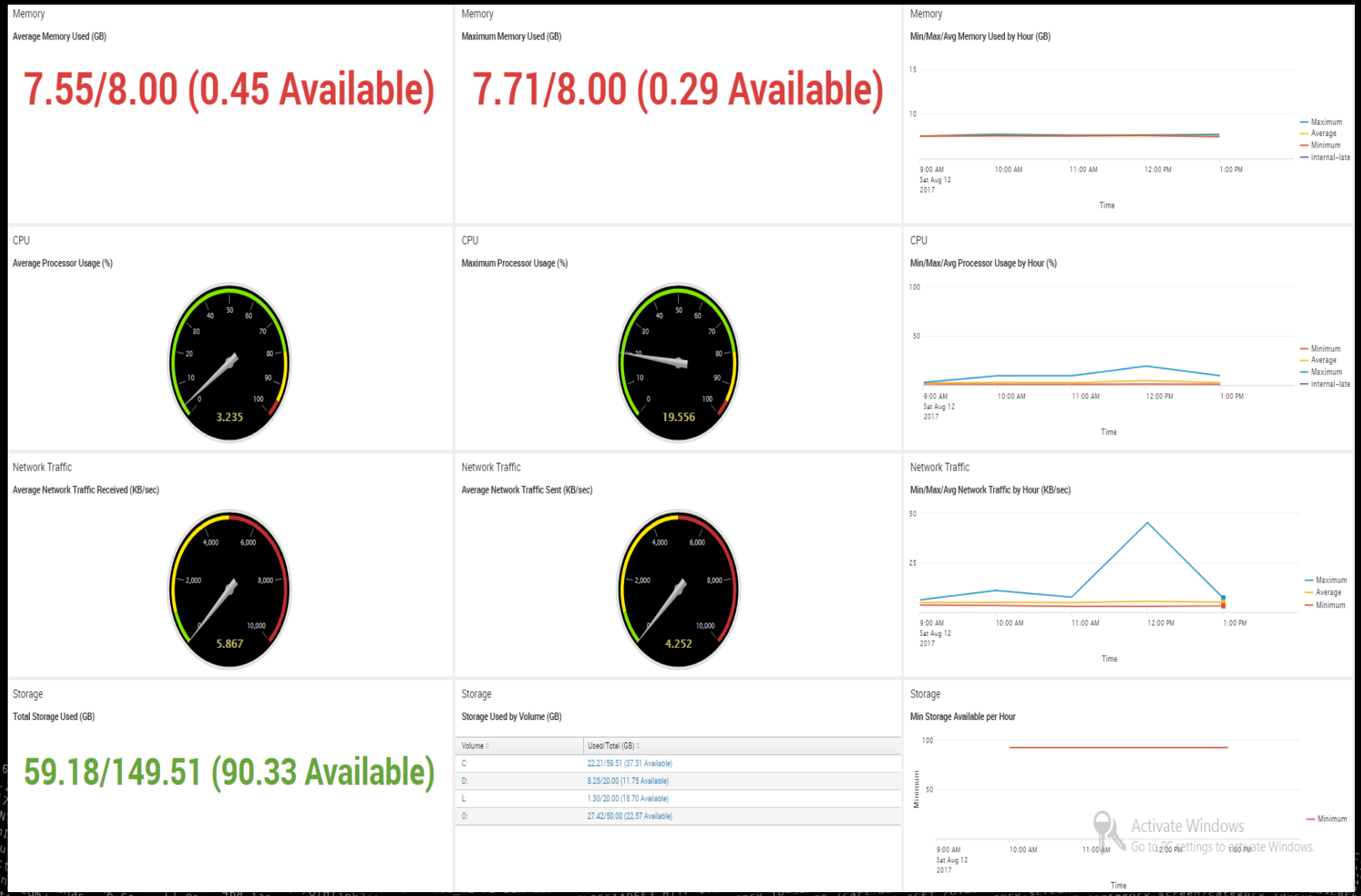
- Metrics are fed in from secondary detailed dashboards.
- Systems with critical issues highlighted in red.
- Metrics column indicates the issue without drilling into the detailed dashboard.

splunk> .conf2017

© 2017 SPLUNK INC.

Detailed Dashboard

System Information Dashboard



- System details include:
  - Memory Utilization
  - CPU Utilization
  - Network Utilization
  - Storage Utilization
  - Process Details

Activate Windows
Go to PC settings to activate Windows.

splunk> .conf2017

© 2017 SPLUNK INC.

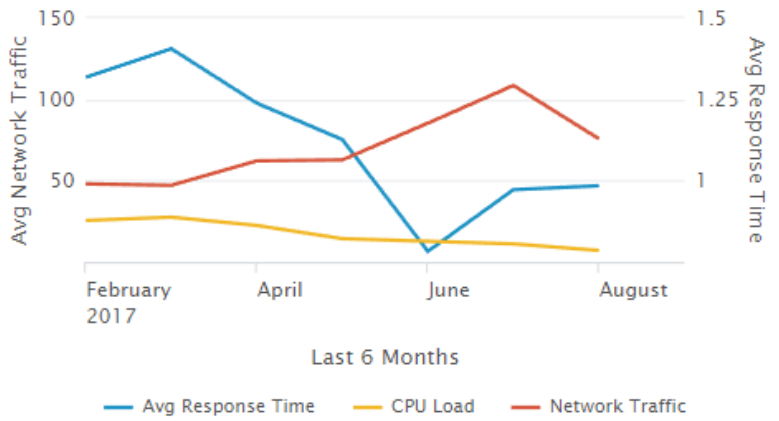
Reports

Regularly Scheduled Reports – Overview of Systems

System Experience (Last 6 Months)

Edit | Export | ...

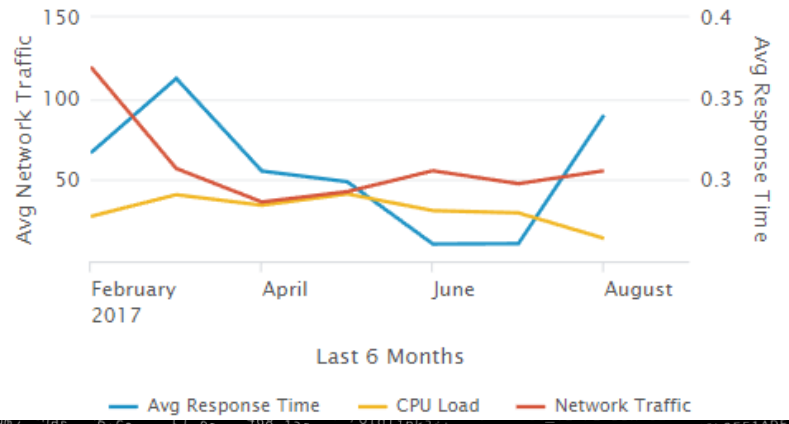
BPM Management (Last 6 months)



BPMS Management (Last 6 Months Breakdown)

	Time	Avg Response Time	CPU Load	Network Traffic
1	2017-February	1.318074	25.516119	48.104010
2	2017-March	1.405723	27.515971	47.117176
3	2017-April	1.238157	22.419293	62.152502
4	2017-May	1.126328	14.287948	62.739027
5	2017-June	0.782503	12.679279	85.345958
6	2017-July	0.972003	11.065989	108.532483
7	2017-August	0.984483	7.053980	75.586557

IMS Management (Last 6 months)



IMS Management (Last 6 Months Breakdown)

	Time	Avg Response Time	CPU Load	Network Traffic
1	2017-February	0.316696	27.576913	119.832177
2	2017-March	0.362426	40.897140	57.031809
3	2017-April	0.305458	34.423068	36.444340
4	2017-May	0.298866	41.357101	42.789996
5	2017-June	0.260584	31.118744	55.646087
6	2017-July	0.260805	29.715888	47.693286
7	2017-August	0.339867	14.089298	55.750892

- SLA Reports
- Backup Reports
- Inventory Reports
- Security Reports
- User Experience Reports
- Benchmarking Reports

splunk> .conf2017

© 2017 SPLUNK INC.

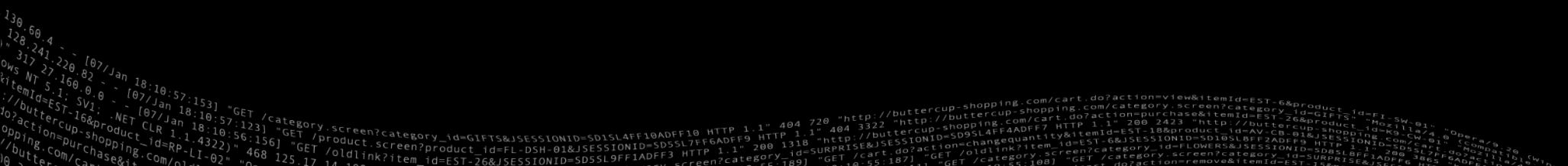
Reports

Regularly Scheduled Reports – Overview of Systems

BPMS (The Top 10 Slowest URI's based on the Top 10 Most Active Users)

	User	Web Page	Avg Response Time
1	User6	/metastorm/eFolder.aspx	45.914625
2	User7	/Metastorm/eFolder.aspx	34.444485
3	User2	/Metastorm/Default.aspx	28.875000
4	User4	/Metastorm/eFolderFormContents.ashx	25.687000
5	User8	/Metastorm/eFolder.aspx	25.511435
6	User1	/metastorm/eFolderFormContents.ashx	24.367000
7	User8	/Metastorm/eFolderFormContents.ashx	23.086000
8	User4	/Metastorm/eForm.aspx/StartAction	21.433174
9	User7	/Metastorm/eFolderFormContents.ashx	21.278000
10	User5	/Metastorm/eActionFormContents.ashx	21.105000

- SLA Reports
- Backup Reports
- Inventory Reports
- Security Reports
- User Experience Reports
- Benchmarking Reports



splunk> .conf2017

© 2017 SPLUNK INC.

Before & After Splunk

Example Scenario of a System Outage

Without Splunk Monitoring

- Server outage also takes down the application(s) on the server.
- No notifications sent
- User of the system/application notices the outage and submits a trouble ticket
  - Ticket is received & confusion begins
  - Is it the app or the server?
  - Which group will fix it?

It could be hours if not days before the issue is addressed

With Splunk Monitoring

- Splunk detects issue, sends out alert
- Based on the alert, operations determines the cause
  - Splunk also knows which applications run on this server, therefore alerting that those applications are also impacted.
- The right groups are engaged to fix the issue

System is up in less than 10 minutes

splunk> .conf2017

© 2017 SPLUNK INC.

Lessons Learned & Best Practices

splunk> .conf2017

© 2017 SPLUNK INC.

Lessons Learned & Best Practices

- Switched from VMs to Physical servers
- Separate data into indexes to speed up searches and simplify queries
- Deployment Server to manage forwarders & automate app push
- Scheduled searches for busy dashboards
- Don’t use zero events to trigger alerts (False positive. Ex: indexer down)
- Cron schedule for mass inputs. Inputs kick off upon restart and slowdown system
- Splunk DB Connect is a must have

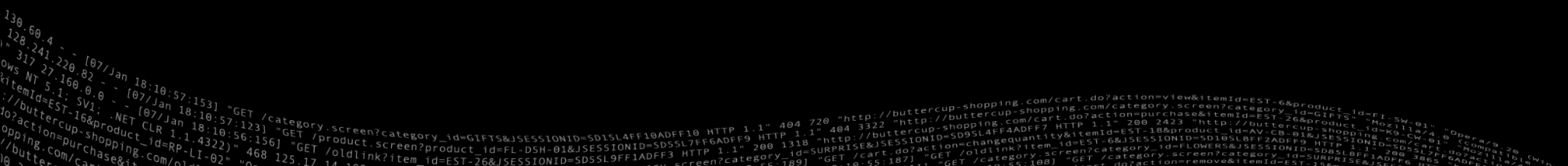
splunk> .conf2017

© 2017 SPLUNK INC.

Current IT Operations Value Drivers

Yearly Value of : $1,493,589 using Splunk to date

#1 - Reduce the number of system incidents by	45%	Cost Avoidance (5400 hours saved) - Direct Benefit	$281,250
#2 - Accelerate investigation of system incidents by	90%	Cost Avoidance (4752 hours saved) - Direct Benefit	$247,500
#3 - Reduce service desk calls from fewer system incidents by	85%	Cost Avoidance (0 hours saved) - Direct Benefit	$0
#4 - Avoid financial impact from fewer system outages by	85%	Increased Margins - Direct Benefit	$659,880
#5 - Reduce business process impact by	85%	Cost Avoidance (0 hours saved) - Direct Benefit	$0
#6 - Streamline system problem management by	90%	Cost Avoidance (1588 hours saved) - Direct Benefit	$78,553
#7 - Optimize server capacity by	5%	Cost Avoidance - Direct Benefit	$0
#8 - Consolidate operational tools and/or external services by	100%	Cost Avoidance (0 hours saved) - Direct Benefit	$0
#9 - Optimize storage capacity management by	5%	Cost Avoidance - Direct Benefit	$0
#10 - Automate repetitive NOC procedures by	70%	Reduced Expenses (3780 hours saved) - Direct Benefit	$226,406



splunk> .conf2017

© 2017 SPLUNK INC.

Security

© 2017 SPLUNK INC.

User Behavior

Continues User Monitoring

Account Usage

host	Account Lockouts	Account Login with Explicit Credentials	Built-In Account Activity	Failed User Account Login
	0	3	0	766
	0	11	0	255
	1	9	1	8
	1	11	1	7
	1	10	1	7
	0	15	0	6
	0	9	0	2
	0	4	0	2
	0	3	0	2
	0	5	0	2

« prev 1 2 3 4 5 6 7 8 9 10 next »

Event Logs Cleared

host	Count: Event Log was Cleared	Count: Security Log was Cleared	Trend: Event Log was Cleared	Trend: Security Log was Cleared
	40	20		
	22	11		
	22	11		
	20	10		
	20	10		
	20	10		
	20	10		
	20	10		
	20	10		
	20	10		

« prev 1 2 3 4 5 6 7 next »

- Monitoring user account activities
- Identify unusual behavior
- Identify privileged users and their activities

splunk> .conf2017

© 2017 SPLUNK INC.

User Behavior

Continuous Monitoring

Software and Service Installation

host	MSI File Removed	New Kernel Filter Driver	New MSI File Installed	New Windows Service	Windows Update Installed
[redacted]	0	16	0	2	0
	0	14	0	2	0
	0	7	0	1	0
	0	7	0	1	0
	0	7	0	1	0
	0	8	0	1	0
	0	8	0	1	0
	0	7	0	1	0
	0	8	0	1	0
	0	8	0	1	0

« prev 1 2 3 4 5 6 7 8 9 10 next »

- Monitor suspicious software activity on systems
- Windows Event logs
- Custom PowerShell scripts

splunk> .conf2017

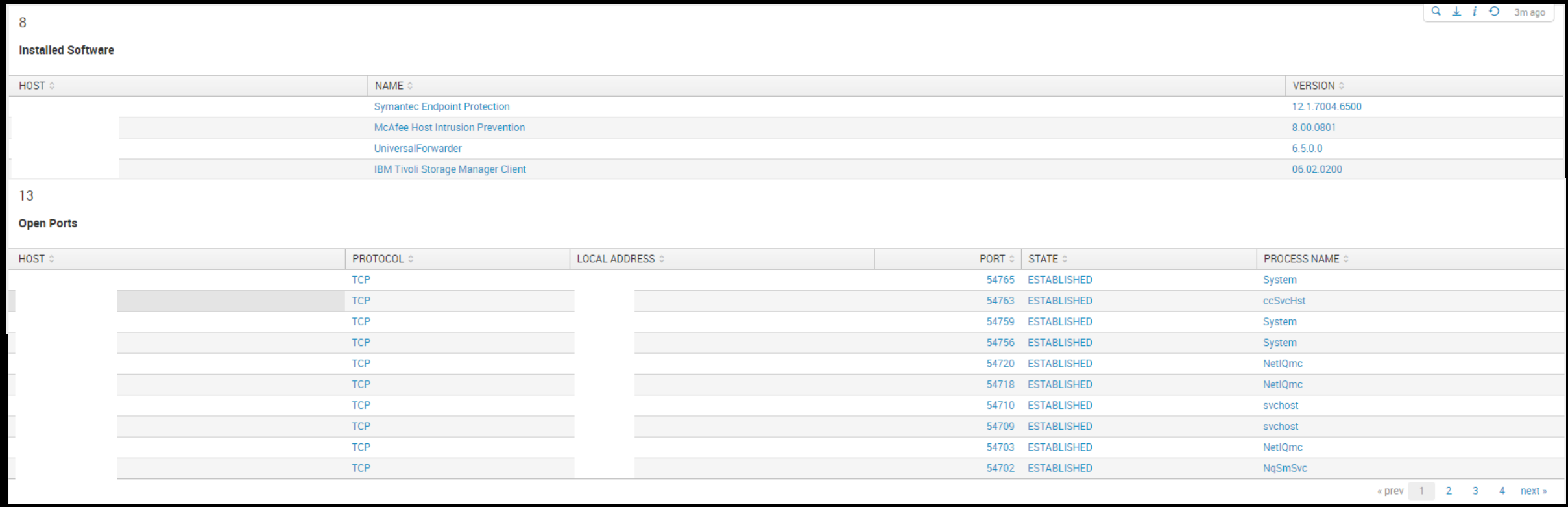
© 2017 SPLUNK INC.

Compliance

© 2017 SPLUNK INC.

Security Compliance

Automated System Assessment



8

Installed Software

HOST	NAME	VERSION
	Symantec Endpoint Protection	12.1.7004.6500
	McAfee Host Intrusion Prevention	8.00.0801
	UniversalForwarder	6.5.0.0
	IBM Tivoli Storage Manager Client	06.02.0200

13

Open Ports

HOST	PROTOCOL	LOCAL ADDRESS	PORT	STATE	PROCESS NAME
	TCP		54765	ESTABLISHED	System
	TCP		54763	ESTABLISHED	ccSvcHst
	TCP		54759	ESTABLISHED	System
	TCP		54756	ESTABLISHED	System
	TCP		54720	ESTABLISHED	NetIQmc
	TCP		54718	ESTABLISHED	NetIQmc
	TCP		54710	ESTABLISHED	svchost
	TCP		54709	ESTABLISHED	svchost
	TCP		54703	ESTABLISHED	NetIQmc
	TCP		54702	ESTABLISHED	NqSmSvc

« prev 1 2 3 4 next »

- System assessments were done manually
- Extremely labor intensive
- Single system could take weeks to complete
- With Splunk: Immediate access to assessment data

splunk> .conf2017

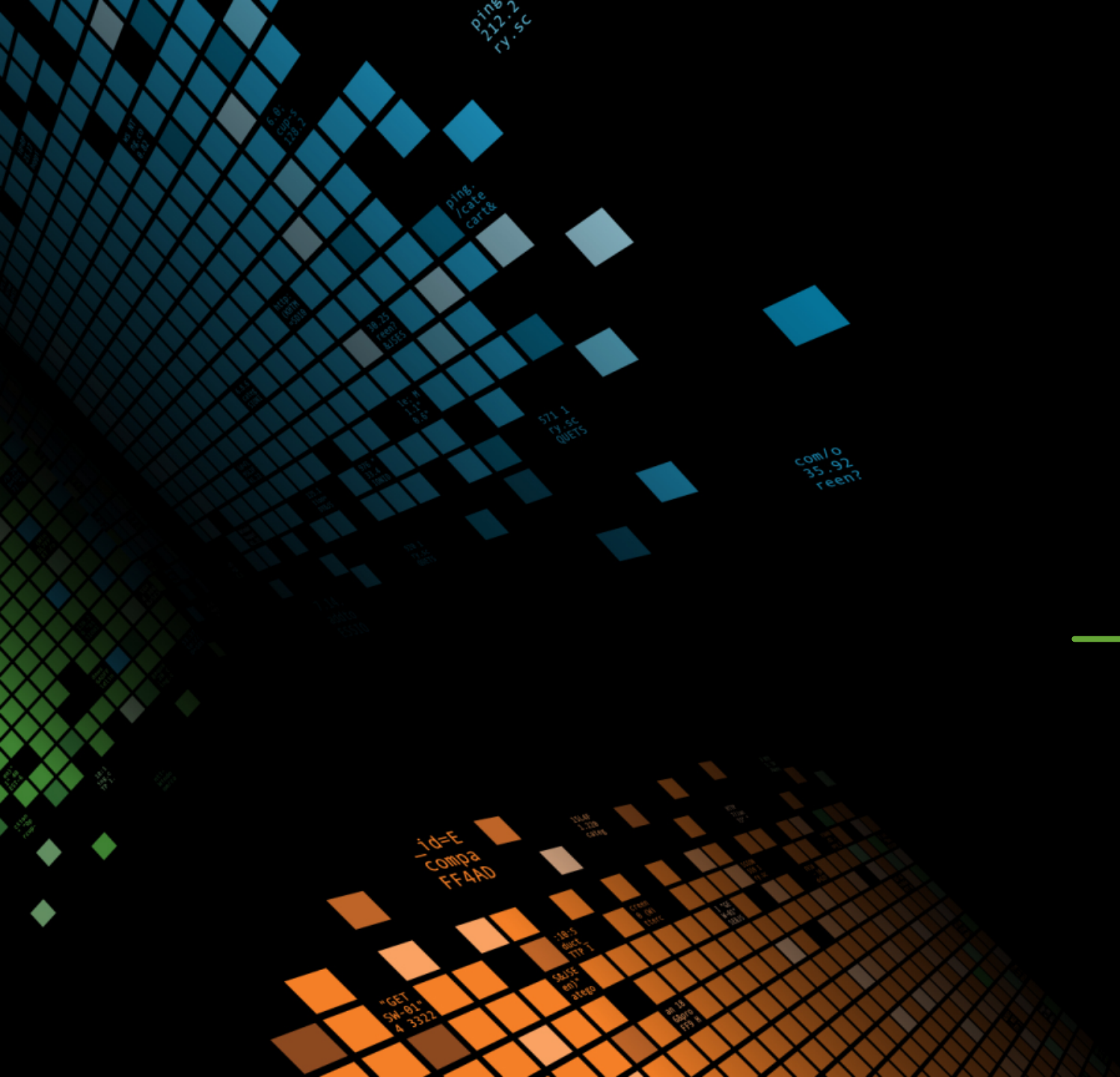
© 2017 SPLUNK INC.

What's Next

Continuous Innovation

- Machine Learning
  - Adaptive Thresholds
  - Fraud Detection
- Automated Account Management
- Self service portal (alerts/reports)
- Splunk for FISMA app
- Move infrastructure to the cloud

© 2017 SPLUNK INC.



Q&A

© 2017 SPLUNK INC.

Thank You

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