

splunk® > live!

APRIL 20TH, 2017 | MINNEAPOLIS, MN

splunk® > live!

APRIL 20TH, 2017 | MINNEAPOLIS, MN

Building the Analytics-Driven SOC

Chris Bauer | Solution Engineering Director

Safe Harbor Statement

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.

Agenda

1. A look at traditional security operations
2. Best practices and emerging trends
3. The security ops technology stack
4. How to use Splunk solutions for an Analytics-Driven SOC
5. Customer Successes

44%



do not have an SOC.



51%

Only 51% of organizations with a SOC initiate an investigation within one hour of a discovered incident

Source : EY Global Information Security Survey 2015



23%

Only 23% consider their SOC to be tightly integrated with heads of business to regularly understand business concerns

42%

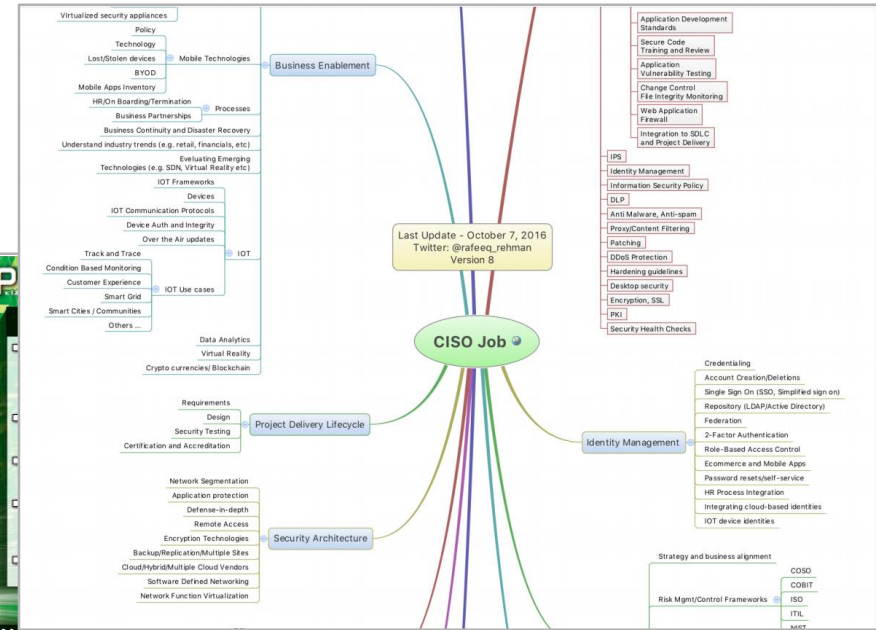
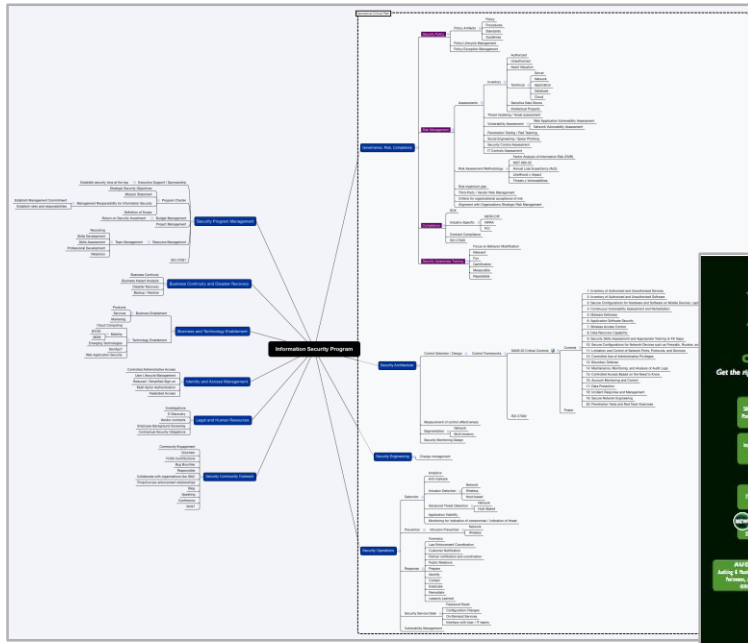
of organizations claim not to have had a significant incident

Source : EY Global Information Security Survey 2015

Traditional Security Operations



Security Programs: The Big Picture



[13] <https://www.sans.org/security-resources/posters/leadership/security-leadership-poster-135>

[14] <http://rafeeqrehman.com/2016/10/07/announcing-ciso-mindmap-2016/>

Security Programs: The Big Picture



[13] <https://www.sans.org/security-resources/posters/leadership/security-leadership-poster-135>

[14] <http://rafeegrehman.com/2016/10/07/announcing-ciso-mindmap-2016/>

What do we see?

A Traditional Security Critical Path

Security Operations: part of the bigger picture...

**Risk &
Compliance**

**Security
Operations**
(Includes SOC)

**Security
Architecture**

**Security
Engineering**

Types of Traditional SOC's...

- ▶ Virtual SOC (VSOC)
- ▶ Multifunction NOC/SOC
- ▶ Command SOC
- ▶ Co-Managed SOC
- ▶ Crew SOC? (This one's ours)

[1] <https://www.gartner.com/doc/3479617>

Traditional SOC

Alert Pipeline?



“A perception of the SOC as a big alert pipeline is outdated and does not allow the organization to make use of more active processes such as internal TI generation and threat hunting.”

- [1] Anton Chuvakin
<https://www.gartner.com/doc/3479617>

Three Interrelated Components of Security



Bottom Line



Technology exists to serve people and processes.

Traditional SOC Challenges (1)

Efficacy



splunk® live!



Challenges with the traditional SOC (3)

Remember this?

**Risk &
Compliance**

**Security
Operations
(Includes SOC)**

**Security
Architecture**

**Security
Engineering**

Challenges with the traditional SOC (3)

Silo-ization



Challenges with the traditional SOC (4)



COST

... and opportunity cost

Trends in Security Operations

A SOC By Any Other Name...

- ▶ Security Analytics Center
- ▶ Cyber Fusion Center
- ▶ Cyber Defense Center
- ▶ Threat Defense Center
- ▶ Detection and Response Team

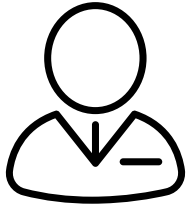


New Capabilities in the SOC

- ▶ Alert Management
- ▶ Incident Response
- ▶ Toolchain engineering
- ▶ Threat intelligence (consumption and creation)
- ▶ Threat hunting
- ▶ Vulnerability management
- ▶ Red team

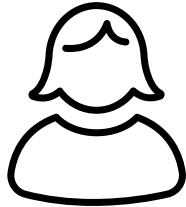


SOC Persona



Security Analyst

Responsible for investigating alerts, incidents and triage



SIEM Admin, Tools Engineer

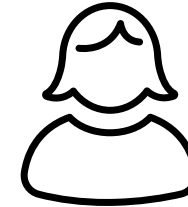
Responsible for the technology, product, upgrades



Hunter, Incident Responder

Proactively/reactively hunts for threats.

Details investigations, determine scope of incident, breach and takes actions



SecOps / SOC Manager / Director

Responsible for SOC process, initiatives, often budget



CISO / VP / Head InfoSec

Head or Exec of Info Security, Security

Managed Security Services are Common

- ▶ Tier-1
- ▶ Off hours
- ▶ Toolchain ops
- ▶ Outside Help With Specialties
 - Reverse Engineering
 - Forensics
 - Advanced IR
 - Red team

Improved Processes in the SOC

Naming The Rules

- 4002-EXP-Host with same recurring malware infection
- 4-002 "4" Indicates it is in the 4th stage of the kill chain
- 4-002 "002" Indicates it is in the 2nd rule of the 4th stage
- "EXP" Indicates it is in the exploit stage
- Lastly, the name of the rule
- When conversing about the rule, it has been very efficient
- It has been a small effort

4002-EXP-Host with

Contents [hide]

- 1 Rule Basics
- 2 Query
- 3 Throttling
- 4 Notable Event Details
- 5 Risk Modifier
- 6 Workflow/Testing
- 7 Links
- 8 Tuning History
- 9 Signatures

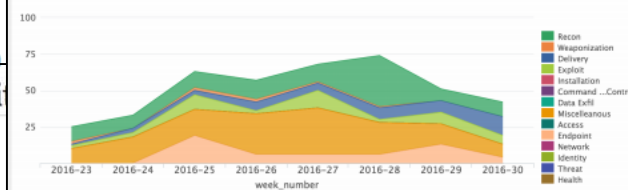
Rule State	Rule Acceptance
Disabled	Disabled

1 Rule Basics

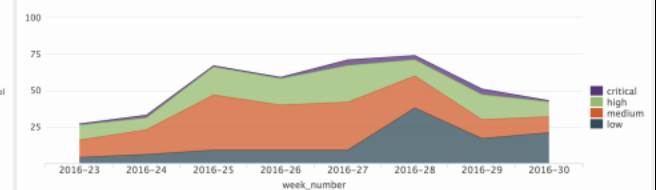
Rule Name	4002-EXP-Host
Kill Chain/Category	REC WEA DEL EXP INS CAC DEX MISC ACC END NET IDT THR HEA
App	SA-EndpointProtection
Data Feeds	Indexes mcafee_epo Data Models Malware

Notable Metrics Continued

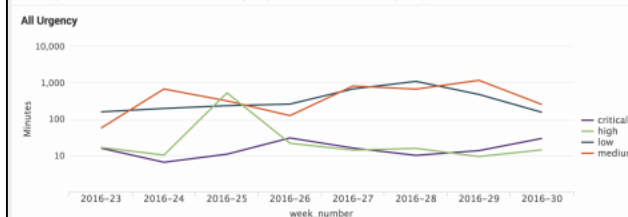
Count of Notable Events By Kill Chain Stage and Week Number



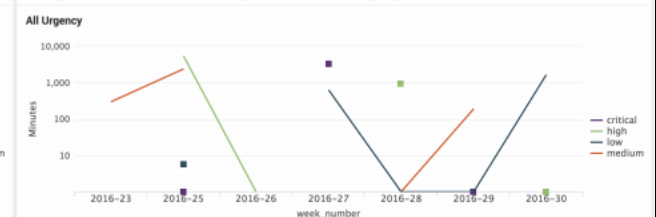
Count of Notable Events By Urgency and Week Number



Average Time in Minutes To Acknowledge By Week Number and Urgency



Average Time in Minutes To Resolve By Week Number and Urgency



20

splunk> .conf2016

13

splunk> .conf2016

<https://conf.splunk.com/files/2016/slides/maturing-workdays-soc-with-splunk.pdf>

splunk> live!

Maturing Use of Threat Intelligence

- ▶ Threat list + raw log feed = Noise
- ▶ Alert enriched by threat intel = Insight
- ▶ High maturity:
 - Gather your own threat intel
 - Share threat intel meaningfully



“Beware the threat list wind tunnel”

– *Splunk Customer*

Network (Meta)data

Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr == 192.168.1.6` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
19511	995.233558000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19512	995.233597000	192.168.1.8	192.168.1.6	ICMP	Redirect (Redirect for host)
19513	995.233631000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19514	995.248689000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19515	995.248710000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19516	995.260447000	192.168.1.6	82.192.95.92	TCP	55552 > http [FIN, ACK] Seq=200 Ack=1154 Win=16368 Len=0
19520	995.312985000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19521	995.313009000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19522	995.314343000	192.168.1.6	82.192.95.92	TCP	55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19523	995.314363000	192.168.1.6	82.192.95.92	TCP	[TCP Dup ACK 19522#1] 55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19524	995.324651000	82.192.95.92	192.168.1.6	TCP	http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19525	995.324668000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19524#1] http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19527	995.325988000	192.168.1.6	82.192.95.92	TCP	[TCP segment of a reassembled PDU]
19528	995.326010000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] 55555 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=205
19529	995.326263000	192.168.1.6	82.192.95.92	HTTP	POST /cgi-bin/iavs4stats.cgi HTTP/1.1 (iavs4/stats)
19530	995.326278000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
19531	995.375611000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19532	995.375625000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19531#1] http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19533	995.380658000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19534	995.380678000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19533#1] http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19535	995.382891000	82.192.95.92	192.168.1.6	HTTP	HTTP/1.1 204 No Content
19536	995.382911000	82.192.95.92	192.168.1.6	HTTP	[TCP Retransmission] HTTP/1.1 204 No Content
19539	995.505191000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19540	995.505232000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19550	996.308269000	192.168.1.6	149.7.96.236	TCP	55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19551	996.308324000	192.168.1.8	192.168.1.6	ICMP	Redirect (Redirect for host)
19552	996.308363000	192.168.1.6	149.7.96.236	TCP	55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

▶ Frame 9164: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
 ▶ Ethernet II, Src: HonHaiPr_26:b5:30 (c0:cb:38:26:b5:30), Dst: Azurewav_43:90:de (00:15:af:43:90:de)
 ▶ Internet Protocol Version 4, Src: 68.126.7.59 (68.126.7.59), Dst: 192.168.1.6 (192.168.1.6)
 ▶ Transmission Control Protocol, Src Port: 19207 (19207), Dst Port: 55400 (55400), Seq: 1, Ack: 1, Len: 23

```

0000  00 15 af 43 90 de c0 cb 38 26 b5 30 08 00 45 00  ...C.... 8&.0..E.
0010  00 3f 57 57 40 00 ef 06 26 fa 44 7e 07 3b c0 a8  ..?WW@... &.D~.;...
0020  01 06 4b 07 d8 68 00 00 00 0f 49 3f 88 50 14    ..K..h... ..I?.P.
0030  00 00 5a f6 00 00 47 6f 20 61 77 61 79 2c 20 77  ..Z...Go away, w
0040  65 27 72 65 20 6e 6f 74 20 68 6f 6d 65        e're not home
  
```

eth1: <live capture in progress> File: Packets: 19552 Displayed: 5155 Marked: 0 Profile: Default

Network (Meta)data

Splunk Stream

- Succinct
- 5-tuple + traffic size
- Easily searchable!
- Tuneable
- Adaptive fidelity
- Additional context
- Payload elements

NetFlow (or variant)

- Succinct
- 5-tuple + traffic size
- Easy™ to analyze
- Cost effective
- No payload

PCAP

- Voluminous
- Ground truth
- Ultimate context
- Full payload
- Lots of storage / overhead

Threat Hunting – Where Does it Fit?

Threat hunting is what happens just past the horizon of automated detection capabilities. What you learn while hunting should extend that horizon.

- Paraphrased from Robert M. Lee SANS Forensics 578

The Security Operations Toolchain

Log Data Platform

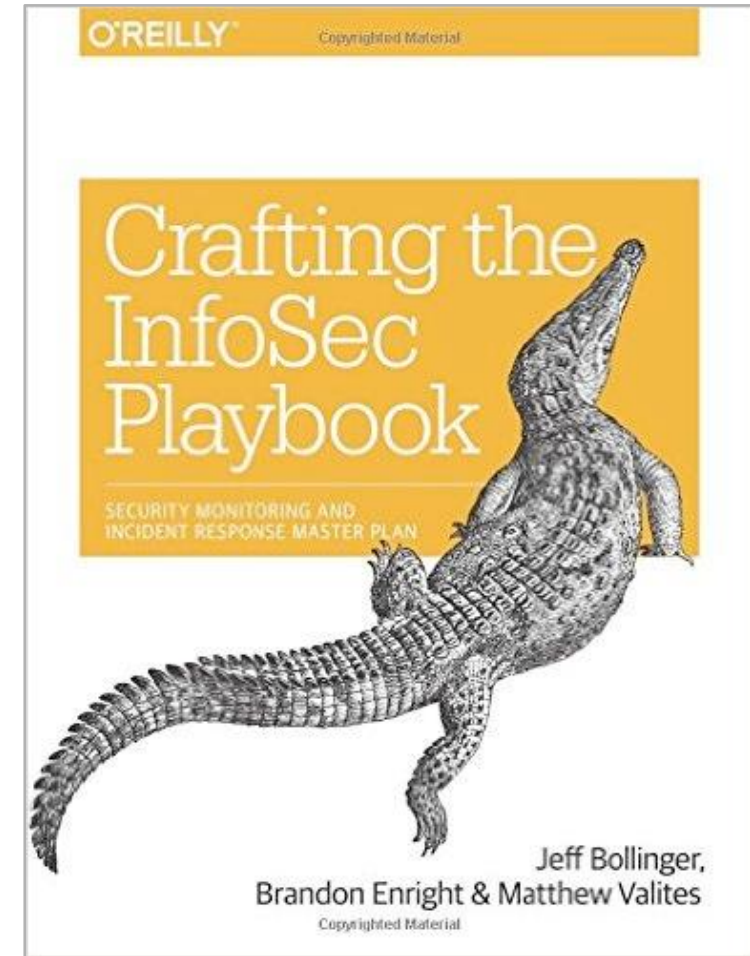
- ▶ Single source of truth
- ▶ Retention and integrity
- ▶ Any data source
- ▶ Easy correlation
- ▶ Automation / integration
- ▶ Performant and scalable
- ▶ Full fidelity
- ▶ Normalized?
- ▶ Hunting
- ▶ Forensic investigation
- ▶ Alerting
- ▶ Dashboards
- ▶ Visualization
- ▶ Analytics (ML?)

Data Normalization is Mandatory for your SOC

“The organization consuming the data must develop and consistently use a standard format for log normalization.”

– Jeff Bollinger et. al., Cisco CSIRT

**Your fields don't match?
Good luck creating
investigative queries.**



Asset Inventory and Identity Data

- ▶ Often multiple sources of record – that's OK
 - CMDB, Vuln scans, Passive detection, DHCP, NAC
 - Active directory, LDAP, IAM
- ▶ Network diagrams
- ▶ Categorization
 - PCI, ICS, Administrative, Default
- ▶ Comprehensive yet lightweight and easy to maintain
- ▶ Must be easy to correlate to log data

Case and Investigation Management

1. Ticketing system
2. Workflow
3. Supports prioritization
4. Supports collaborative investigation
5. Provides metrics
6. Supports automation
7. Auditable

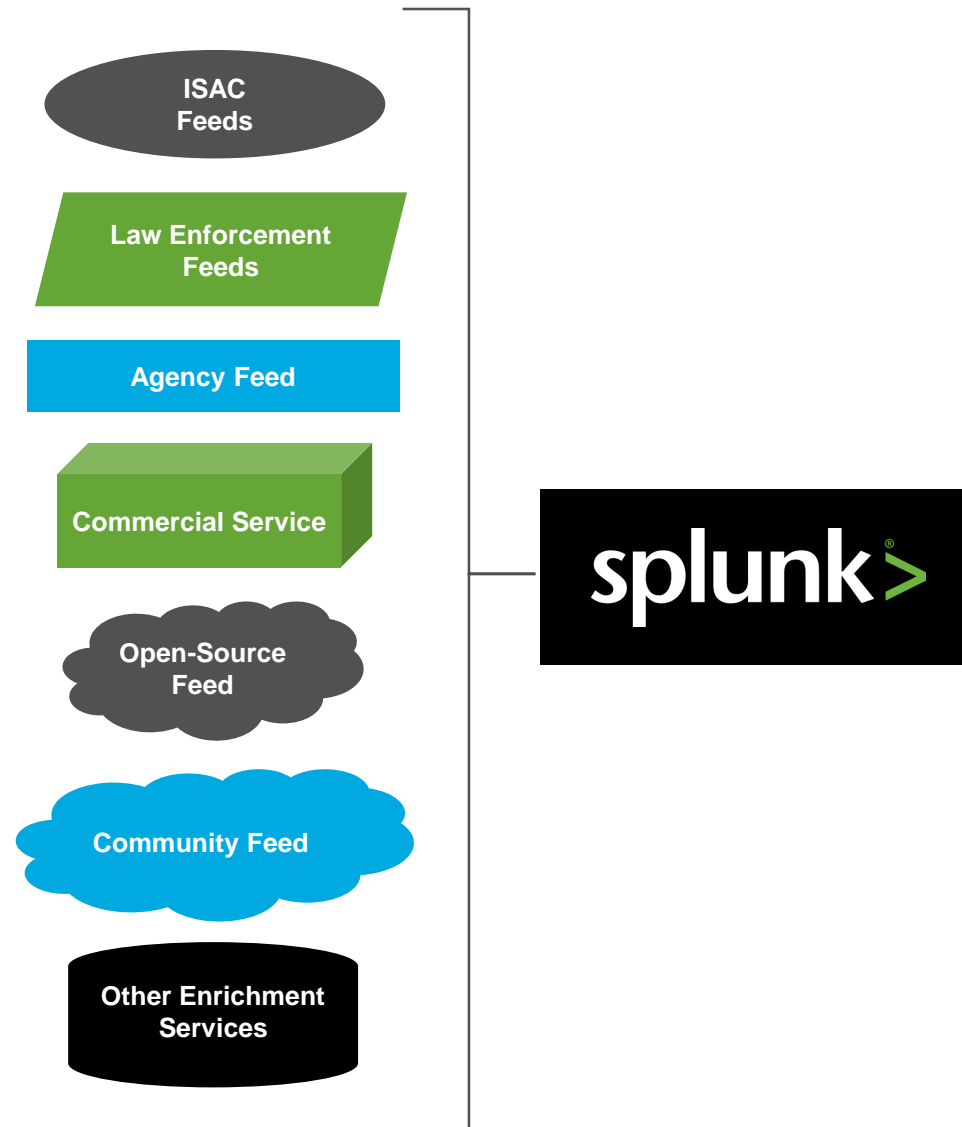
Common SOC Data Sources

1. Assets and Identities
2. Threat intel
3. Firewall
4. Network metadata
5. Authentication
6. Server (Windows / Linux)
7. Endpoint
8. IDS / IPS
9. VPN
10. Application
11. Vulnerability

Splunk for Analytics-Driven SOC

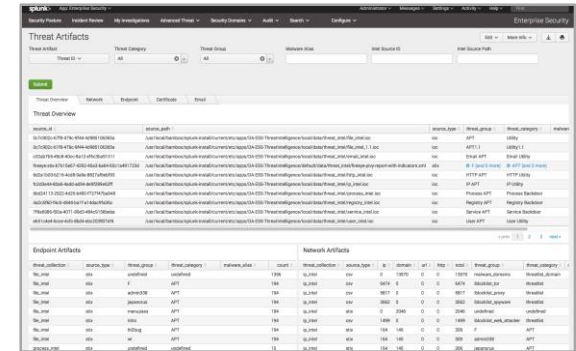
1. Threat Intelligence – ES Threat Intel Framework

- ▶ **Automatically** collect, aggregate and de-duplicate threat feeds from a broad set of sources
- ▶ Support for STIX/TAXII, OpenIOC, Facebook
- ▶ Build your own data to create your own Threat Intel
- ▶ Out of the box **Activity** and **Artifact** dashboards



- ▶ Determine impact on network, assets
- ▶ Use for analysis / IR
- ▶ Collect / provide forensics
- ▶ Use to hunt / uncover / link events
- ▶ Share info with partners

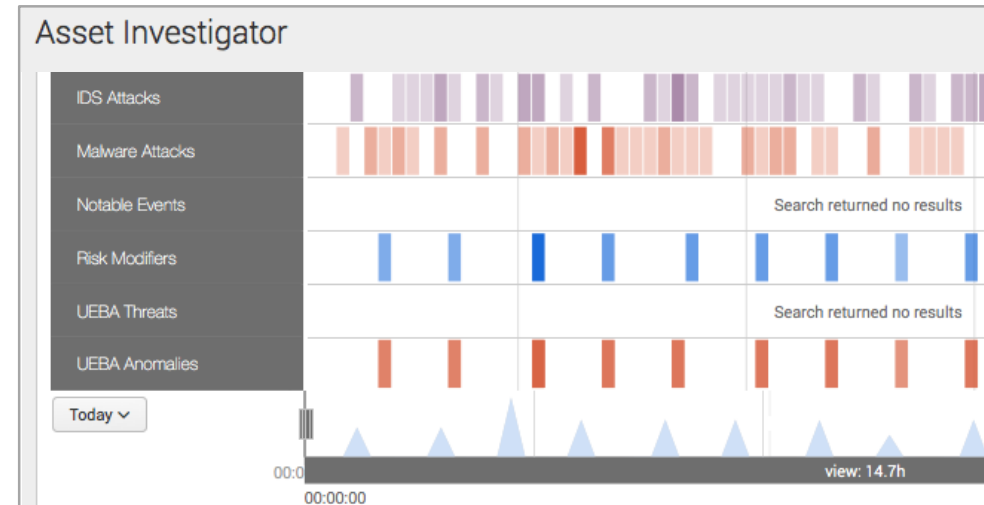
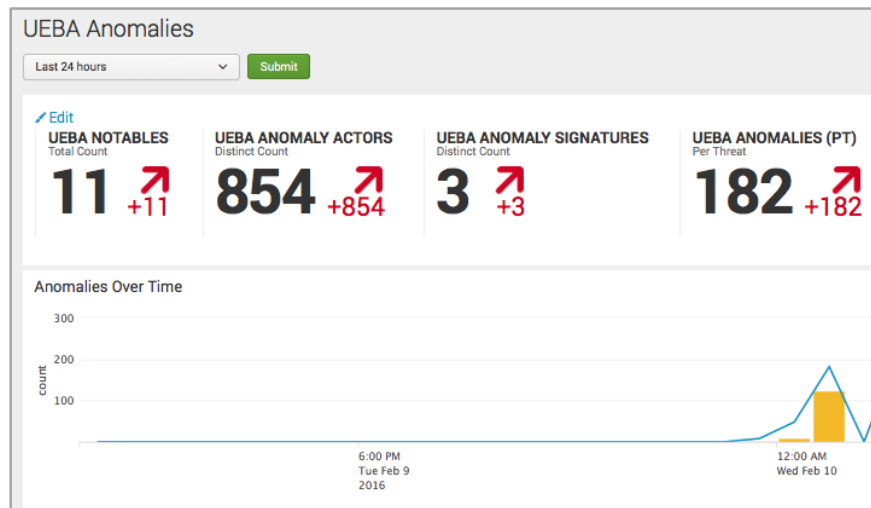
Search



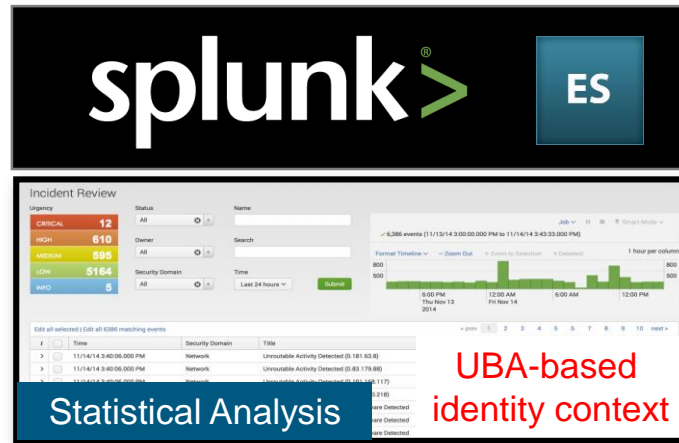
Data Search

2. Use Advanced Analytics – Native ML and UBA

- ▶ Simplify detection and focus on real alerts
- ▶ Accelerate anomaly and threat detection – minimize attacks and insider threat
- ▶ Use machine learning toolkit - solutions to suit your workflow
- ▶ Premium machine learning solution - User Behavior Analytics
 - Flexible workflows for SOC Manager, SOC analyst and Hunter/Investigator within SIEM



Advanced Analytics and Machine Learning

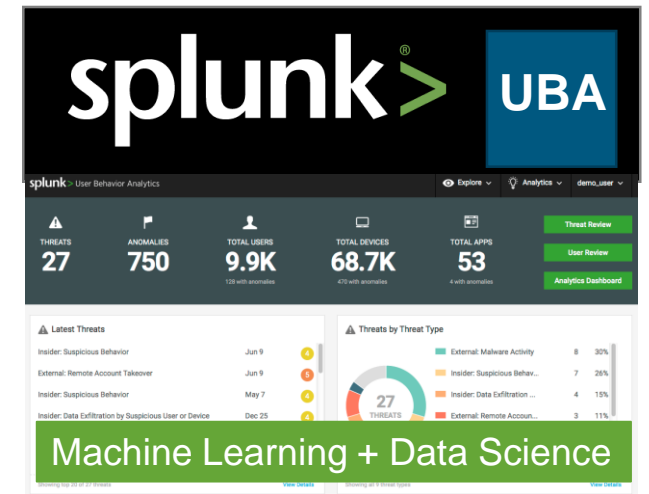


workflow

Alert driven
detection

Entity
Resolution

UBA-based
identity context



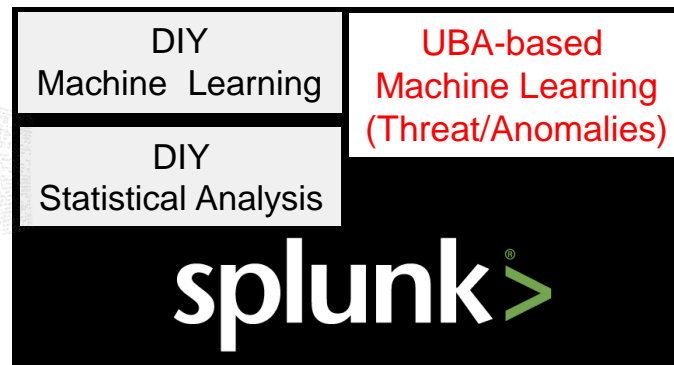
Threats
Anomalies

UBA-based
Machine Learning
(Threat/Anomalies)

101111101010010001000001
111011111011101111101010
010001000001111011111011

UBA-based
Machine Learning
(Threat/Anomalies)
Packaged

UBA-based
ML + DS
(Custom Threats)



3. Automate When Feasible

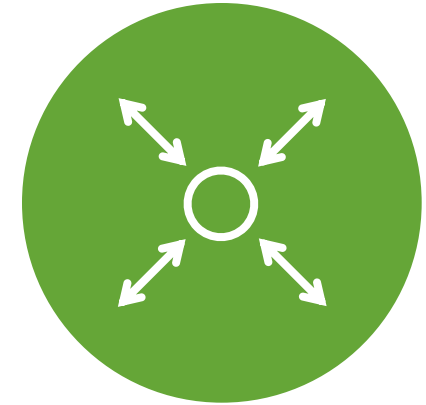
- ▶ Use rules to automate routine aspects of detection and investigation
- ▶ Extract insights from existing security stack by use of common interface
- ▶ Take actions with confidence for faster decisions and response
- ▶ Automate any process along the continuous monitoring, response and analytics cycle

Splunk Adaptive Response



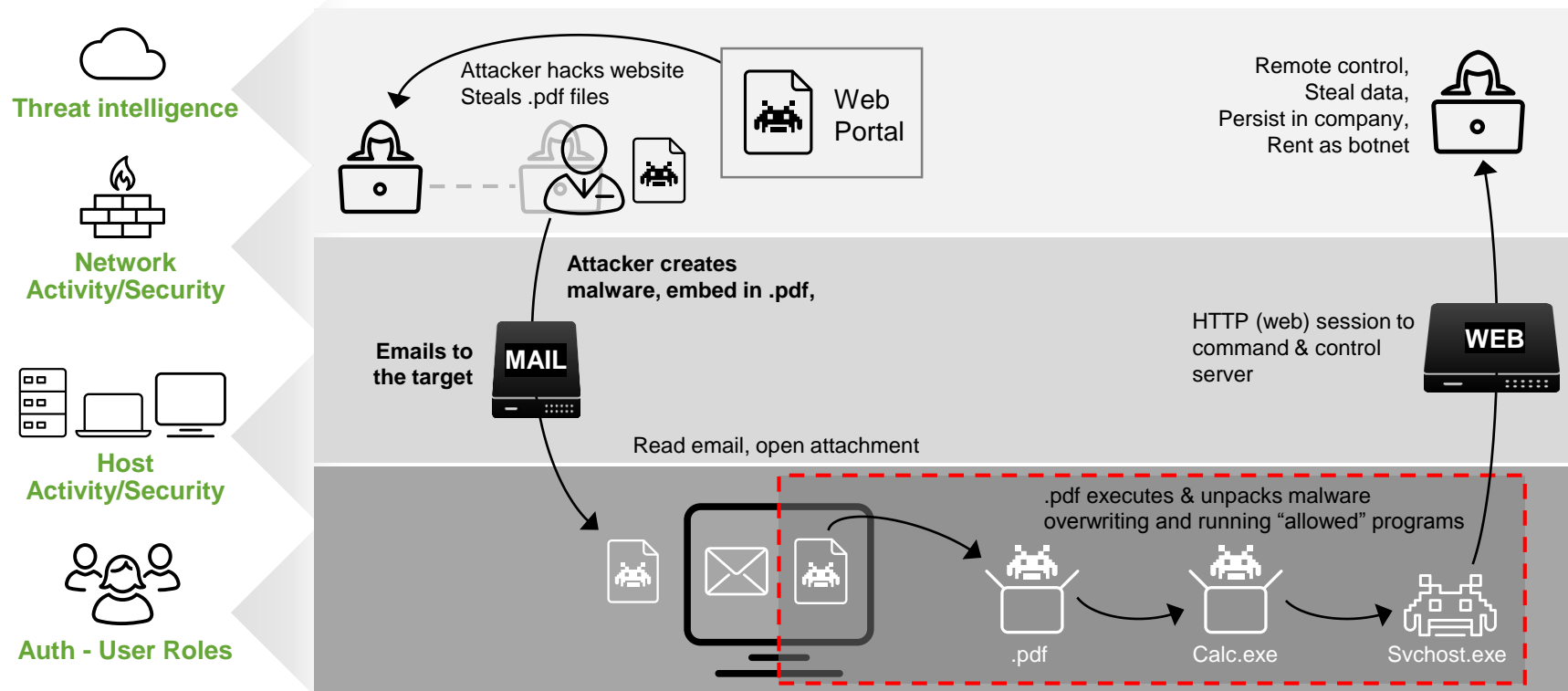
Adaptive Response: Analytics-Driven Decisions, Automation

- ▶ **Centrally automate** retrieval, sharing and response action resulting in improved detection, investigation and remediation times
- ▶ **Improve operational efficiency** using workflow-based context with automated and human-assisted decisions
- ▶ **Extract new insight** by leveraging context, sharing data and taking actions between Enterprise Security and Adaptive Response partners

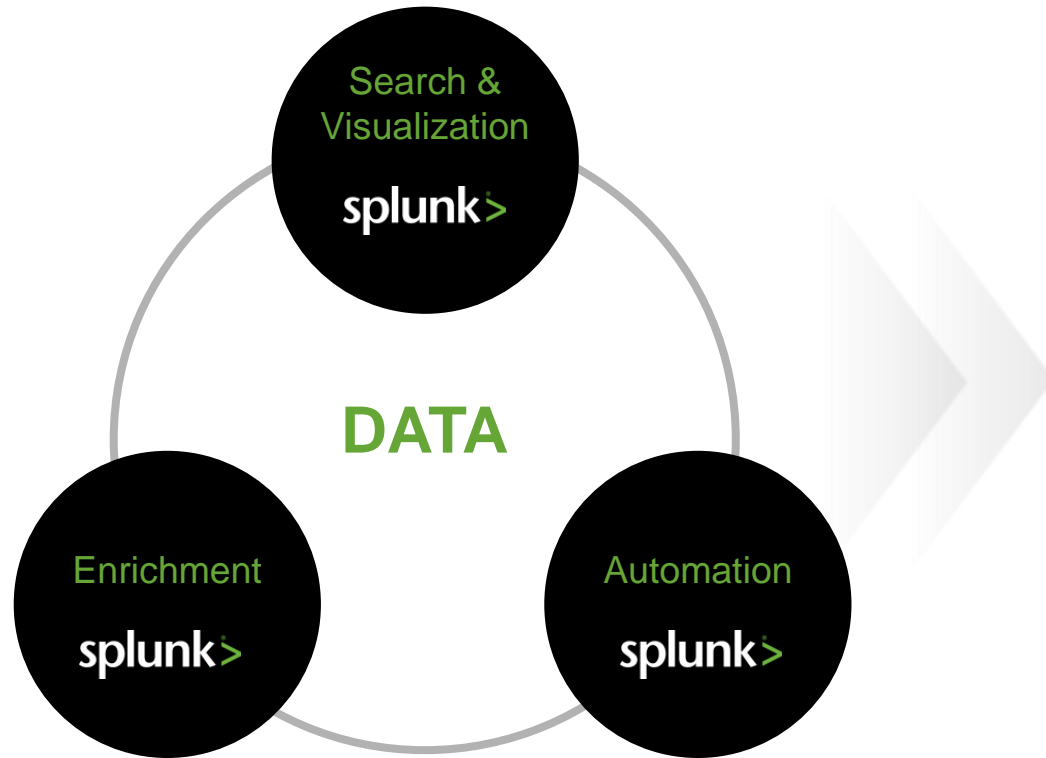


4. Proactively Hunt and Investigate - Considerations

- ▶ Organizational maturity
- ▶ Domain and product experience
- ▶ Tools: Network, Endpoint, Threat Intel, Access
- ▶ Security relevant data, historical, raw data
- ▶ Flexibility and ad hoc



How Splunk Helps You Drive Threat Hunting Maturity



Threat Hunting Enablement

Integrated & out of the box automation tooling from artifact query, contextual “swim-lane analysis”, anomaly & time series analysis to advanced data science leveraging machine learning

Threat Hunting Data Enrichment

Enrich data with context and threat-intel across the stack or time to discern deeper patterns or relationships

Search & Visualize Relationships for Faster Hunting

Search and correlate data while visually fusing results for faster context, analysis and insight

Ingest & Onboard Any Threat Hunting Machine Data Source

Enable fast ingestion of any machine data through efficient indexing, a big data real time architecture and ‘schema on the read’ technology

splunk>

Data Science
and Machine
Learning

Automated
Analytics

Visualisation

Data and
Intelligence
Enrichment

Data Search

Hypotheses

MATURITY

splunk>live!

5. Adopt an Adaptive Security Architecture

To Prevent, Detect, Respond and Predict – need:

- ▶ Correlation across all security relevant data
- ▶ Insights from existing security architectures
- ▶ Advanced analytics techniques such as machine learning

Splunk Security Solutions



Splunk Enterprise Security™



Splunk User Behavior Analytics™

1,000+ Apps and Add-ons



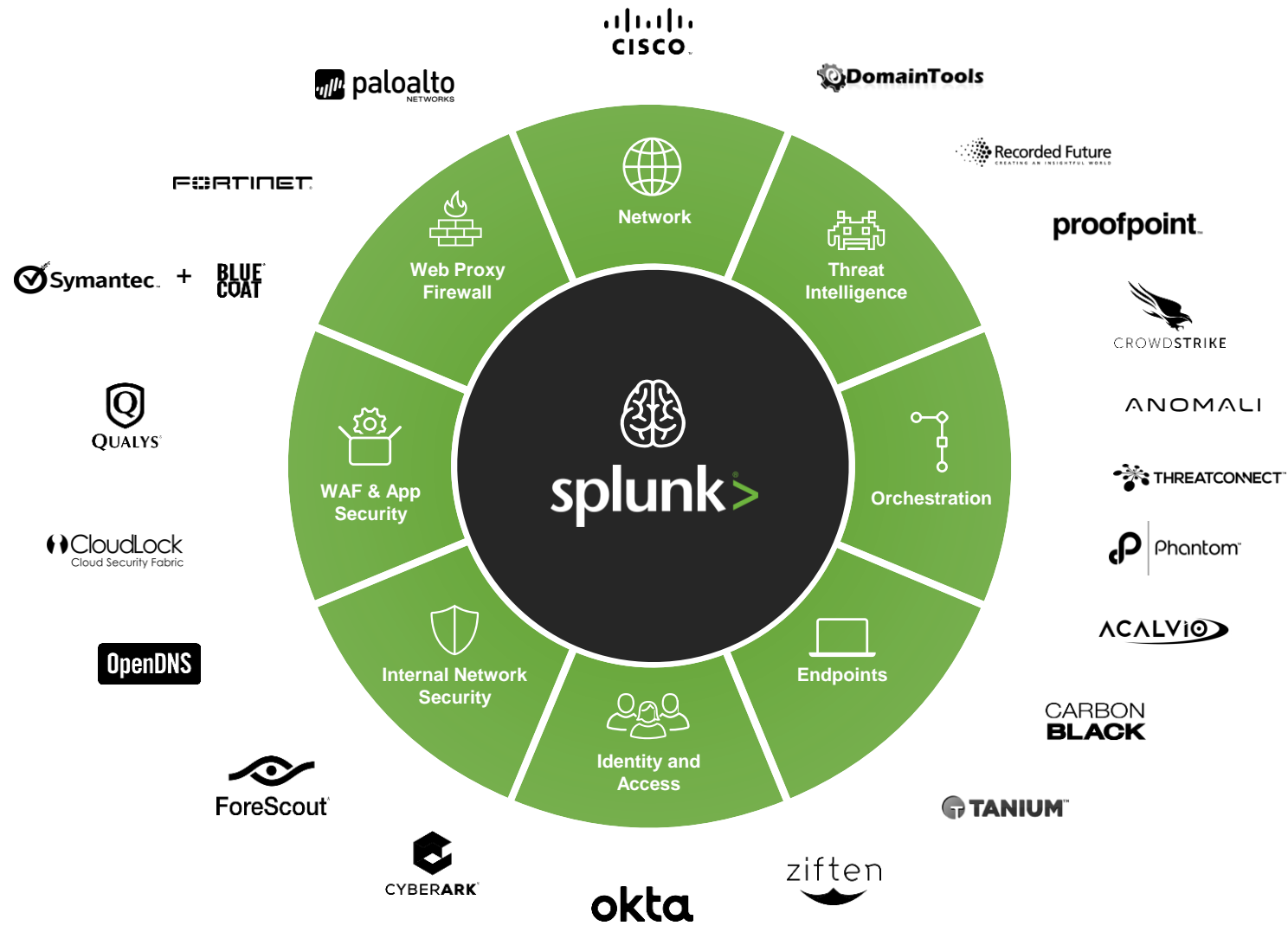
splunk>enterprise

splunk>cloud

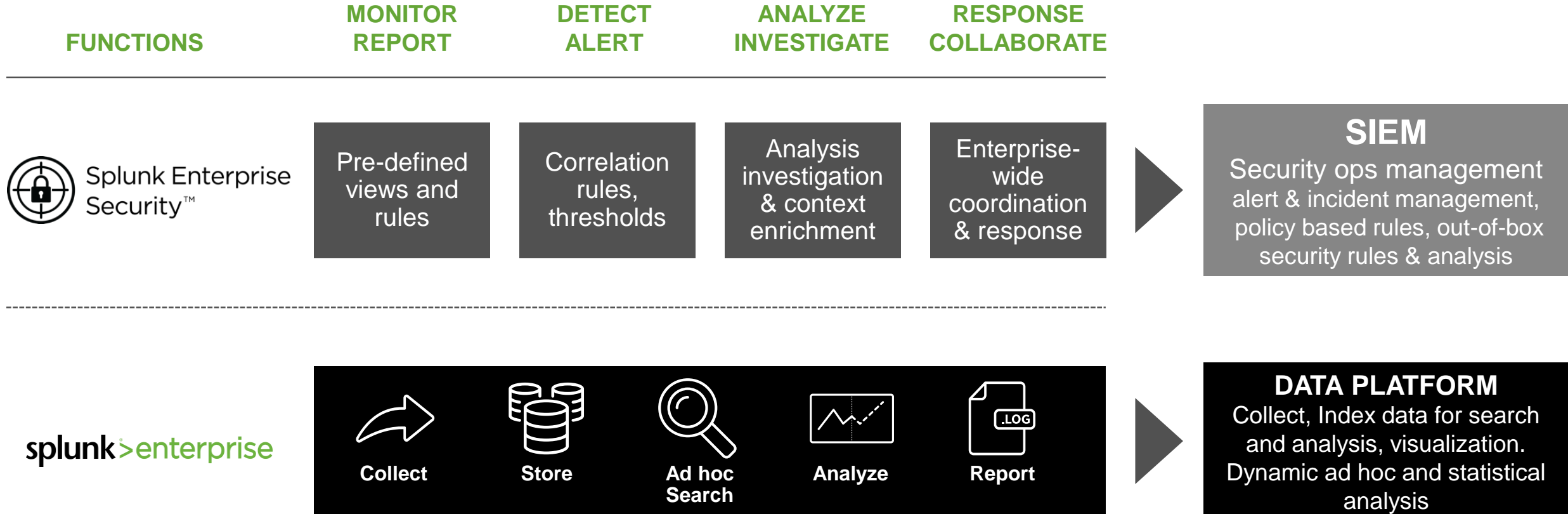
splunk>live!

Insight From Across Ecosystem

Effectively leverage security infrastructure to gain a holistic view



Splunk Analytics-Driven SIEM



Splunk Enterprise Security

A collection of Frameworks



Splunk Enterprise
Security™

ASSET AND
IDENTITY
CORRELATION

NOTABLE
EVENT

THREAT
INTELLIGENCE

RISK
ANALYSIS

ADAPTIVE
RESPONSE

splunk> Platform for Operational Intelligence

splunk>live!

Splunk Enterprise Security: Frameworks

Framework	Detail
Notable Events	Identify noteworthy incidents from events and then manage state
Asset & Identity	performs asset and identity correlation for fields that might be present in an event
Threat Intelligence	Consume and manage threat feeds, data
Risk Analysis	Identify actions that raise the risk profile of individuals or assets
Adaptive Response	Interface for retrieving, sending and running actions by integrating with external applications

Splunk Solutions Portfolio

Across Data Sources, Use Cases & Consumption Models

**Splunk Premium
Solutions**



Splunk IT Service
Intelligence™



Splunk Enterprise
Security™



Splunk User Behavior
Analytics™

**Rich Ecosystem of
Apps & Add-Ons**



service**now**



splunk>enterprise

splunk>cloud

splunk> Platform for Operational Intelligence



Forwarders



Syslog/
TCP



Mobile



IoT
Devices



Network
Wire Data



Hadoop



Relational
Databases



Mainframe
Data

splunk>live!

Splunk Quick Start for SIEM

Rapidly Determine Advanced Malware and Threat Activity

Complete with a Splunk license, selection of Splunk Apps and Add-Ons, professional services, education credits, and user conference passes—this Quick Start is your one-stop shop for Operational Intelligence.

Bundle Size	Splunk Enterprise License	Splunk Enterprise Security License	Splunk Apps and Add-Ons	Expert Guidance	Free Education	.conf Event Passes
Medium	50 GB/day	50 GB/day	✓	15 Days	20 Credits	1
Large	100 GB/day	100 GB/day	✓	15 Days	20 Credits	2

Malware Center Dashboard

Threat Activity Dashboard

Customer Success

TECHNOLOGY

Building an Intelligence Driven SOC

The SAIC logo is displayed in blue text within a white circle. The background of the slide features a blue-toned image of server racks with various icons like a car, a lightbulb, a house, and a person, suggesting a high-tech, intelligence-driven environment.**SAIC®**

Challenges

- ▶ Existing SIEM not adequate - struggled to bring in appropriate data
- ▶ Unable to perform advanced investigations, severe scale/performance issues
- ▶ Looking to build a new SOC with modern solution

Customer Solution

- ▶ Centralized logging of all required machine data at scale and full visibility
- ▶ Retain all relevant data from 10+ data sources which is used by 25+ SOC/CSIRT users
- ▶ Tailored advanced correlation searches & IR workflow
- ▶ Faster and deeper incident investigations
- ▶ Greater SOC efficiencies - all SOC/CSIRT working off same UI/data
- ▶ Executive dashboards to measure and manage risk

PUBLIC SECTOR

Citywide SOC for Situational Awareness



Challenges

- ▶ Slow responses to security incidents
- ▶ Inadequate situational awareness of security events
- ▶ Limited threat intelligence
- ▶ Disparate logs from over 40 departments were difficult to aggregate

Customer Solution: Splunk Cloud with Enterprise Security

- ▶ Real-time, citywide, 24/7 network surveillance
- ▶ Stronger protection of digital assets and infrastructure
- ▶ Shared threat intelligence with federal agencies
- ▶ Reduced headcount and lower operational costs

TECHNOLOGY

Maturing SOC



Challenges

- ▶ Legacy SIEM: Unstable, Inflexible, Clunky
- ▶ Limited skilled resources
- ▶ High false negative and false positive

Customer Solution: Splunk Cloud With Enterprise Security

- ▶ Developed processes: Rule set, naming
- ▶ SOC process: Playbook, training, automated documentation
- ▶ Enabled SOC to identify patterns of behavior in a single event rather than be bombarded by thousands of low-value incidents

TELECOM

Build an Insourced SOC in Months



Challenges

- ▶ Wide range of security requirements
 - Internal audits (financial, PCI)
 - Protect internal info and assets
 - Cloud firewall, DDOS
- ▶ Cultural and Organizational
 - Security not a priority, Outsourced SecOps
 - Information hoarding and data silos

Customer Solution: Splunk Enterprise Security

- ▶ Changed culture - security first mindset with controls
- ▶ Detect, prevent and respond to attacks in own environment, with 24/7 security analysis of customers
- ▶ Rapid detection and deep investigation
- ▶ Detect Web App attacks, discover compromised cards

Wrapping up

Get started in minutes – splunk.com

1

FREE CLOUD TRIAL

2

FREE SOFTWARE
DOWNLOAD

3

FREE
ENTERPRISE SECURITY
SANDBOX

splunk®

Resources Cited (1)

1. How to Plan, Design, Operate and Evolve a SOC

- <https://www.gartner.com/doc/3479617>

2. Crafting the InfoSec Playbook

- <https://www.amazon.com/Crafting-InfoSec-Playbook-Security-Monitoring/dp/1491949406>

3. Splunk SOC Advisory Services

- <https://www.splunk.com/pdfs/professional-services/soc-advisory-services.pdf>

4. Ten Strategies of a World-Class Cybersecurity Operations Center

- <https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf>

5. Maturing Workday's SOC with Splunk

- <https://conf.splunk.com/files/2016/slides/maturing-workdays-soc-with-splunk.pdf>

6. The Five Characteristics of an Intelligence Driven Security Operations Center

- <https://www.gartner.com/doc/3160820/characteristics-intelligencedriven-security-operations-center>

7. The Who, What, Where, When, Why and How of Effective Threat Hunting

- <https://www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785>

Resources Cited (2)

8. Exploring the Frameworks of Splunk Enterprise Security

- <https://conf.splunk.com/files/2016/slides/exploring-the-frameworks-of-splunk-enterprise-security.pdf>

9. Recruiting and Retaining Cybersecurity Ninjas

- <https://www.csis.org/analysis/recruiting-and-retaining-cybersecurity-ninjas>

10. Building Threat Hunting Strategies with the Diamond Model

- <http://www.activeresponse.org/building-threat-hunting-strategy-with-the-diamond-model/>

11. Using Robots to Fight Bad Guys

- <https://sroberts.github.io/2014/05/14/using-robots-to-fight-bad-guys/>

12. Building a SOC with Splunk

- <https://www.splunk.com/pdfs/technical-briefs/building-a-soc-with-splunk-tech-brief.pdf>

13. SANS Security Leadership Poster

- <https://www.sans.org/security-resources/posters/leadership/security-leadership-poster-135>

14. 2016 CISO MindMap – What do InfoSec Professionals Do?

- <http://rafeeqrehman.com/2016/10/07/announcing-ciso-mindmap-2016/>

Your help can strengthen the community

- ▶ If you have Enterprise Security deployed in your environment
 - ▶ You want to enhance your security posture with analytics
 - ▶ You commit to give us feedback
 - ▶ Email ES-SOC@splunk.com to schedule a preview
-
- ▶ Use prebuilt detections, analysis and automation out of the box
 - ▶ No need for writing searches or manually investigating alerts
 - ▶ Developed by Splunk's Security Research team of red and blue teamers
 - ▶ Next round of Alphas start in a couple of weeks



.../533.4 (KHTML, like Gecko) Chrome/50.0.375.38
..._id=FT-SW-01&JSESSIONID=...
...com/category.screen?category_id=EST-26&JSESSIONID=...
... HTTP 1.1" 200 1976 "http://buttercup-shopping.com/cart.do?action=pur-...
... (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 163 131.
... [07/Jan 18:10:57:123] "GET /prod-...
... Mozilla/4.0 = " " 200 1318
... 5.0; Windows NT 5.1; SV1; .NET CLR...
... HTTP 1.1" 200 2423 "http://butter-...
... .97 - - [07/Jan 18:10:55:189]
... buttercup-shopping.com/old-...
... EST-6&JSESSIONID=SD10SL8FF2ADFF9 HTTP...
... NT 5.1; U; en)" 553 62.216.64.19 - -
... opping com/cart do?action=re-...
... "GET /category.screen?category_id=SUR-...
... npatible; MSIE 6.0; Windows NT 5.1)" 606
... 7ADFF7 HTTP 1.1" 200 205 "http://butter-...
... SV1) 163 131.178.233.243 - -
... g.com/cart.do?action=pur- 6
... ML, like Gecko) Chrome/50.0.375.38
... JSESSIONID=SD10SL3FF1ADFF4 HTTP 1.1" 404
... a/9.20 (Windows NT 6.0; U; -...
... 1.1" 404 3322 "http://buttercup-sho...
... [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-264...
... SL7FF...
... mId=EST-15&product_id=AV-SB-02&JSESSIONID=SD4SL1FF7ADFF7 HTTP 1.1" 200 205 "http://butter-...
... i11a/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 163 131.178.233.243 - -
... 200 1976 "http://buttercup-shopping.com/cart.do?action=pur-



.conf2017

.conf2017

The 8th Annual Splunk Conference

SEPT 25-28, 2017

Walter E. Washington Convention Center
Washington, D.C.

SAVE OVER \$450

You will receive an email after registration opens with a link to save over \$450 on the full conference rate.

You'll have 30 days to take advantage of this special promotional rate!

conf.splunk.com

splunk > live!

Workshops: Get Splunk Hands-on Experience

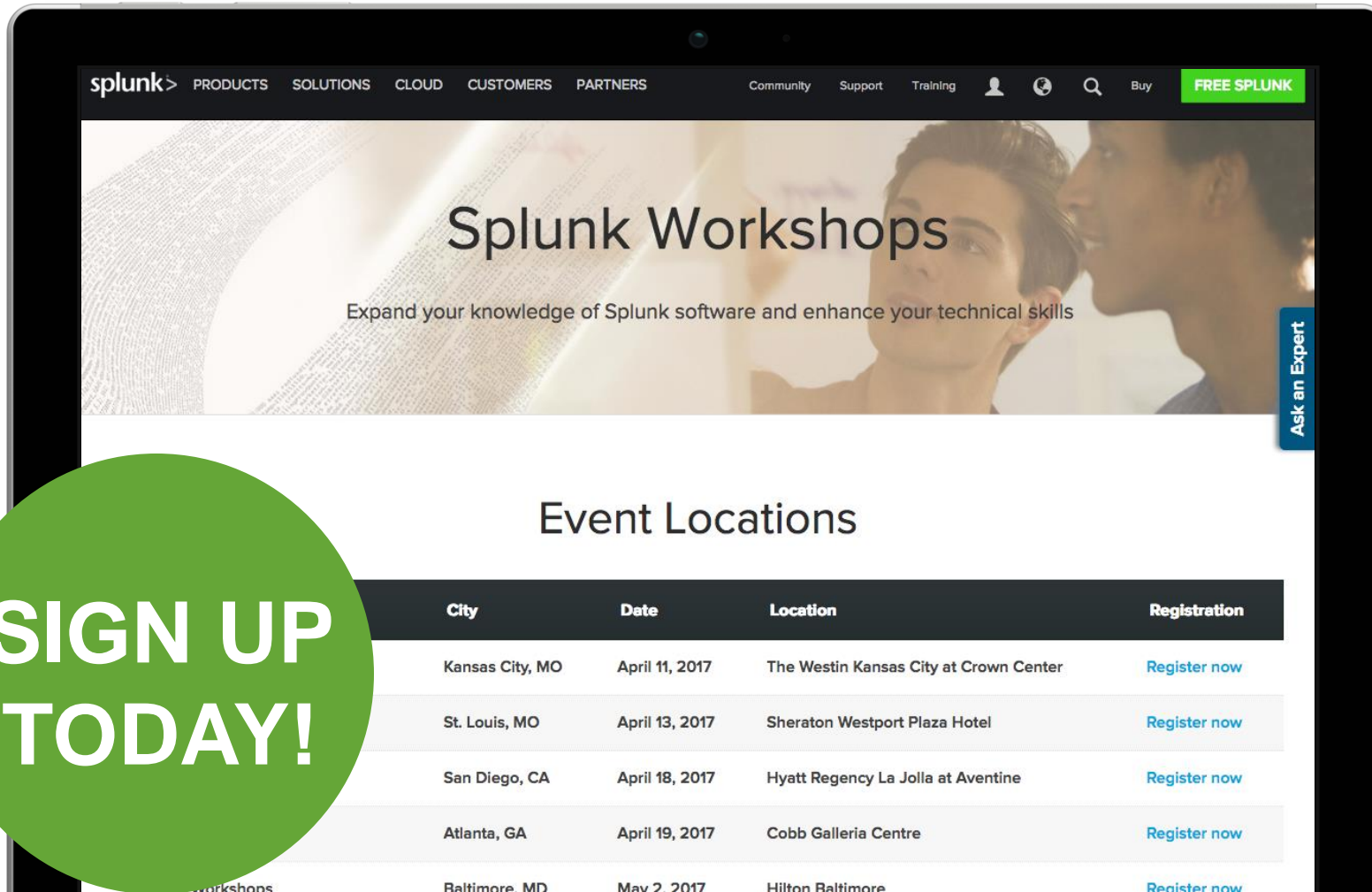
Attend a Splunk Workshop

splunk.com/workshops

June 14: Minneapolis

- ▶ **Venue:** Hyatt Regency Minneapolis
- ▶ **Time:** 8:30am
- ▶ Register Soon!
 - splunk.com/workshops

**SIGN UP
TODAY!**



Event Locations

City	Date	Location	Registration
Kansas City, MO	April 11, 2017	The Westin Kansas City at Crown Center	Register now
St. Louis, MO	April 13, 2017	Sheraton Westport Plaza Hotel	Register now
San Diego, CA	April 18, 2017	Hyatt Regency La Jolla at Aventine	Register now
Atlanta, GA	April 19, 2017	Cobb Galleria Centre	Register now
Baltimore, MD	May 2, 2017	Hilton Baltimore	Register now

Take the Survey on Pony Poll



ponypoll.com/slmn

Complete the survey for
your chance to win a
.conf2017 pass

130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20131026.1011414; Windows NT 6.0; WOW64; Trident/6.0" 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; Trident/6.0; rv:11.0) like Gecko" 317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; Trident/6.0; rv:11.0) like Gecko" 130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20131026.1011414; Windows NT 6.0; WOW64; Trident/6.0" 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; Trident/6.0; rv:11.0) like Gecko" 317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; Trident/6.0; rv:11.0) like Gecko" 130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5L4FF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20131026.1011414; Windows NT 6.0; WOW64; Trident/6.0" 128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; Trident/6.0; rv:11.0) like Gecko" 317 27.160.0.0 - - [07/Jun 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP 1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=FL-SW-01" "Mozilla/5.0 (Windows NT 6.0; WOW64; Trident/6.0; rv:11.0) like Gecko"