splunk> live!

APRIL 13, 2017 | SAN FRANCISO, CA

splunk> live!

APRIL 13, 2017 | SAN FRANCISCO, CA

Building the Analytics-Driven SOC

Dave Herrald | Splunk

Girish Bhat | Splunk

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>live!

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

splunk>live!

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

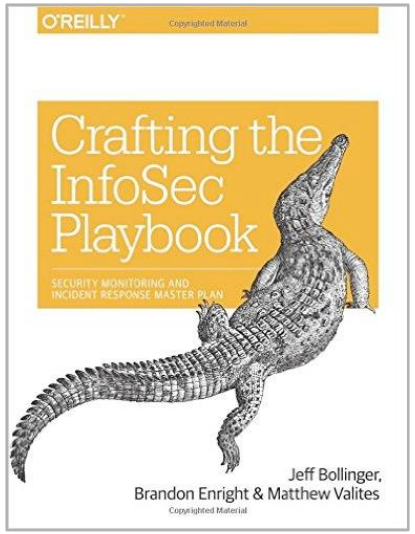
Source : EY Global Information Security Survey 2015

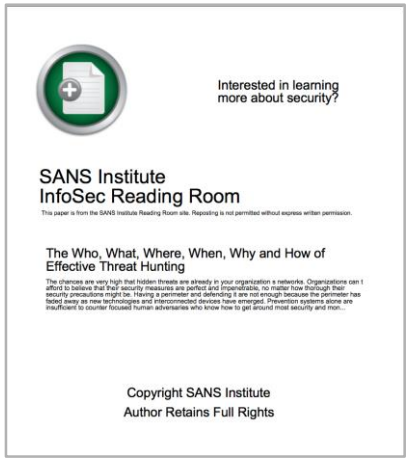
splunk>live!

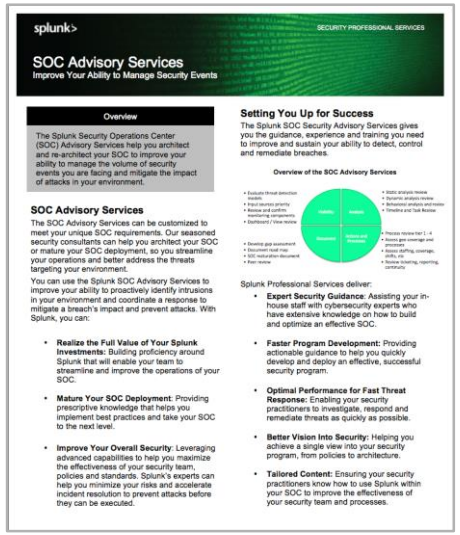
Traditional Security Operations

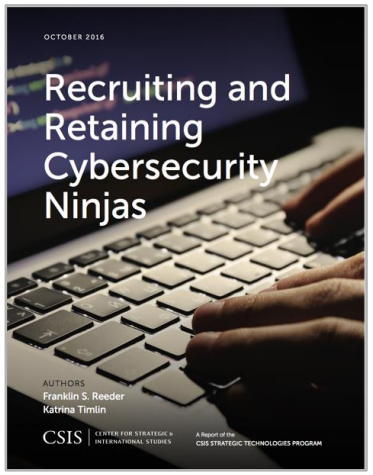
splunk>live!

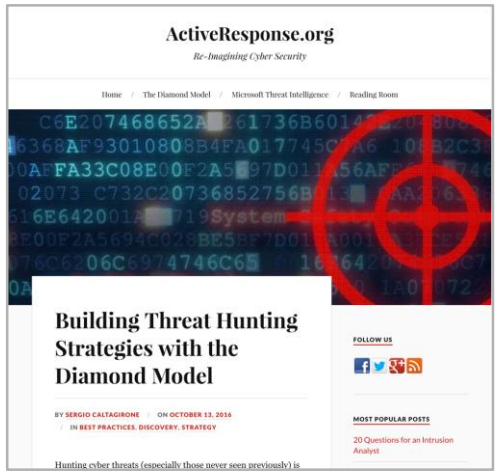
How-to guides…





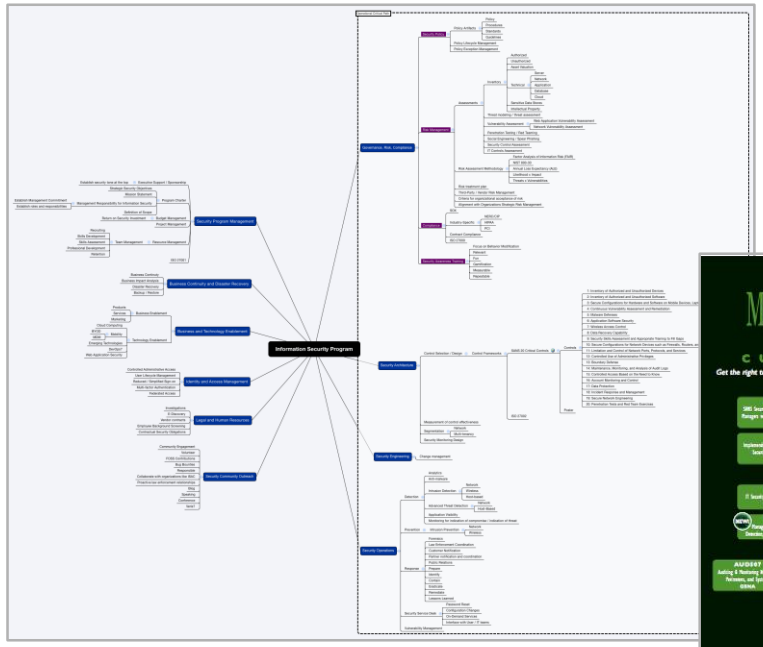


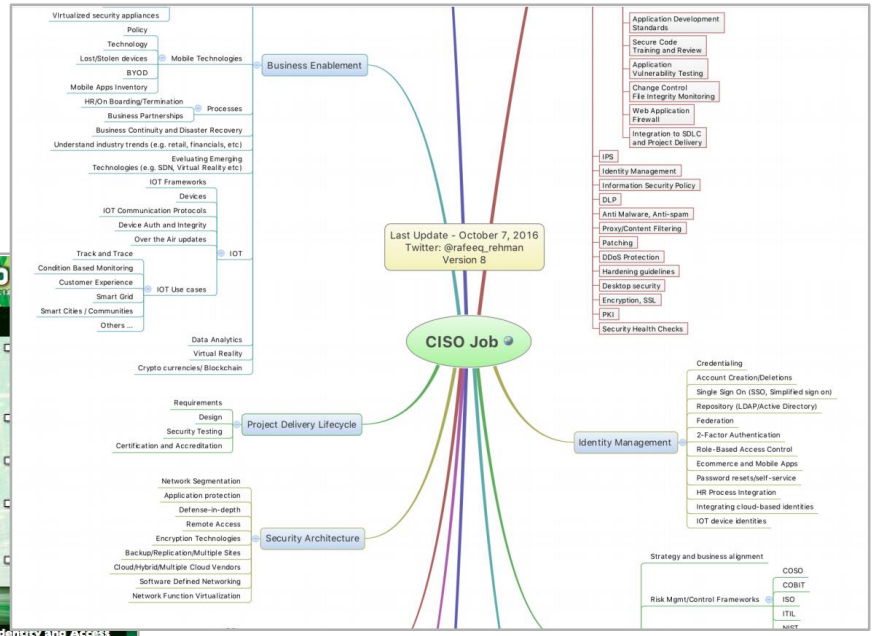




splunk>live!

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/

splunk>live!

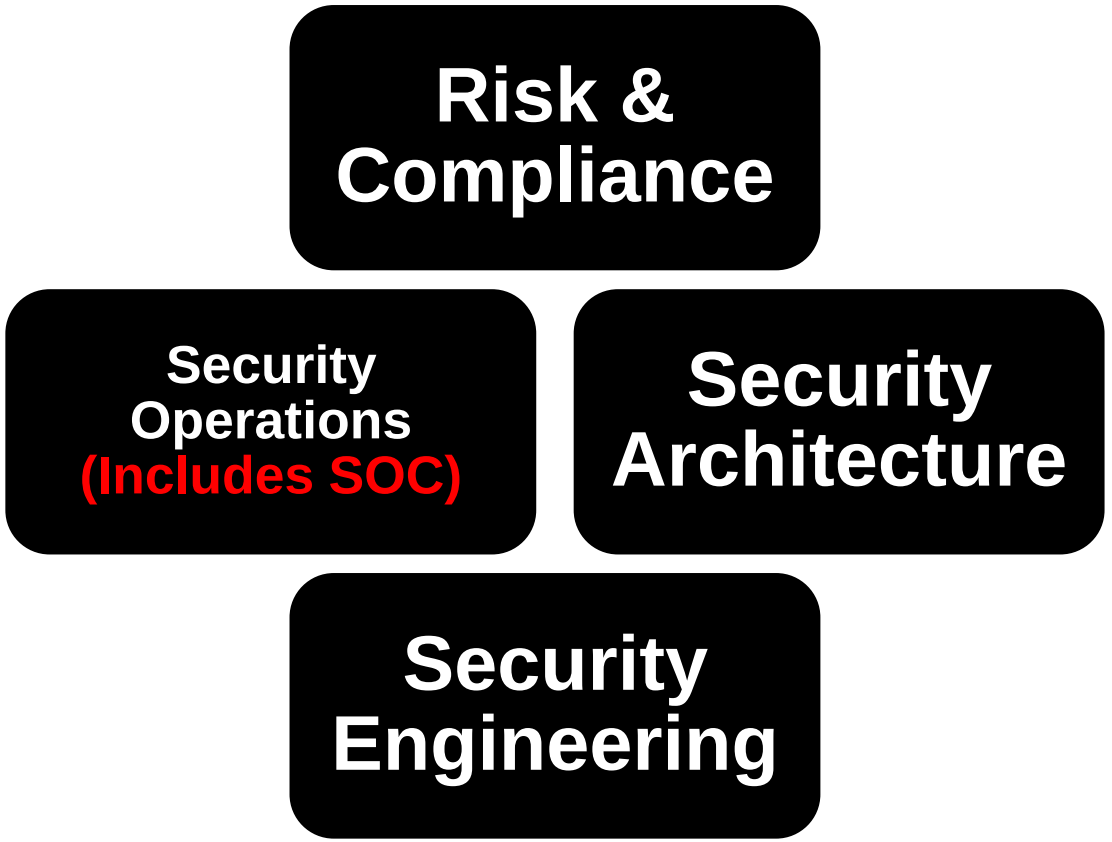
Security Programs: The Big Picture

[13] https://www.sans.org/security-resources/posters/leadership/security-leadership-poster-135
[14] http://rafeeqrehman.com/2016/10/07/announcing-ciso-mindmap-2016/

splunk>live!

What do we see?
A Traditional Security Critical Path

Security Operations: part of the bigger picture…



Types of Traditional SOCs…

- 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

Process

Technology

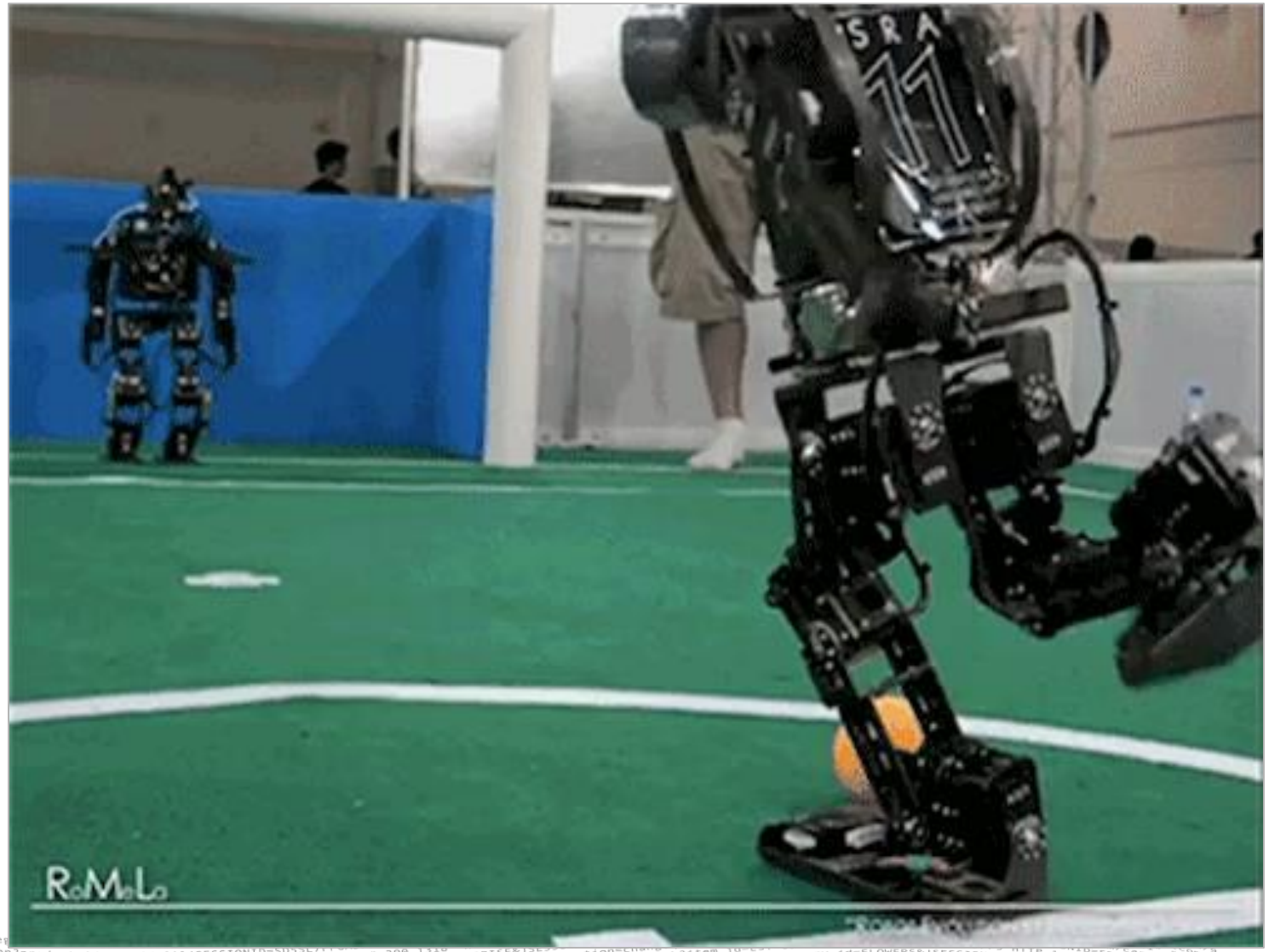
People

Bottom Line

Technology exists to serve people and processes.

Traditional SOC Challenges (1)

Efficacy



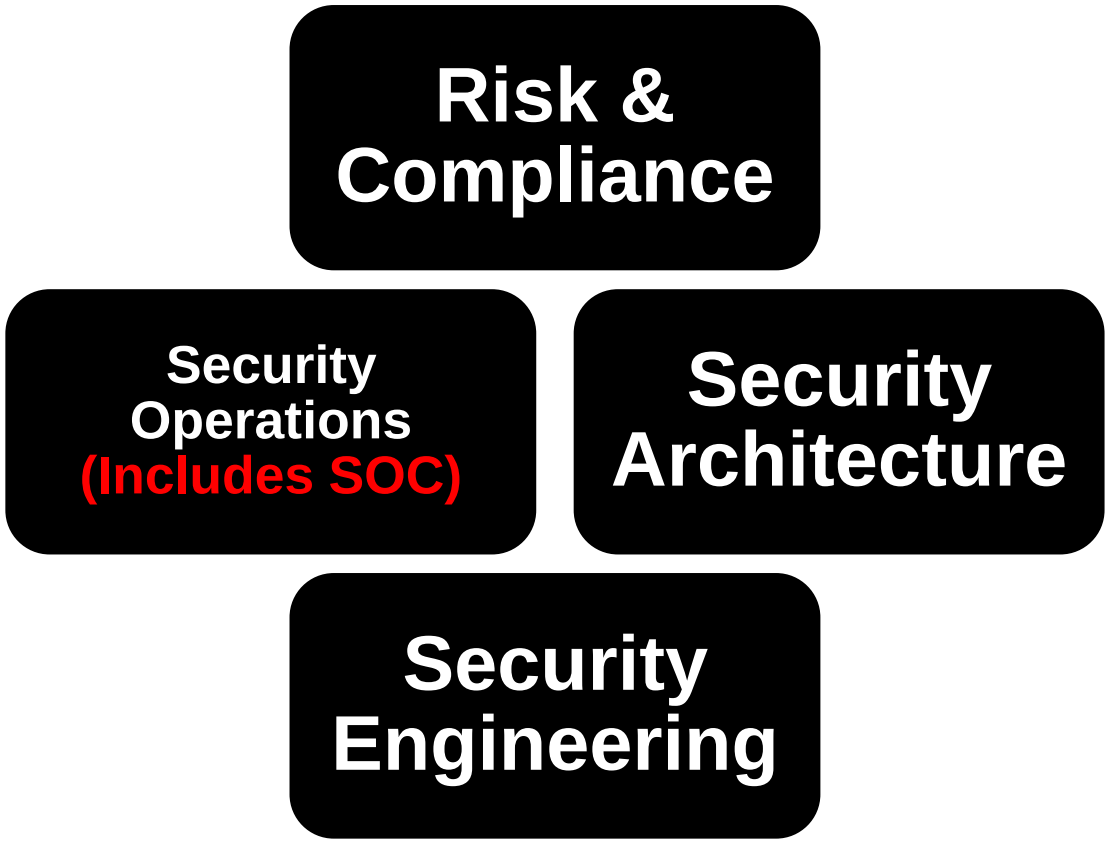
Traditional SOC Challenges (2)

Staffing

splunk>live!

Challenges with the traditional SOC (3)

Remember this?



Challenges with the traditional SOC (3)

Silo-ization

splunk>live!

Challenges with the traditional SOC (4)

COST

… and opportunity cost

Trends in Security Operations

splunk>live!

A SOC By Any Other Name…

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

splunk>live!

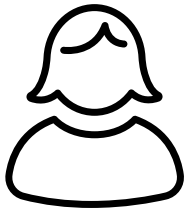
New Capabilities in the SOC

- 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



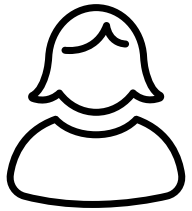
SIEM Admin, Tools Engineer

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

splunk>live!

Managed Security Services are Common

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

splunk>live!

Automation in the SOC

- Seeking to “Automate Tier 1”
- What do you automate?
  - Context gathering/enrichment – definitely
  - Configuration changes – maybe
  - Evidence collection – probably
- High premium on toolchain integration
- Security engineers are quickly becoming programmers

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
- “EXP” Indicates it is in t
- Lastly, the name of the
- When conversing abou
  been very efficient
- It has been a small effo

4002-EXP-Host wi

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

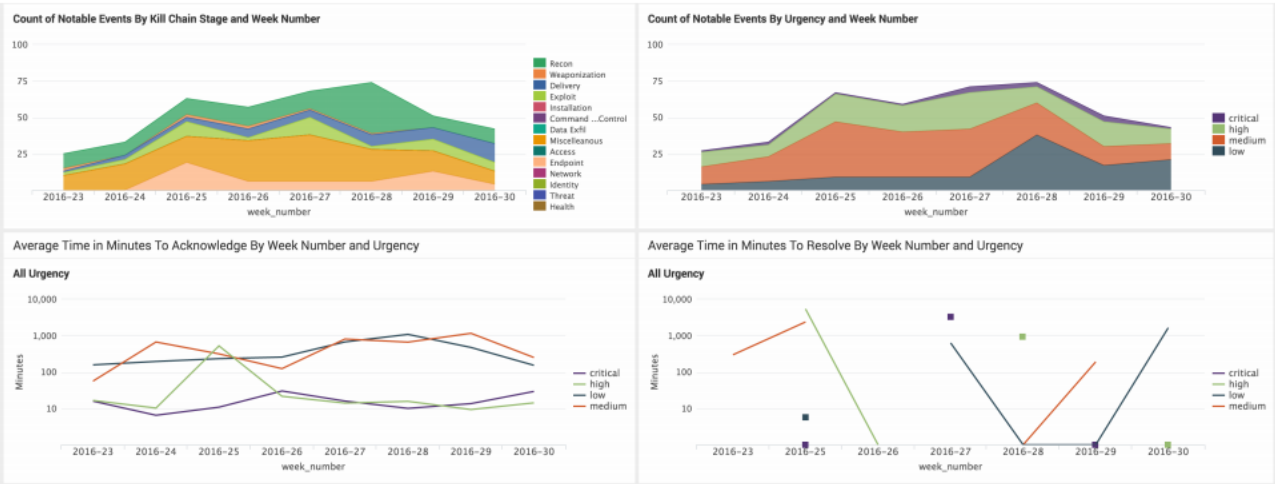
1 Rule Basics

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												

13

splunk> .conf2016

Notable Metrics Continued



20

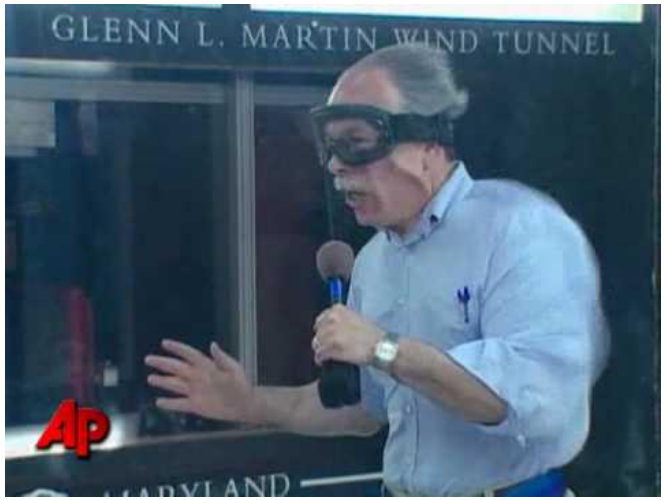
splunk> .conf2016

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

splunk>live!

Maturing Use of Threat Intelligence

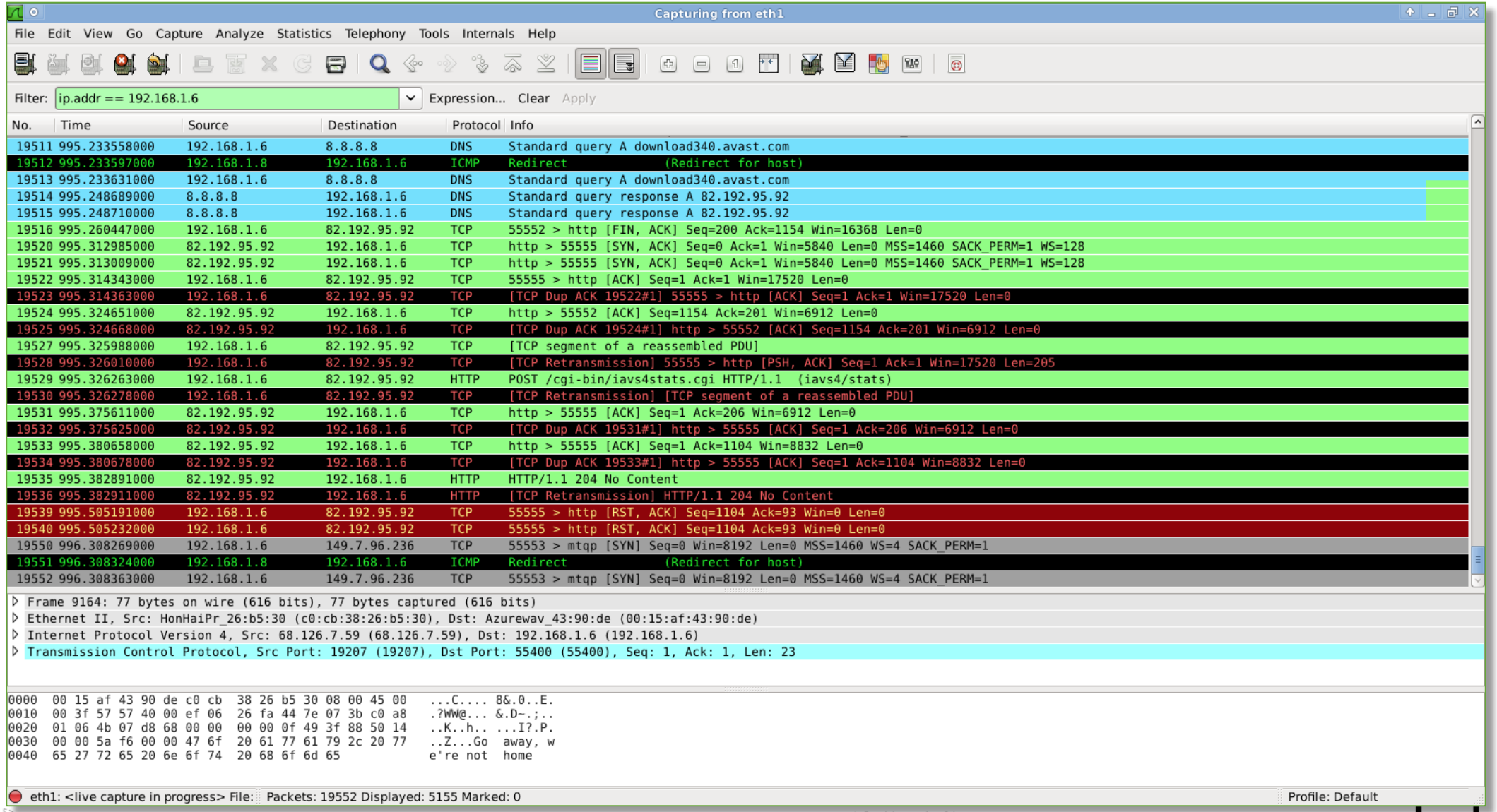
- Threat list + raw log feed = Noise
- Alert enriched by threat intel = Insight
- High maturity:
  - Gather your own threat intel
  - Share threat intel meaningfully



"Beware the threat list wind tunnel"

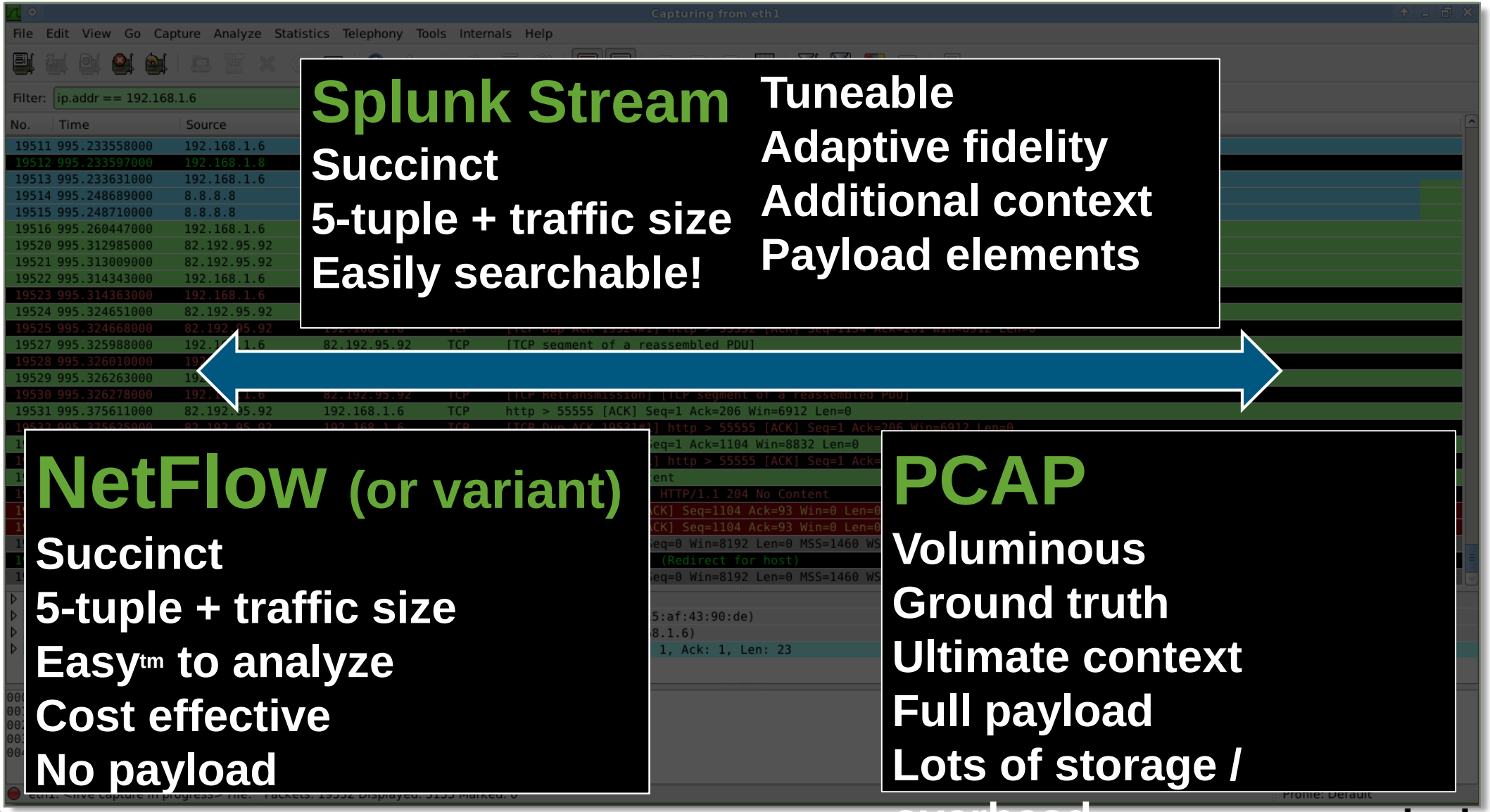
– Splunk Customer

Network (Meta)data



splunk>live!

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

splunk>live!

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**

splunk>live!

The Security Operations Toolchain

splunk>live!

Log Data Platform

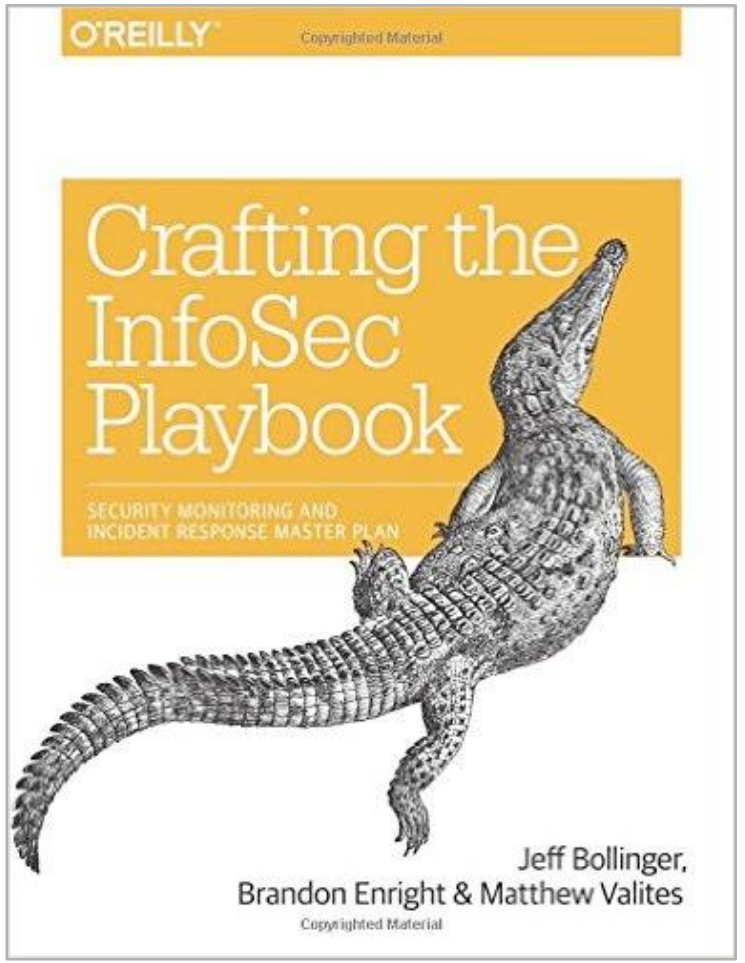
- Single source of truth
- Retention and integrity
- Any data source
- Easy correlation
- Automation / integration
- Performant and scalable
- Full fidelity

- 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

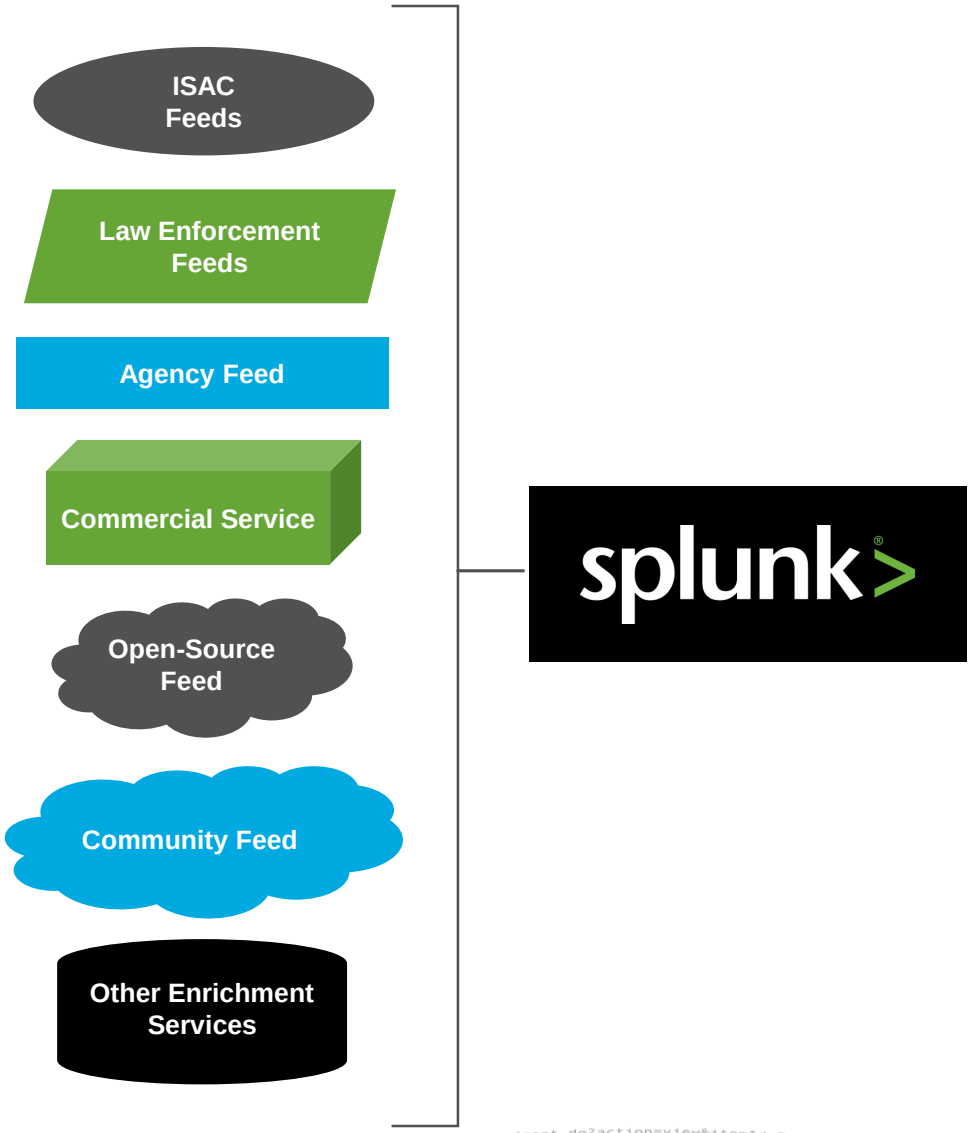
1. Assets and Identities
2. Threat intel
3. Firewall
4. Network metadata
5. Authentication
6. Server **(Windows / Linux)**
7. Endpoint
8. IDS / IPS
9. VPN
10. Application
11. Vulnerability

Splunk for Analytics-Driven SOC

splunk>live!

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

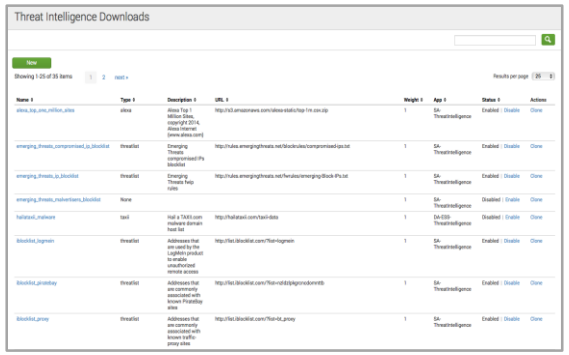


- Determine impact on network, assets
- Use for analysis / IR
- Collect / provide forensics
- Use to hunt / uncover / link events
- Share info with partners

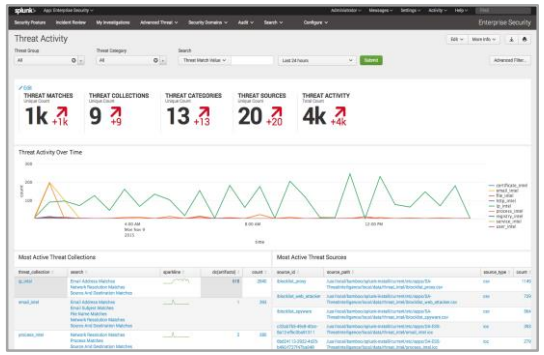
splunk>live!

Threat Intelligence Framework

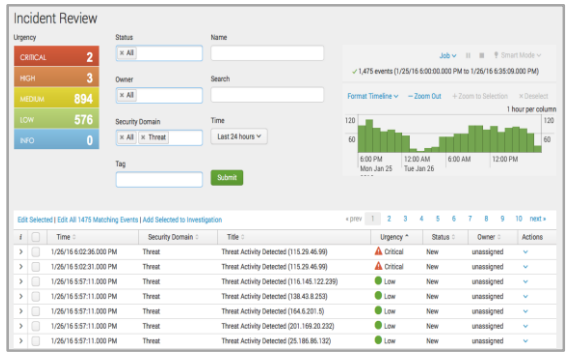
Collect, Manage → Categorize → Correlate → Search



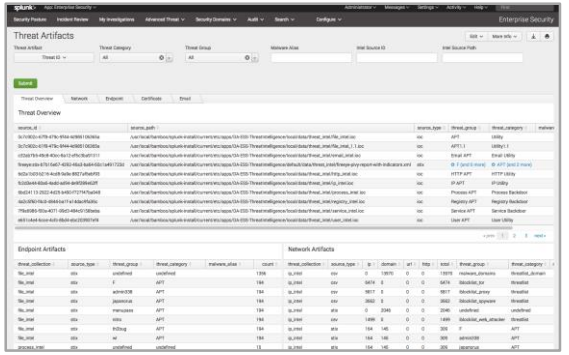
Data Management



Threat Activity



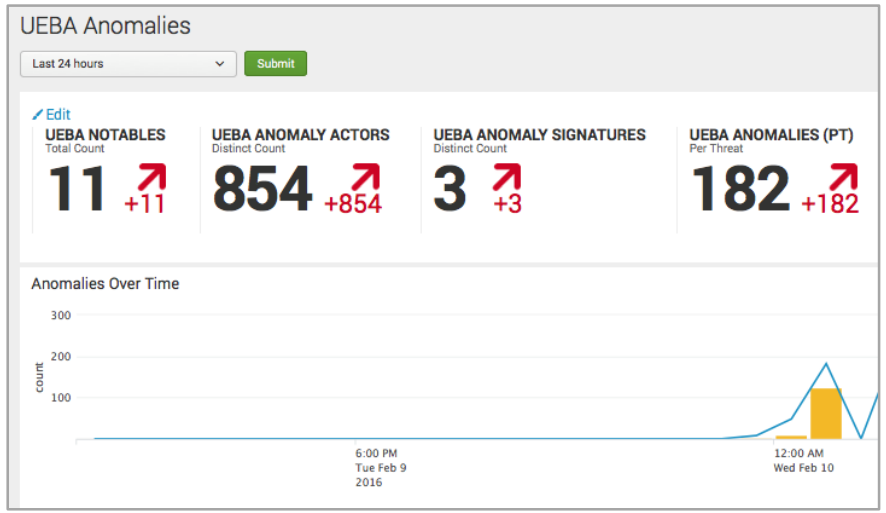
Correlation Data / Notable Events

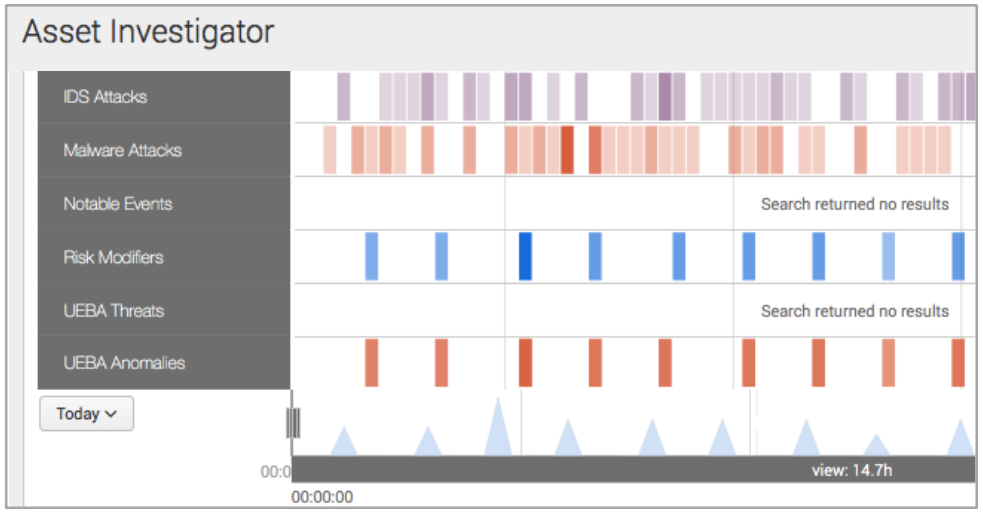


Data Search

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



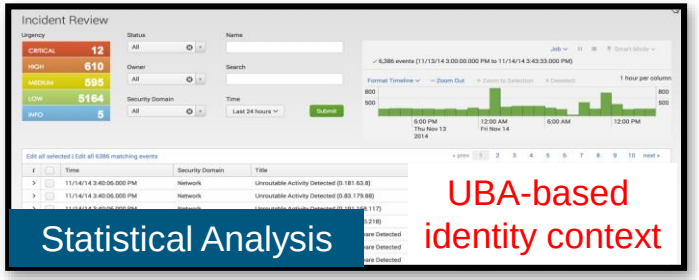


splunk>live!

Advanced Analytics and Machine Learning

splunk> ES

workflow

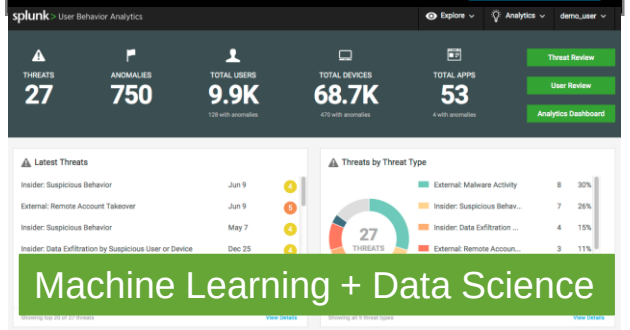


UBA-based identity context

Alert driven detection

Entity Resolution

splunk> UBA



DIY Machine Learning

DIY Statistical Analysis

UBA-based Machine Learning (Threat/Anomalies)

splunk>

Threats Anomalies

101111101010010001000001
111011111011101111101010
010001000001111011111011

UBA-based Machine Learning (Threat/Anomalies) Packaged

UBA-based ML + DS (Custom Threats)

splunk>live!

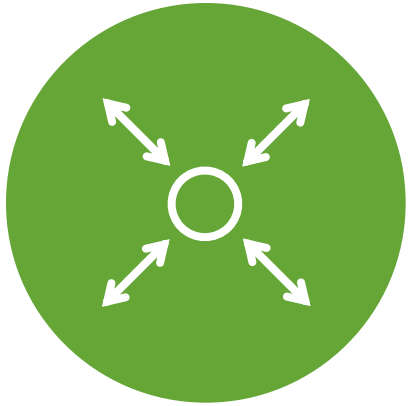
3. Automate When Feasible

- 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

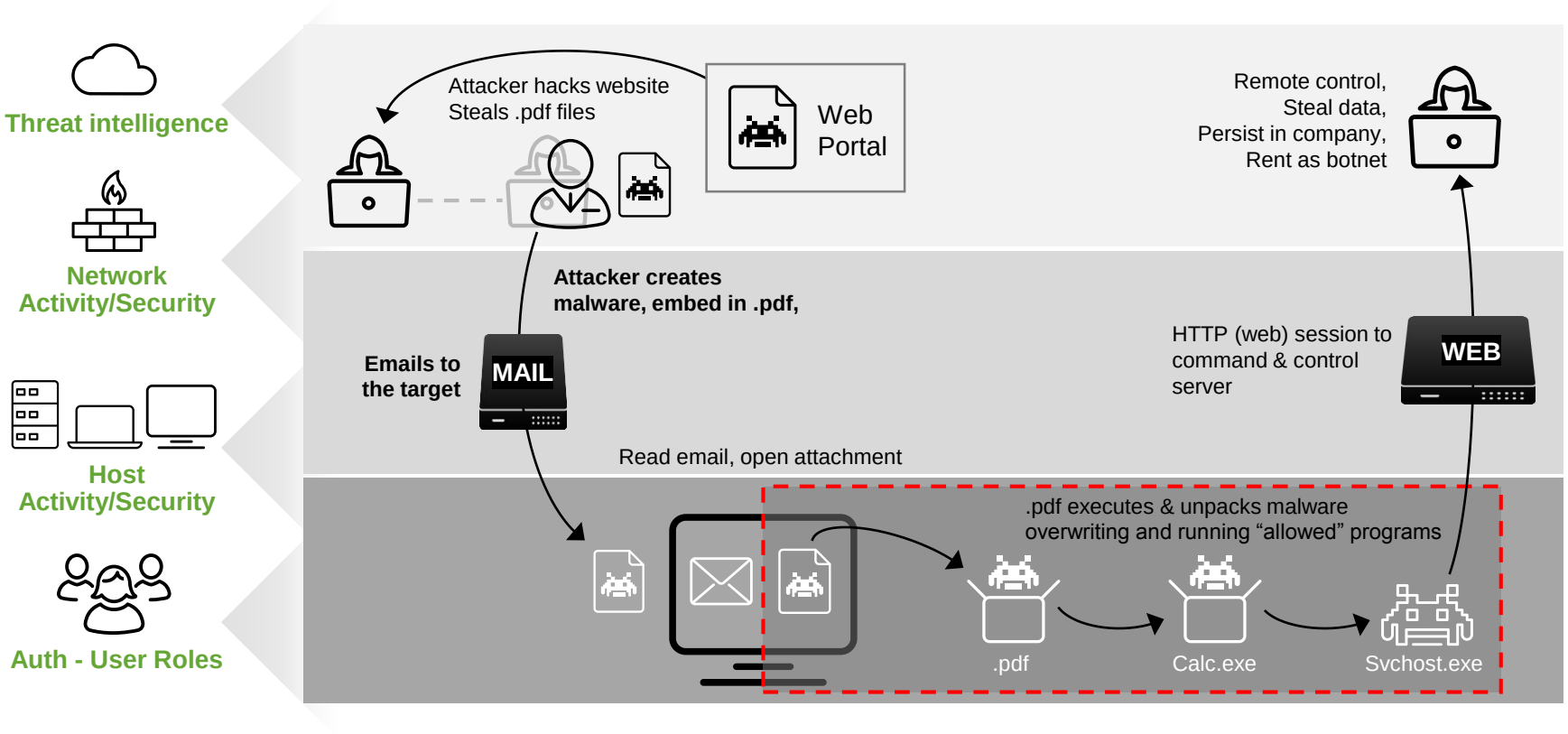
Adaptive Response: Analytics-Driven Decisions, Automation

- **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



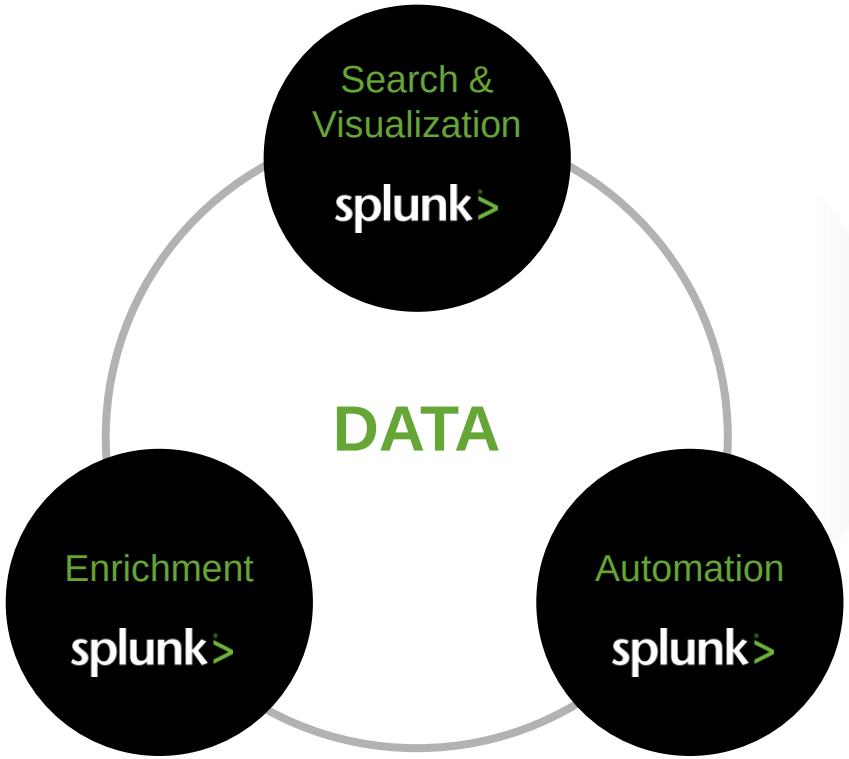
4. Proactively Hunt and Investigate - Considerations

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



splunk>live!

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

Microsoft .NET, Symantec, cisco, salesforce, kepware, paloalto networks, NetApp, servicenow, amazon web services, Linux

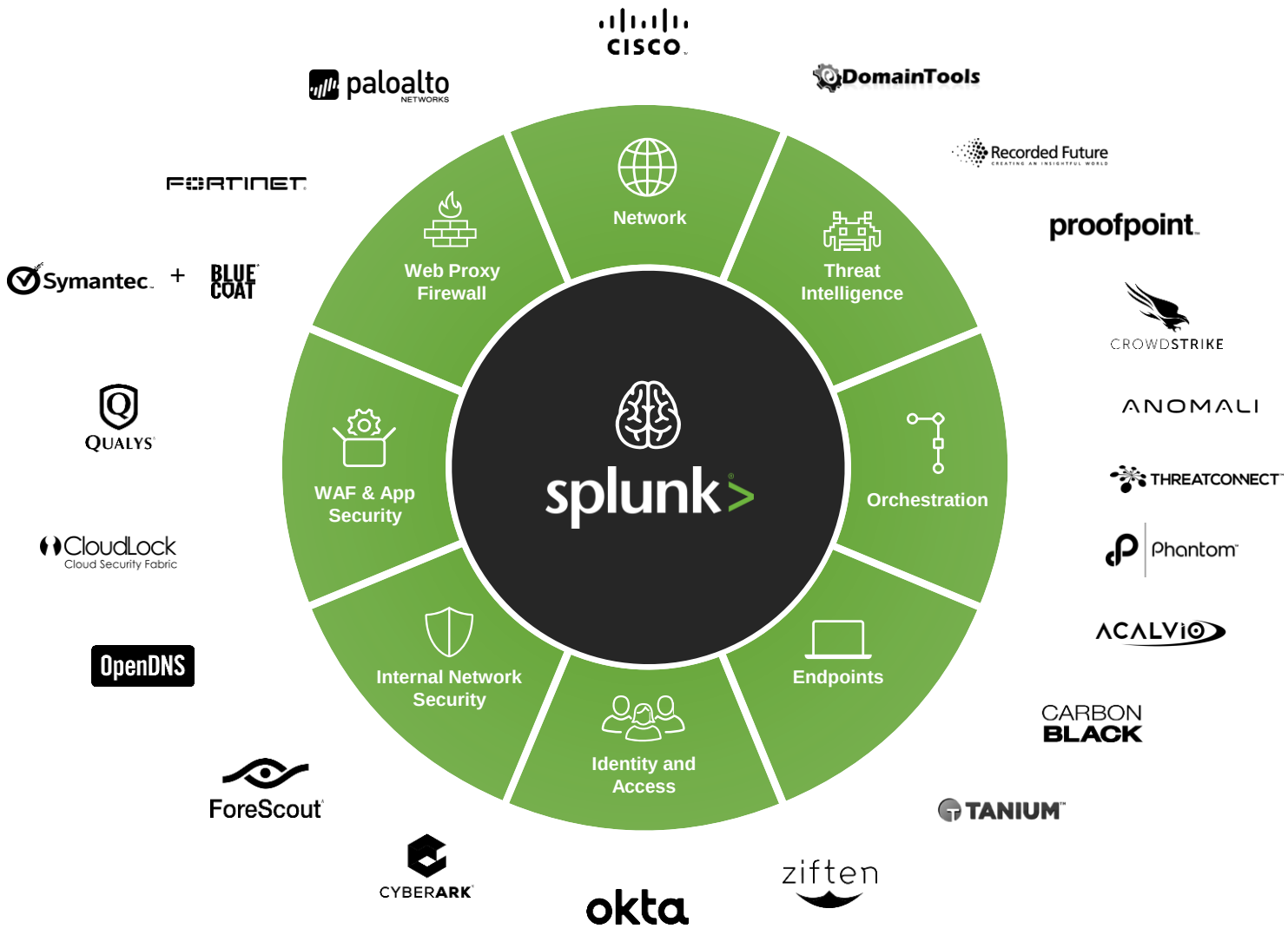
splunk>enterprise

splunk>cloud

splunk>live!

Insight From Across Ecosystem

Effectively leverage security infrastructure to gain a holistic view



splunk>live!

Splunk Analytics-Driven SIEM

FUNCTIONS	MONITOR REPORT	DETECT ALERT	ANALYZE INVESTIGATE	RESPONSE COLLABORATE
Splunk Enterprise Security™	Pre-defined views and rules	Correlation rules, thresholds	Analysis investigation & context enrichment	Enterprise-wide coordination & response

SIEM
Security ops management
alert & incident management, policy based rules, out-of-box security rules & analysis

splunk>enterprise

DATA PLATFORM
Collect, Index data for search and analysis, visualization. Dynamic ad hoc and statistical analysis

splunk>live!

Splunk Enterprise Security

A collection of Frameworks

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

Microsoft .NET, Symantec, cisco, salesforce, paloalto NETWORKS, kepware, NetApp, servicenow, amazon web services

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

splunk>live!

Customer Success

splunk>live!

TECHNOLOGY

Building an Intelligence Driven SOC

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

splunk>live!

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

splunk>live!

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

splunk>live!

Wrapping up

splunk>live!

Get started in minutes – splunk.com

1

FREE CLOUD TRIAL

2

FREE SOFTWARE DOWNLOAD

3

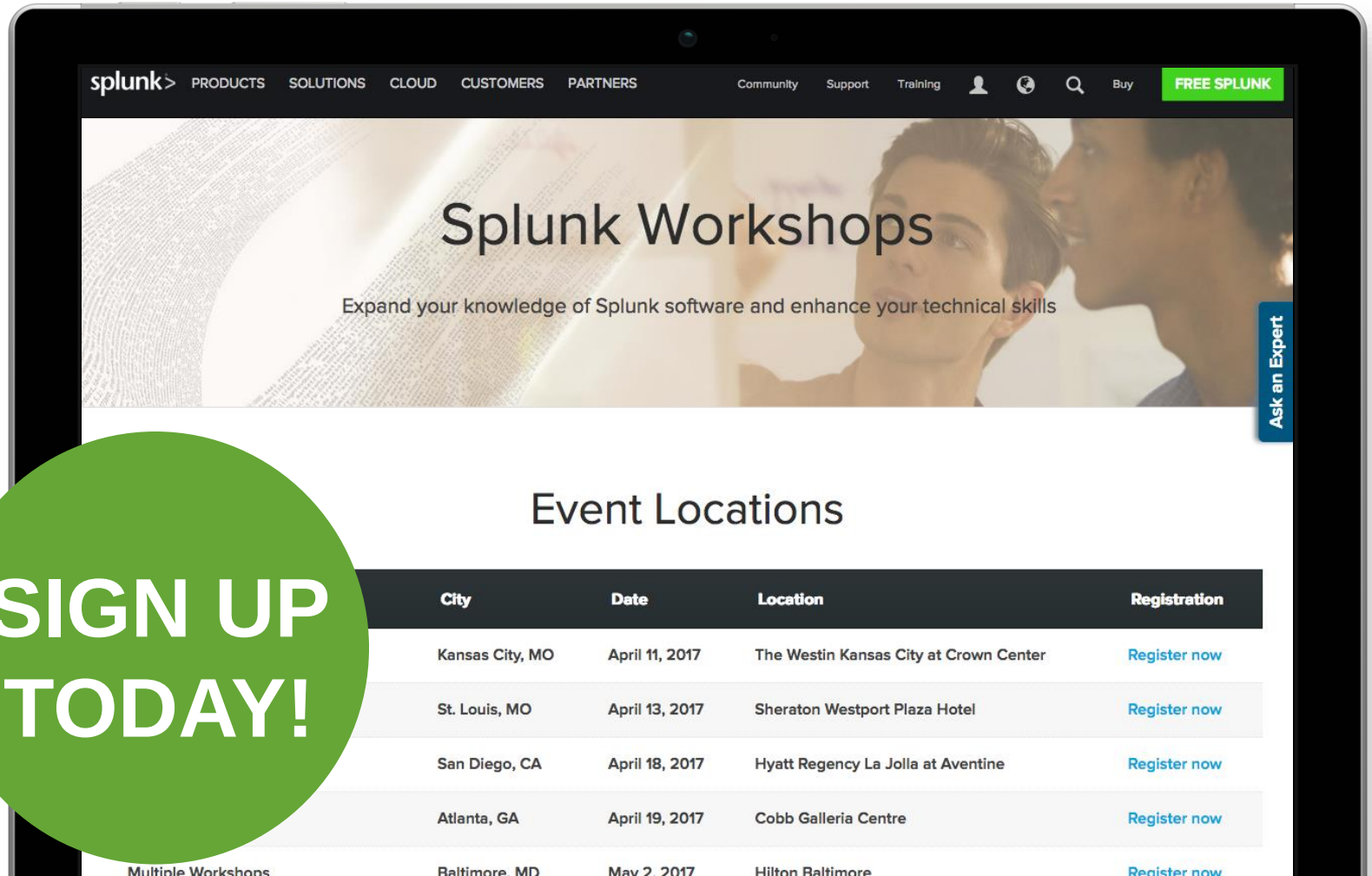
FREE ENTERPRISE SECURITY SANDBOX

splunk>

Workshops: Get Splunk Hands-on Experience

Attend a Splunk Workshop

splunk.com/workshops



SIGN UP TODAY!

May 23: San Francisco

- **Venue:** Sheraton Fisherman's Wharf
- **Time:** 8:30am
- Register Soon!
  - splunk.com/workshops

May 25: Sacramento

- **Venue:** Hyatt Regency Sacramento
- **Time:** 8:30am
- Register Now!
  - splunk.com/workshops

splunk>live!

.conf2017

The 8th Annual Splunk Conference

SEPT 25-28, 2017

Walter E. Washington Convention Center

Washington, D.C.

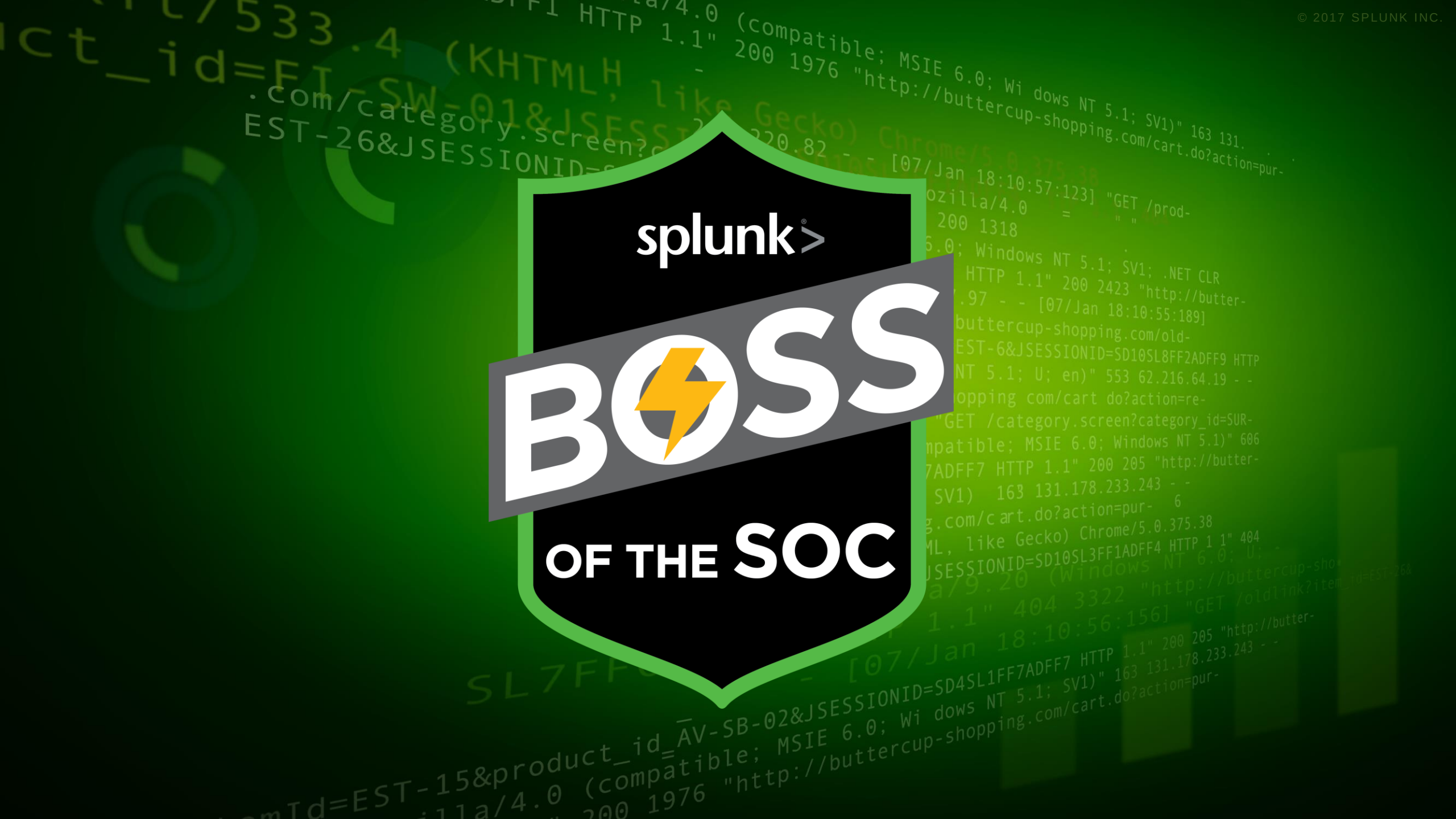
SAVE OVER $450

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!



Take the Survey on Pony Poll

ponypoll.com/slsf

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

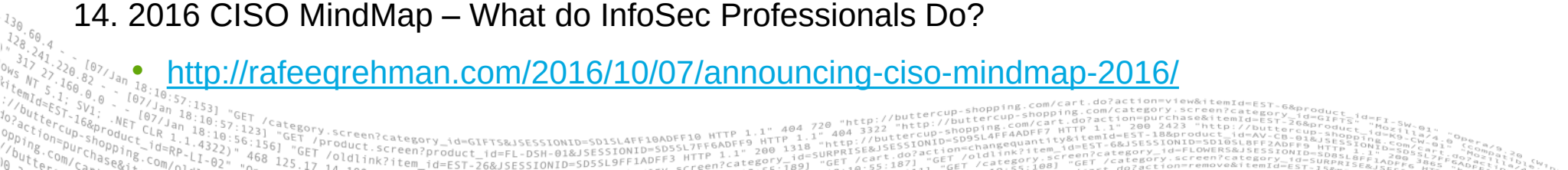
Resources Cited (1)

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

splunk>live!

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/



splunk>live!