splunk> live!

APRIL 20 | MINNEAPOLIS, MN

Build a Security Portfolio That Strengthens Your Security Posture

David Clawson | SplunkYoda @ 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!

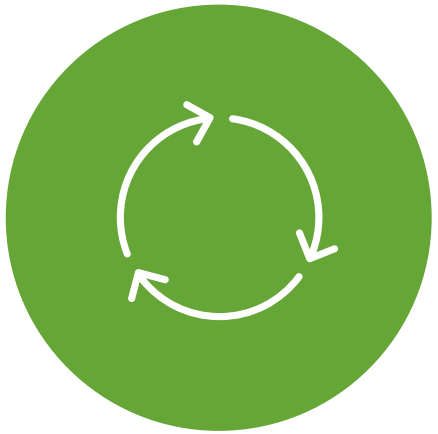
What Can You Expect From This Session?

1. Common Security Challenges
2. How to Strengthen Your Security Posture with a few approaches
3. Are you Ready? CIS Controls

Security is Still a Reactive Game

Tools

“Alerts”
not “Insights”



Process

Not
Optimized

People

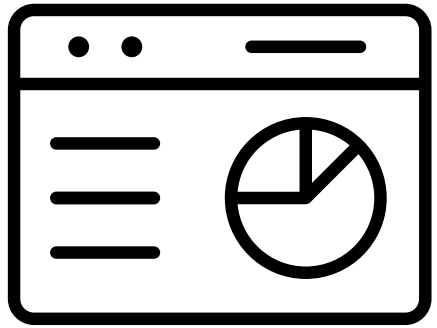
Alert
Overload

Scale

Across
Environments

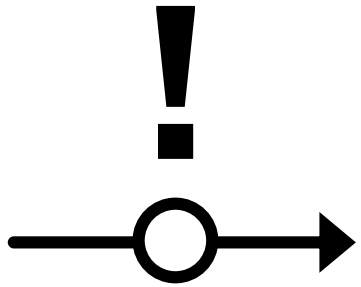
splunk>live!

Strengthen Your Security Posture



Centralize Analysis

Streamline Investigations



Enforce Critical Controls

Central Analysis

splunk>live!

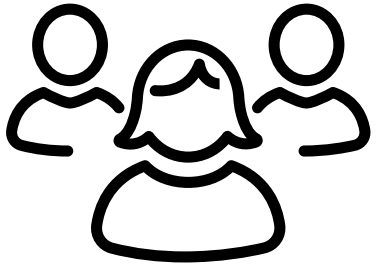
What Tools Do You Have Today?

Problem	Solution
Protect Endpoint	Antiviruses: Symantec, McAfee
Protect Network: Unauthorized Traffic	Firewalls/Web Filter: Palo Alto, Cisco
Indicators of Malicious Activity	Threat Intelligence
Control User Access	Authentication/2-Factor: AD, RSA, Badges
Network Attacks, Stolen Information, Phishing	IDS/IPS: Cisco, Palo Alto Email Filter: Cisco, Proofpoint
Unpatched Systems, versions with bugs	Scanners/Patching: Nessus, SCCM

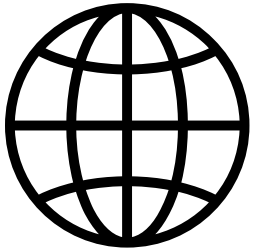
splunk>live!

4 Use Cases to Improve Your Posture

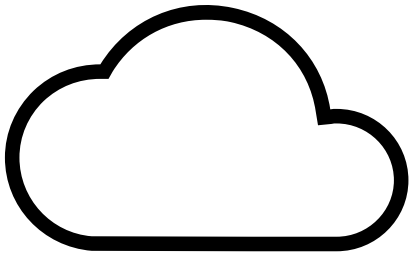
Endpoint



Access/Identity



Network



Threat Intelligence

Understanding Your Endpoints

Endpoint Intelligence and User Activity

Endpoints

End Point System:
Windows Sysmon, Network, File Info

End Point Security:
Virus, Malware, Spyware, Whitelisting, Behaviors

What You Discover

- Frequency of application executions, unique applications
- Non-corporate approved applications

Benefit

- Visibility into application executions
- Understanding of unknown applications – whom and where and frequency

splunk>live!

Endpoint Domain Demo

Endpoint

Access/Identity

Network

Threat Intelligence

Symantec

CISCO

paloalto NETWORKS

Custom APP

splunk> Platform for Operational Intelligence

splunk>live!

Splunk Demo

Endpoint Protection at a glance

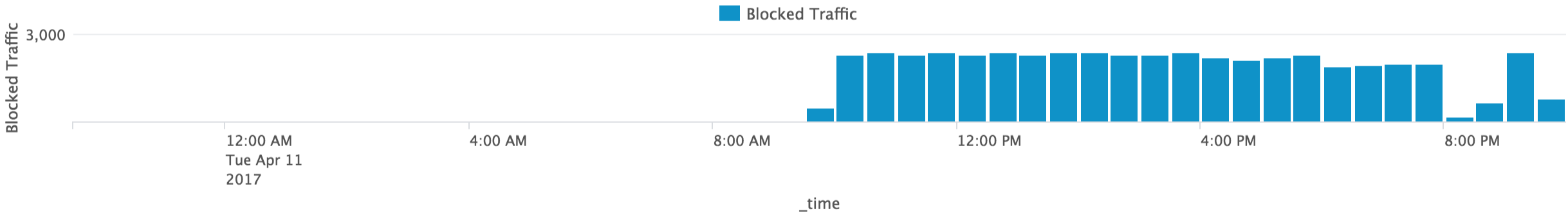
Show Filters | Edit | Export | ...

IPS (Vantage)	File Reputation (Insight)	AntiVirus Engine	Suspicious Files	Users At Risk	All Files Inspected
264 N/A	54 N/A	135 N/A	135 N/A	186 N/A	459 N/A

1

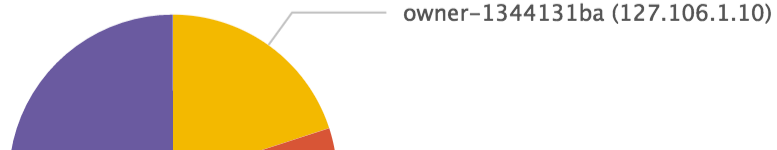
Blocked Traffic

Endpoint level - Traffic Block Status : Increase in the amount of network access blocks at the endpoint layer.



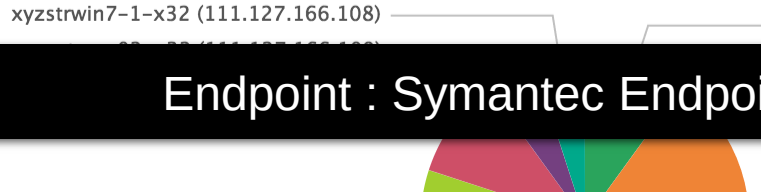
Local Hosts By Conviction

Top host detected with violations (Local Network)



Remote Hosts By Conviction

Top host detected with violations (Remote Network)



Endpoint : Symantec Endpoint Protection Analysis

Access and Identity

Who, Why and Credential Abuse

Access/Identity

Windows Security Events:
Active Directory and Authentication Logs

What You Discover

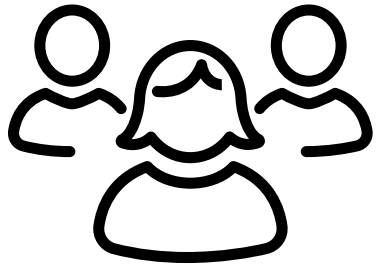
- Credentials used in multiple locations, or shared by users
- Admin credential abuse
- Login frequencies, users moving around quickly
- Users failing authentications trying to discover internal/external resources

Benefit

- Uncover unusual login patterns
- Track user behavior

Access/Identity Domain Demo

Endpoint



Access/Identity

Network

Threat Intelligence

Symantec

CISCO

paloalto NETWORKS

Custom APP

splunk> Platform for Operational Intelligence

splunk>live!

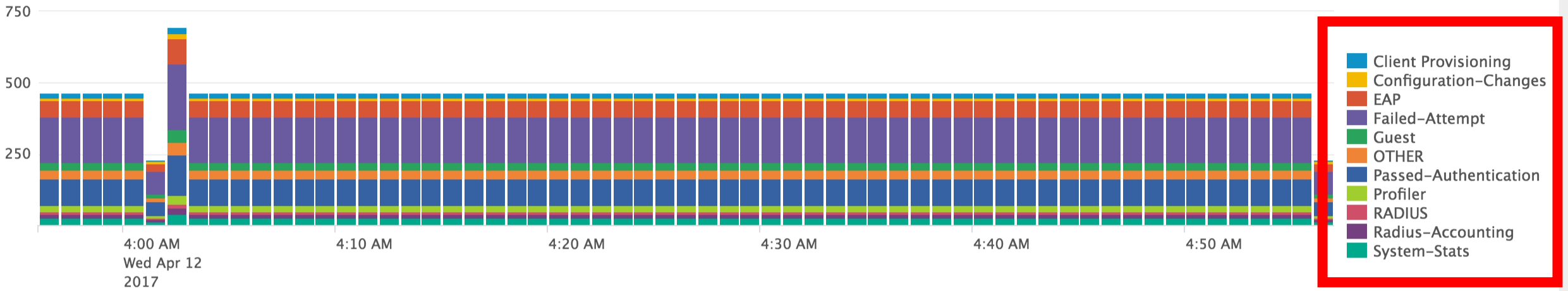
Splunk Demo

ISE Summary View

Show Filters

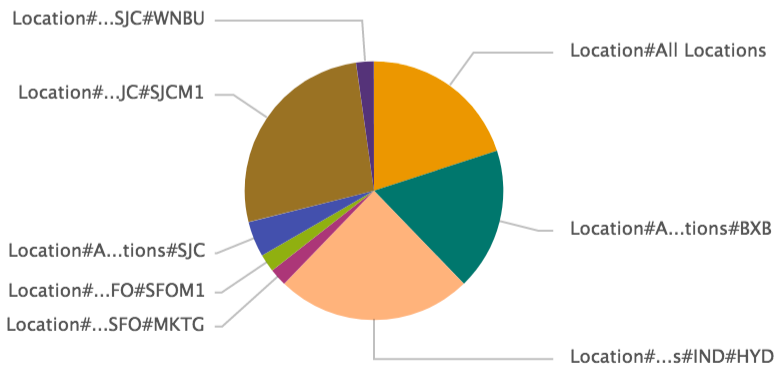
Export ...

ISE events

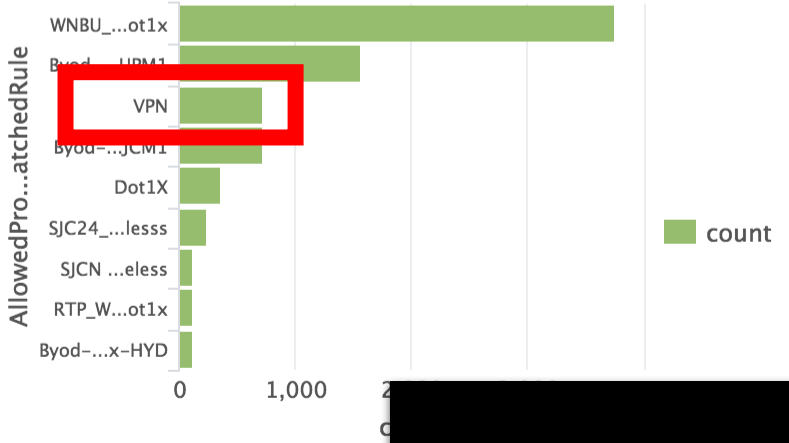


1m ago

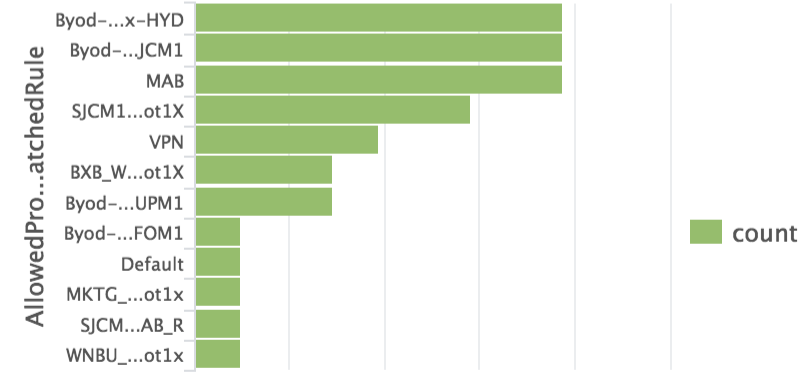
Location Summary



Failures by Protocol Rule



Passed Auths by Protocol Rule



Access / Authentication : Cisco ISE App

Top Alarms

Authentication Summary

Network Activity

Detecting Exfiltration and IP Theft

Network

Network Access:
ForeScout

Firewall:
Cisco, Palo Alto

Network:
DNS – Splunk Stream, DNS Server

What You Discover

- Who talked to whom, traffic volumes (in/out)
- Malware download/delivery, C2, exfiltration
- Horizontal and vertical movement

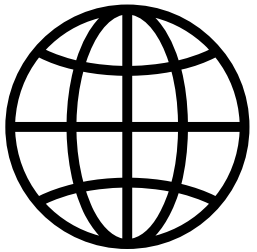
Benefit

- Determine how threats got in
- Systems communicating internally
- Detect intellectual property theft, insiders

Network Domain Demo

Endpoint

Access/Identity



Network

Threat Intelligence

splunk> Platform for Operational Intelligence

splunk>live!

Splunk Demo

Palo Alto Networks | Traffic | Threat | Content | WildFire | Endpoint | GlobalProtect | Console | Search

Traffic Dashboard

Edit | Export | ...

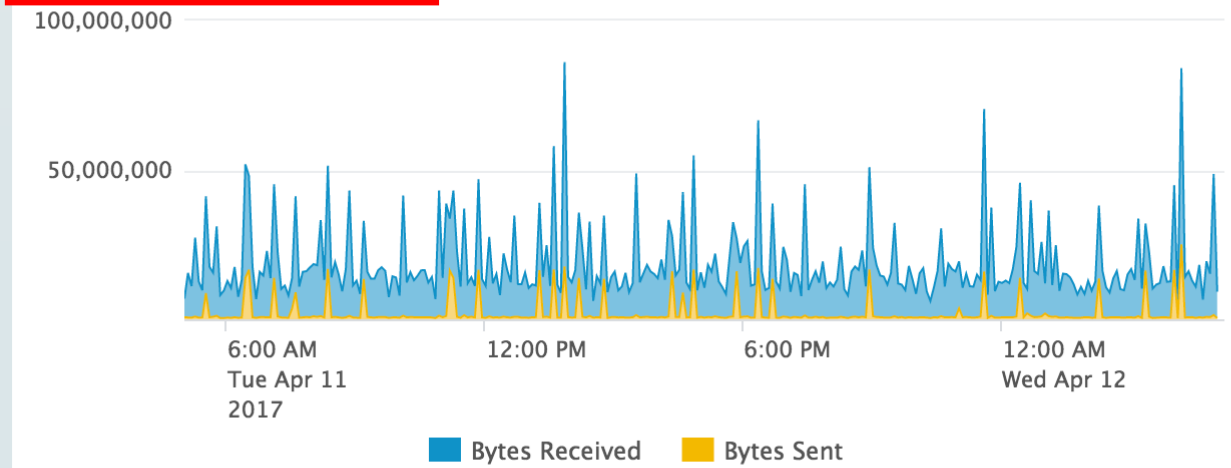
Source IP | Destination IP | Destination Port | Source User

Last 24 hours

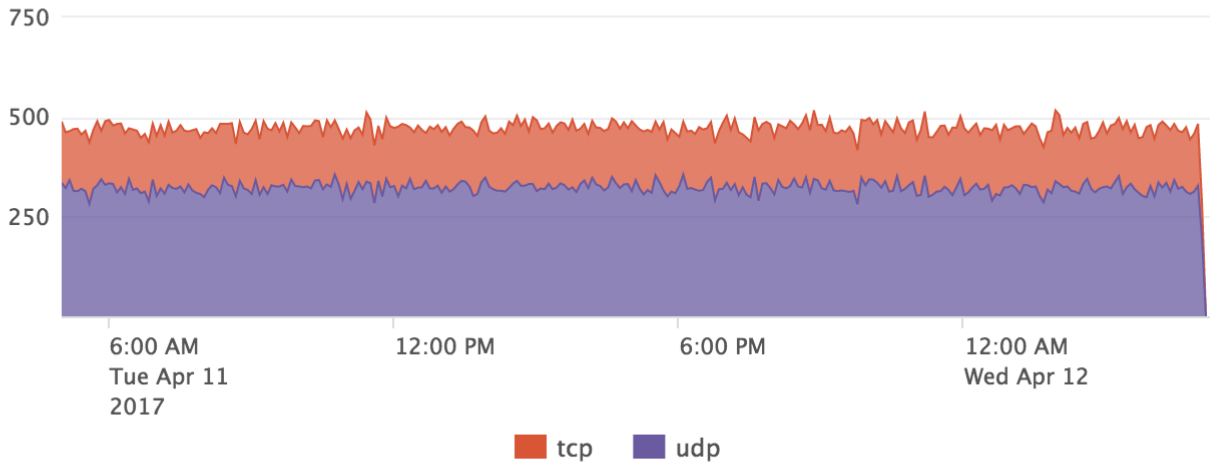
Application | Action

Submit | Hide Filters

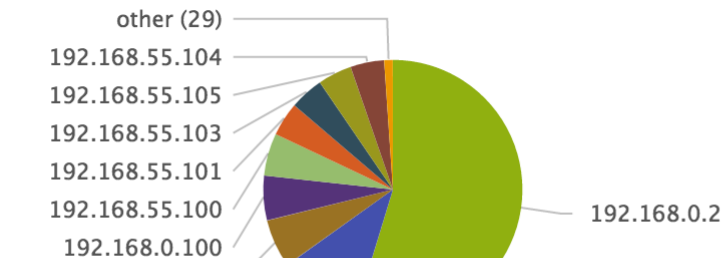
Bytes Transfered Over Time



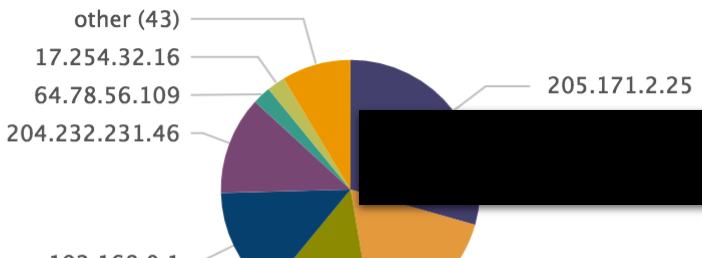
Protocols Over Time



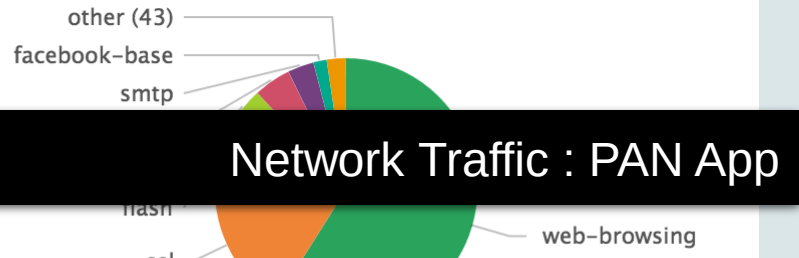
Source IP



Destination IP



Applications by Bytes Transfered



Network Traffic : PAN App

Threat Intelligence

Known and Early Warning Indicators

Threat Intelligence

Threat Feeds: Public, Free, Private, Paid or Custom – ThreatConnect, Anomali

Firewall: Cisco, Palo Alto Neworks

What You Discover

- High risk behaviors and patterns
- Malware not blocked, malware and command & control activities
- Known indicators of compromise

Benefit

- Early warning of malicious activity
- Find traffic going to compromised or watch-listed sites
- Compromised systems communicating with each other
- Compromised endpoints

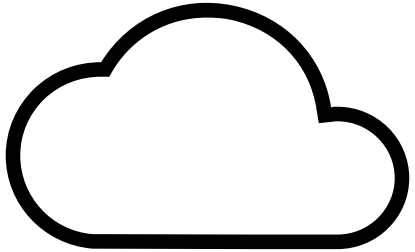
splunk>live!

Threat Intelligence Domain Demo

Endpoint

Access/Identity

Network



Threat Intelligence

splunk> Platform for Operational Intelligence

splunk>live!

Splunk Demo

01 - Network Traffic Overview

Edit Export ...

Search Host: *

Traffic Type:

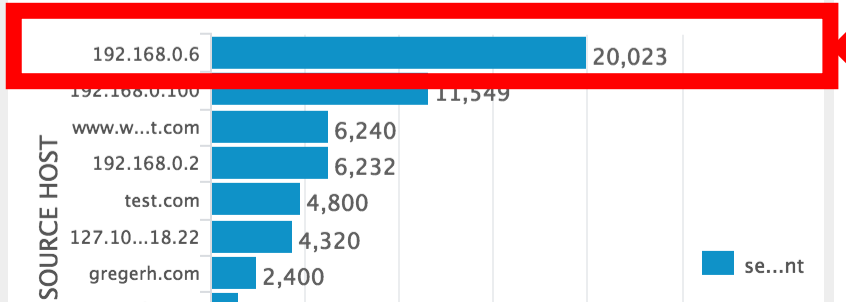
Time Window: Last 60 minutes Submit Hide Filters

HOST TRAFFIC STATUS

Top Bandwidth Host

src	sum_bytes
192.168.0.6	93,743,952 Bytes
192.168.0.3	58,561,312 Bytes
10.0.1.20	35,493,395 Bytes
192.168.0.2	31,000,720 Bytes
126.217.138.9	902,224 Bytes
137.211.71.90	902,224 Bytes
137.8.153.223	902,224 Bytes
225.212.141.91	902,224 Bytes
89.3.77.76	902,224 Bytes
154.219.33.132	387,209 Bytes

Top Session Host



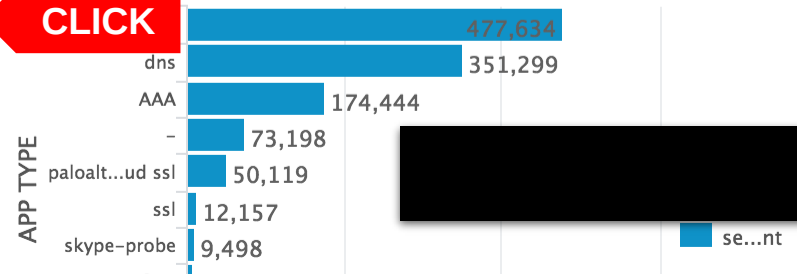
CLICK

APPLICATION TRAFFIC STATUS

Top Bandwidth Application

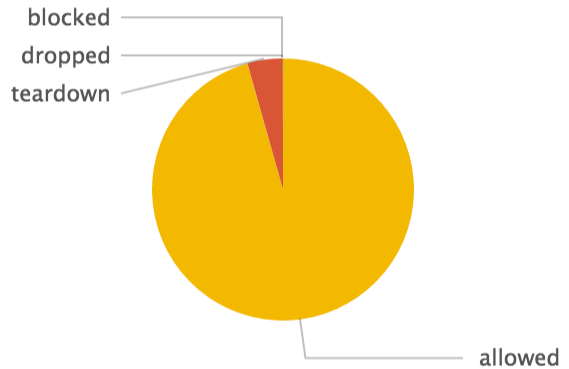
app	sum_bytes
web-browsing	161,314,329 Bytes
flash	28,787,981 Bytes
AAA	10,081,079 Bytes
google-safebrowsing	8,511,099 Bytes
sourceforge	8,308,223 Bytes
smtp	6,643,107 Bytes
ssl	1,994,996 Bytes
facebook-base	1,396,501 Bytes
hotmail	414,459 Bytes
flickr-base	370,635 Bytes

Top Session Application

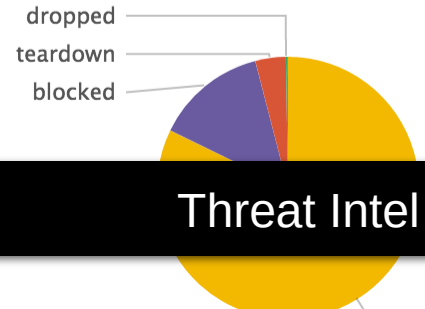


ACTIONS ON TRAFFIC

Top Bandwidth Actions



Top Session Actions



Threat Intel : Custom App

Investigation

splunk>live!

Investigation is a Foundational Skill for Everyone

"Investigate" – gather data, analyze, pinpoint digital evidence

- Helps anyone handling alerts

- Gain control of posture
  - Old way – "escalate or ignore"
  - New way – find out WTF is actually going on

If each alert takes 10 min to investigate

If you reduce to 5 min

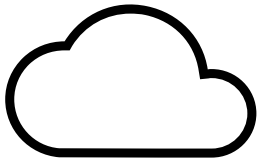
If you handle 100 alerts a month
(5 alerts a day, 20 days in month)
100x10 = 1,000 min/60 = 16 hours
100x5 = 500 min/60 = 8 hours

You get a day back (8 hours)

14 – 28 cases in a shift*

splunk>live!

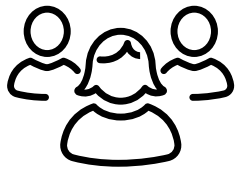
Security technologies designed to detect bad/suspicious activity



Threat Intelligence

Network

Endpoint



Access/Identity

Alert

Indicator

Information

Data

Data Breach

Infection (s)

Account Take Over

Application Fault

Misconfiguration

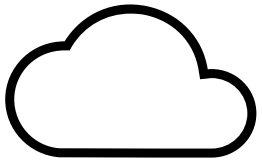
Missing patch

User Error

Other (Ignore)

splunk>live!

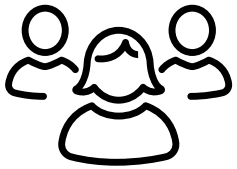
The Typical Investigative Cycle



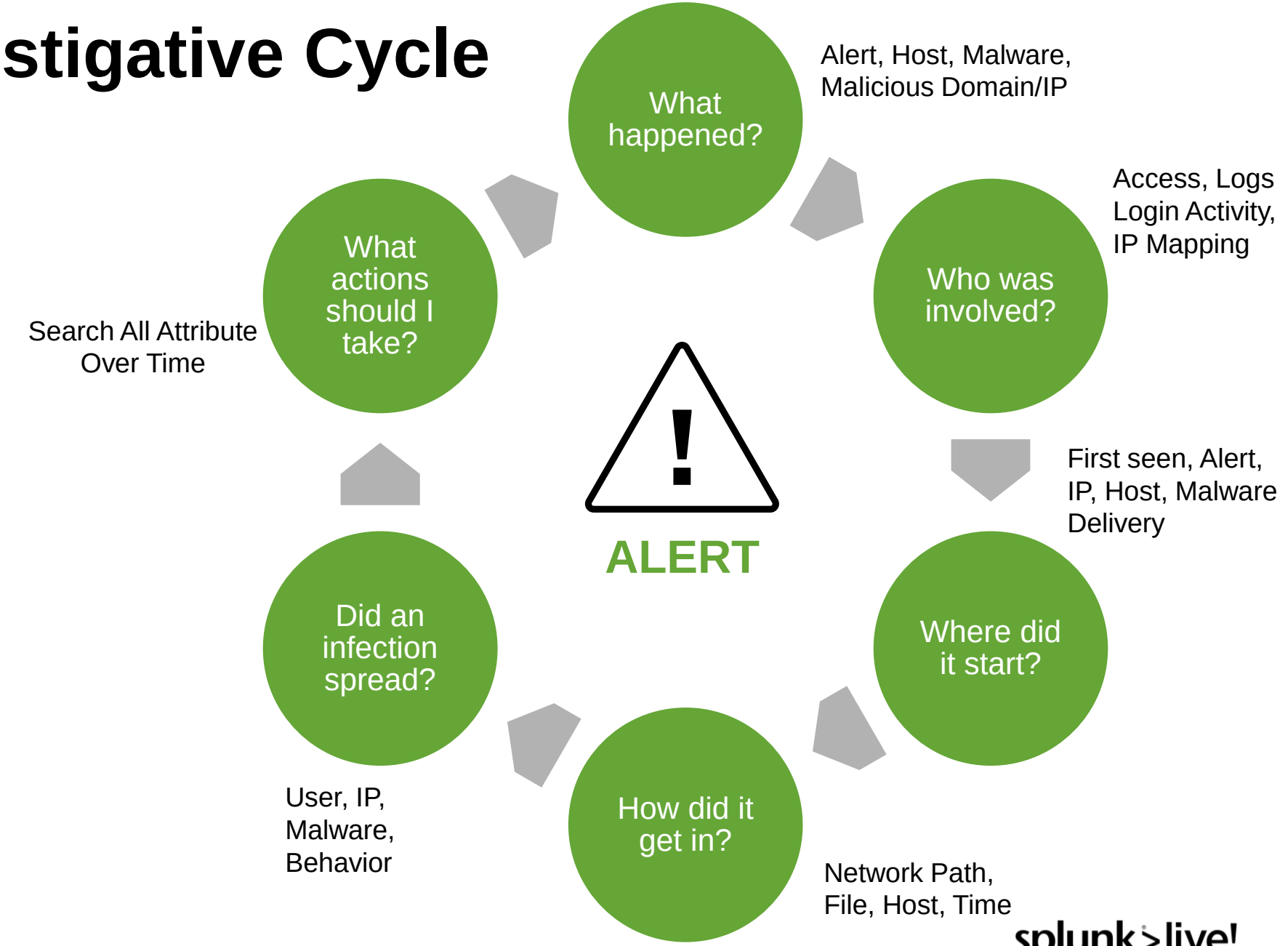
Threat Intelligence

Network

Endpoint

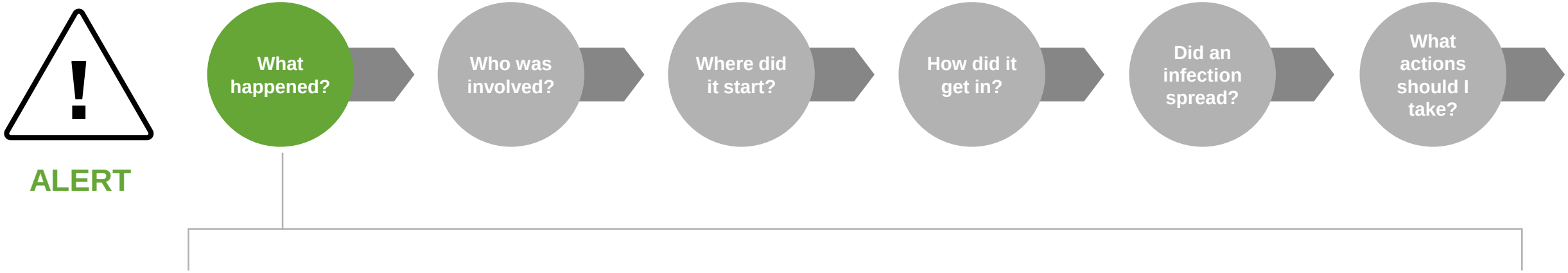


Access/Identity



splunk>live!

The Investigation – Analytics Cycle



Question	Logic	Example	Data
Is the system actually compromised?	Index logs and search for matches against alert criteria	Verify malware detected alert on host against known file hash	Endpoint logs Authentication logs Network logs Threat intelligence

The Investigation – Analytics Cycle

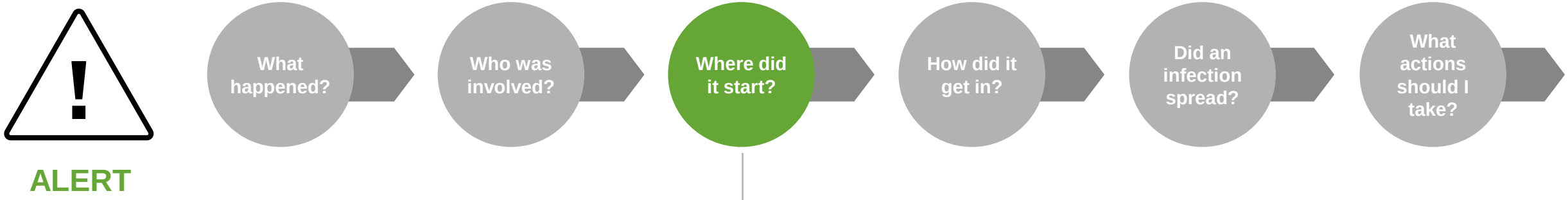
ALERT

What happened? → **Who was involved?** → Where did it start? → How did it get in? → Did an infection spread? → What actions should I take?

Question	Logic	Example	Data
What accounts / users are associated with that system?	Determine IP to asset to identity mapping	Jane Doe IP = 10.10.200.20 Workstation running Win10	Identity system DNS log Authentication logs Asset repository

splunk>live!

The Investigation – Analytics Cycle



Question	Logic	Example	Data
Timeline of activities leading up to and during the alert?	Integrate your asset system	Resolve the location via reverse geo IP lookup	All Available Data

splunk>live!

The Investigation – Analytics Cycle

ALERT

What happened? → Who was involved? → Where did it start? → **How did it get in?** → Did an infection spread? → What actions should I take?

Question	Logic	Example	Data
Is there a logical connection to other activity, IPs, hosts, malware, other alerts?	Index event logs and trace network hops to determine initial entry	Mapped network diagram shows vector in via mail proxy, user in finance victim of spear phishing	Network devices Firewall Web proxy Mail proxy DNS Authentication VPN

splunk>live!

The Investigation – Analytics Cycle

ALERT

What happened? → Who was involved? → Where did it start? → How did it get in? → **Did an infection spread?** → What actions should I take?

Question	Logic	Example	Data
Has the attack progressed beyond system infection?	Identify whether malware has spread via statistical analysis	Ransomware infection spread goes undetected by signature-based tools	Endpoint Firewall DHCP Web proxy Mail proxy Wire data

splunk>live!

The Investigation – Analytics Cycle

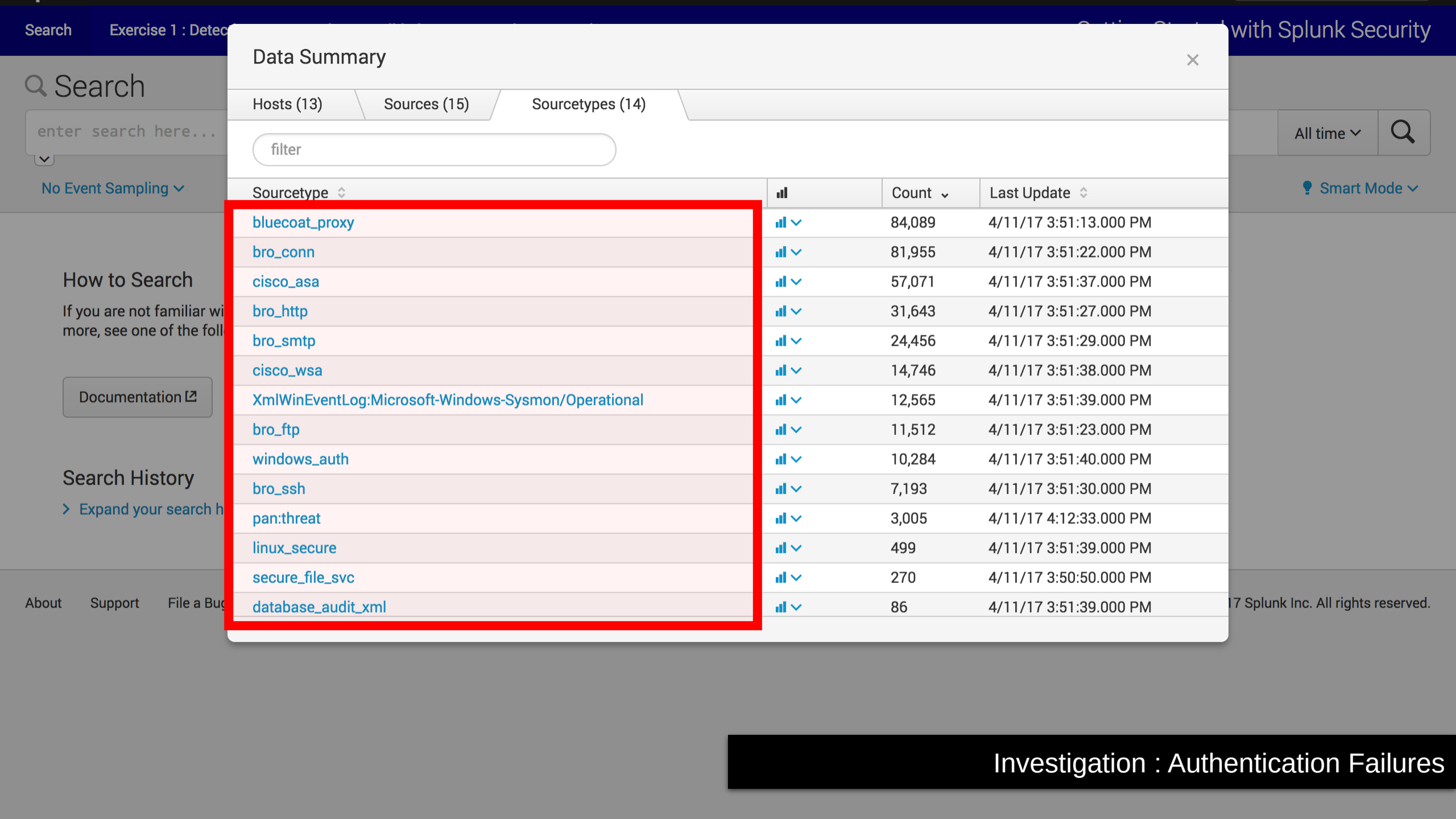
ALERT

What happened? → Who was involved? → Where did it start? → How did it get in? → Did an infection spread? → What actions should I take?

Question	Logic	Example	Data
Is there any indication the attacker has gained access to the environment?	Identify any C&C Identify lateral movement	Beaconing to known bad IP in remote geo – add to dynamic address group on FW	Threat intelligence Subscriptions Network / FW / Proxy DNS Wire data

splunk>live!

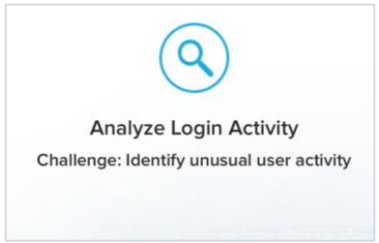
Splunk Demo


Search
Exercise 1 : Detec
with Splunk Security
Search
enter search here...
All time
No Event Sampling
Smart Mode
How to Search
If you are not familiar wi
more, see one of the foll
Documentation
Search History
Expand your search h
About
Support
File a Bug
17 Splunk Inc. All rights reserved.
Data Summary
Hosts (13)
Sources (15)
Sourcetypes (14)
filter
Sourcetype
Count
Last Update
bluecoat_proxy 84,089 4/11/17 3:51:13.000 PM
bro_conn 81,955 4/11/17 3:51:22.000 PM
cisco_asa 57,071 4/11/17 3:51:37.000 PM
bro_http 31,643 4/11/17 3:51:27.000 PM
bro_smtp 24,456 4/11/17 3:51:29.000 PM
cisco_wsa 14,746 4/11/17 3:51:38.000 PM
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational 12,565 4/11/17 3:51:39.000 PM
bro_ftp 11,512 4/11/17 3:51:23.000 PM
windows_auth 10,284 4/11/17 3:51:40.000 PM
bro_ssh 7,193 4/11/17 3:51:30.000 PM
pan:threat 3,005 4/11/17 4:12:33.000 PM
linux_secure 499 4/11/17 3:51:39.000 PM
secure_file_svc 270 4/11/17 3:50:50.000 PM
database_audit_xml 86 4/11/17 3:51:39.000 PM
Investigation : Authentication Failures

Try It Yourself

Security Investigation Online Demo Experiences

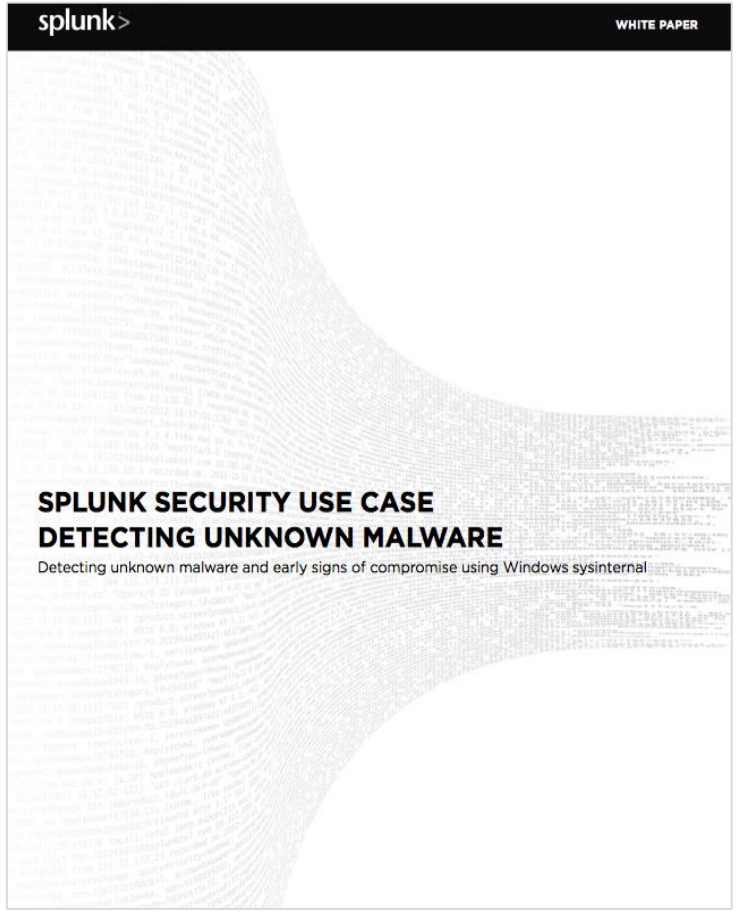
Explore security investigation use cases in our free, online demo environment.



- **What happened (verify alert)**
  - Login
    - Exercise 2 – Assessment

- **Did an infection spread**
  - Endpoint
    - Exercise 1 – Infection: Statistical Analysis

- **What actions should I take**
  - Network
    - Exercise 1 -- C&C activity detection

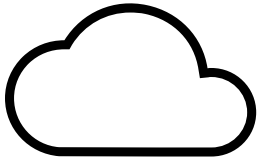


splunk>live!

Security Readiness

splunk>live!

Security Technologies Across Your Company



Threat Intelligence

Getting updates?

Network

Controls in place?

Endpoint

Patching level?

Access/Identity

Privileged users?

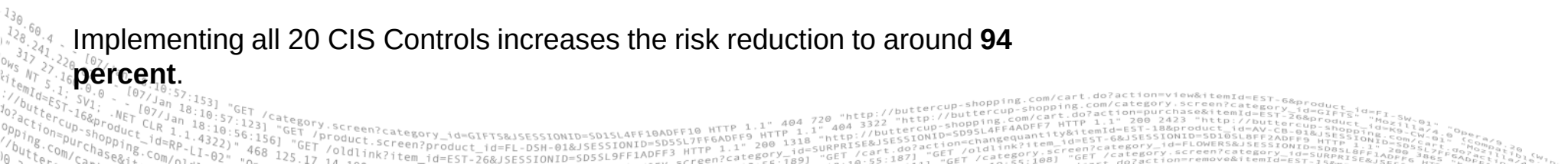
Top 5 CIS Controls

- CSC 1: Inventory of Authorized and Unauthorized Devices.
- CSC 2: Inventory of Authorized and Unauthorized Software.
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges.

Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around **85 percent**.

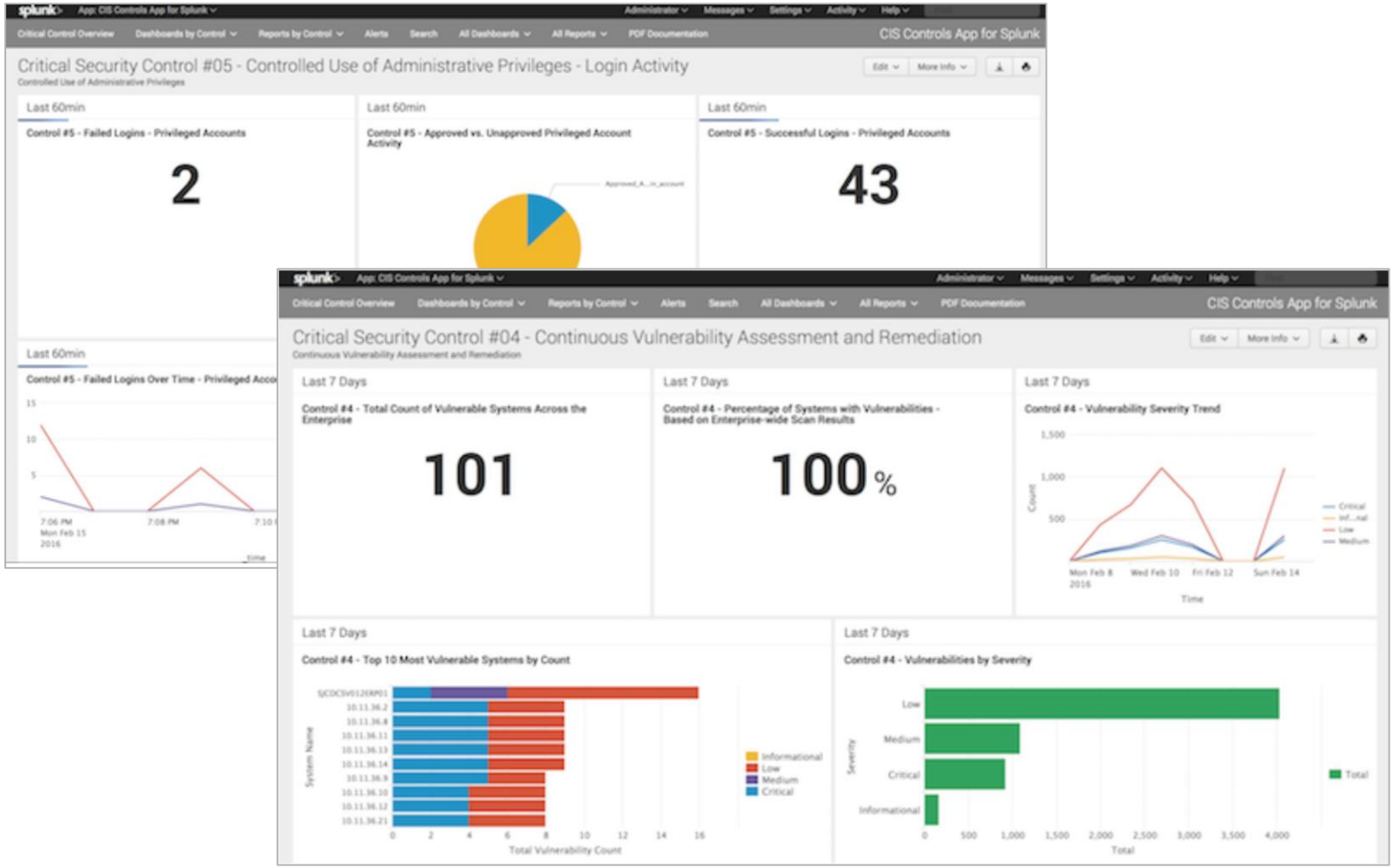
Implementing all 20 CIS Controls increases the risk reduction to around **94 percent**.

SOURCE: Center for Internet Security
https://www.cisecurity.org/critical-controls.cfm

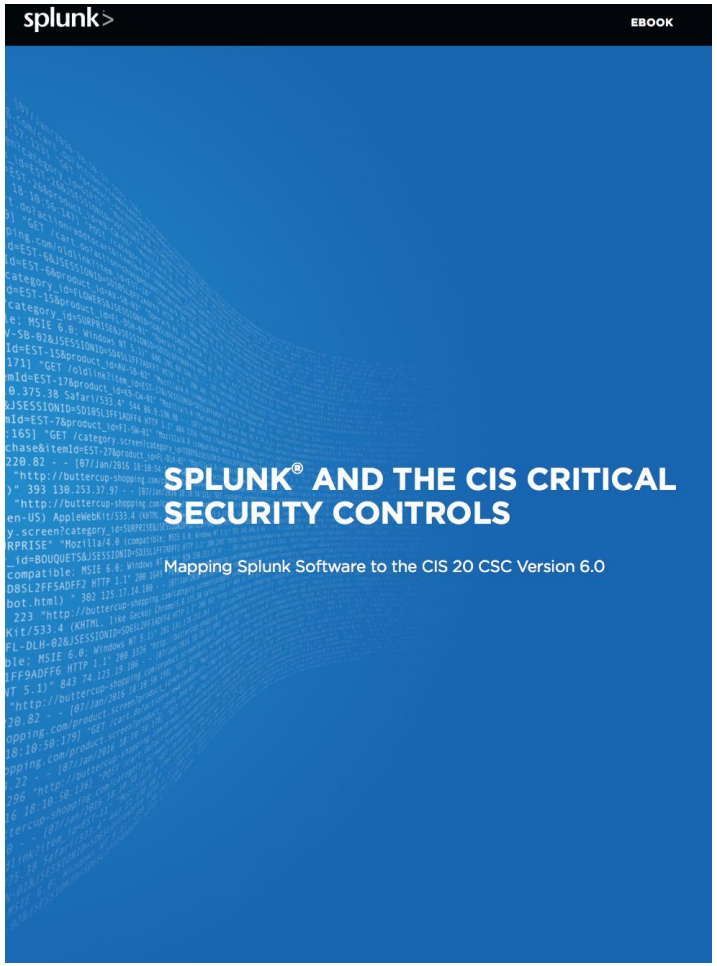


splunk>live!

CIS Critical Security Controls



https://splunkbase.splunk.com/app/3064/#/overview



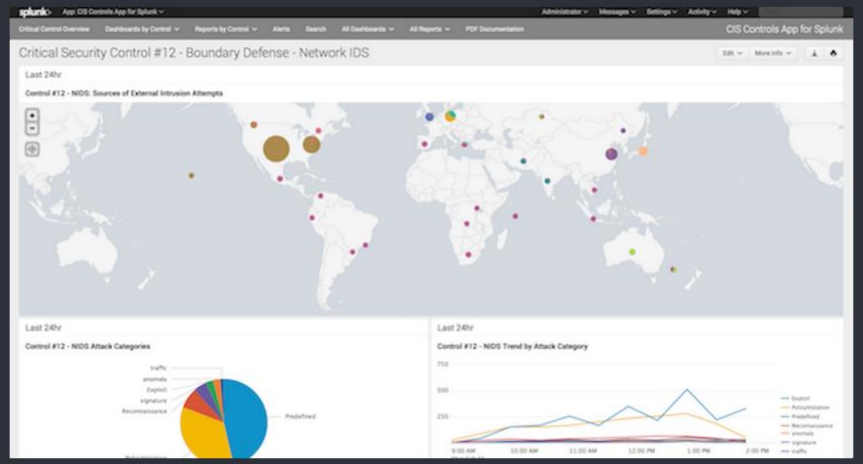
https://www.splunk.com/goto/Top20CSC

splunk>live!

Splunk Demo

CIS Critical Security Controls

3 reviews



ADMINISTRATOR TOOLS: View App | View Analytics

Overview | Details

The CIS Critical Security Controls app for Splunk was designed to provide a consolidated, easily-extensible framework for baseline security "best-practices" based on the Top 20 Critical Security Controls v6.1 published by the Center for Internet Security.

325 Installs

1,748 Downloads

Download

Rate this App

Release Notes

Strengthen Your Security Posture

1. Centralize Analysis
2. Streamline Investigations
3. Enforce Critical Controls

Analytics-Driven Security

Monitoring, Correlations, Alerts

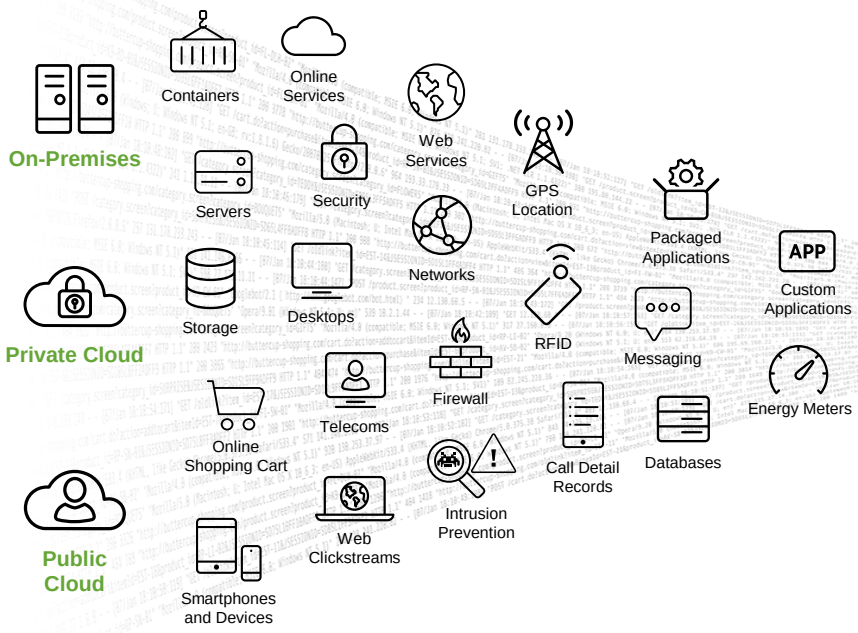
Search and Investigate

Dashboards and Reports

Analytics and Virtualization

Adaptive Response

Index Untapped Data: Any Source, Type, Volume



500+ Security Apps

Splunk Enterprise Security

Splunk User Behavior Analytics

splunk> Platform for Operational Intelligence

External Lookups

Asset and CMDB

Employee Info

Threat Intelligence

Applications

Data Stpres

splunk>live!

Analytics-Driven Security Platform and Apps

MONITOR REPORT	DETECT ALERT	ANALYZE INVESTIGATE	RESPONSE COLLABORATE
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

500+
Security Apps

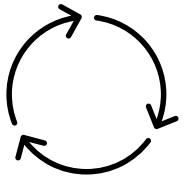
Splunk
Enterprise Security

Splunk User
Behavior Analytics

splunk> Platform for Operational Intelligence

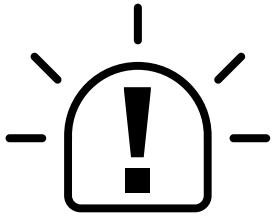
splunk>live!

Analytics- Driven Detection



Behavior Baselining & Modelling

Threat & Anomaly Detection



Unsupervised Machine Learning

500+
Security Apps

Splunk
Enterprise Security

Splunk User Behavior Analytics

splunk> **Platform for Operational Intelligence**

splunk>live!

Splunk Security Solutions

- INCIDENT INVESTIGATIONS AND FORENSICS
- SECURITY AND COMPLIANCE REPORTING
- REAL-TIME MONITORING OF KNOWN THREATS
- DETECT UNKNOWN THREATS
- FRAUD DETECTION
- INSIDER THREAT
- MORE ...

500+ Security Apps

PCI, NetFlow Logic, f5, Cisco, ForeScout, proofpoint

Splunk Enterprise Security

Splunk User Behavior Analytics

splunk> Platform for Operational Intelligence

splunk>live!

Splunk Quick Starts for Security Investigation

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 Security Intelligence.

Bundle Size	Splunk Enterprise License Size	Expert Guidance	Free Education	.conf Event Passes	Splunk Apps and Add-ons	Pricing
Small	20 GB/day	3 days	10 Credits	1	✔	Base pricing starts at $30,000 USD
Medium	50 GB/day	4 days	20 Credits	1	✔	Contact Sales
Large	100 GB/day	5 days	20 Credits	2	✔	Contact Sales

Infrastructure Quick Start Apps / Add-Ons

- Carbon Black — Free Download
- ForeScout — Free Download
- Cylance Protect — Free Download
- Tanium — Free Download
- Microsoft Sysmon TA — Free Download
- Ziften — Free Download
- Microsoft Windows TA — Free Download

Endpoint Quick Start Apps / Add-Ons

- Palo Alto Networks App for Splunk — Free Download
- Splunk Add-on for Bro IDS — Free Download
- Cisco Security Suite — Free Download
- FireEye App for Splunk Enterprise v3 — Free Download
- Fortinet FortiGate App for Splunk — Free Download
- Splunk Add-on for Blue Coat ProxySG — Free Download

splunk>live!

Analytics-Driven Security

Connecting Data and People

Risk-Based

Context and Intelligence

splunk>live!

Explore:

Dowload the CIS Critical Security Controls App

https://splunkbase.splunk.com/app/3064/

Join:

Our Community with Apps, Ask Questions or join a SplunkLive! event

https://www.splunk.com/en_us/community.html

Try:

Splunk Security Online Experience (No Download)

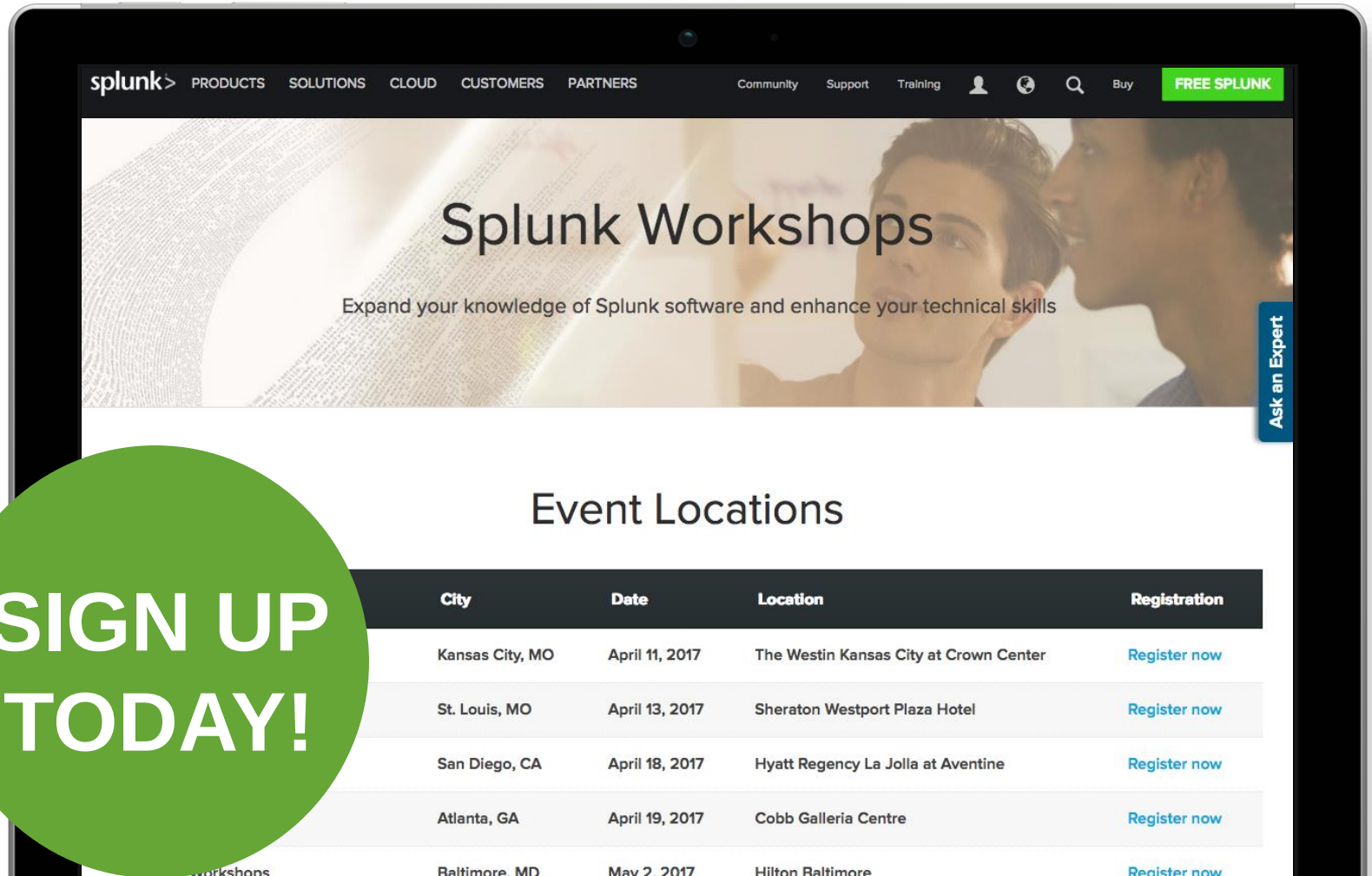
https://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud/security-investigation/getting-started.html

Q&A
Thank you

Workshops: Get Splunk Hands-on Experience

Attend a Splunk Workshop

splunk.com/workshops



SIGN UP TODAY!

June 14: Minneapolis

- **Venue:** Hyatt Regency Minneapolis
- **Time:** 8:30am
- Register Soon!
  - 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/slmn

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