splunk>live!

APRIL 13 | SAN FRANCISCO, CA

Build a Security Portfolio That Strengthens Your Security Posture

Jae Lee | Product Marketing Director

Young Cho | Technical Marketing Manager

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.

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

Strengthen Your Security Posture

Centralize Analysis

Streamline Investigations

Enforce Critical Controls

Central Analysis

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

4 Use Cases to Improve Your Posture

Threat Intelligence

Network

Endpoint

Access/Identity

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

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

Network Intelligence

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

- Detect intellectual property theft
- Detect insiders
- Compromised systems communicating internally
- Compromised endpoint

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

- Detect intellectual property theft
- Detect insiders
- Compromised systems communicating internally
- Compromised endpoint

Splunk Demo

Investigation

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

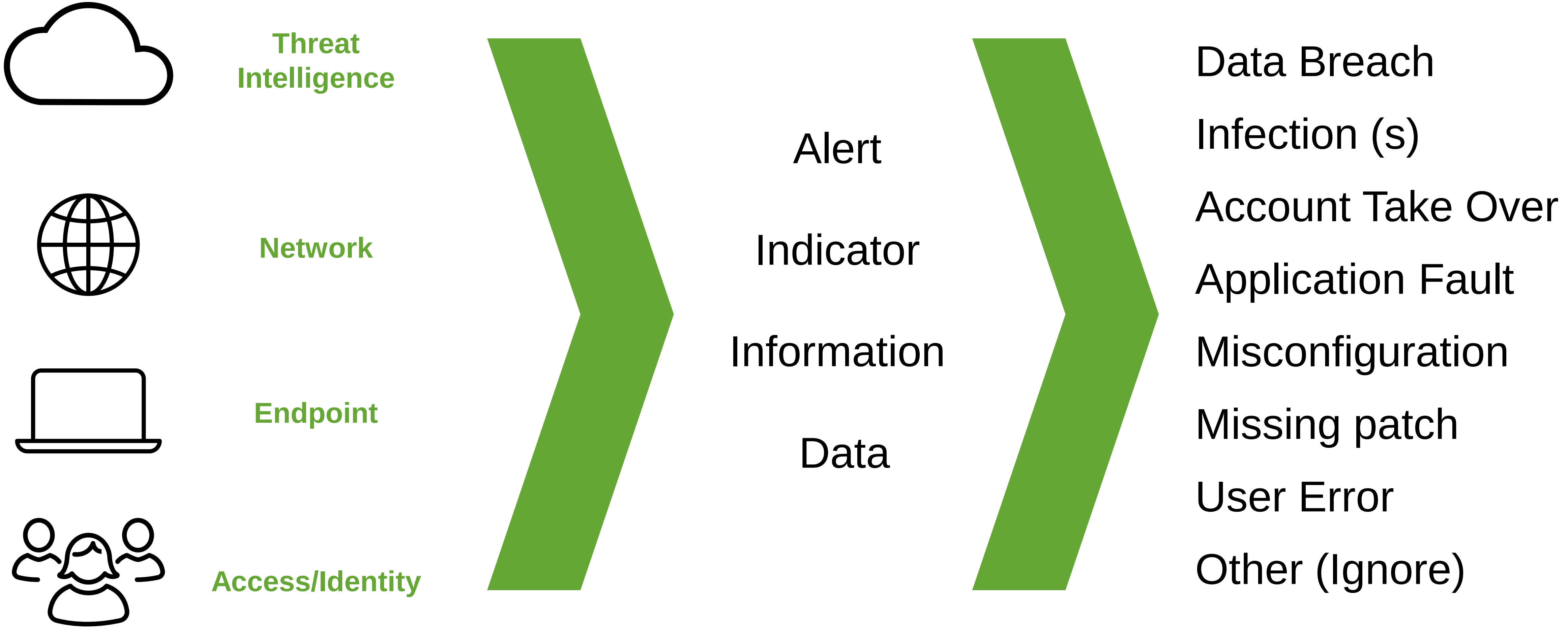
If you reduce to 5 min

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*

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)

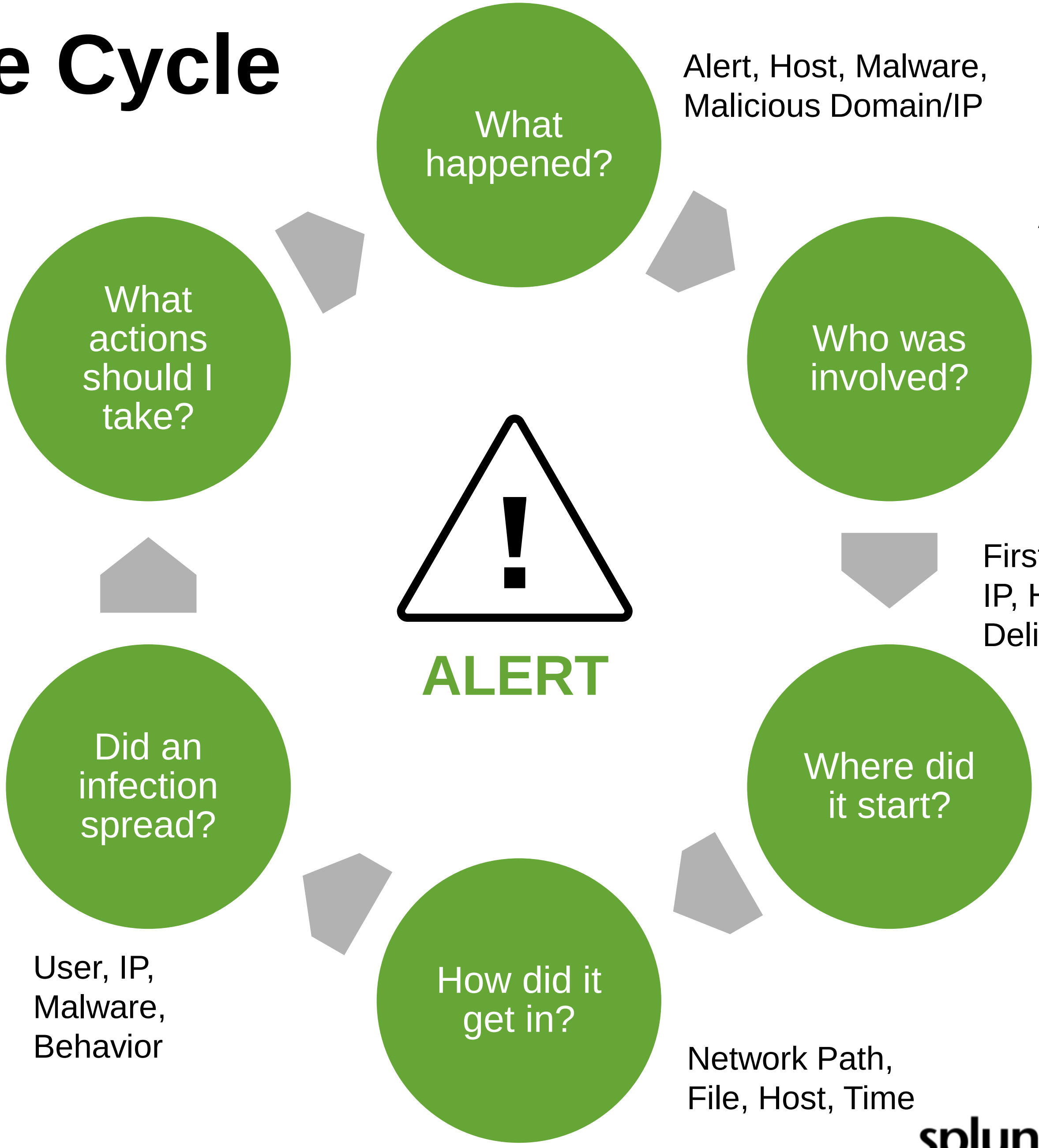
The Typical Investigative Cycle

Threat Intelligence

Network

Endpoint

Access/Identity



Alert, Host, Malware, Malicious Domain/IP

Access, Logs Login Activity, IP Mapping

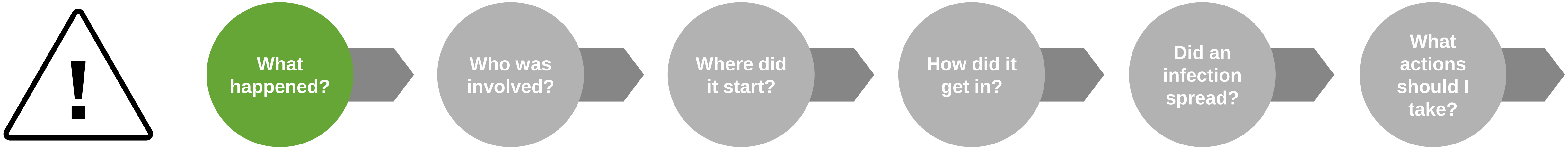
First seen, Alert, IP, Host, Malware Delivery

Network Path, File, Host, Time

User, IP, Malware, Behavior

Search All Attribute Over Time

The Investigation – Analytics Cycle



ALERT

What happened?

Who was involved?

Where did it start?

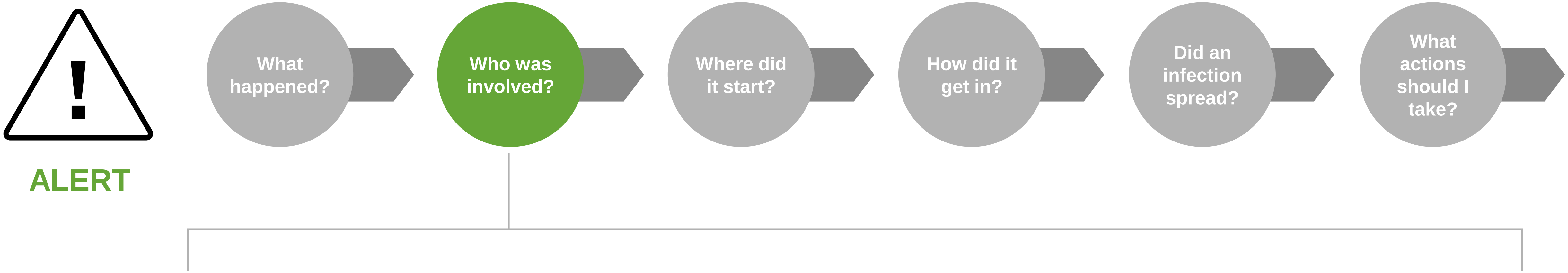
How did it get in?

Did an infection spread?

What actions should I take?

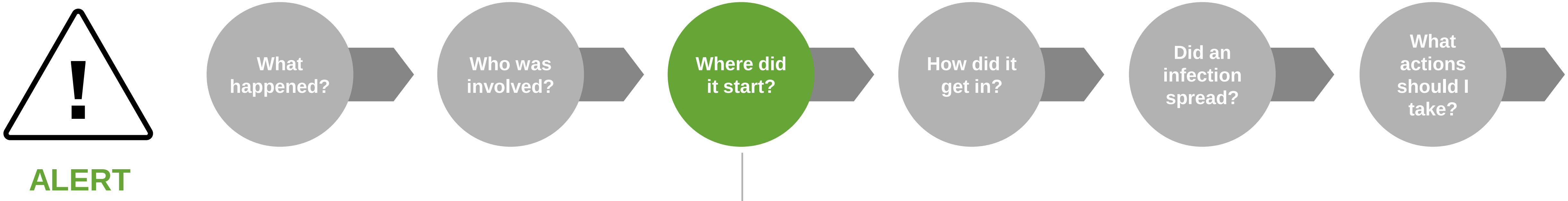
Question	Logic	Example	Data
Is the system actually compromised?	Index logs and search for matches against alert criteria	Verify malware detected alert on host against known file hash	**Endpoint logs** Authentication logs **Network logs** Threat intelligence

The Investigation – Analytics Cycle



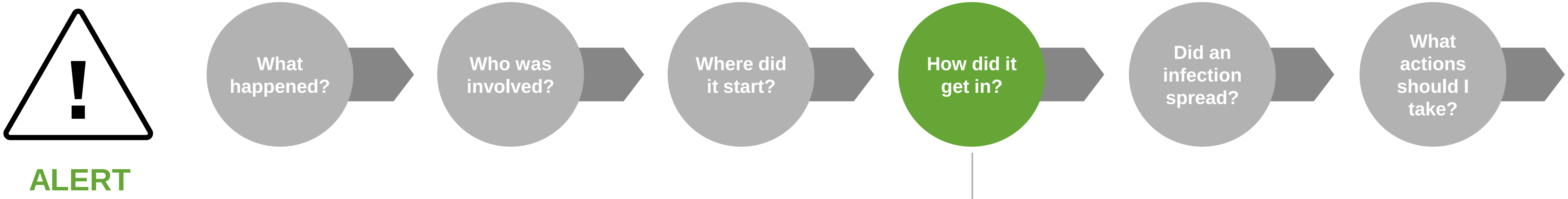
Question	Logic	Example	Data
What accounts / users are associated with that system?	Determine IP to asset to identity mapping	Jane Doe IP = 10.10.200.20 Workstation running Win10	Identity system DNS log Authentication logs Asset repository

The Investigation – Analytics Cycle



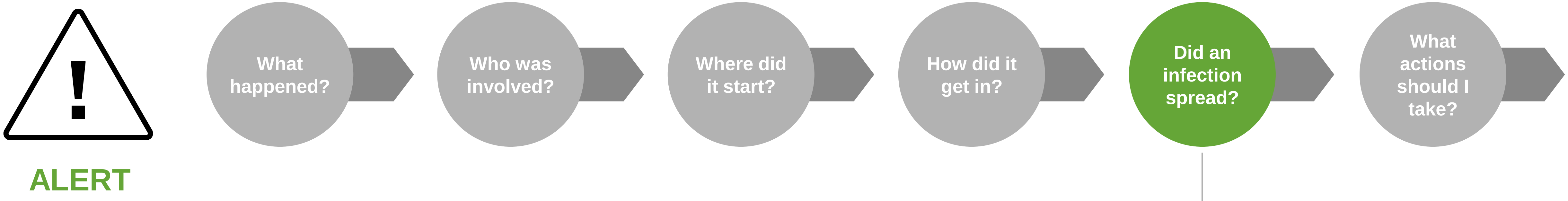
Question	Logic	Example	Data
Timeline of activities leading up to and during the alert?	Integrate your asset system	Resolve the location via reverse geo IP lookup	All Available Data

The Investigation – Analytics Cycle



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

The Investigation – Analytics Cycle



ALERT

What happened?

Who was involved?

Where did it start?

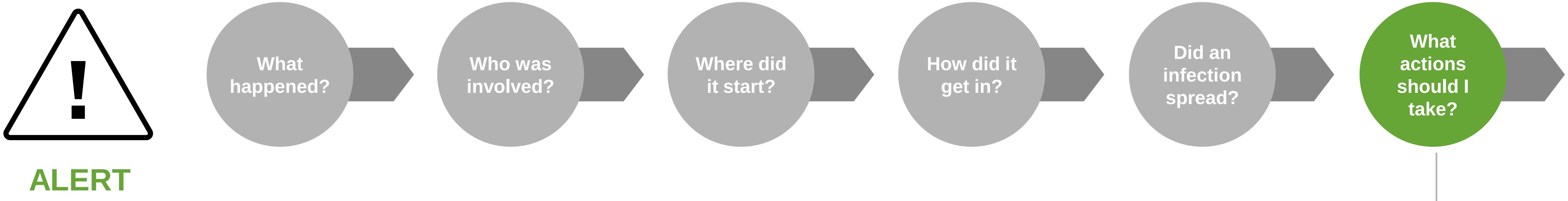
How did it get in?

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

The Investigation – Analytics Cycle

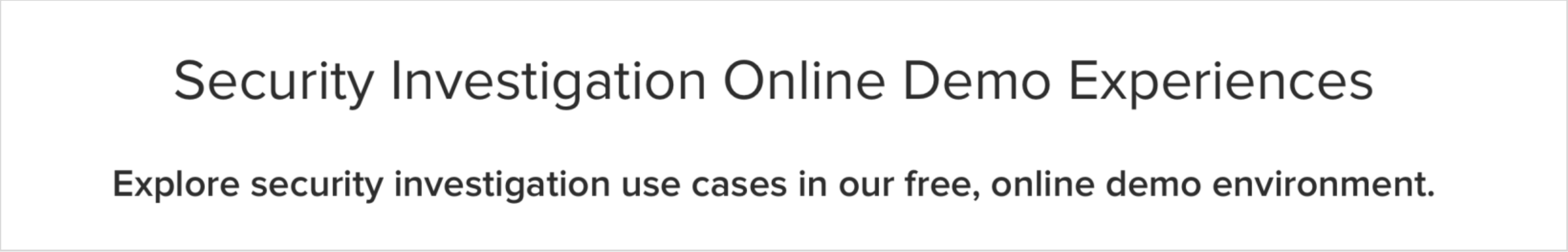


Question	Logic	Example	Data
Is there any indication the attacker has gained access to the environment?	Identify any C&C Identify lateral movement	Beaconing to known bad IP in remote geo – add to dynamic address group on FW	Threat intelligence Subscriptions Network / FW / Proxy DNS Wire data

splunk>live!

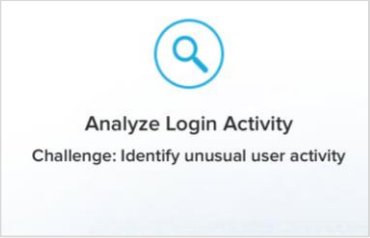
Splunk Demo

Try It Yourself



Security Investigation Online Demo Experiences

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



Analyze Login Activity

Challenge: Identify unusual user activity

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

Analyze Endpoint Activity

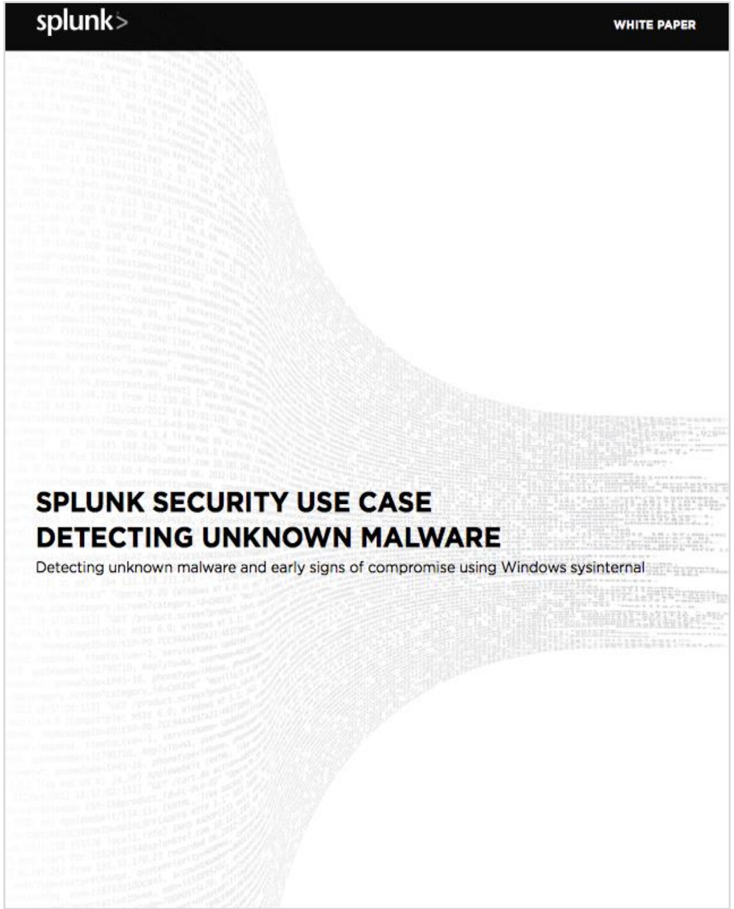
Challenge: Identify the root cause of the infection

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

Analyze Network Events

Challenge: Identify how an attacker entered your network

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



splunk> WHITE PAPER

SPLUNK SECURITY USE CASE
DETECTING UNKNOWN MALWARE

Detecting unknown malware and early signs of compromise using Windows sysinternal

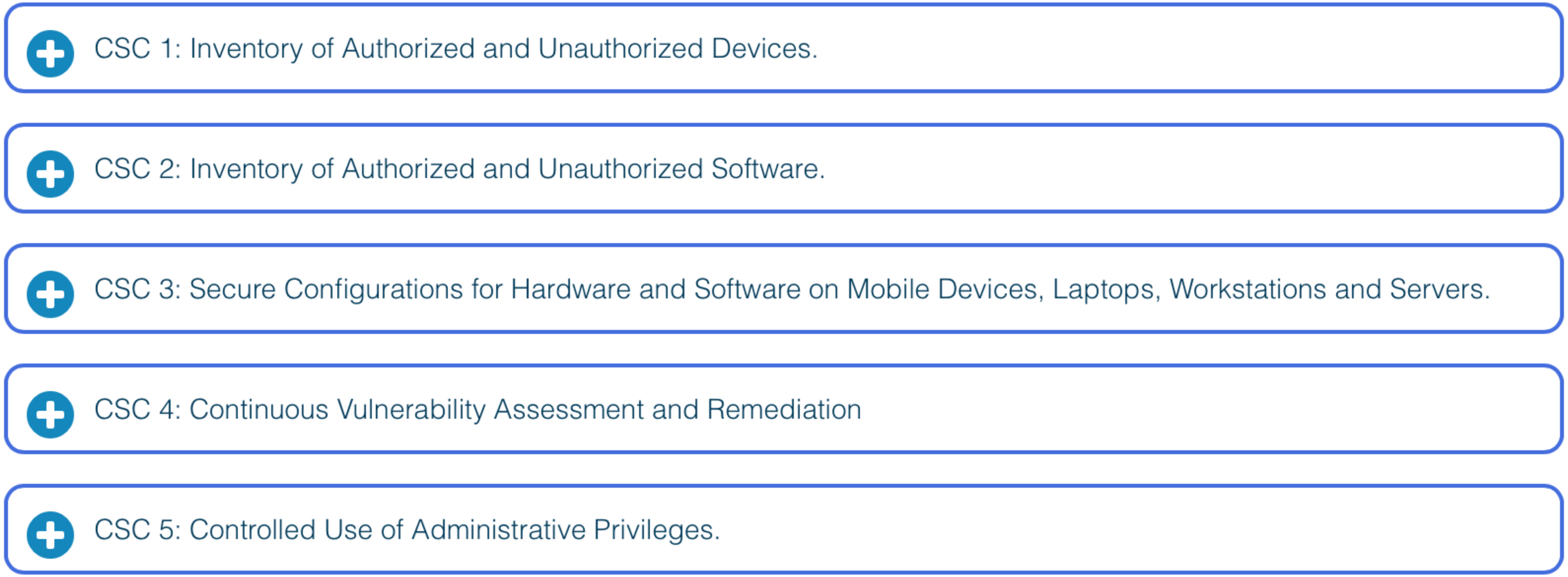
splunk>live!

Security Readiness

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

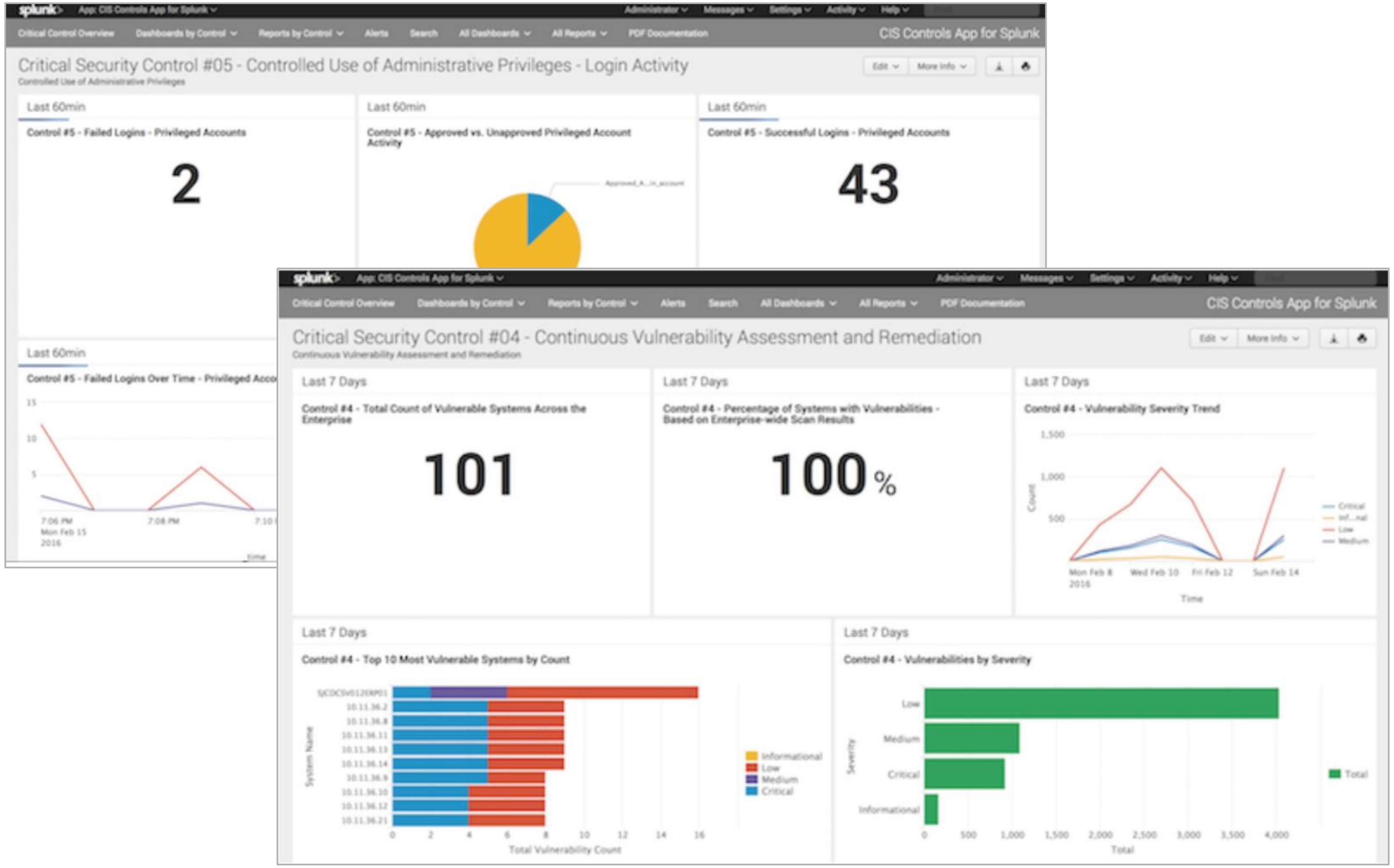
CSC 5: Controlled Use of Administrative Privileges.

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

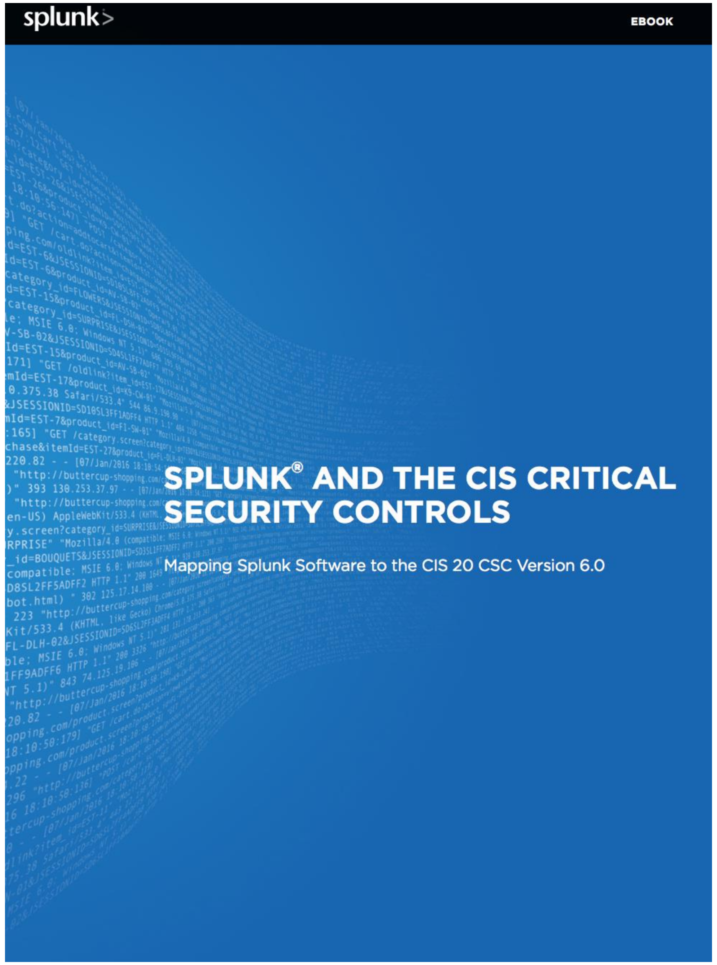
Implementing all 20 CIS Controls increases the risk reduction to around **94 percent**.

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

CIS Critical Security Controls


CIS Controls App for Splunk
Critical Security Control #05 - Controlled Use of Administrative Privileges - Login Activity
Last 60min
Control #5 - Failed Logins - Privileged Accounts
2
Control #5 - Approved vs. Unapproved Privileged Account Activity
Control #5 - Successful Logins - Privileged Accounts
43
Control #5 - Failed Logins Over Time - Privileged Accounts
Critical Security Control #04 - Continuous Vulnerability Assessment and Remediation
Last 7 Days
Control #4 - Total Count of Vulnerable Systems Across the Enterprise
101
Control #4 - Percentage of Systems with Vulnerabilities - Based on Enterprise-wide Scan Results
100%
Control #4 - Vulnerability Severity Trend
Control #4 - Top 10 Most Vulnerable Systems by Count
Total Vulnerability Count
Informational
Low
Medium
Critical
Control #4 - Vulnerabilities by Severity
Total

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



splunk> EBOOK

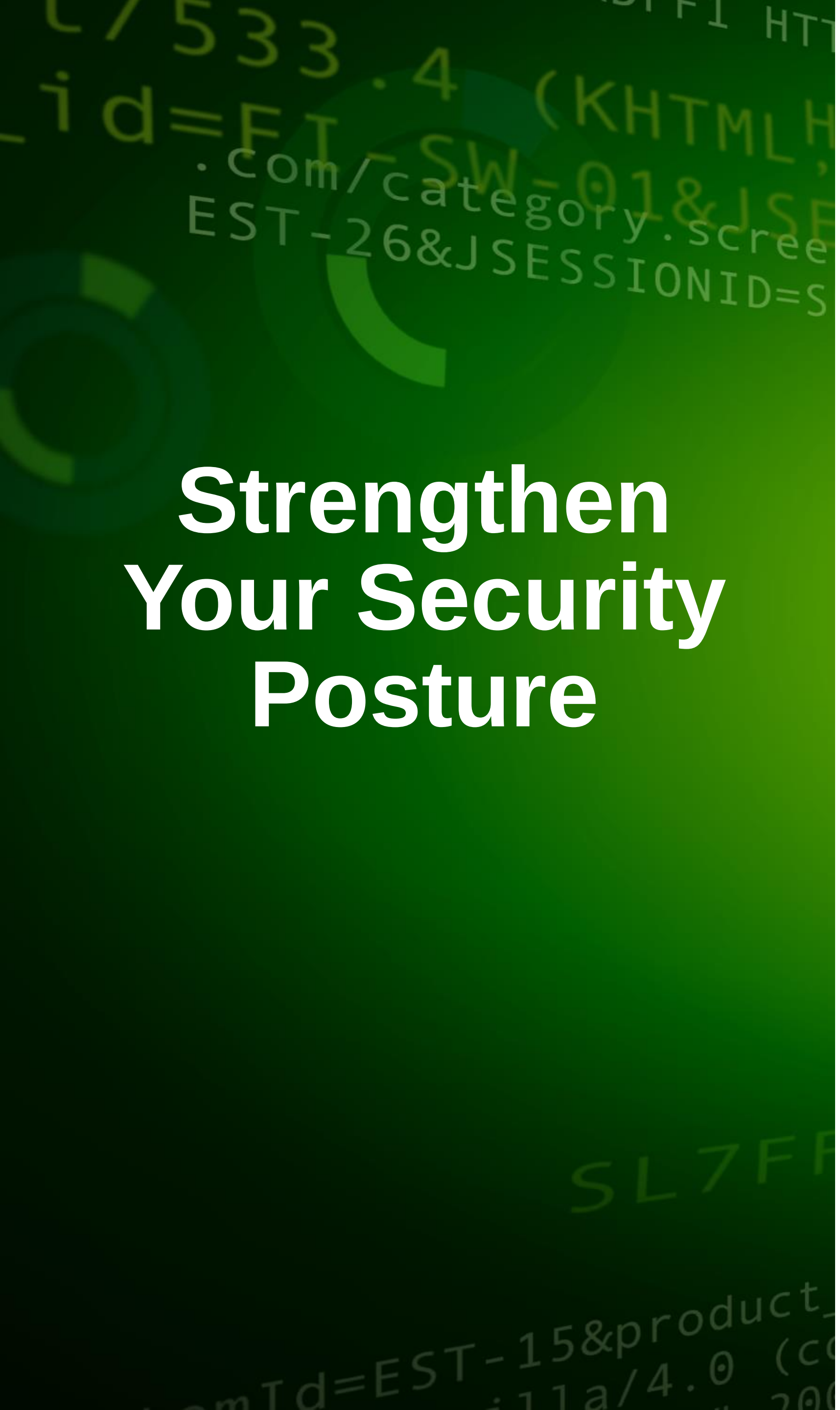
SPLUNK® AND THE CIS CRITICAL SECURITY CONTROLS

Mapping Splunk Software to the CIS 20 CSC Version 6.0

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

splunk>live!

Splunk Demo



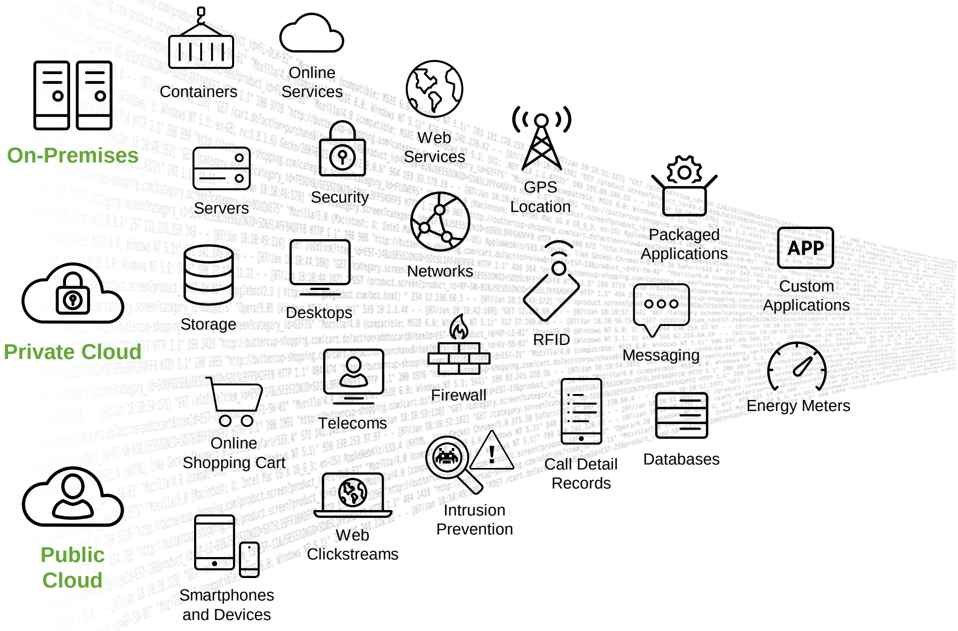
Strengthen Your Security Posture

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

Pre-defined views and rules

DETECT
ALERT

Correlation rules, thresholds

ANALYZE
INVESTIGATE

Analysis investigation & context enrichment

RESPONSE
COLLABORATE

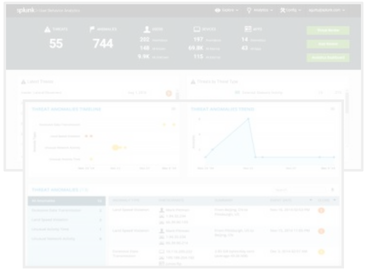
Enterprise-wide coordination & response

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

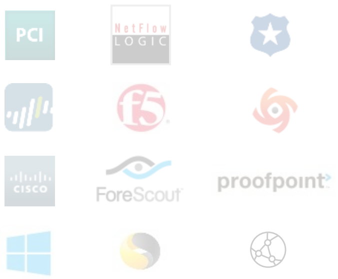
Analytics- Driven Detection

Behavior Baselining & Modelling

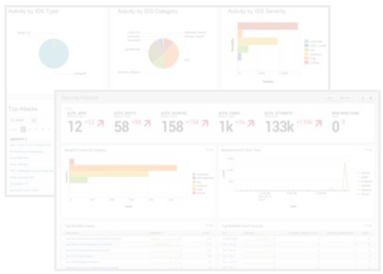
Threat & Anomaly Detection

Unsupervised Machine Learning

500+
Security Apps



Splunk
Enterprise Security



Splunk User
Behavior Analytics

splunk> Platform for Operational Intelligence

Splunk 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
cisco
ForeScout
proofpoint

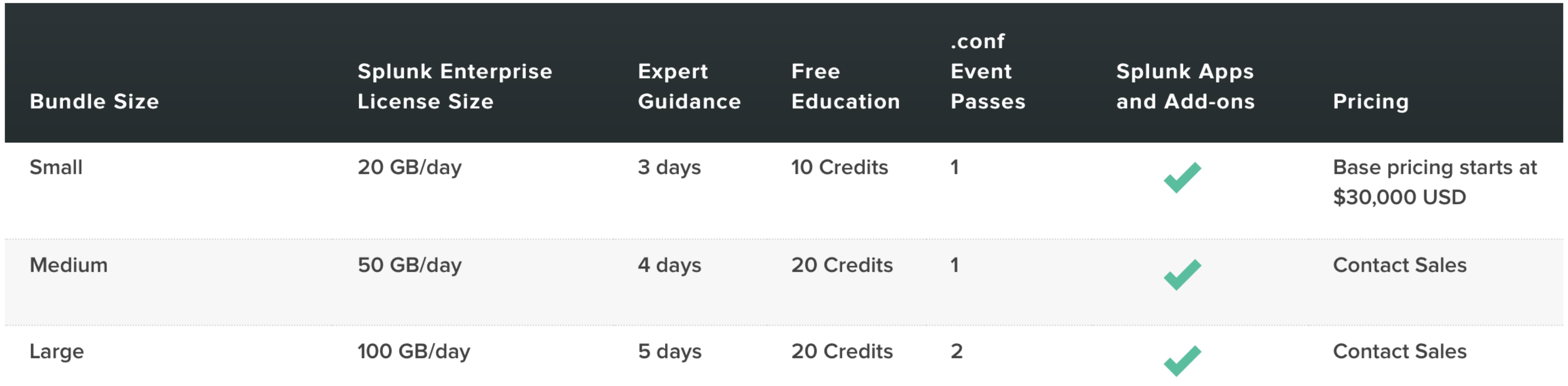
Splunk Enterprise Security

Splunk User Behavior Analytics

splunk> Platform for Operational Intelligence

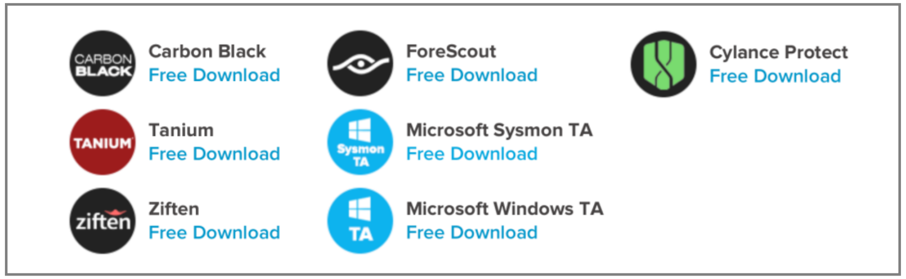
Splunk Quick Starts for Security Investigation

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

Tanium
Free Download

Ziften
Free Download

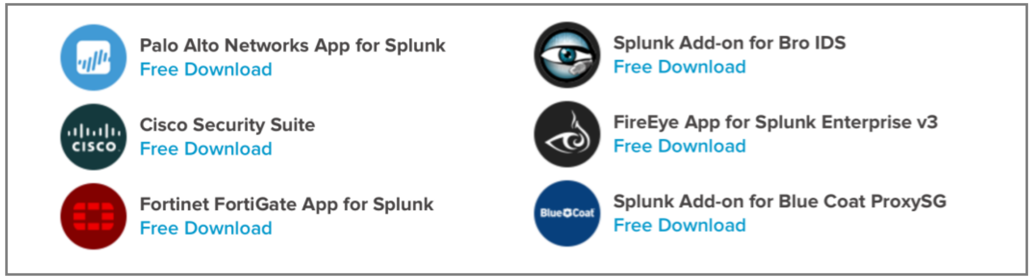
ForeScout
Free Download

Microsoft Sysmon TA
Free Download

Microsoft Windows TA
Free Download

Cylance Protect
Free Download

Endpoint Quick Start Apps / Add-Ons



Palo Alto Networks App for Splunk
Free Download

Cisco Security Suite
Free Download

Fortinet FortiGate App for Splunk
Free Download

Splunk Add-on for Bro IDS
Free Download

FireEye App for Splunk Enterprise v3
Free Download

Splunk Add-on for Blue Coat ProxySG
Free Download

Analytics-Driven Security

Connecting Data and People

Risk-Based

Context and Intelligence

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)

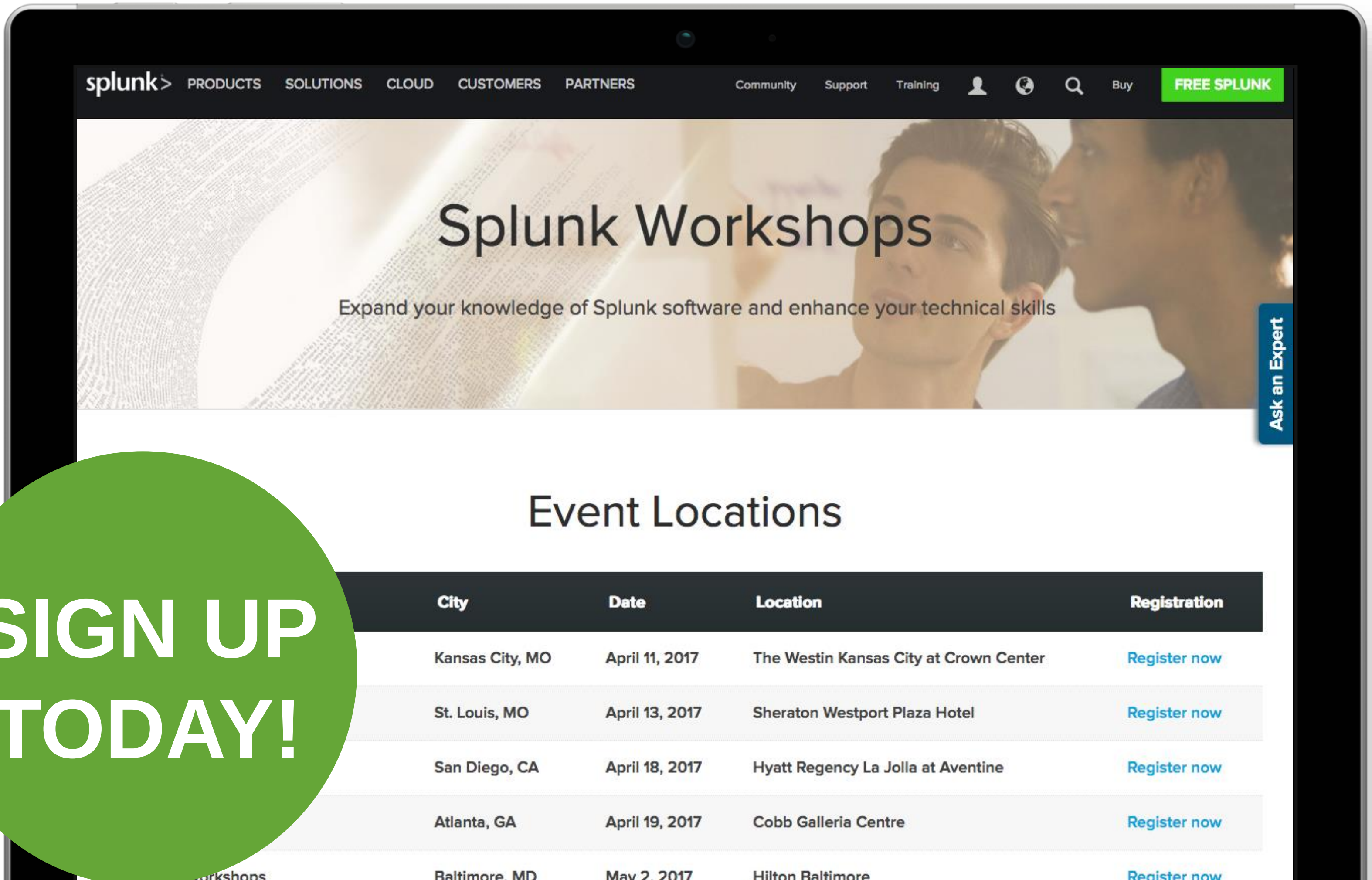
https://www.splunk.com/en_us/solutions/solution-areas/security-and-fraud/security-investigation/getting-started.html

Q&A
Thank you

Workshops: Get Splunk Hands-on Experience

Attend a Splunk Workshop

splunk.com/workshops



Splunk Workshops

Expand your knowledge of Splunk software and enhance your technical skills

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
orkshops	Baltimore, MD	May 2, 2017	Hilton Baltimore	Register now

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/sldc

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

THANK YOU