Make Your SOC Rock

Wissam Ali-Ahmad | Lead Solutions Architect

Meera Shankar | Global Strategic Alliance Manager

October 2018

Forward-Looking Statements

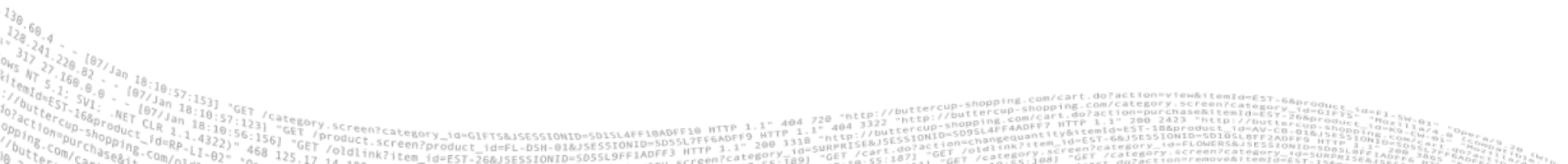
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results 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> listen to your data®

Agenda

- The holes in our SOCs today
- Nerve Center 1.0
- Towards a modern Security Operations Center
- SOAR to new heights with our Security Ecosystem
- Introducing the Adaptive Operations Framework



Frustrated with Your SOC ?

EVOLVING THREATS

$3 Trillion

Expected global cost of cybercrime by 2021

LACK OF VISIBILITY

70+

Security tools to manage

SKILL SHORTAGE

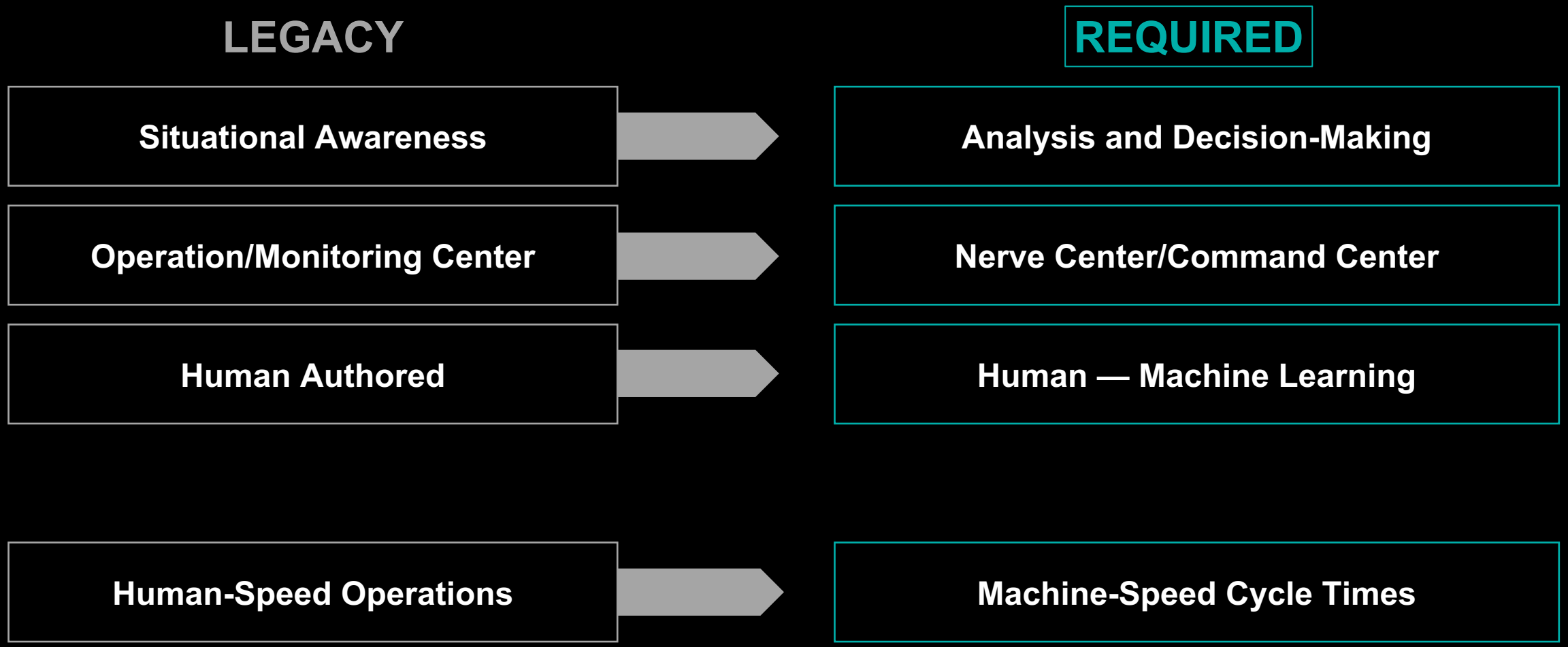
3.5 Million

Unfilled cybersecurity jobs by 2021

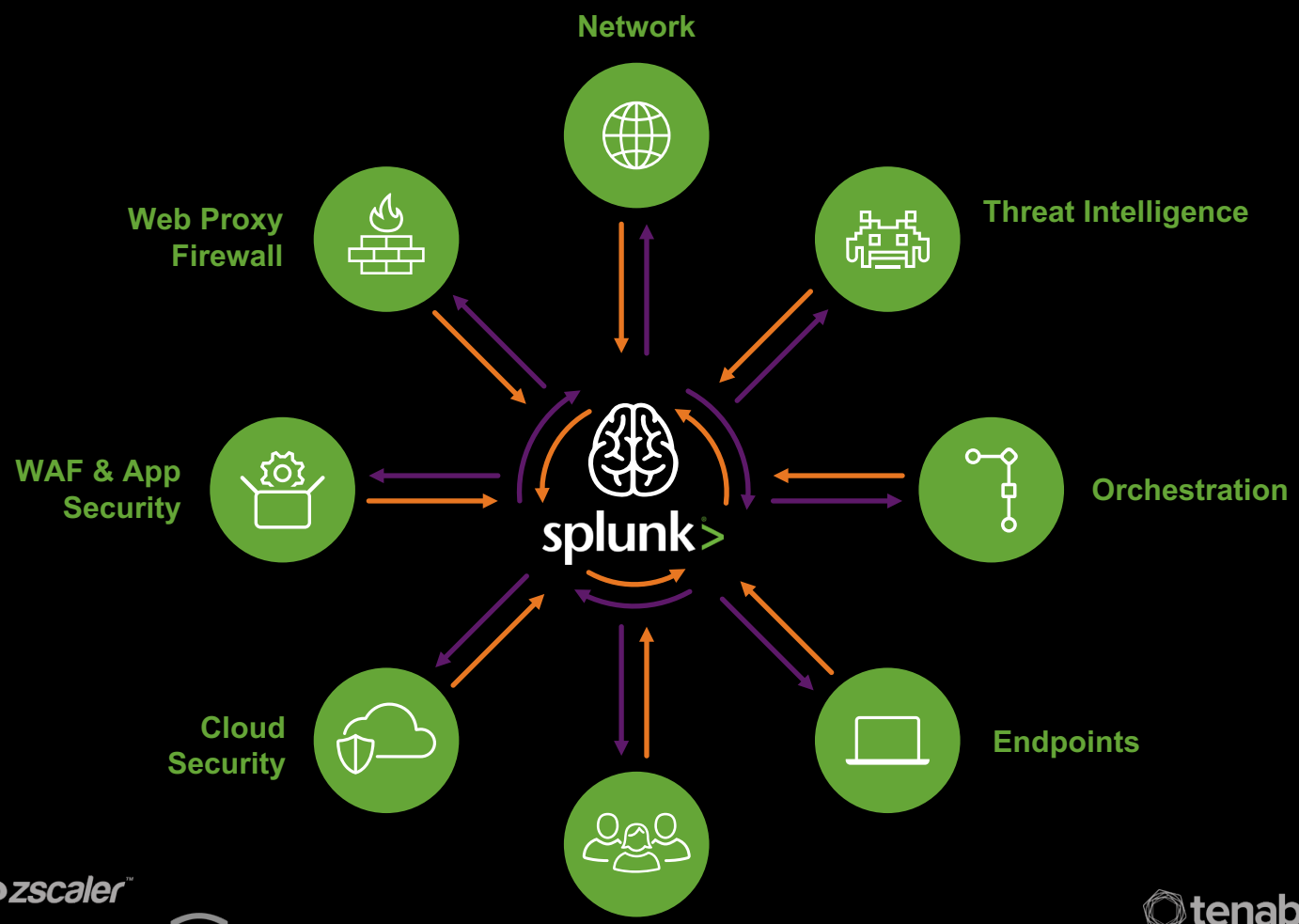
75% YOY increases

splunk> .conf18

Towards the Next Gen SOC



Nerve Center 1.0



paloalto NETWORKS
Booz | Allen | Hamilton
ATLASSIAN
VALIMAIL
illumio
AWAKE
Corvil
TANIUM
DEMISTO
Symantec
COFENSE
CYBERSPONSE ADAPTIVE SECURITY
FORTINET
VMRAY
SailPoint
REDSEAL
INTERNET STORM CENTER
RESOLVE SYSTEMS
datophy
resilient an IBM Company
ziften
zscaler
amazon web services
ForeScout
Recorded Future
QUALYS

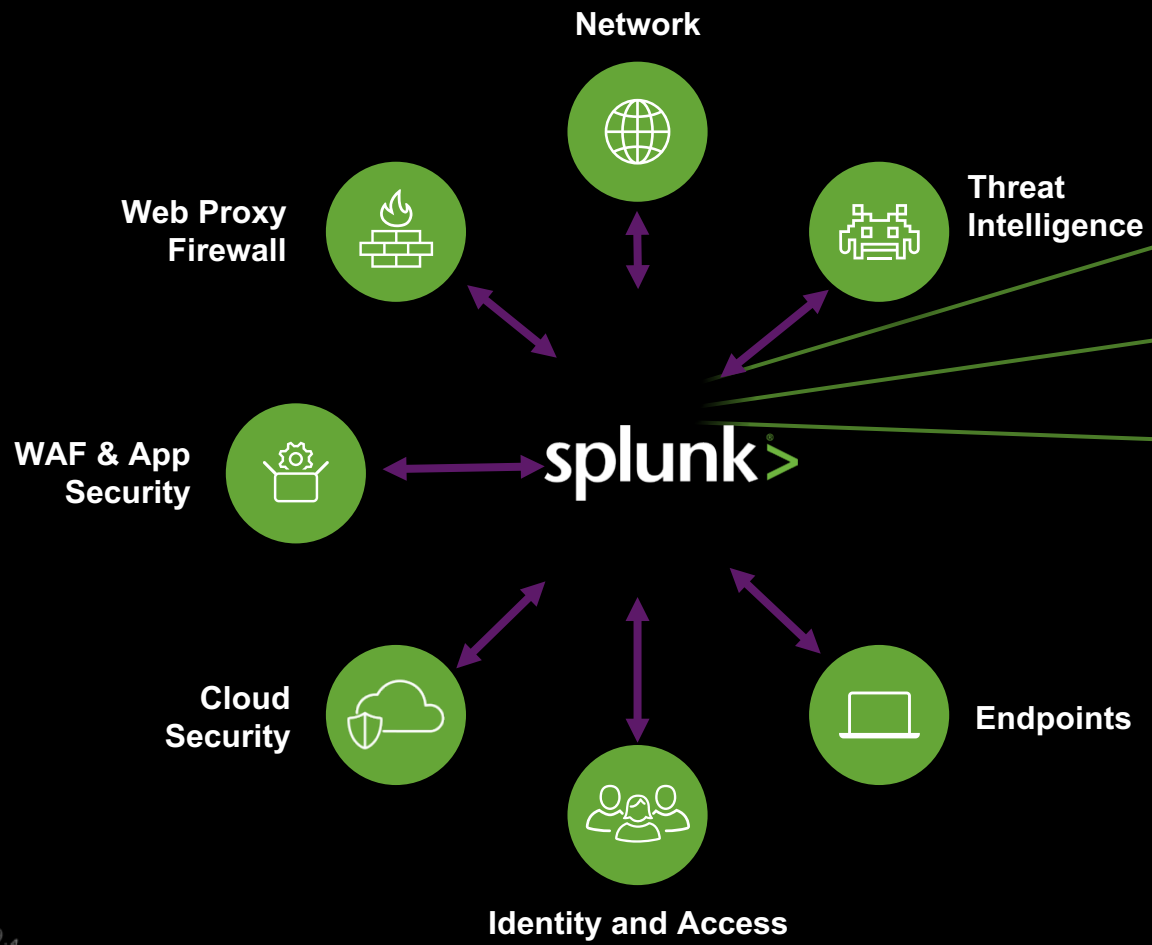
DomainTools
Cisco Umbrella
SWIMLANE
CYLANCE
Signal Sciences
CYBERARK
THREATCONNECT
LogicHub
ANOMALI
netskope
CROWDSTRIKE
Pinn AuthX
cisco
SHODAN
CARBON BLACK
SYNCURITY
Phantom
okta
ACALVIO
TCELL
SentinelOne
Gigamon
tenable
algosec
proofpoint
graphistry
accenture
Cisco Cloudlock

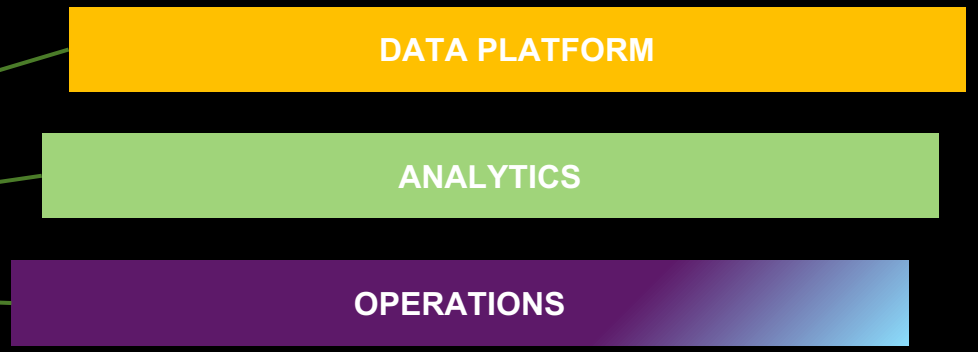
You Spin My Head Right Round…

splunk> .conf18

Toward a Modern SOC

SOAR Accelerates Splunk's Nerve Center security vision





splunk>phantom

- **Advance cyber defense** and reduce risk using an analytics-driven approach
- **Respond faster** by accelerating incident response
- **Work smarter** and reduce staffing and skills challenges

SOAR With Splunk & Phantom

Security Operations Challenges

- INEFFICIENT & INCONSISTENT PROCESS
- STAFFING CHALLENGES
- INCREASING EXPOSURE

Outcomes with Phantom

- EFFICIENCY
- REPEATABLE & AUDITABLE
- DECREASING DWELL TIMES

BEFORE PHANTOM
SITUATION

- Limited & stretched resources
- Complex infrastructure with wide range of technologies from multiple security vendors
- Alert fatigue
- Expanding/changing attack surface

AFTER PHANTOM
SITUATION

- Resources can focus on strategic security activities
- Faster investigations across complex infrastructure
- Increase SecOps process and team efficiency
- Reduce the attack surface risk through automation

Blackstone

- Reduced alert investigation times from **30-45 minutes** to less than **one minute**
- Applied a consistent approach to alert management and investigation, eliminating human error
- Increased resource efficiency by turning manual, repetitive tasks into automated processes

Ecosystem Content Drives the Nerve Center

Splunk Apps and Add-ons

Security integrations using Splunk Core

Phantom and AR integrations

3rd party APIs/Integrations using either ES or Phantom

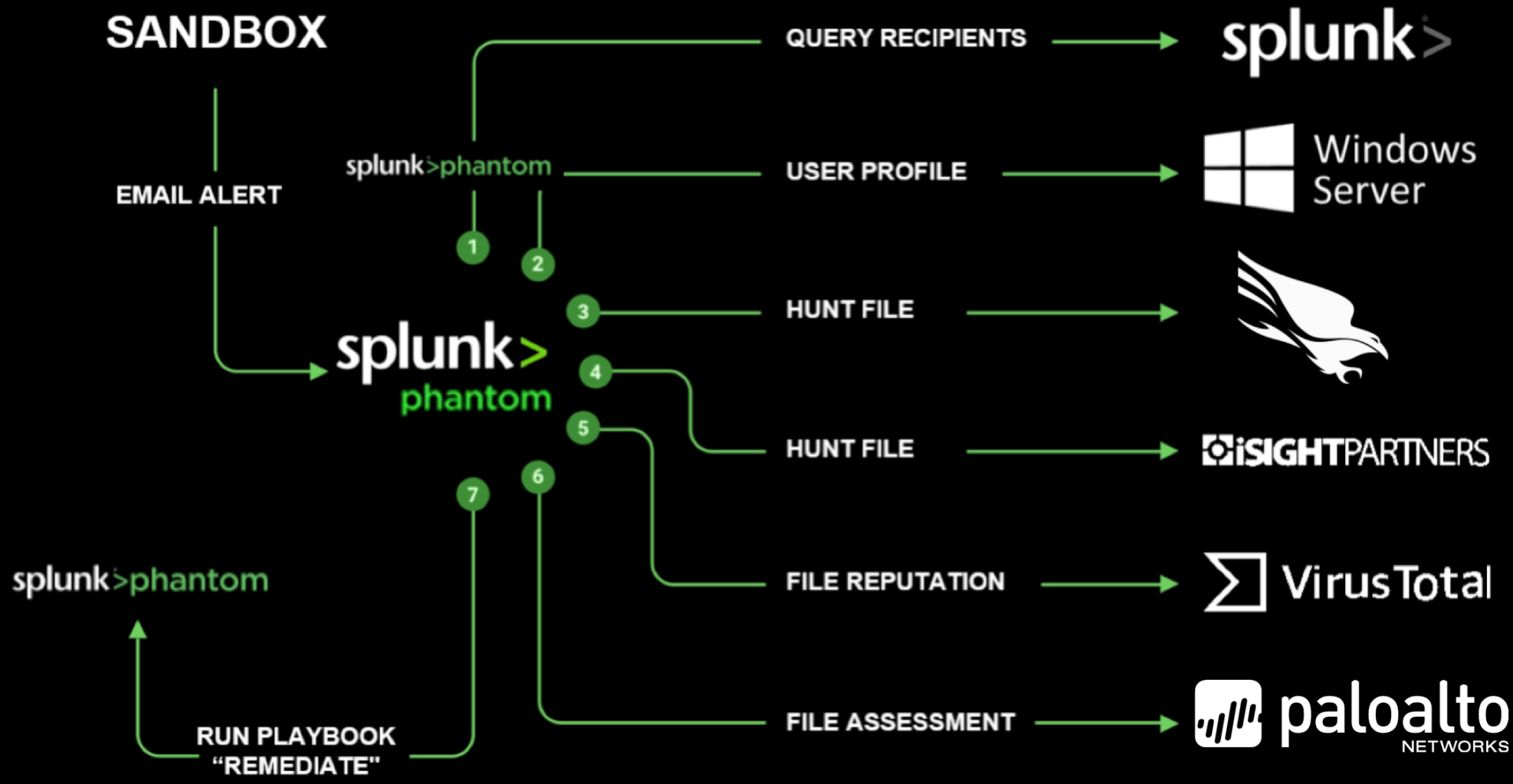
Analytic Stories (ES Content Update)

Correlation searches and AR actions for Threat Detection & Response

Phantom Playbooks

Advanced automation/orchestration with 3rd party applications

Ecosystem Actions Drive Orchestration



Adaptive Operations Framework

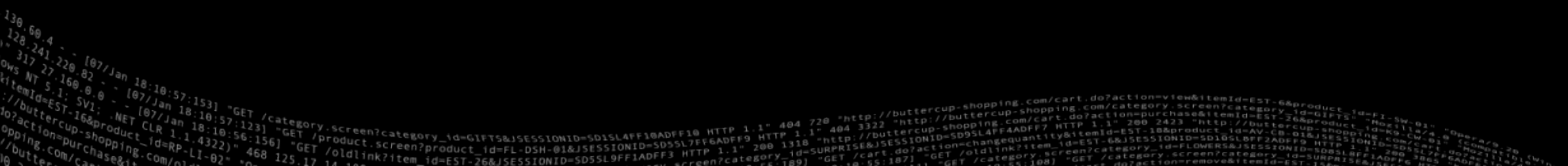
Open ecosystem of security vendors committed to improving cyber defense and security operations.

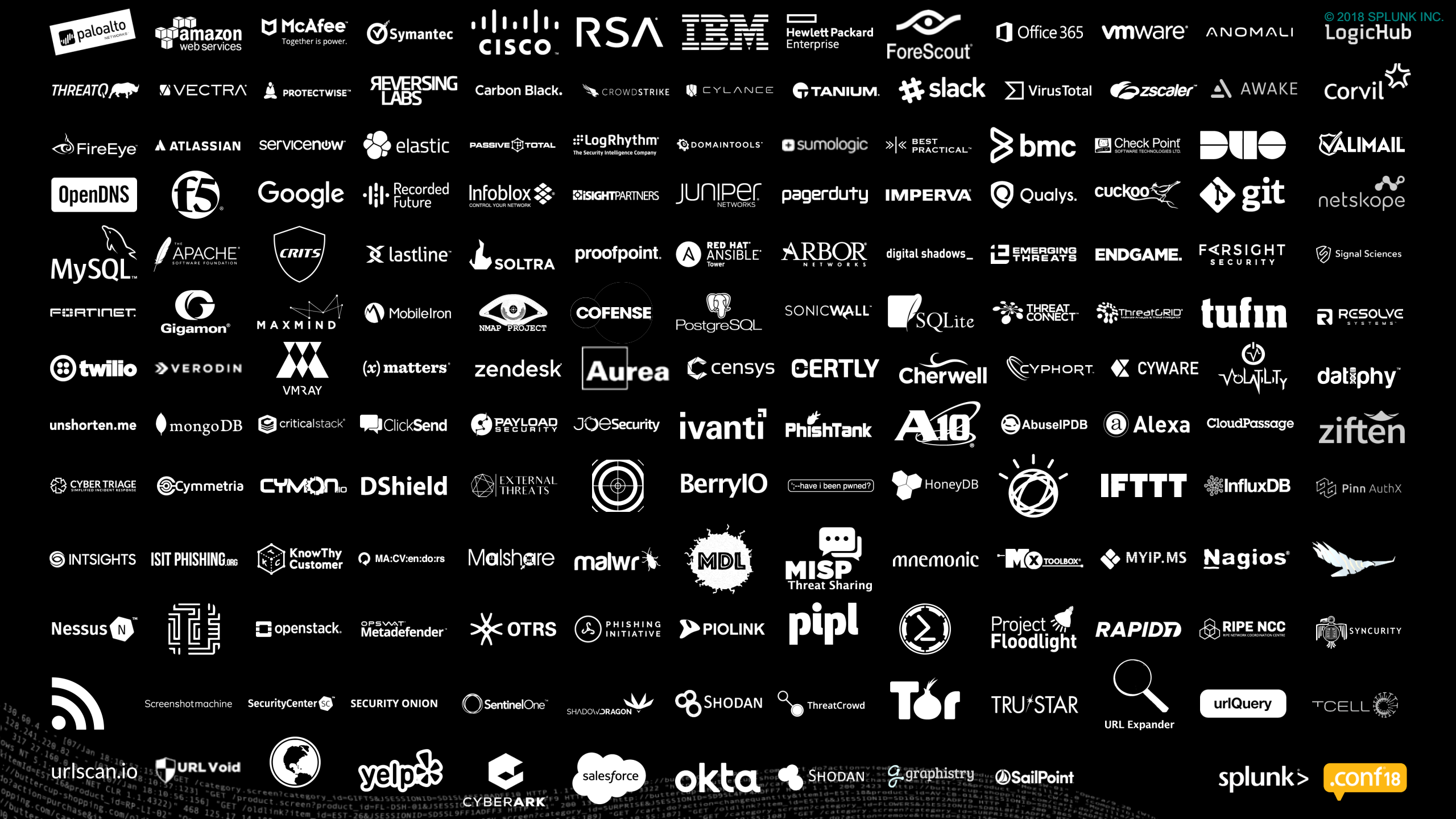
Splunk Adaptive Operations Framework

Largest Community of Innovative Security Vendors

Improve Cyber Defense

Streamline Security Operations



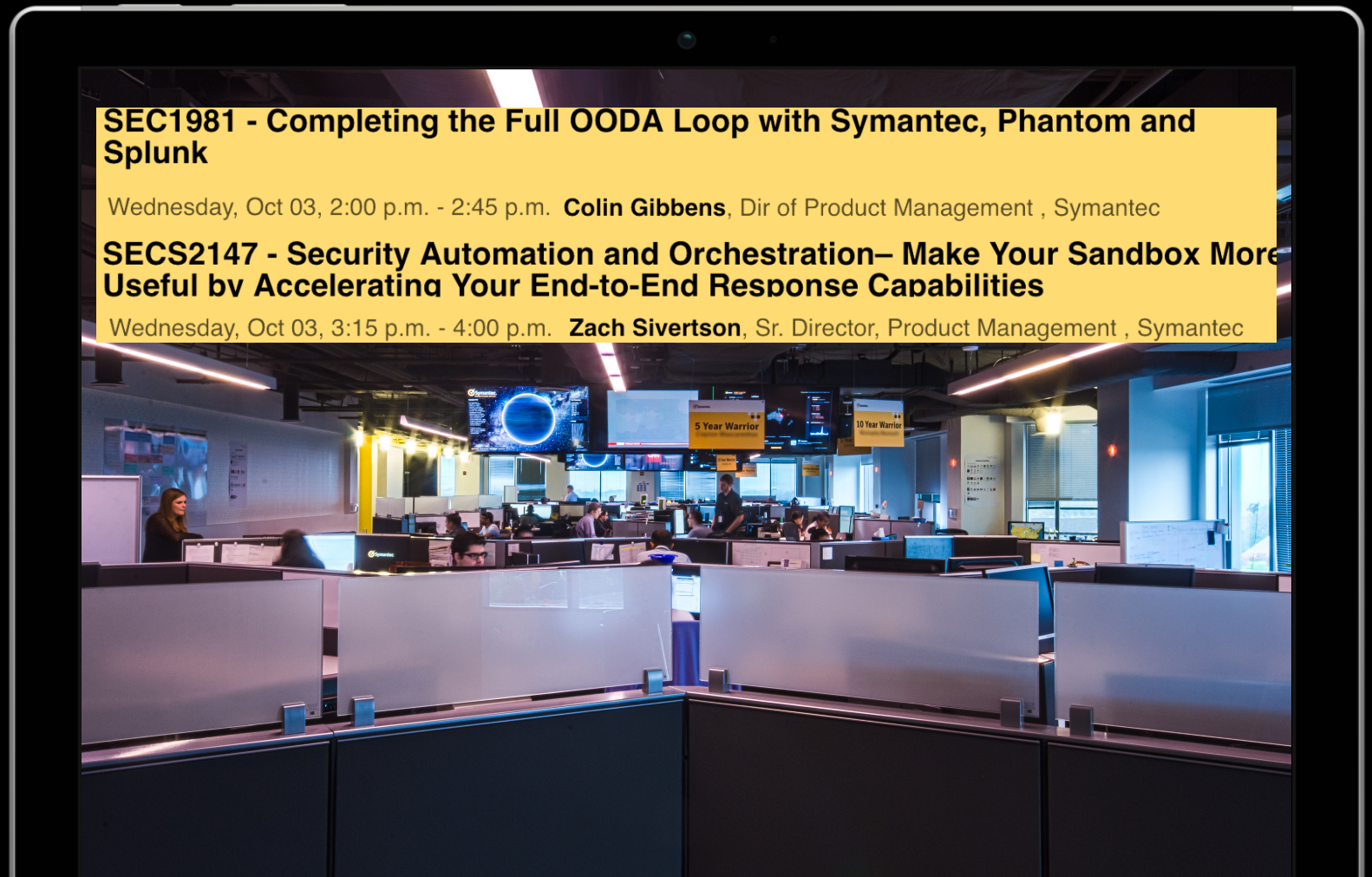

© 2018 SPLUNK INC.
paloalto NETWORKS
amazon web services
McAfee Together is power.
Symantec
cisco
RSA
IBM
Hewlett Packard Enterprise
ForeScout
Office 365
vmware
ANOMALI
LogicHub
THREATQ
VECTRA
PROTECTWISE
REVERSING LABS
Carbon Black.
CROWDSTRIKE
CYLANCE
TANIUM
slack
VirusTotal
zscaler
AWAKE
Corvil
FireEye
ATLASSIAN
servicenow
elastic
PASSIVE TOTAL
LogRhythm The Security Intelligence Company
DOMAINTOOLS
sumologic
BEST PRACTICAL
bmc
Check Point SOFTWARE TECHNOLOGIES LTD.
DUO
VALIMAIL
OpenDNS
f5
Google
Recorded Future
Infoblox CONTROL YOUR NETWORK
iSIGHTPARTNERS
JUNIPER NETWORKS
pagerduty
IMPERVA
Qualys.
cuckoo
git
netskope
MySQL
THE APACHE SOFTWARE FOUNDATION
CRITS
lastline
SOLTRA
proofpoint.
RED HAT ANSIBLE Tower
ARBOR NETWORKS
digital shadows_
EMERGING THREATS
ENDGAME.
FARSIGHT SECURITY
Signal Sciences
FORTINET
Gigamon
MAXMIND
MobileIron
NMAP PROJECT
COFENSE
PostgreSQL
SONICWALL
SQLite
THREAT CONNECT
ThreatGRID
tufin
RESOLVE SYSTEMS
twilio
VERODIN
VMRAY
(x) matters
zendesk
Aurea
censys
CERTLY
Cherwell
CYPHORT
CYWARE
VOLATILITY
datto
unshorten.me
mongoDB
criticalstack
ClickSend
PAYLOAD SECURITY
JOESecurity
ivanti
PhishTank
A10
AbuseIPDB
Alexa
CloudPassage
ziften
CYBER TRIAGE SIMPLIFIED INCIDENT RESPONSE
Cymmetria
CYMON.IO
DShield
EXTERNAL THREATS
BerryIO
';--have i been pwned?
HoneyDB
IFTTT
InfluxDB
Pinn AuthX
INTSIGHTS
ISIT PHISHING.ORG
KnowThy Customer
MA:CV:en:do:rs
Malshare
malwr
MDL
MISP Threat Sharing
mnemonic
MX TOOLBOX
MYIP.MS
Nagios
Nessus
openstack.
OPSWAT Metadefender
OTRS
PHISHING INITIATIVE
PIOLINK
pipl
Project Floodlight
RAPID7
RIPE NCC
SYNCURITY
Screenshotmachine
SecurityCenter SC
SECURITY ONION
SentinelOne
SHADOWDRAGON
SHODAN
ThreatCrowd
Tor
TRUSTAR
URL Expander
urlQuery
TCELL
urlscan.io
URLVoid
yelp
CYBERARK
salesforce
okta
SHODAN
graphistry
SailPoint
splunk>
.conf18

Demo

AOF-Driven Incident Response

Symantec JSOC

Powered by Splunk Phantom



- 6 worldwide SOC locations
- Global team of few hundred analysts
- Handling 150 billion security events per day
- Using Phantom for:
  - Automation & Orchestration
  - Consolidation of security tools and alerts

splunk> .conf18

AOF Logo

Powering
The Next Gen SOC

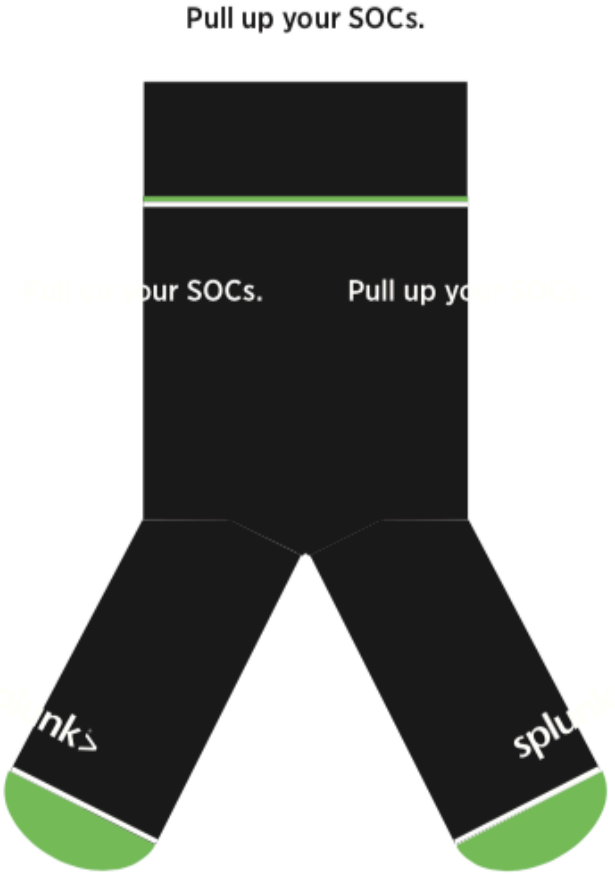
Nerve center for security

Collaborative SOC

Establish security operations

Solve across multiple domains

Specific problem



For more information on
Splunk Adaptive Operations Framework,
visit http://splunk.com/aof

splunk> .conf18

Thank You

Don't forget to rate this session in the .conf18 mobile app