



splunk>

And You Get Security! And You Get Security...And You Too!

Free Good Stuff!

Elyssa Christensen
Sr. Product Marketing Manager, Security

Oct 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, 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. © 2018 Splunk Inc. All rights reserved.

This Session is Brought to You By....

ELYSSA CHRISTENSEN

**Sr. Product Marketing Manager
Former Sr. Sales Engineer for 5 Years
15 Years of BI Experience
Amateur Kayaker!**



The Splunk Platform for Security Intelligence

200+ APPS



Cisco Security Suite



Palo Alto Networks



OSSEC

Windows/ AD/
Exchange

FireEye



DShield



STM

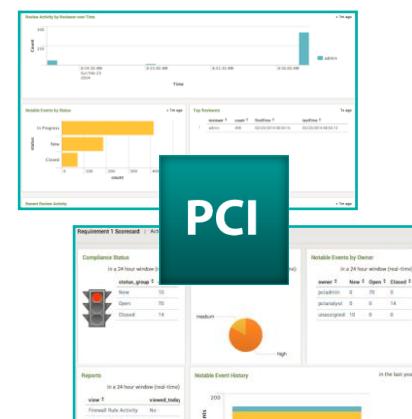


Bit9



DNS

Splunk for Security



Splunk-Built Apps



splunk>

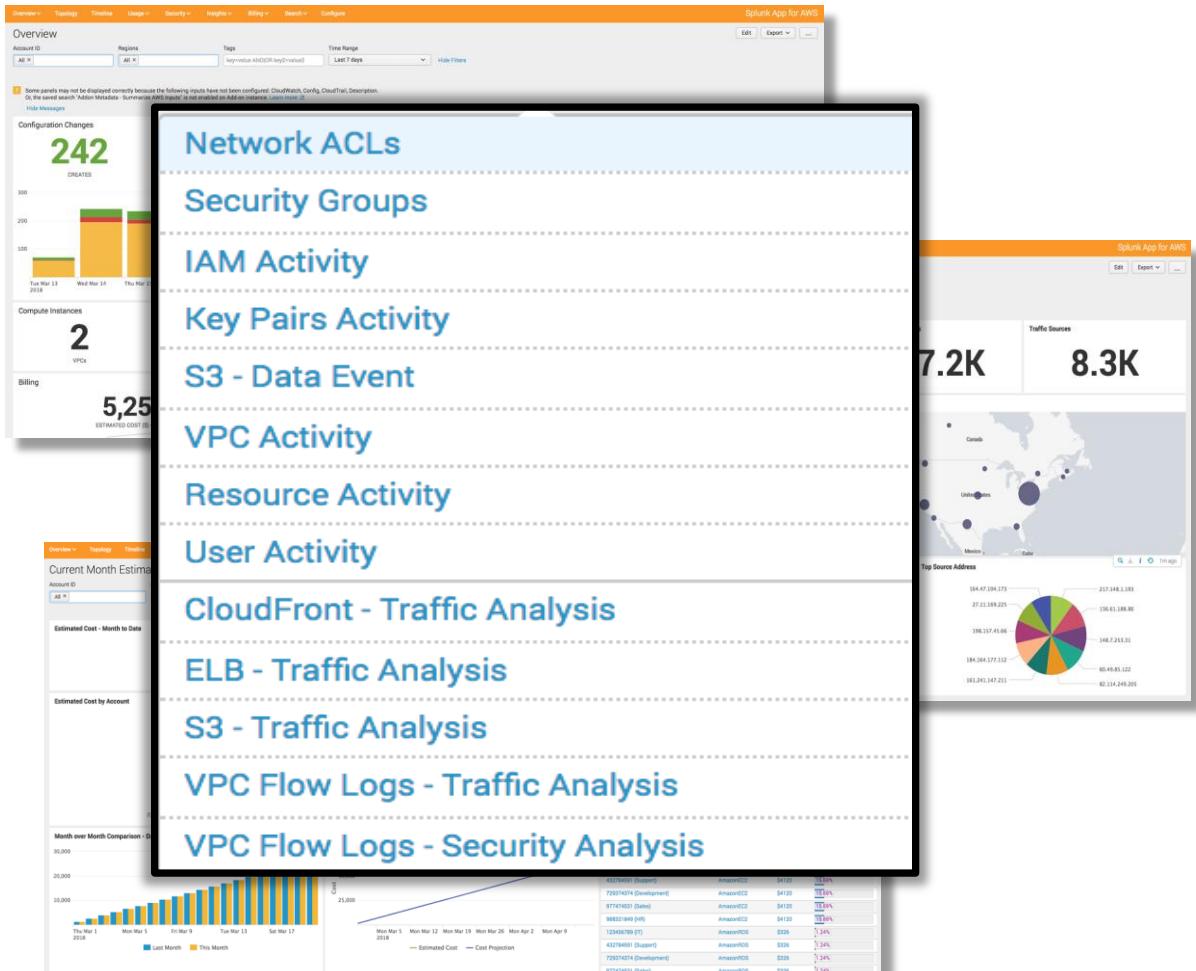
Security for AWS

Splunk for AWS

Pre-Built Searches, Reports, and Dashboards for Detailed Analysis

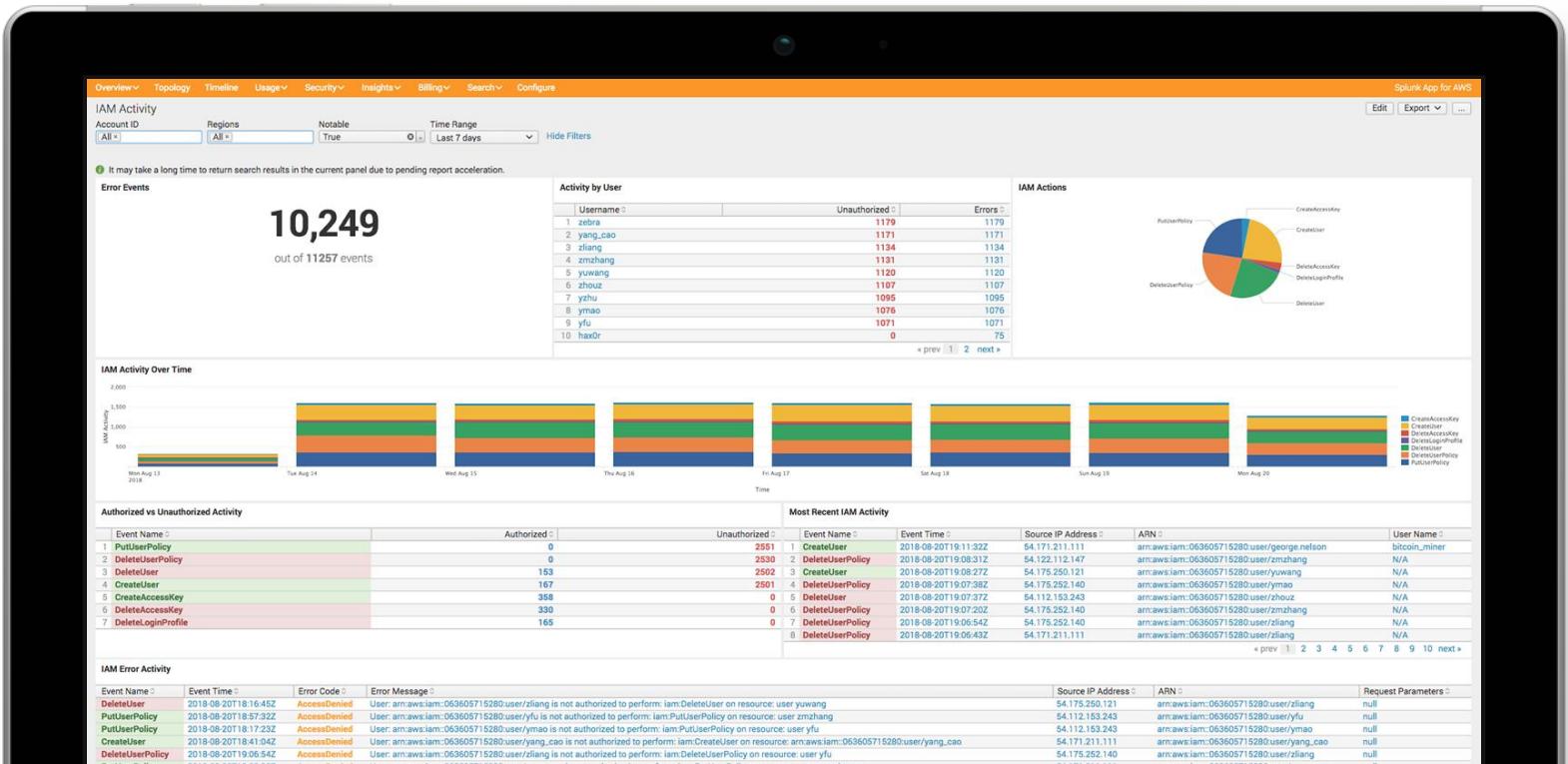
▶ Provides Deep Insight

- For **Compliance & Security** across Network ACLs, Groups, IAM Activity, S3, VPC Activity, Resource & User Activity, ELB/Cloudfront/S3/VPC Flow Traffic
- **Billing** including a Budget Planner, Historical Bill Analysis, and Current Monthly Estimated Billing
- **Utilization** across EC2 Instances, EBS Volumes, Lambda, API Gateway and more with Capacity and Reserved Instance Planning insight
-And a whole lot more!!



Splunk for AWS

IAM Activity



You see servers and devices, apps and logs, traffic and clouds. We see data—everywhere. Splunk® offers the leading platform for Operational Intelligence. It enables the curious to look closely at what others ignore—machine data—and find what others never see: insights that can help make your company more productive.

- ▶ Identifies changes to roles
- ▶ Logon/logoff activity
- ▶ Use of credentials
- ▶ Users potentially trying to do things they shouldn't be able to do

Splunk for AWS

Cloudfront: Traffic Analysis

- ▶ CDN Entire picture of what is being requested/accessed
- ▶ Can review users/clients interacting with web proxies
- ▶ Denial of Service attacks

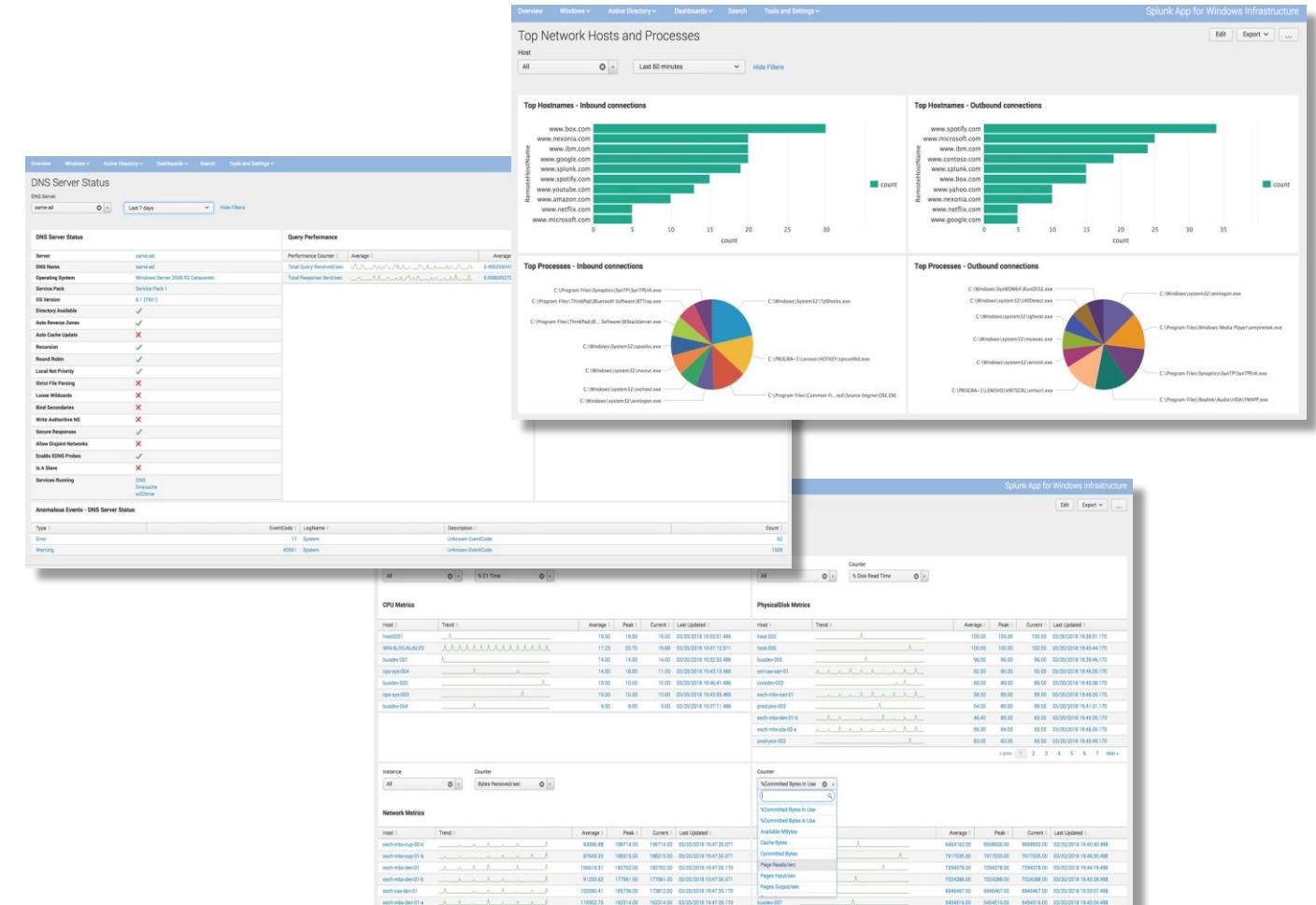


Security for Microsoft

Splunk for Microsoft

Pre-built Searches, Reports, Dashboards for Detailed Analysis

- ▶ Visibility into your entire Microsoft Stack with Monitoring by Event, Network, Host, Process, Application, Disk, and Printer



- ▶ Active Directory analysis by Domain, Domain Controller, DNS, User, Computers, Groups, Policy, Organizational Unit, and more.

Splunk for Microsoft

Microsoft Infra: Anomalous Logons

- ▶ Exchange, Office365, Azure
- ▶ Authentication Events
- ▶ Windows Firewall
- ▶ Messaging
- ▶ AD Audit
 - Domain & Authentication issues
 - Printer abuse

Anomalous Logons

Overview Windows Active Directory Core Views Search Tools and Settings

Forest Site Domain Server

Last 24 hours Hide Filters

Users logging in from more than one Site

Username	Domain	Sites
Administrator	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
Bypass Security	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
NoGuestsAllowed	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
aaron	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
abel	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
abraham	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
admin_HaxOr	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
adrian	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
alan	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name
albert	NULL SID SEATTLE	Default-First-Site-Name Default-Second-Site-Name

Logs from Multiple Workstations

No results found.

Attempted Access to Disabled or Expired Accounts

Username	Domain	IP Address	Site	count	Workstation	src_nt_domain
Bypass Security	SEATTLE	172.16.80.191	Default-First-Site-Name	49	SEATTLE\Bypass Security	SEATTLE
Bypass Security	SEATTLE	172.16.80.191	Default-Second-Site-Name	62	SEATTLE\Bypass Security	SEATTLE
abel	SEATTLE	172.16.210.11	Default-First-Site-Name	46	SEATTLE\abel	SEATTLE
abel	SEATTLE	172.16.210.11	Default-Second-Site-Name	60	SEATTLE\abel	SEATTLE
abraham	SEATTLE	172.16.120.10	Default-First-Site-Name	5	SEATTLE\abraham	SEATTLE
abraham	SEATTLE	172.16.120.10	Default-Second-Site-Name	15	SEATTLE\abraham	SEATTLE

Splunk for Microsoft

Microsoft Infra: User Audit

User Audit

Account Domain: SEATTLE | Filter User List: B* | User Account: Bob BroHax0r | Last 15 minutes | Submit | Hide Filters | Edit | Export | ...

Group Membership - User

groupDN	groupName	primaryGroupID
CN=Domain Users,CN=Users,DC=seattle,DC=contoso,DC=com	Domain Users	513
CN=Contractors,OU=Contractors,OU=Departments,DC=seattle,DC=contoso,DC=com	Contractors	359059

Account Lockout Activity - User

_time	Workstation	Reason
2018-08-24 16:54:24	cont_bbrohax0r	A user account was locked out

Failed Logon Activity - User

Workstation	IP Address	Reason	Earliest	Latest	count
cont_bbrohax0r_wkstrn	172.16.210.129	An account failed to log on	2018-08-24 16:49:44	2018-08-24 16:59:36	10
cont_bbrohax0r_wkstrn	172.16.210.129	User name is correct but the password is wrong	2018-08-24 16:48:25	2018-08-24 16:48:25	1

Top

Common-Name	Bob BroHax0r
DS-Core-Propagation-Data	160101000417.0Z 20150409151826.0Z 20150409152841.0Z 20150409155849.0Z
Display-Name	Bob BroHax0r
Instance-Type	WRITE
Is-Member-Of-DL	CN=Contractors,OU=Contractors,OU=Departments,DC=seattle,DC=contoso,DC=com
Obj-Dist-Name	CN=Bob.BroHax0r,OU=Contractors,OU=Departments,DC=seattle,DC=contoso,DC=com
Object-Category	CN=Person,CN=Schema,CN=Configuration,DC=seattle,DC=contoso,DC=com
Object-Class	organizationalPerson
person	
top	
user	

Object-Guid

RDN	145f278d-9645-424b-afef-40ec73a0ca1f
Bob BroHax0r	

RDN

USN-Changed	10669243
	5741906

USN-Created

When-Changed	20151016173752.0Z
	20150408162230.0Z

Mail-Recipient

Common-Name	Bob BroHax0r
-------------	--------------

Organizational-Person

Country-Code	0
Given-Name	Bob

Person

Common-Name	Bob BroHax0r
Surname	BroHax0r

Security-Principal

Object-Sid	S-1-5-21-3623811017-899348573-30300820-2800
SAM-Account-Name	cont_bbrohax0r
SAM-Account-Type	NORMAL_USER_ACCOUNT

User

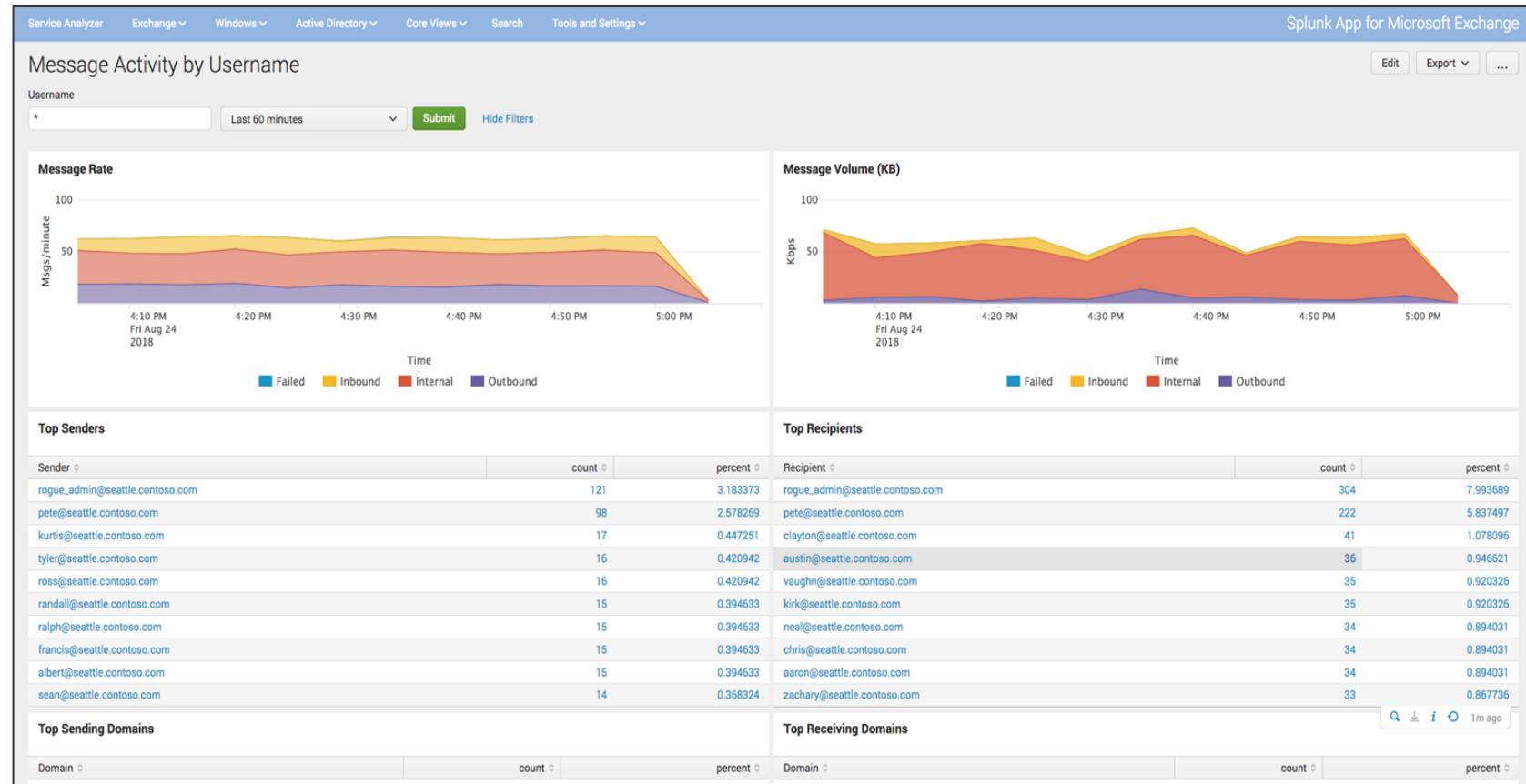
Account-Expires	(never)
Bad-Password-Time	2015-10-16T17:37:52.456000Z
Bad-Pwd-Count	12
Code-Page	0

► Lockout Activity

► Failed Logon

Splunk for Microsoft

Microsoft Exchange: Message Activity

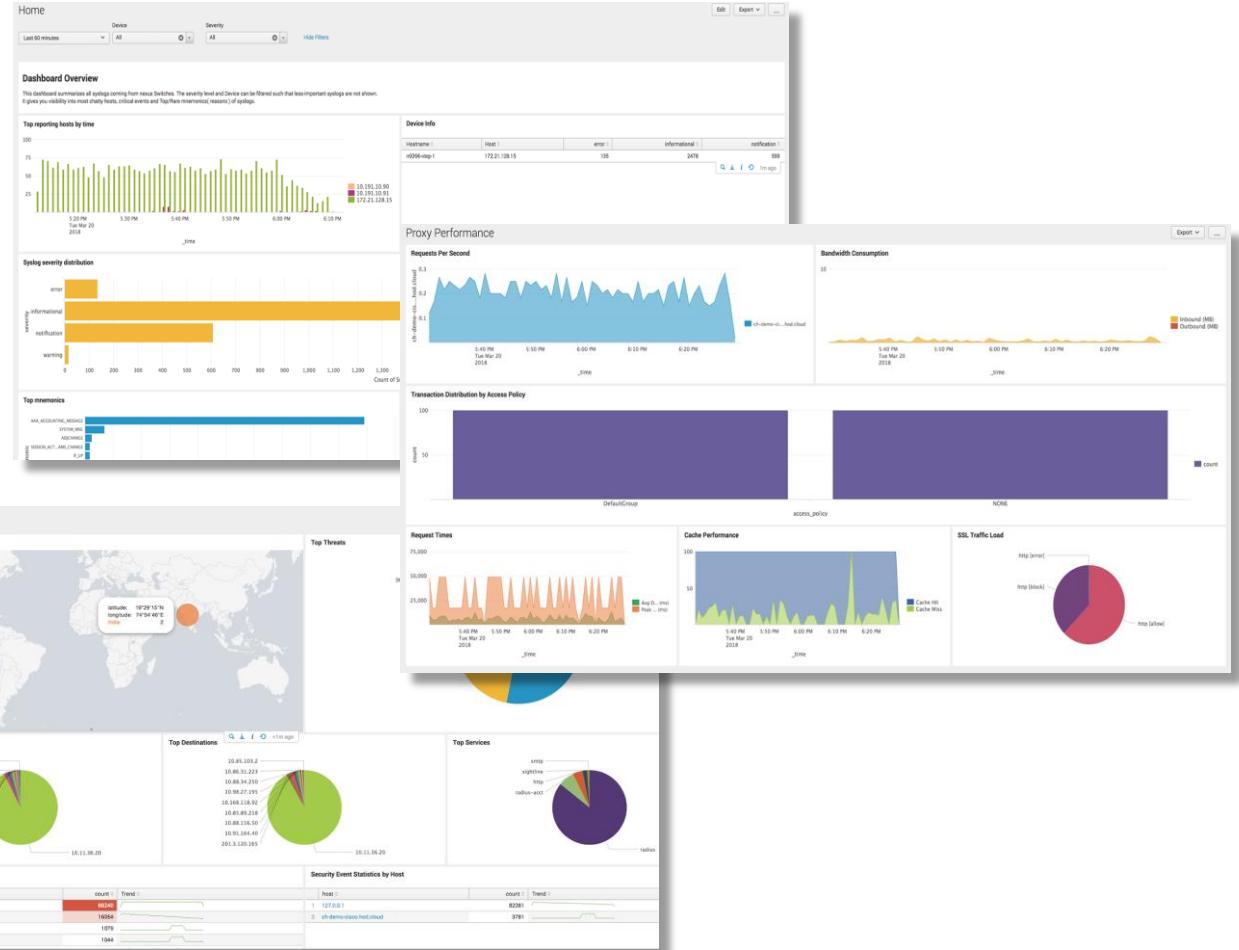


Security for Cisco

Splunk for Cisco Suite

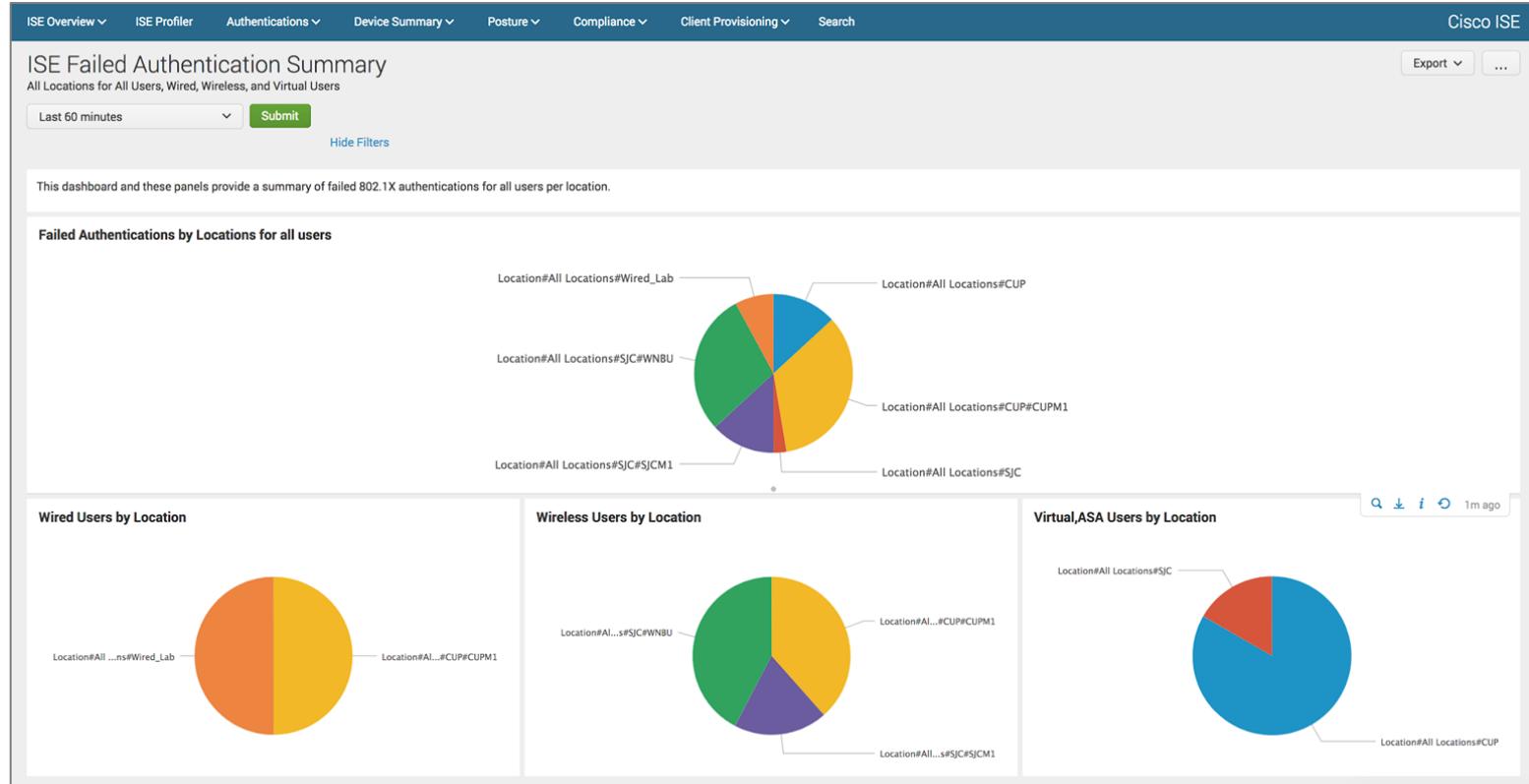
Pre-built Searches, Reports, Dashboards for Detailed Analysis

- ▶ Emails analysis including Message tracking, Gateway Performance and more
- ▶ Web Analysis by Request, Client, Policies (personal/business use and legal liability)
- ▶ Web Performance by Proxy, Network Resource, and Destination
- ▶ Network analysis by eStreamer, Sensor, Policy, Host, Flow, Malware Events, and Intrusion Events
- ▶ Identity Services Analysis by User Investigation, Pro Device, Posture, Authentications, and more.



Splunk for Cisco Suite

Cisco: ISE Failed Logins

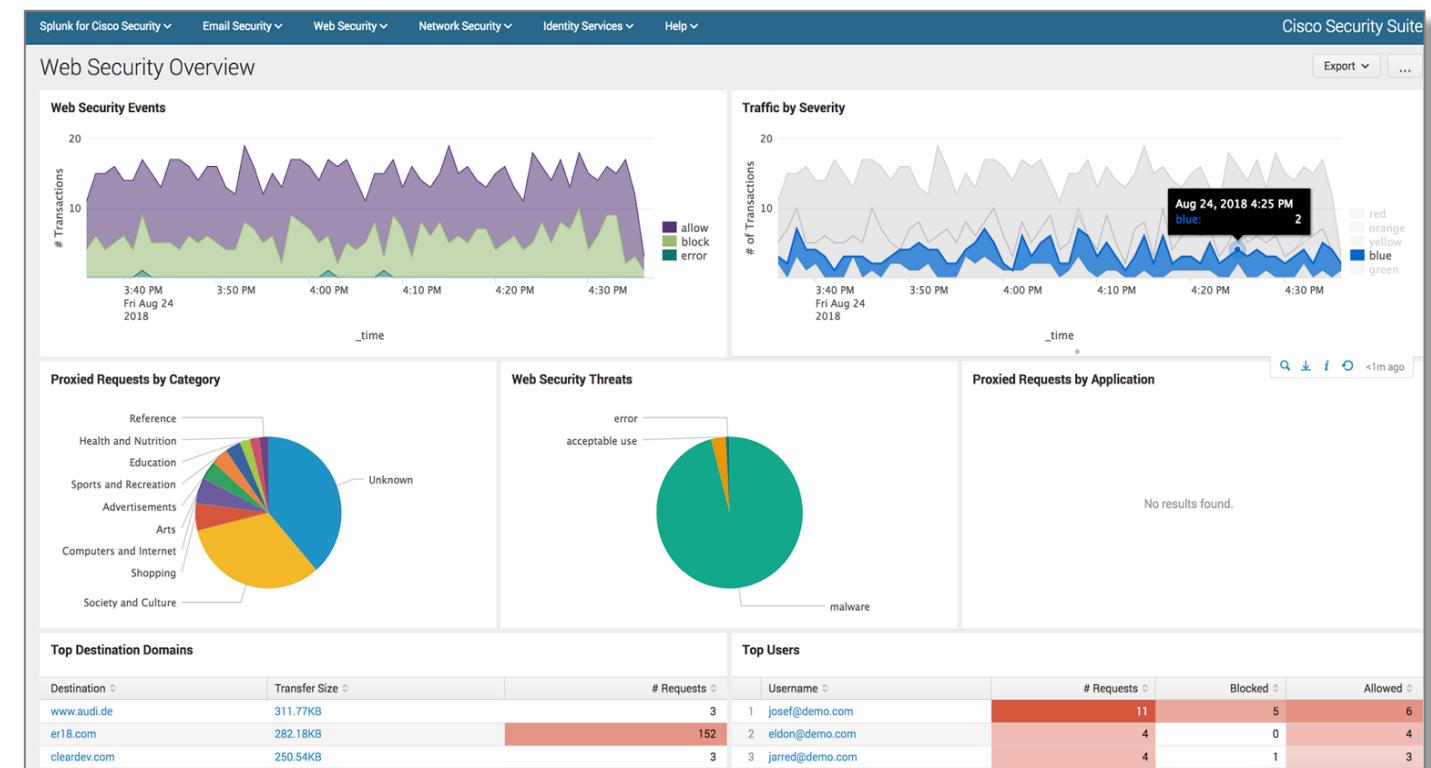


- ▶ Sometimes the Chart isn't pretty but the search is....
- Access abuse
- Potential compromise
- Superman effect

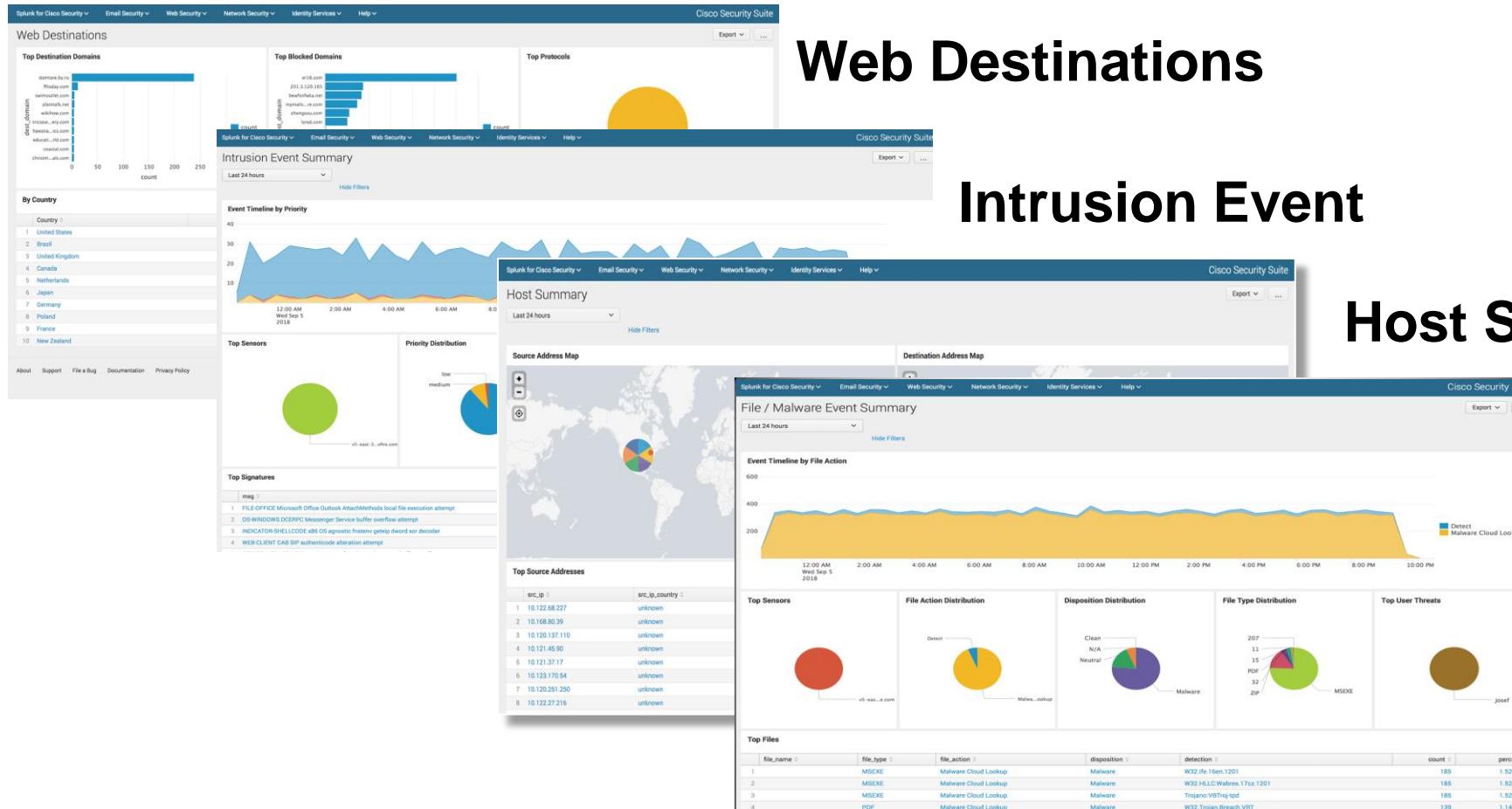
Splunk for Cisco Suite

Cisco: Web Security Overview

- ▶ Visibility into what users are doing from their browser
- ▶ May identify a flight risk employee or behavior that's out of compliance with corporate policy
- ▶ Cloud or file sharing services
- ▶ Upticks in traffic going out to google drive or other locations.



More Cisco Goodness!



Security for Palo Alto



Splunk for Palo Alto Networks

Pre-Built Searches, Reports, and Dashboards for Detailed Analysis

Most Common Use Cases

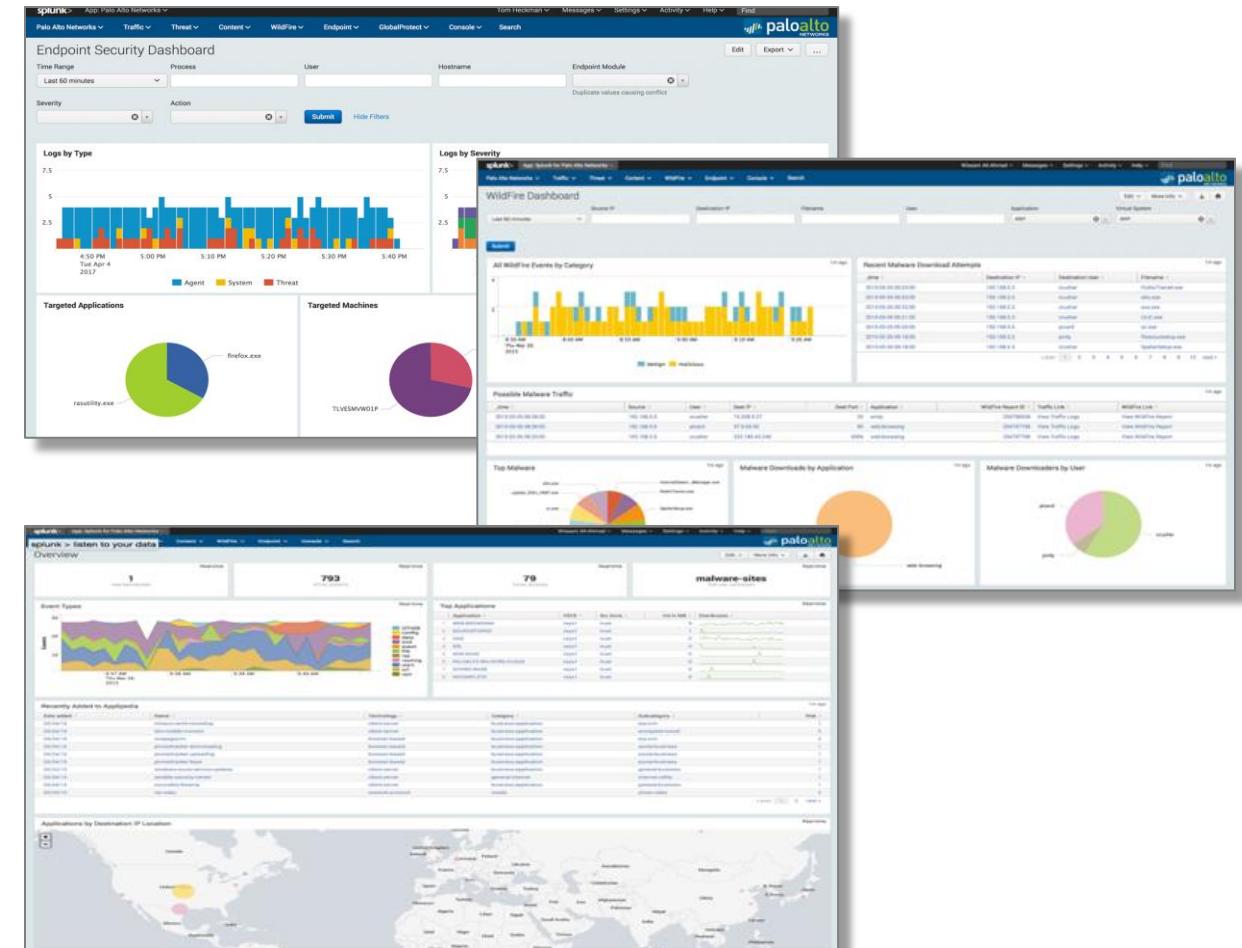
- Security overview, investigation and incident response
- Policy overview, monitoring and adjustment
- Operational overview and configuration management

Data Sources

- Traffic
- Threat
- Wildfire
- Autofocus
- TRAPS
- Aperture

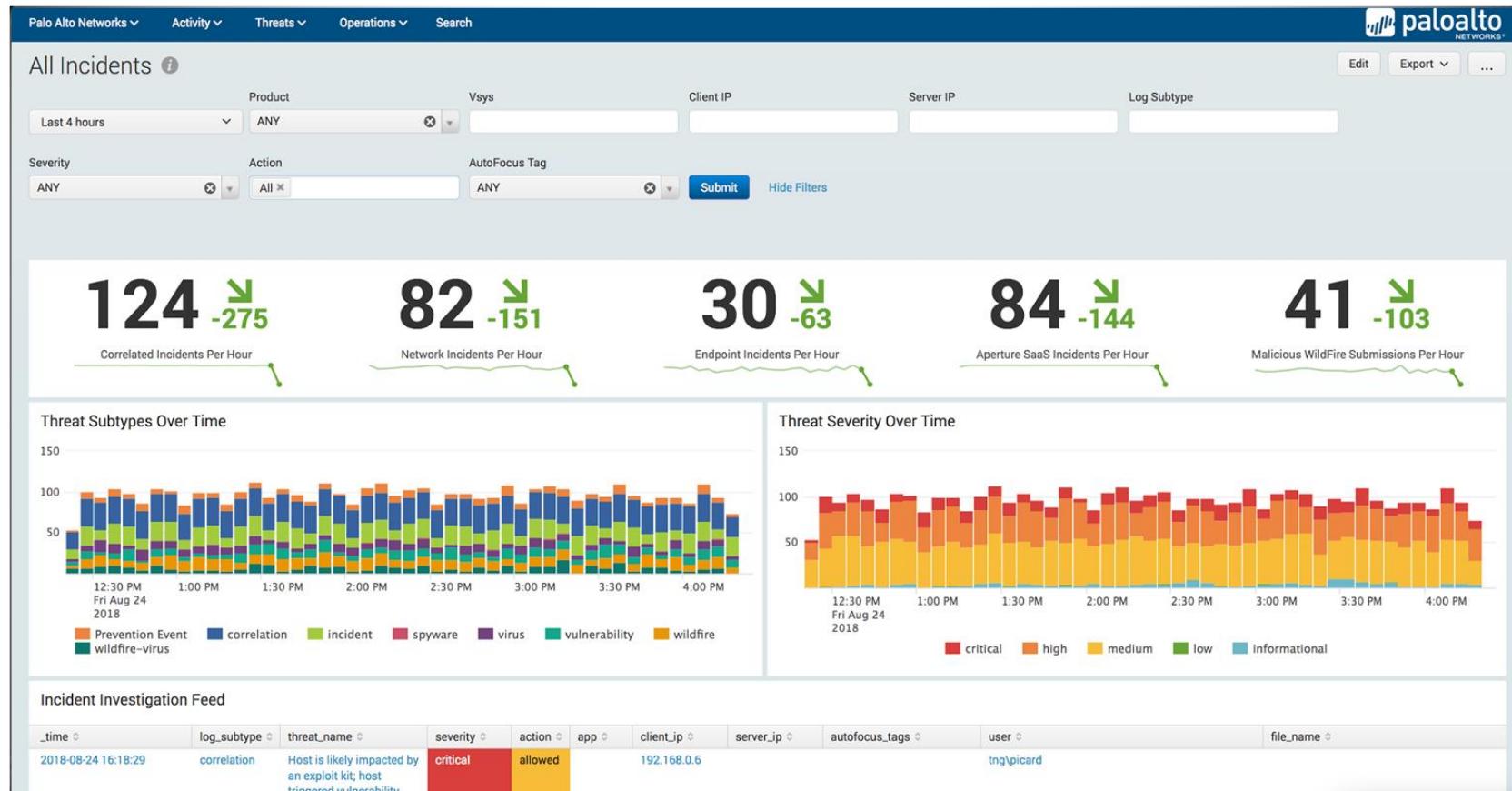
Adaptive Response and Integrations

- Tag IP/Domain on firewall
- On-demand Wildfire
- Enrich with Autofocus
- Common Information Model (CIM) compliant
- Full integration with Splunk Enterprise Security (ES)



Splunk for Palo Alto

PAN: Overall Posture



This should look familiar!!

Splunk for Palo Alto

PAN: Network Security

The screenshot shows the Palo Alto Networks Network Security interface. At the top, there are filters for Log Subtype (Last 60 minutes), Threat, Severity, and Application. Below the filters are sections for "Top Correlation Events" and "Top 20 Vulnerability Events". The "Top Correlation Events" section lists various threat names and their details. The "Top 20 Vulnerability Events" section lists vulnerabilities like "Suspicious Abnormal HTTP Response Found" and "Internet Explorer FTP Response Parsing Heap Overwrite Vulnerability". To the right, there is a "Top 20 Virus and Malware Events" section listing file names, log subtypes, and users affected.

- ▶ Let's You know what your firewall thinks looks off
- ▶ Initial indication of what needs to be addressed by security engineer
- ▶ Great feed into splunk!

Splunk for Palo Alto

PAN: Malware

- ▶ Helps stop endpoint attacks before they get started!

Palo Alto Networks ▾ Activity ▾ Threats ▾ Operations ▾ Search

Malware

Log Subtype	Serial Number	Virtual System	Source IP	Destination IP
Last 60 minutes				
Filename	User	Severity	Application	Action
				All

Malware Families and Campaigns

tag_name	aliases	tag_class	count
Elise		malware_family	65
LotusBlossom		campaign	65
WanaCrypt0r	wannacry wcry	malware_family	117

Top Domains Serving Malware

dest_name	dest_ip	count
qstom.com	116.252.0.0	134
emam.firefoxupdate.com	65.55.17.25	72
api.yontoo.com	4.30.3.61	11
s10.histats.com	173.192.226.69	4

Malware Delivery and Installation

user	threat_name	src
To: ABUL22ZSMIVjHm6AeRBkLsrFDX7K0gN@sLvncAoYxFmbRiyTziiKCZFJuTjJDrnQ.edu;	Backdoor/Win32.Aobot.bwp	66.1
To: AJ@yPxDurfKMsVXHizgvXnYlcYRjv.edu;	Trojan/Win32.StartPage.ews	66.1
To: BNqZSX00D926FPIcQ927P4F9hHHCTuk@fmgbAKwNdTLMStzBSITUYOERfyBohEDY.gov,	Virus/Win32.IRCBot.orbs	66.1
To: CHTBrwBc5a91So11Capc@zbVcfnZWrzKheBongAzGuZU.gov;	Trojan-Downloader/Win32.zlob.bkw	66.1
To: EyeveN6Xa5aPgQWjMe7gnB54VqYdgy@RfRAFNClzL.us;	Backdoor/Win32.Rbot.jl	66.1
To: Fn4ssRPNX6NCur8OBsVr8Tzoa1ivkx@aEHZ.net;	TrojanDownloader/Win32.small.aajxq	66.1
To: IthDGkvbJ91xLmzBuhUrJHNGVF0a@VCxDWQZOXwF.us;	Trojan-PSW/Win32.Lmir.eg	66.1
To: J4RKY@wBzvJDeKMPsSMNZEfcuGljgm.us;	Backdoor/Win32.Rbot.gkd	66.1
To: JtpLvaOQM7K1OeoxzjHyuWOLWeYrtn@DapTriTsHRpgDMGqxPnix.org;	Worm/Win32.Allaple.tc	66.1
To: MkjzH70fW@jkZBprKhXgFPz.com;	Trojan/Win32.Banker.rwa	66.1

Command and Control Traffic

user	threat_name	src_ip	dest_ip	vendor_action	count
pandademo\jerry.corcoran	WGeneric.klfn C2 traffic	192.168.180.131	136.243.54.87	reset-both	1

Malware Events by Product

Malware Events by Action

So Many Vendors

So Many Great Apps!



Booz | Allen | Hamilton®



Check Point
SOFTWARE TECHNOLOGIES LTD

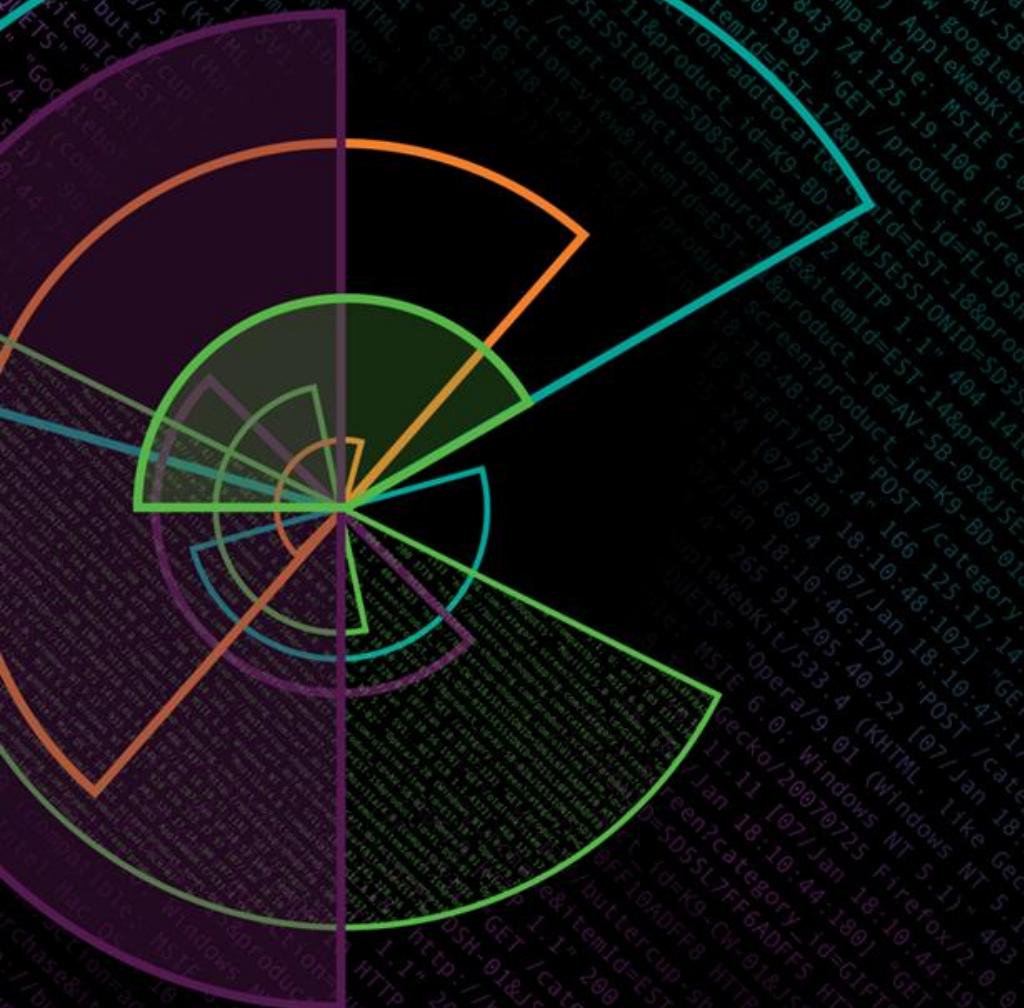


proofpoint.



Carbon Black.





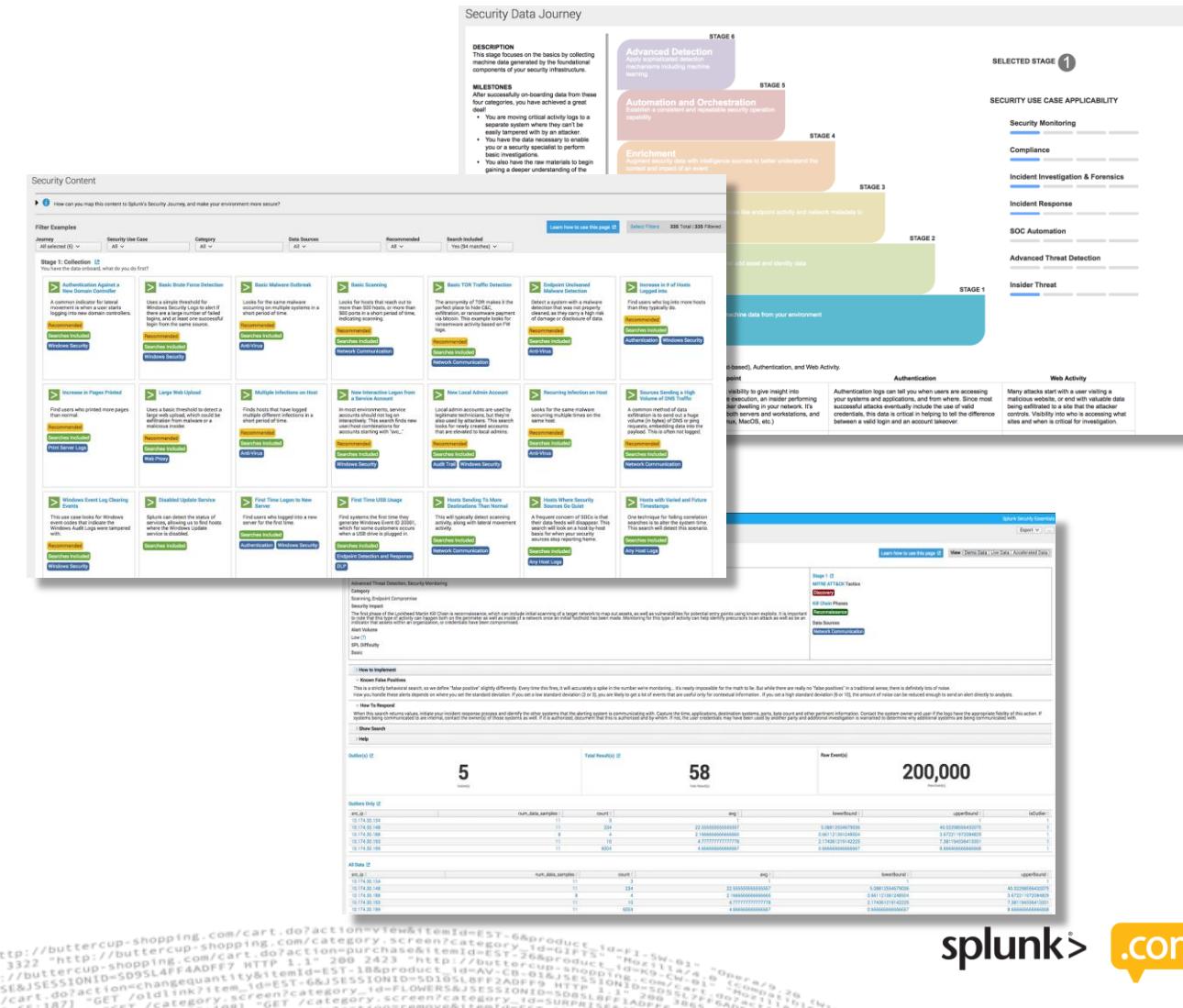
Better than a car...

Splunk for Security Essentials

Free Security Learning Guide

Over 438 Security Use Cases Documented in Detail across:

- Monitoring
- Compliance
- Advanced Threat Detection
- Insider Threat Detection
- Fraud Detection
- Incident Investigation and Forensics



Detailed Data Onboarding Guides

Clearly Aligns to Security Journey through Stages detailing:

- Impact
- Needed Data Sources
- Known False Positives
- Response Guidance and m

Top 20 Security Controls

Critical Control Overview Dashboards by Control ▾ Reports by Control ▾ Other Menus ▾ PDF Documentation CIS To

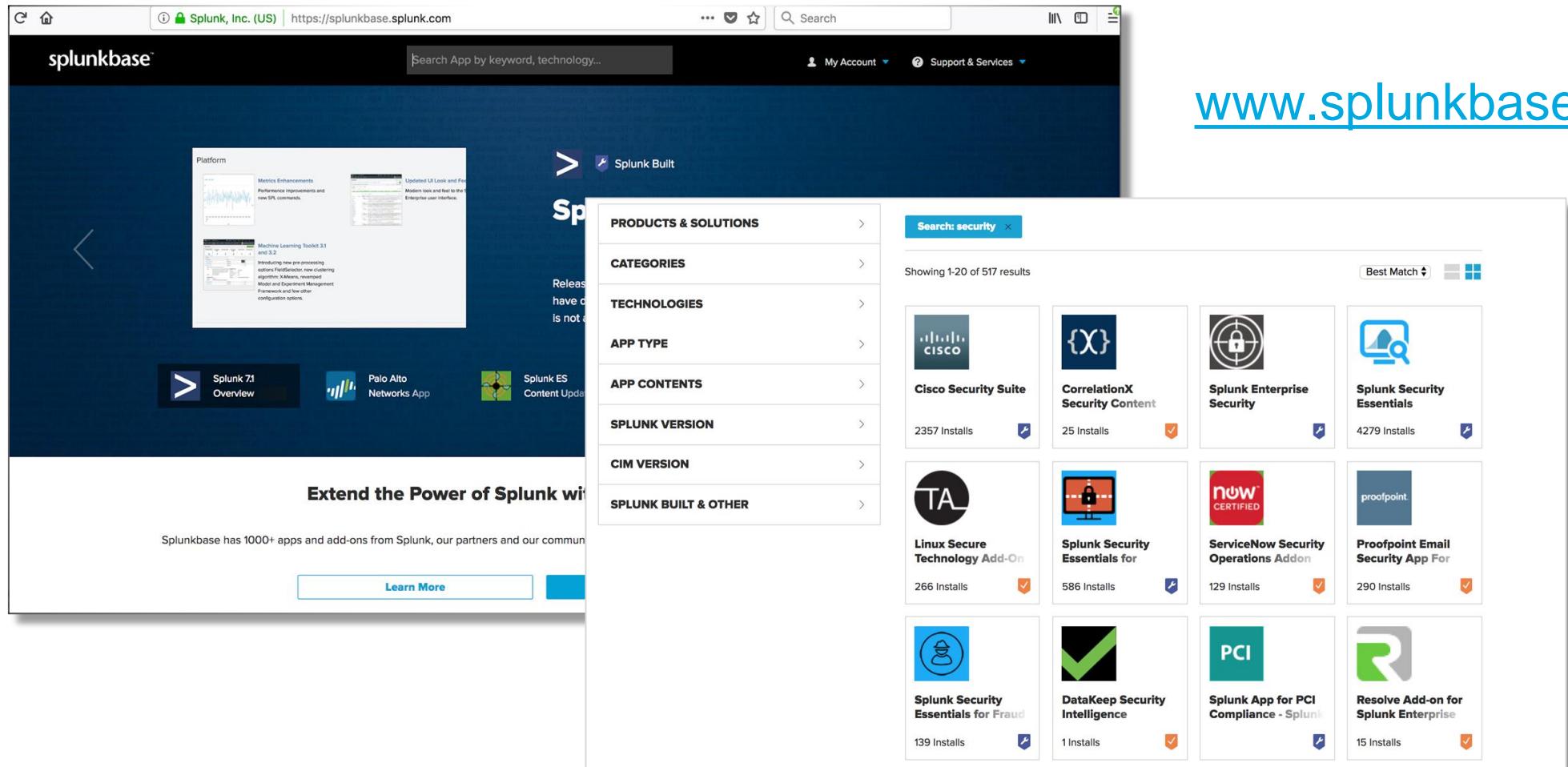
1: Inventory of Authorized and Unauthorized Devices

- 1.1 Deploy automated asset discovery tool**
Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that ...
- 1.2 DHCP Server Logging**
If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory ...
- 1.3 Automatically Update Inventory System**
Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
- 1.4 Maintain an Asset Inventory**
Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset ...
- 1.5 Deploy Network Level Authentication via 802.1x**
Deploy network level authentication via 802.1x
- 1.6 Use Client Certificates to validate and authenticate**
Use client certificates to validate

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software
4: Continuous Vulnerability Assessment and Remediation
5: Controlled Use of Administrative Privileges
6: Maintenance, Monitoring, and Analysis of Audit Logs
7: Email and Web Browser Protections
8: Malware Defenses
9: Limitation and Control of Network Ports
10: Data Recovery Capability
11: Secure Configurations for Network Devices
12: Boundary Defense
13: Data Protection
14: Controlled Access Based on the Need to Know
15: Wireless Access Control

- ▶ Extensible framework for baseline security “best-practices”
- ▶ Based on Top 20 CSC v6.1 published by Center for Internet Security
- ▶ Data agnostic
- ▶ Leverages Splunk CIM
 - Tags
 - Event Types
 - Fields

How do I get this goodness?



The screenshot shows the Splunkbase homepage and a search results page for "security".

Splunkbase Homepage:

- Header: Splunkbase, Search App by keyword, technology...
- Left sidebar: Platform (Metrics Enhancements, Performance Improvements and new SPL commands; Machine Learning Toolkit 3.1 and 3.2), Splunk 7.1 Overview, Palo Alto Networks App, Splunk ES Content Update.
- Middle section: Extend the Power of Splunk with 1000+ apps and add-ons from Splunk, our partners and our community. Learn More button.

Search Results for Security:

- Header: Search: security, Showing 1-20 of 517 results, Best Match.
- Results grid (2 columns):
 - Cisco Security Suite (2357 installs)
 - CorrelationX Security Content (25 installs)
 - Splunk Enterprise Security
 - Splunk Security Essentials (4279 installs)
 - Linux Secure Technology Add-On (266 installs)
 - Splunk Security Essentials for (586 installs)
 - ServiceNow Security Operations Addon (129 installs)
 - Proofpoint Email Security App For (290 installs)
 - Splunk Security Essentials for Fraud (139 installs)
 - DataKeep Security Intelligence (1 installs)
 - Splunk App for PCI Compliance - Splunk (265 installs)
 - Resolve Add-on for Splunk Enterprise (15 installs)

www.splunkbase.com

Thank You!