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.

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

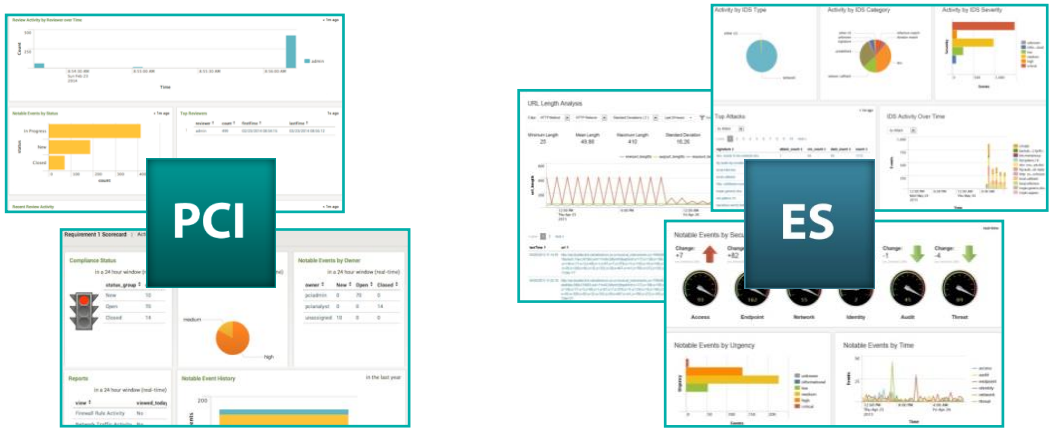
Amateur Kayaker!

The Splunk Platform for Security Intelligence

200+ APPS

- Cisco Security Suite
- Palo Alto Networks
- OSSEC
- Windows/ AD/ Exchange
- FireEye
- DShield
- Stream data
- Bit9
- DNS

Splunk for Security



Splunk-Built Apps

EX SC WIN STM MS DB

splunk>

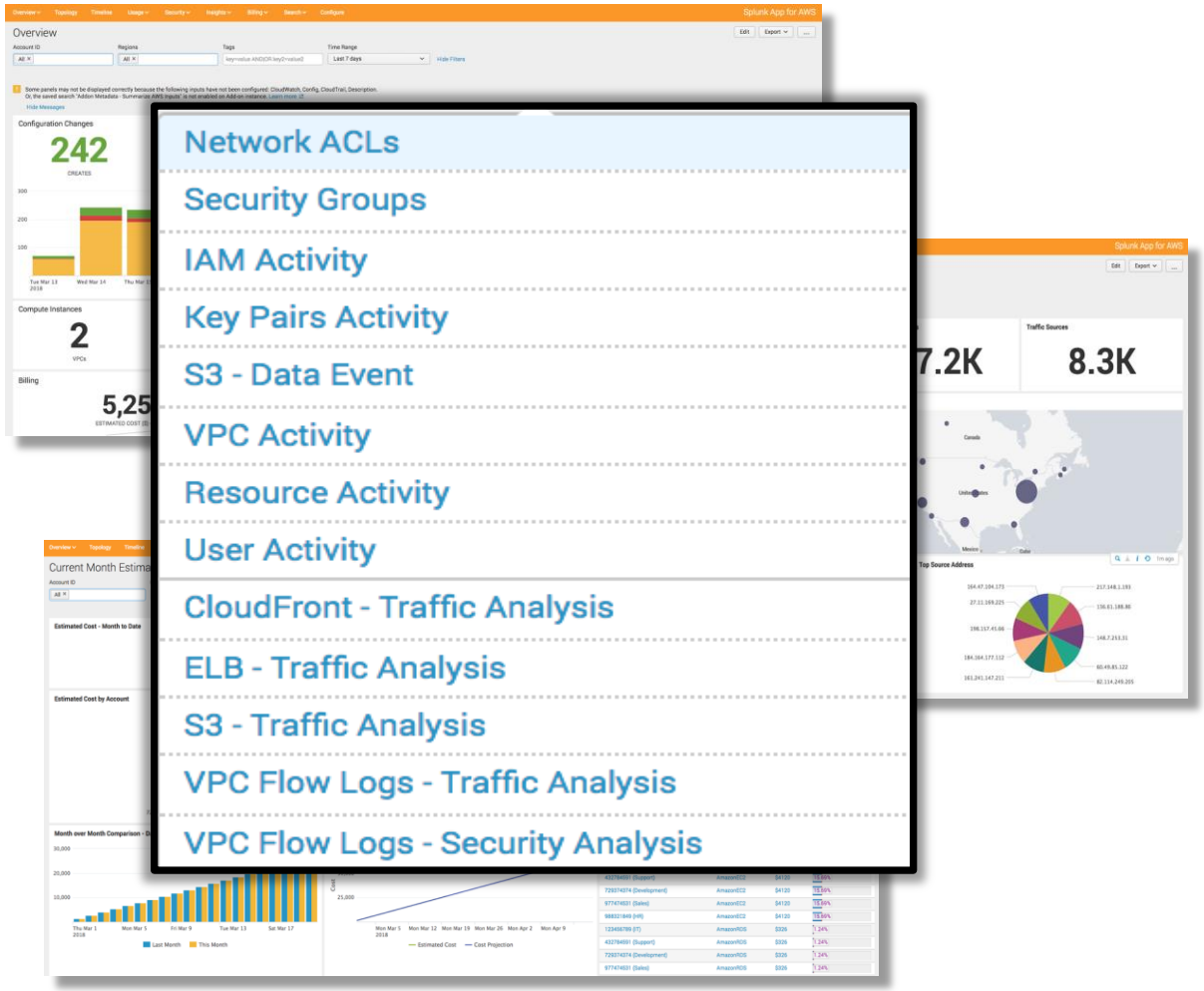
Security for AWS

splunk> .conf18

Splunk for AWS

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

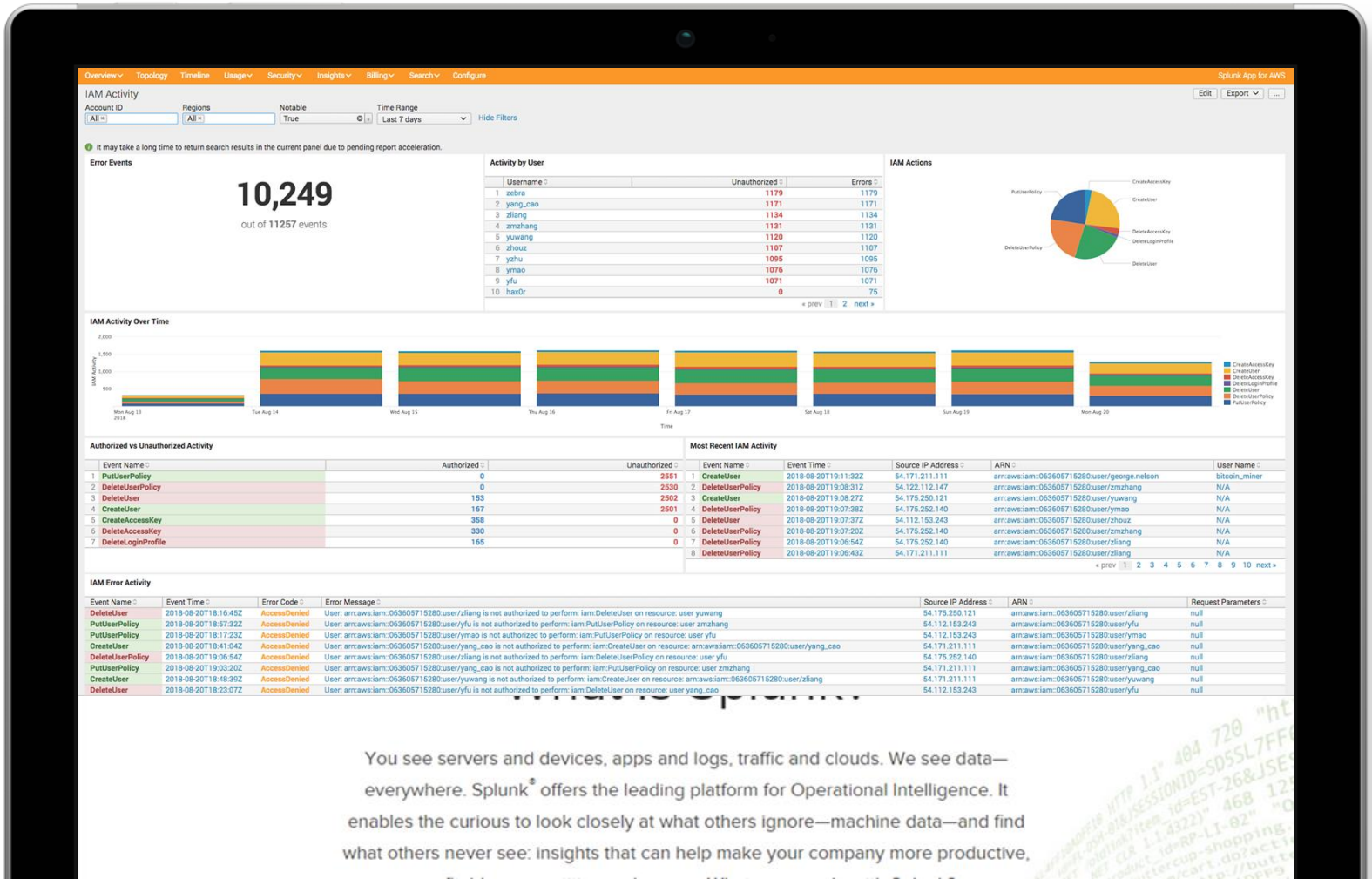
- **Provides Deep Insight**
  - For **Compliance & Security** across Network ACLs, Groups, IAM Activity, S3, VPC Activity, Resource & User Activity, ELB/Cloudfront/S3/VPC Flow Traffic
  - **Billing** including a Budget Planner, Historical Bill Analysis, and Current Monthly Estimated Billing
  - **Utilization**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



splunk> .conf18

Splunk for AWS

IAM Activity



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

splunk> .conf18

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

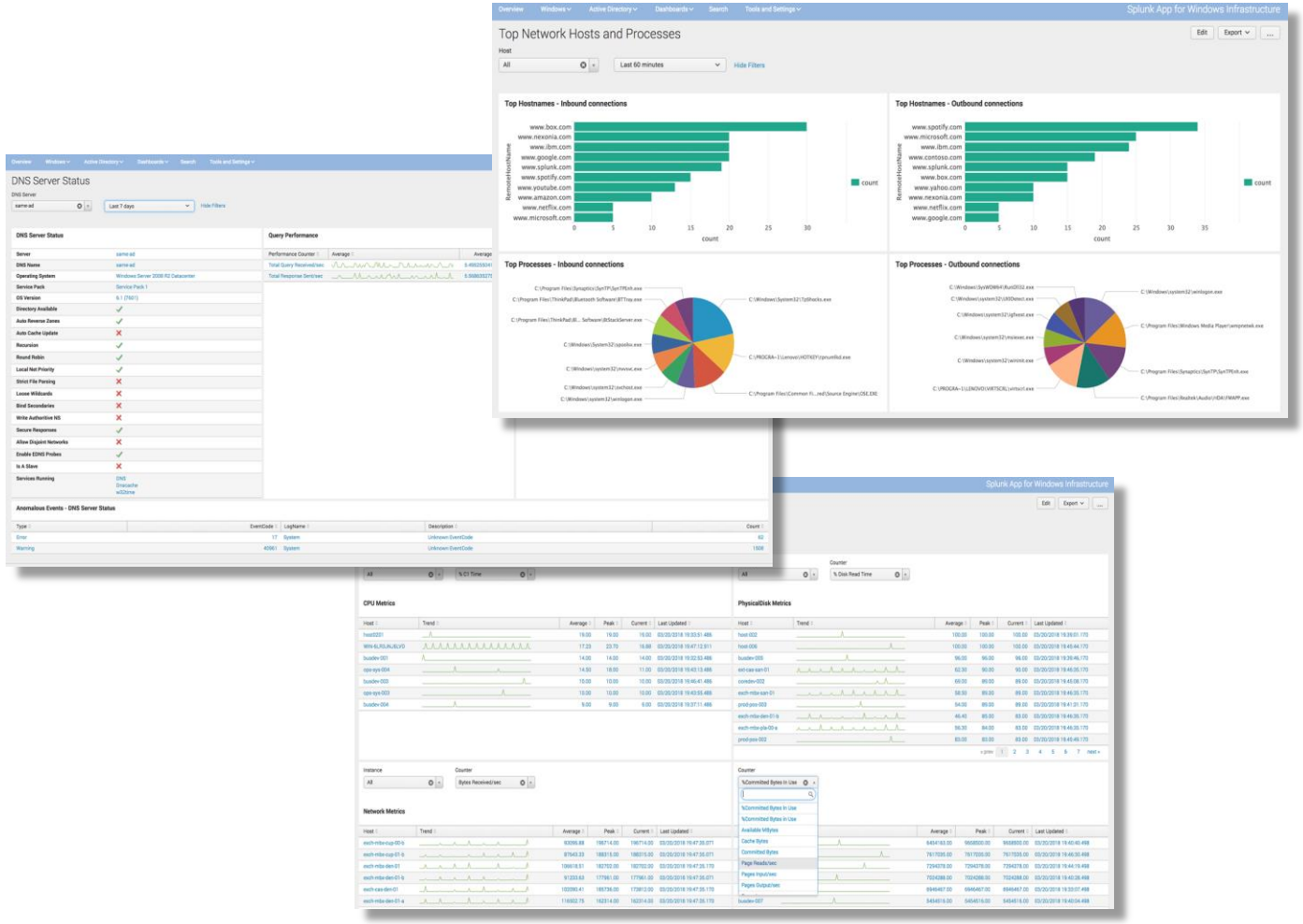
splunk> .conf18

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.

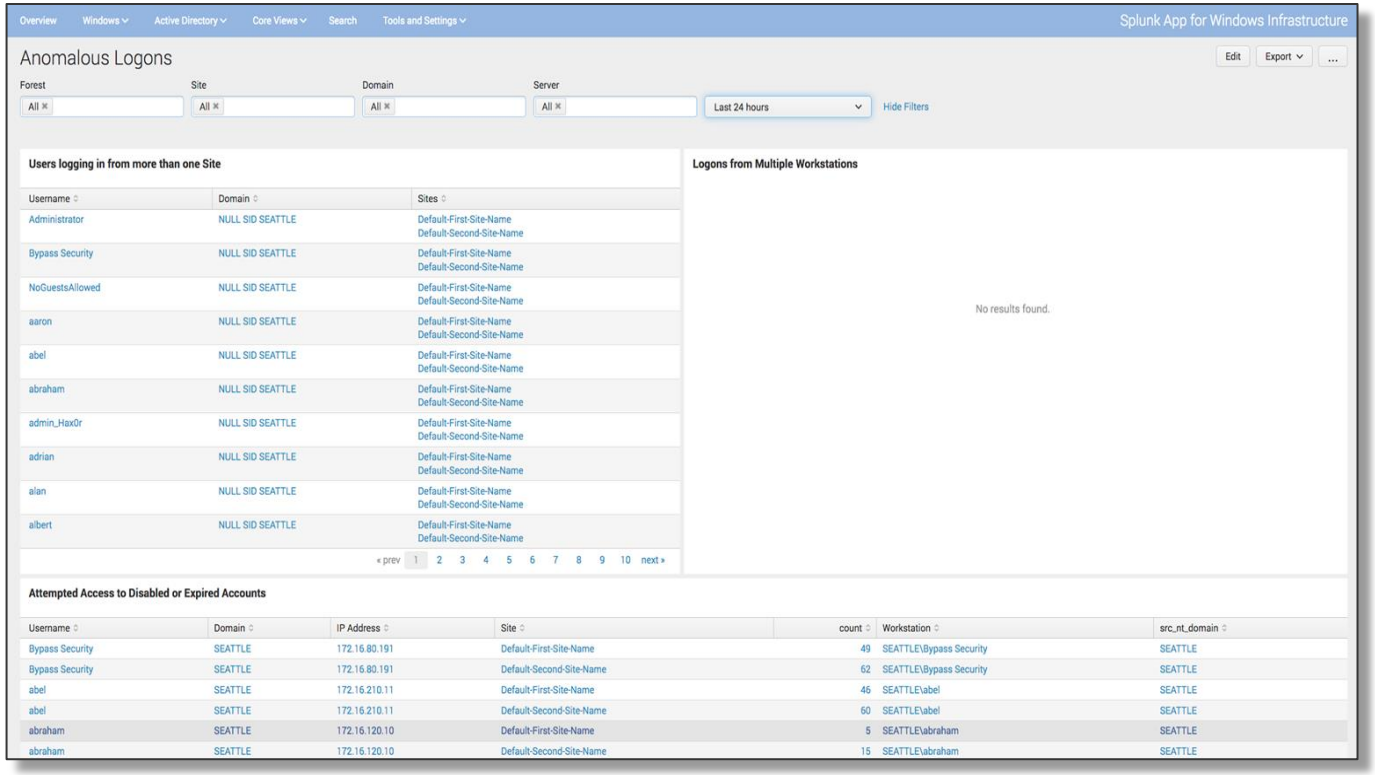


splunk> .conf18

Splunk for Microsoft

Microsoft Infra: Anomalous Logons

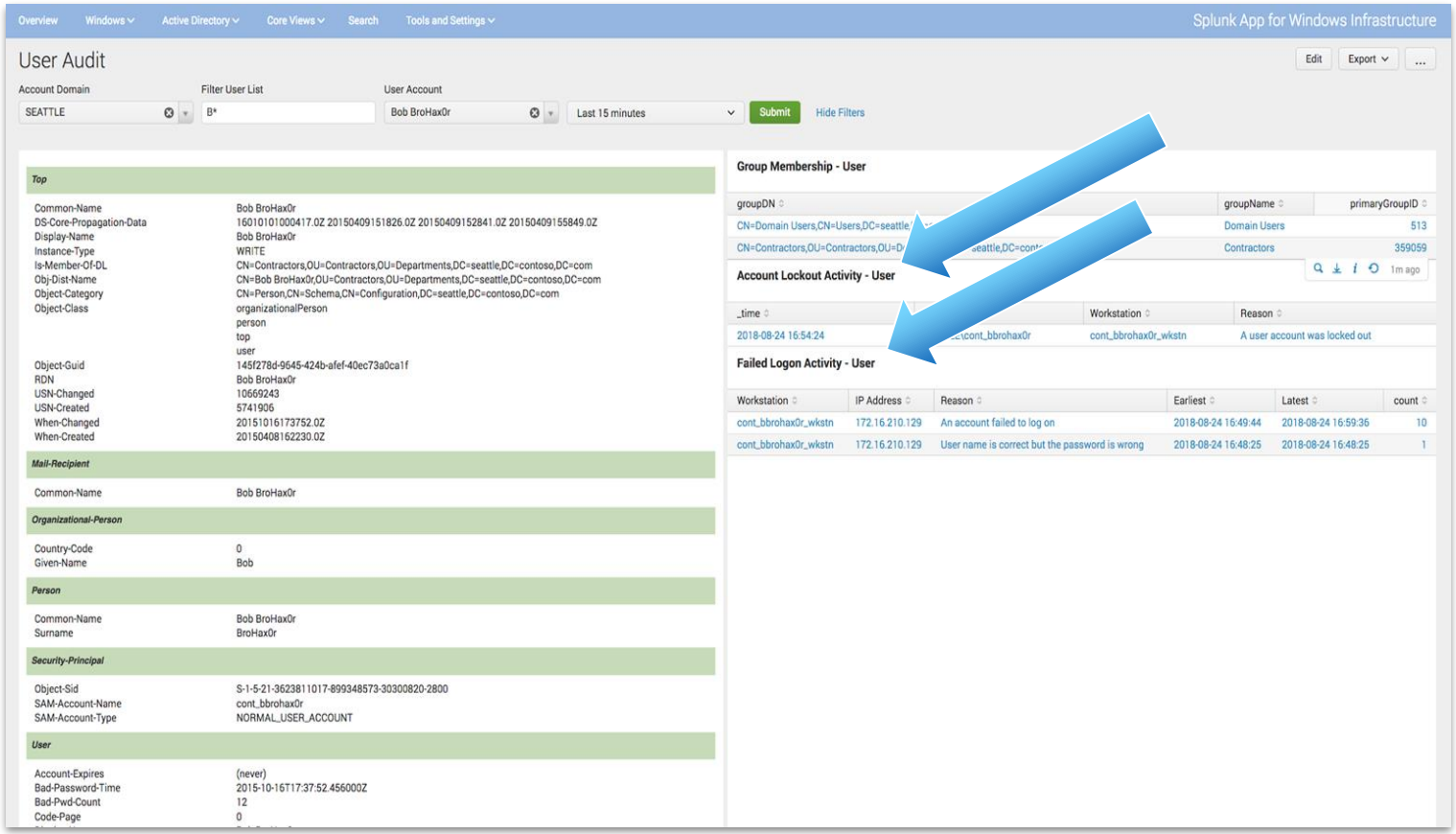
- Exchange, Office365, Azure
- Authentication Events
- Windows Firewall
- Messaging
- AD Audit
  - Domain & Authentication issues
  - Printer abuse



splunk> .conf18

Splunk for Microsoft

Microsoft Infra: User Audit

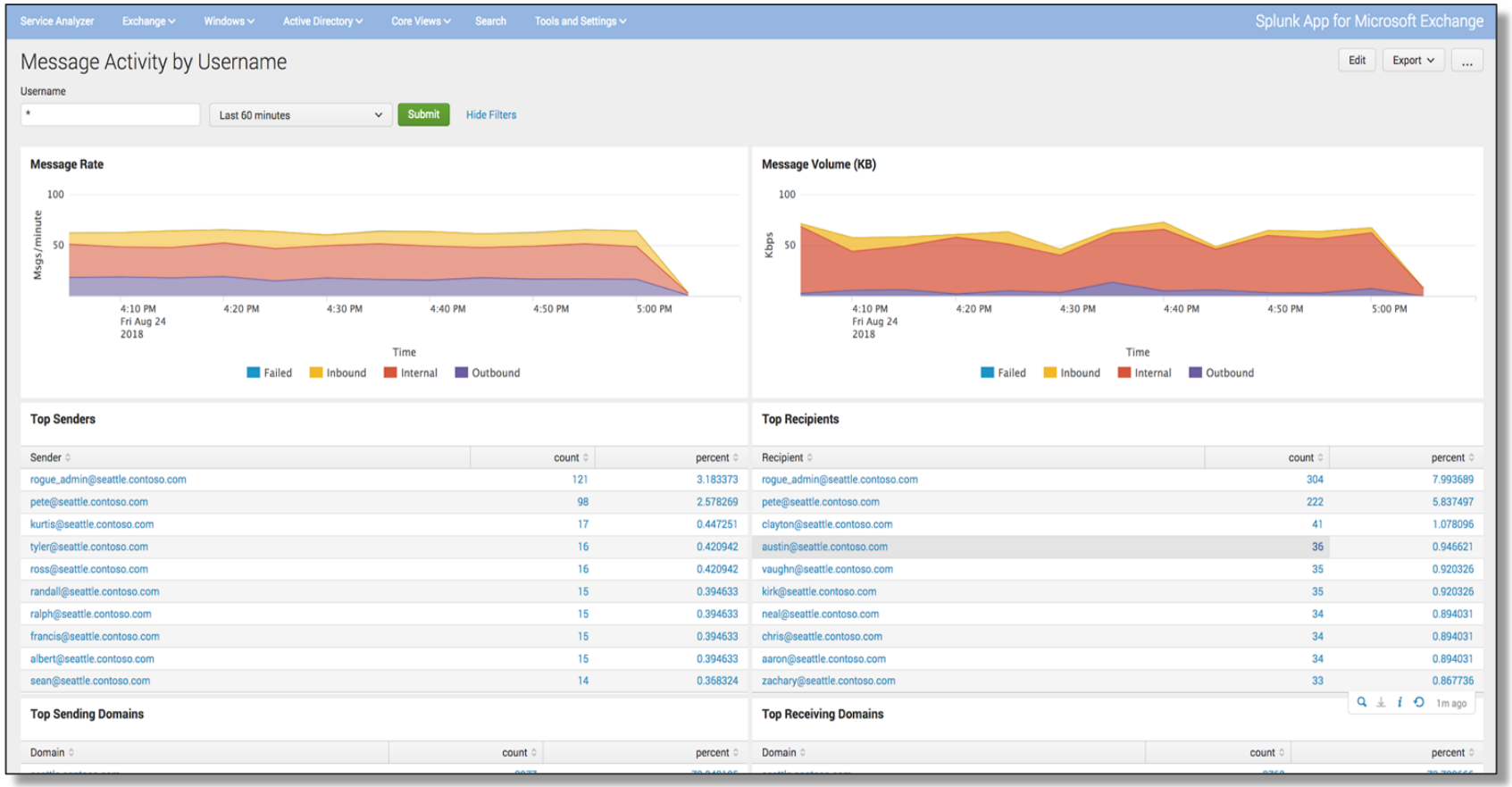


- Lockout Activity
- Failed Logon

splunk> .conf18

Splunk for Microsoft

Microsoft Exchange: Message Activity



splunk> .conf18

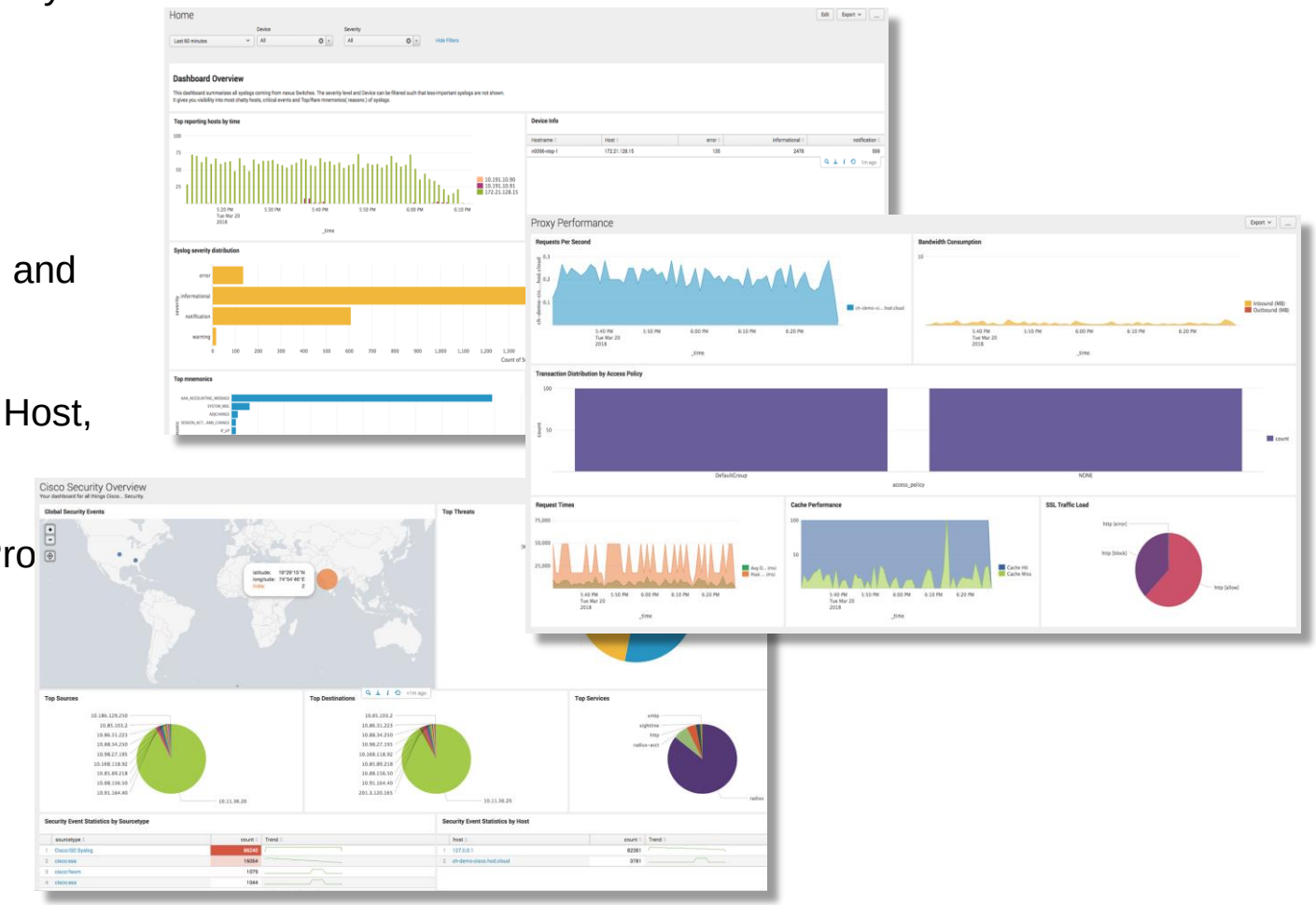
Security for Cisco

splunk> .conf18

Splunk for Cisco Suite

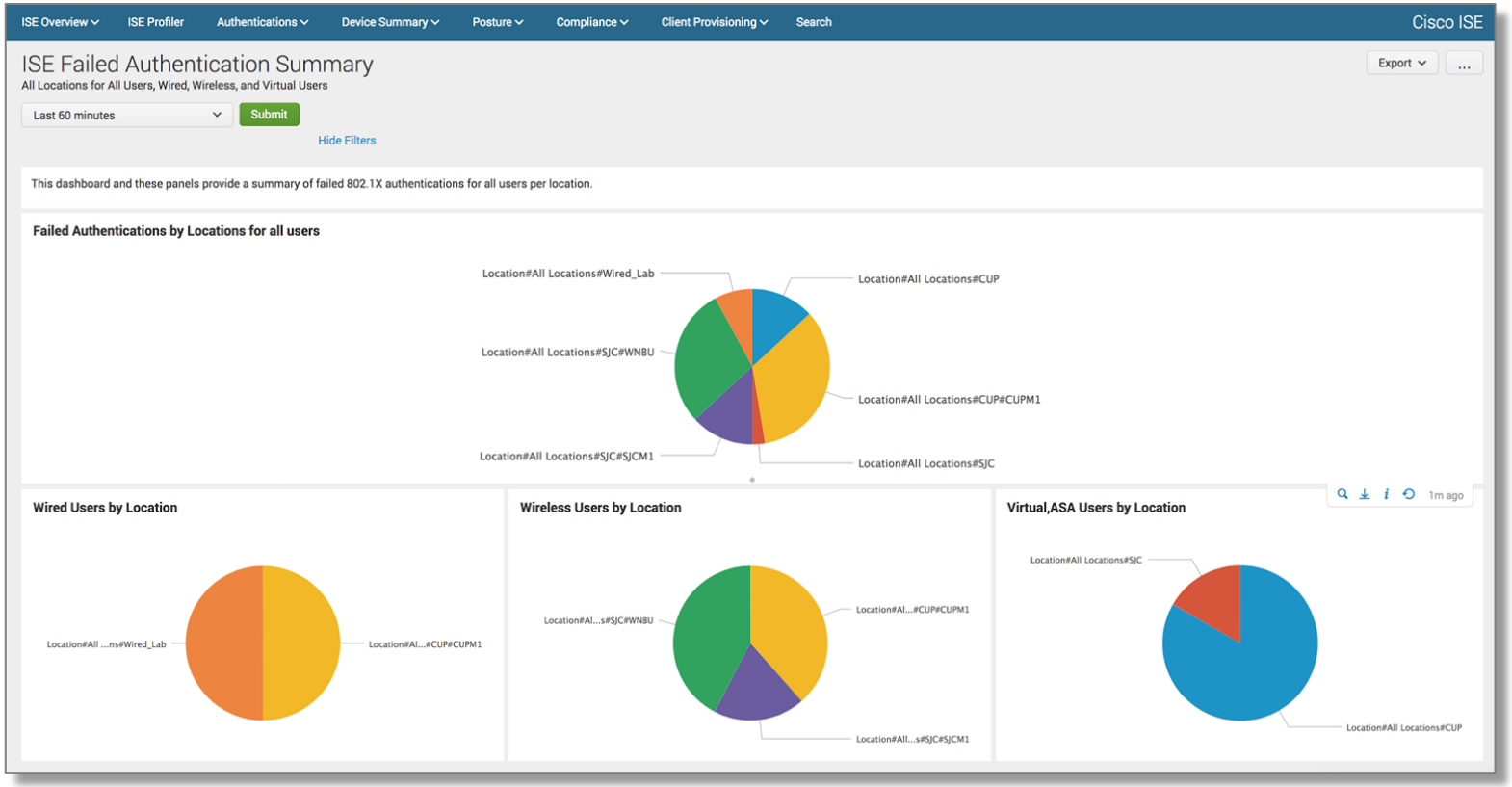
Pre-built Searches, Reports, Dashboards for Detailed Analysis

- 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



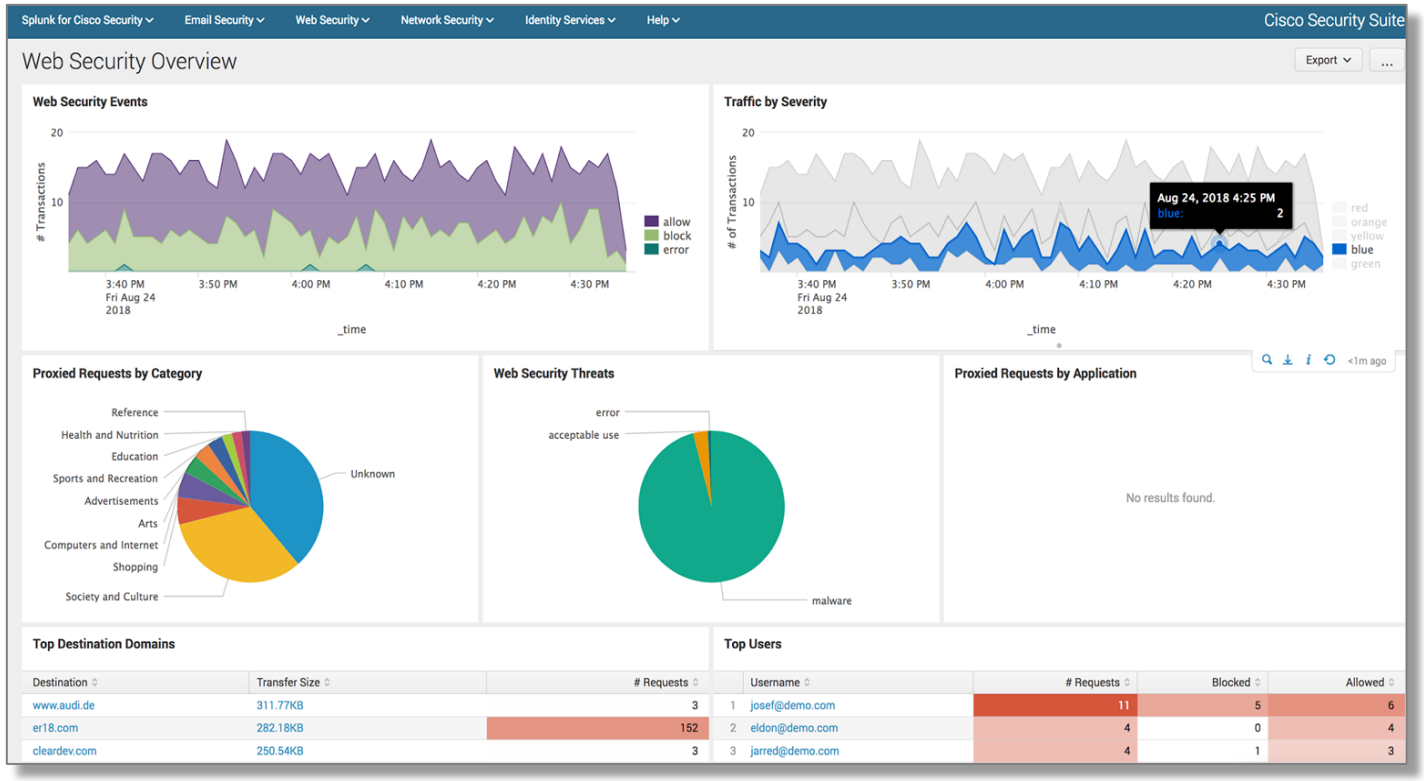
- Sometimes the Chart isn't pretty but the search is….
  - Access abuse
  - Potential compromise
  - Superman effect

splunk> .conf18

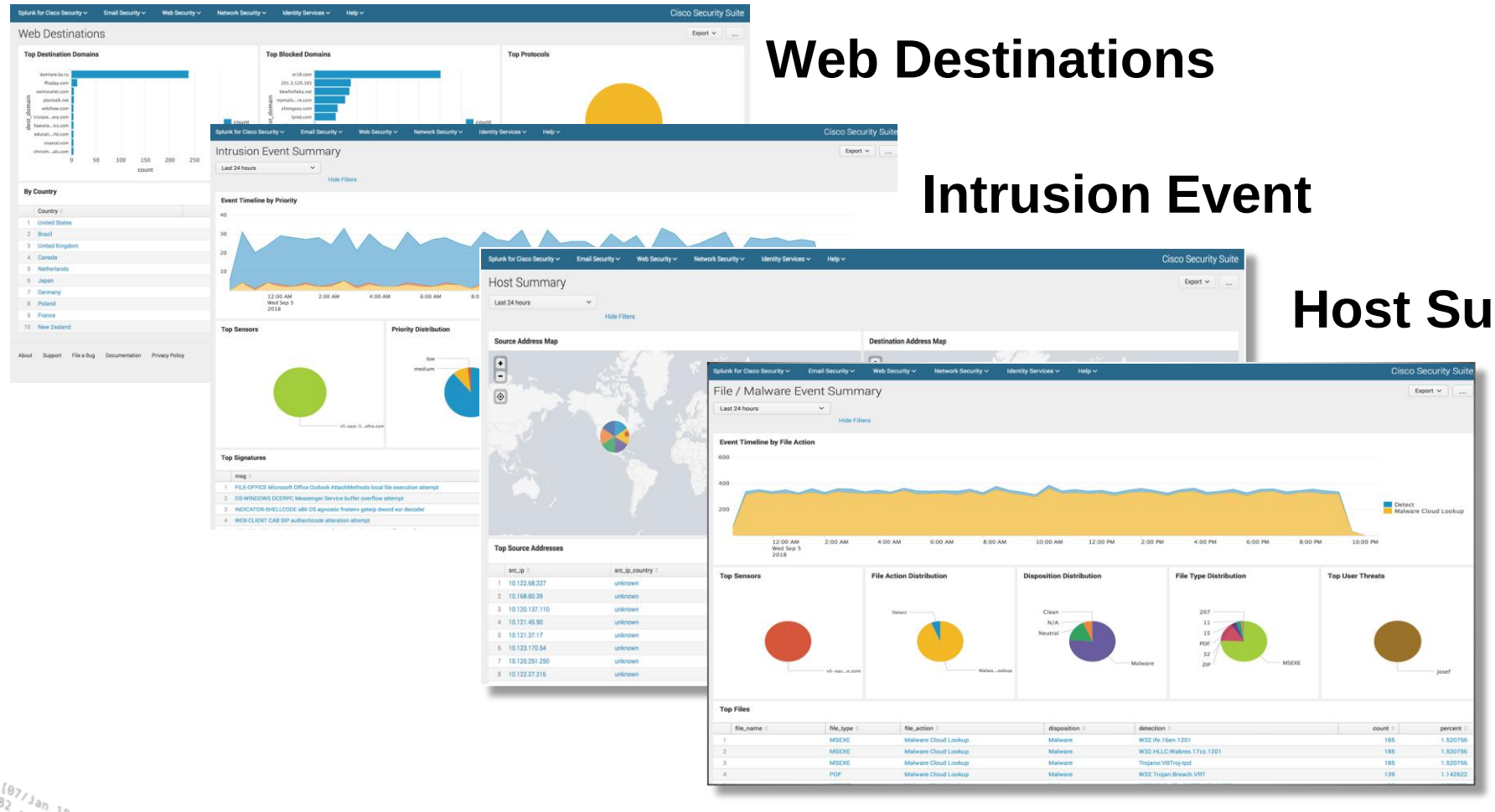
Splunk for Cisco Suite

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!



Web Destinations

Intrusion Event

Host Summary

Malware Event Summary

splunk> .conf18

Security for Palo Alto

splunk> .conf18

Splunk for Palo Alto Networks

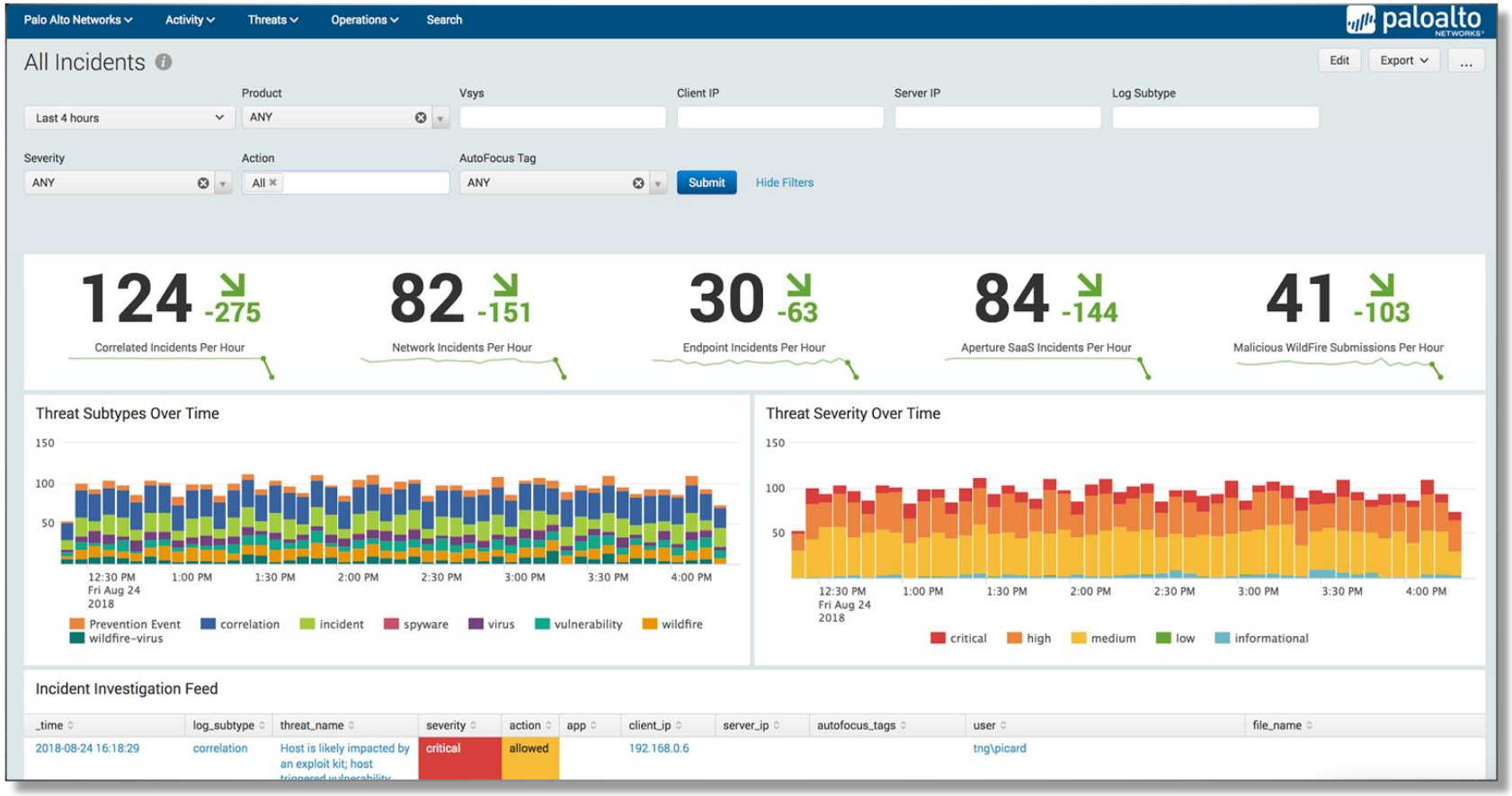
Pre-Built Searches, Reports, and Dashboards for Detailed Analysis

- **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> .conf18

Splunk for Palo Alto

PAN: Overall Posture

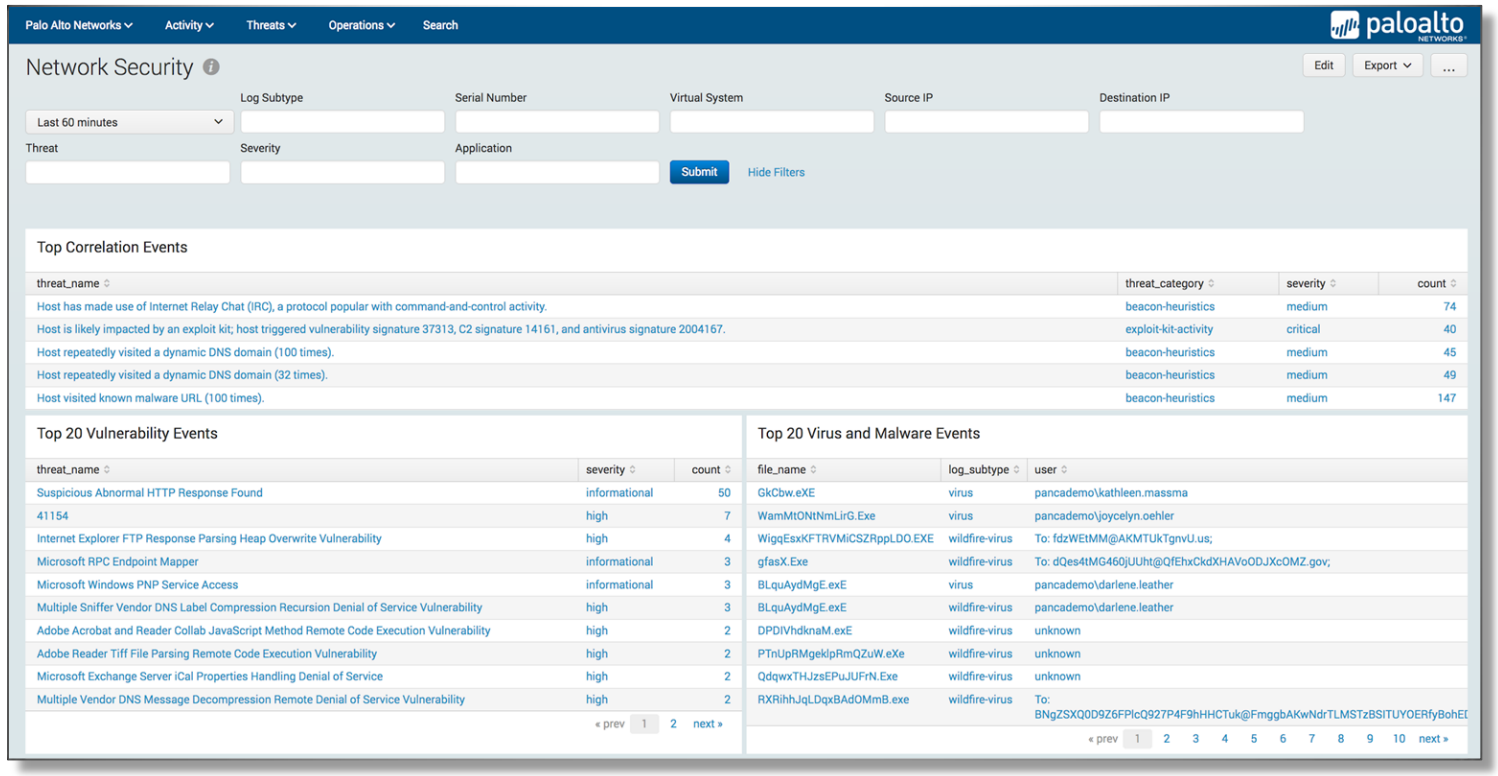


This should look familiar!!

splunk> .conf18

Splunk for Palo Alto

PAN: Network Security

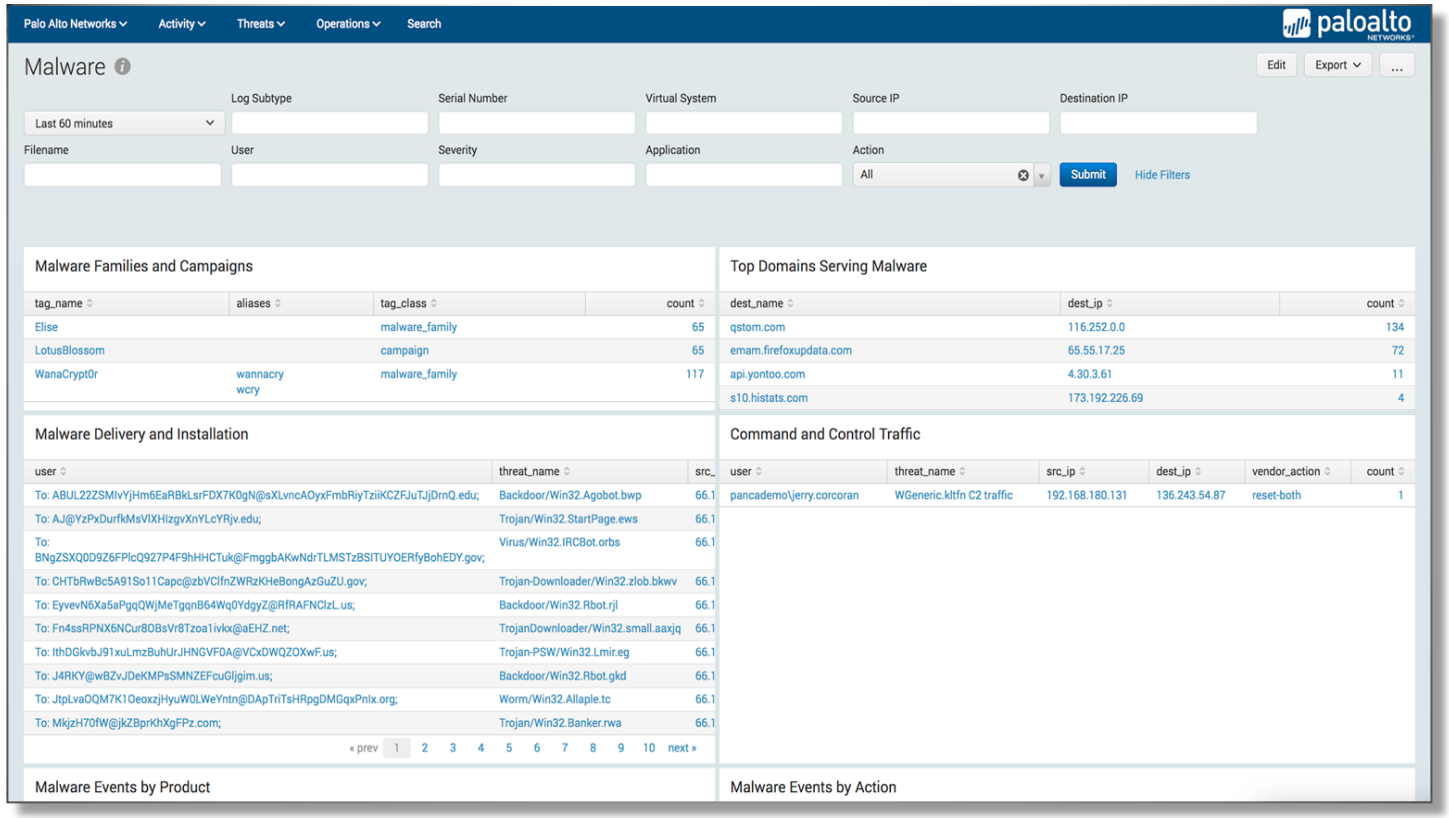


- Let's You know what your firewall thinks looks off
- Initial indication of what needs to be addressed by security engineer
- Great feed into splunk!

Splunk for Palo Alto

PAN: Malware

- Helps stop endpoint attacks before they get started!



splunk> .conf18

So Many Vendors

So Many Great Apps!

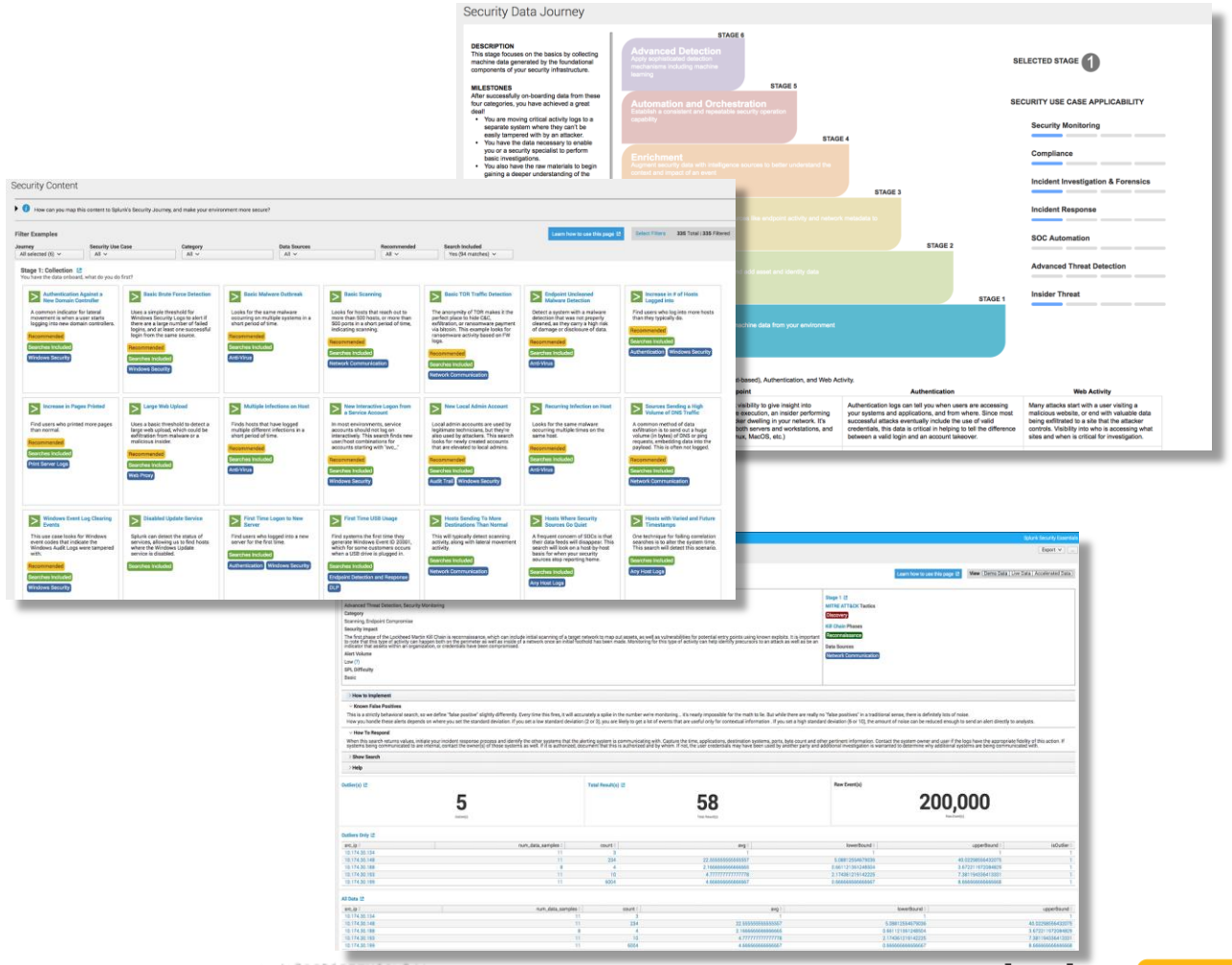
Ping Identity
Microsoft
Booz | Allen | Hamilton
DELL EMC
OPTIV
slack
Check Point SOFTWARE TECHNOLOGIES LTD
Symantec
FORTINET
Jenkins
proofpoint
CROWDSTRIKE
TREND MICRO
CISCO
Carbon Black.
amazon.com
JUNIPER NETWORKS
CYLANCE
paloalto NETWORKS

Better than a car…

Splunk for Security Essentials

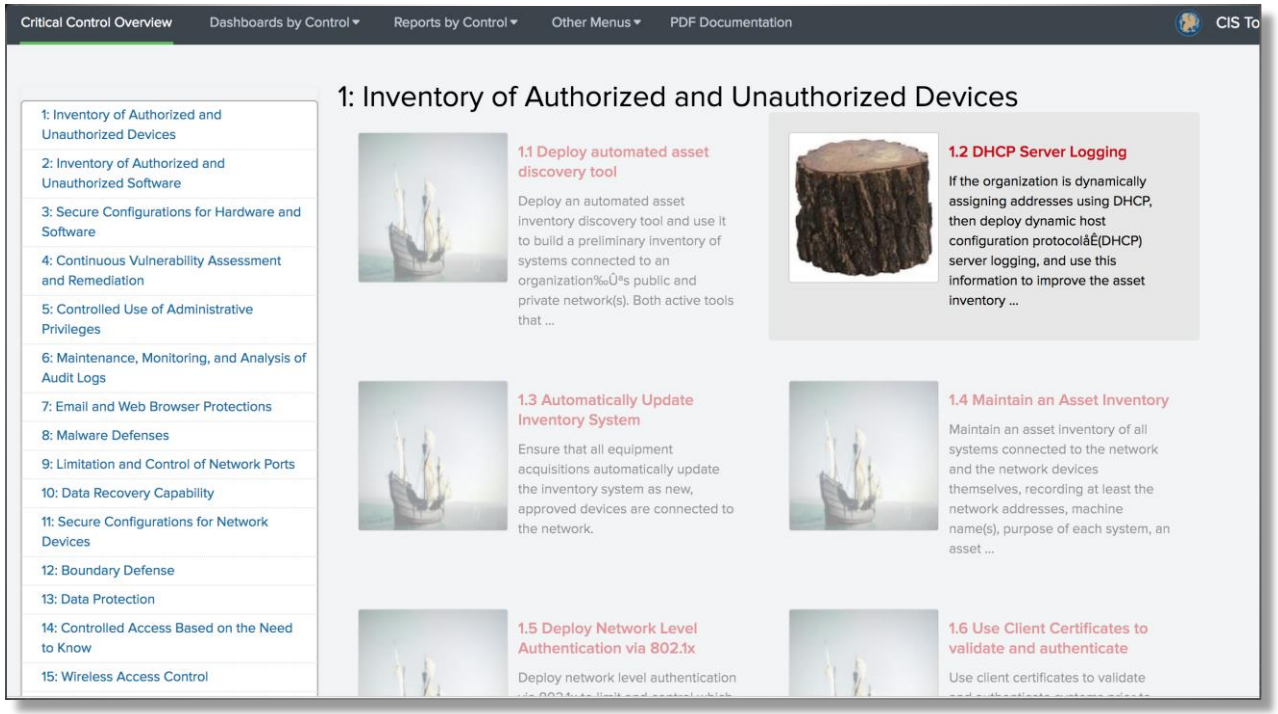
Free Security Learning Guide

- **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



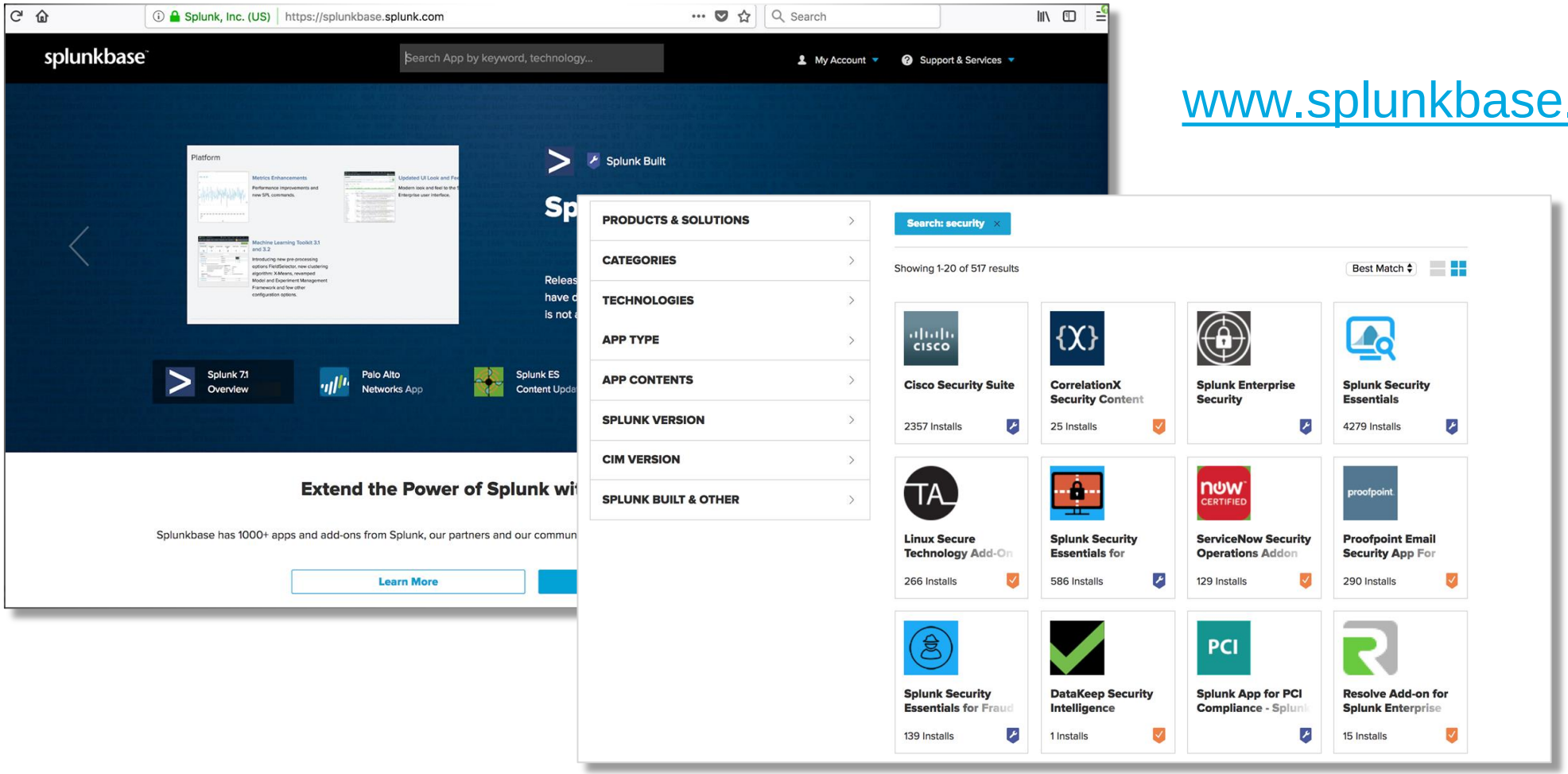
splunk> .conf18

Top 20 Security Controls



- **Extensible framework fore 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?



www.splunkbase.com

splunk> .conf18

Thank You!

splunk> .conf18