# How to Use Splunk for Automated Regulatory Compliance


Joe Goldberg

Product Marketing, Splunk

John Stoner

Federal Security Strategist, Splunk


# Disclaimer

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 the 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.

# Personal introduction

- Joe Goldberg
  - Product marketing for compliance, cybersecurity, anti-fraud
  - 4.5 years at Splunk
  - Previously Symantec, VMware, Sun

- John Stoner
  - Federal Security Strategist
  - 1.5 years at Splunk
  - Formerly HP Enterprise Security (ArcSight), Symantec

# Questions for You—Show of Hands

- Which of these words is in your title/department?
  - Audit or compliance
  - Security

- Who needs to comply with
  - PCI
  - HIPAA
  - FISMA
  - NERC
  - SOX
  - GLBA

# Agenda

- Compliance 101
- Splunk for Compliance, use cases, case studies
- Demos
- Technical Best Practices

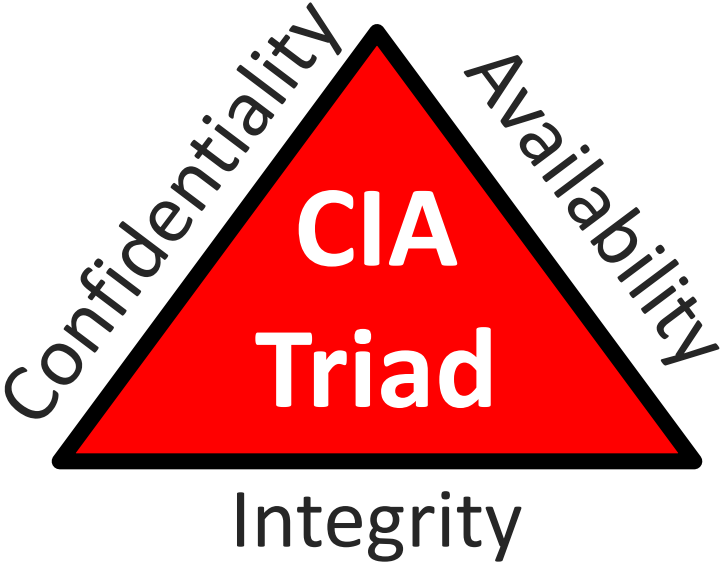
# Compliance 101

# Goal of Compliance: Protect Information/Systems

***All Three Often Covered in A Single Regulation/Framework***

**Private/Not Stolen**

- Credit cards (PCI)
- Personal data
  (GLBA, GDPR, FISMA, RMF)
- Healthcare info (HIPAA)
- Intellectual property




**Accessible/Reliable**

- Electric grid (NERC)
- Processing systems (GDPR)
- Critical systems (FISMA, RMF)

**Accurate/Unchanged**

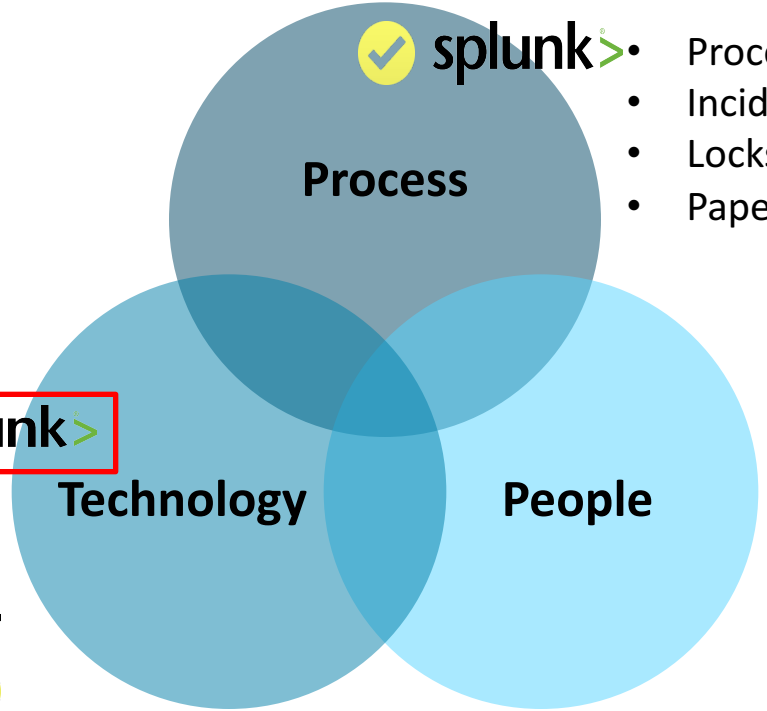
- Financial statements (SoX)
- Personal data (FISMA, RMF, GDPR)
- Healthcare info (HIPAA)

# Controls: How to Protect

***Splunk Enables Compliance; Not = Compliance***

## Non-technical Controls

- Process to detect/respond threats
- Incident response process
- Locks on cabinets and doors
- Paper policies



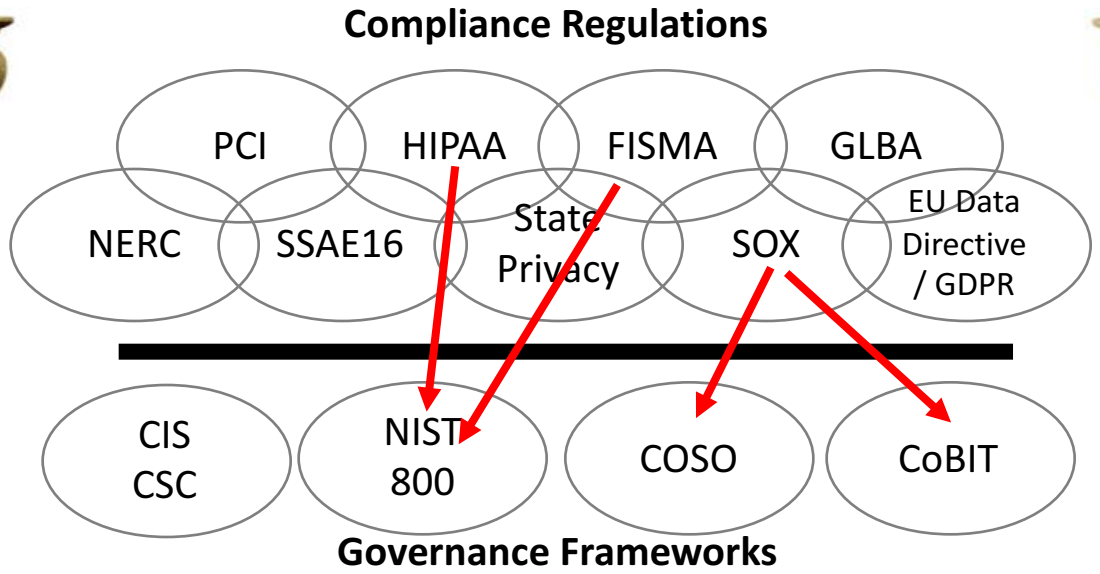

## Technical Controls

- Logging/SIEM
- Strong passwords
- Anti-virus
- Encryption
- Segmented network
- Backup machines

- Must have Compliance officer
- Must have IT Security team

# Compliance Regulations and Frameworks

- Many regulations to comply with & often overlap. Ideally 1 solution for all.
- Often vague & a framework is used




# Splunk for Compliance

# Solution: Splunk, the Platform for Machine Data


Splunk Can Complement OR Replace an Existing SIEM


**Logging / Investigate** | **Compliance Reporting** | **Monitor / Detect**

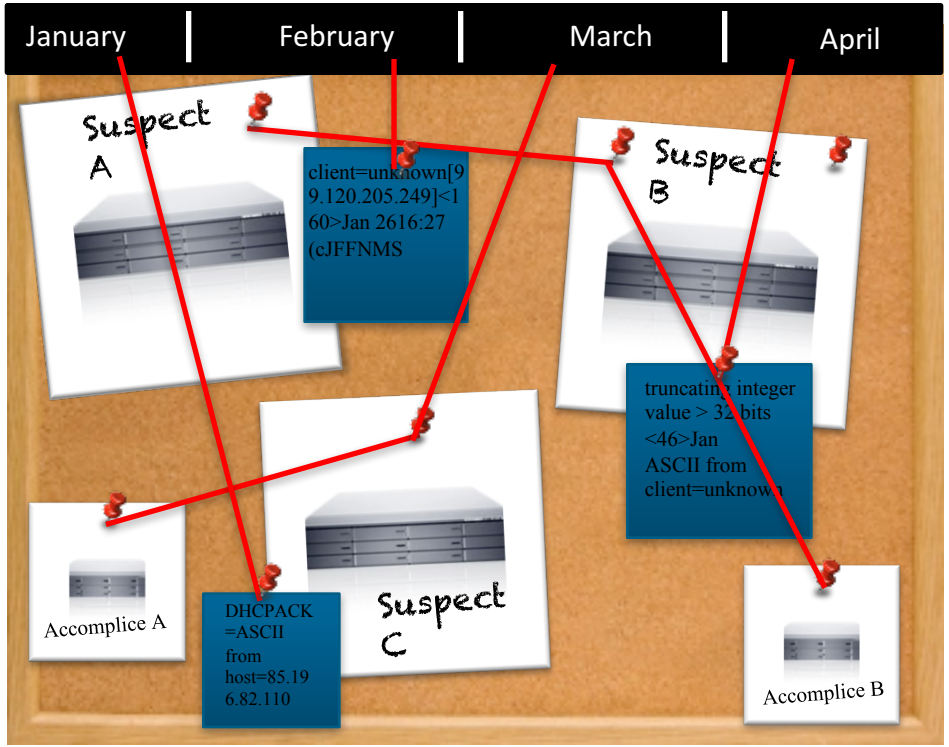
splunk>

**External Lookups**


**Assets** | **Employees** | **Networks** | **Applications**

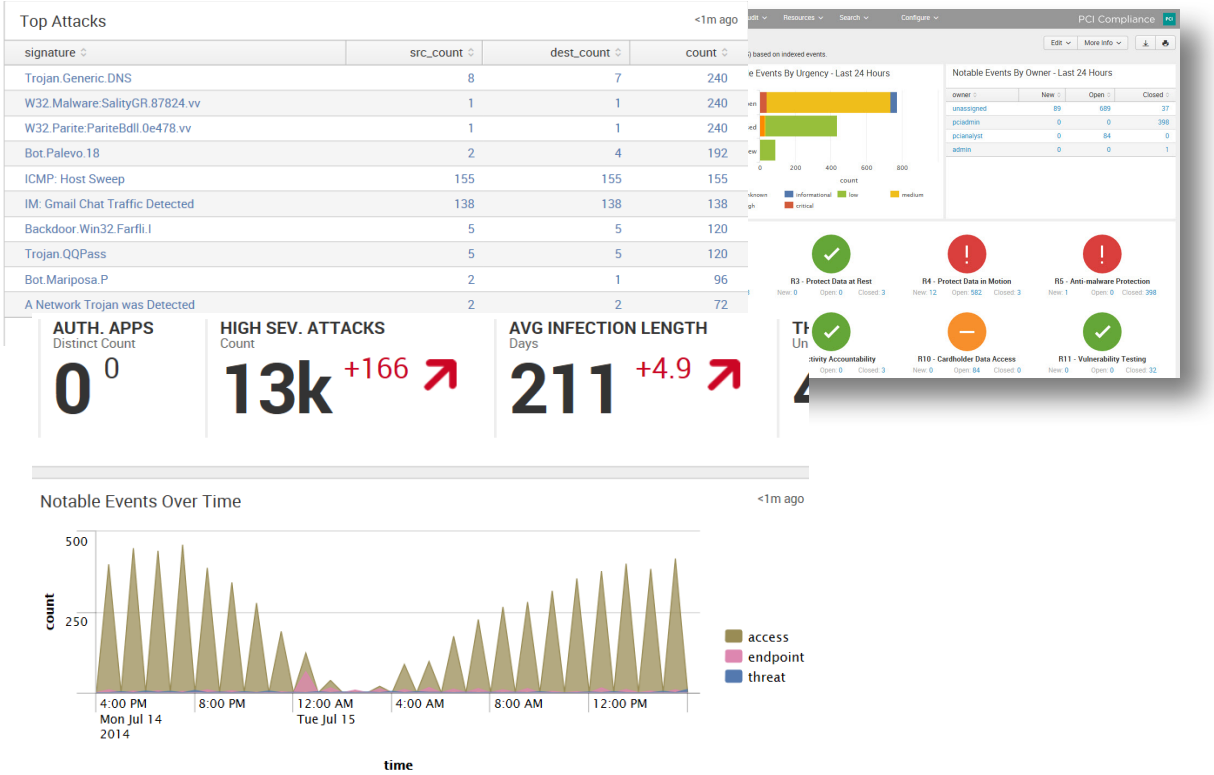
# Use Case 1 – Logging / Investigate

- Centralized logging to meet compliance requirements
- Investigate security threats or data loss
- Need all the original data and fast way to pivot through it



# Use Case 2 – Compliance and Security Reporting

- Show auditors compliance against technical controls
- Many types of visualizations



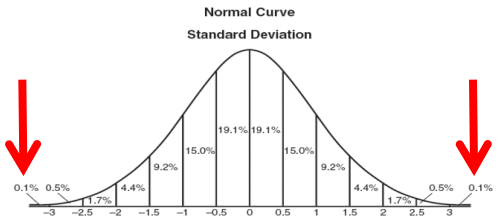
# Use Case 3 - Monitoring / Detection

Many regulations require "continuous monitoring"

1. Correlations/patterns

*A AND B NOT C = THREAT*

2. Anomalies/outliers off baseline



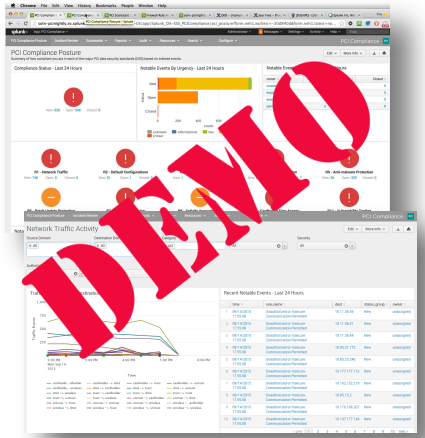

3. Risk scoring

| Asset Risk Scoring | | | | |
|---|---|---|---|---|
| Asset | IPS risk score | AV risk score | Threat Intel | Total |
| Server 12 | 0 | 2 | 0 | **2** |
| Server 8 | 6 | 9 | 20 | **35** |
| Endpoint 35 | 1 | 3 | 1 | **5** |

- Combine 1-3
- Alerts; Optionally can initiate automated remediation

# Splunk for Compliance Offerings

## Splunk App for PCI Compliance




## Splunk Enterprise Security


## Other key apps

CIS CSC App for Splunk (SE)

Qmulos Enterprise Compliance (NIST/FISMA, partner)

HIPAA Privacy & Security (partner)

DEMO

## Splunk User Behavior Analytics


splunk>enterprise

splunk>light

# Splunk Spanning 5+ Regulations


- Ohio State Univ: 63k+ students, 32k+ employees, 14 colleges
- FERPA, HIPAA, PCI, FISMA, GLBA
- Very diverse, heterogeneous IT infrastructure
- Centralized logging of all security events for compliance and security
- Retain 700GB/day from thousands of sources for 92 days


- FIS: 30k+ employees, technology provider to banking industry.
- FFIEC, GLBA, SOX, PCI, SSAE 16. All require log monitoring.
- Prior solutions were cumbersome and not very useful
- With Splunk, advanced investigations, many reports & dashboards, proactive monitoring & alerting
- Splunk used for IT Ops, App Dev, capacity planning

# PCI, HIPAA and Security/IT Ops


- **The old way:** Slow, manual, inefficient process
  - One of the world's largest food & drug retailers with 1600+ stores and 185k+ employees
  - Much of the information needed for compliance was missing
  - Manual correlation of data across thousands of machines and servers
  - Too many tools deployed in their environment

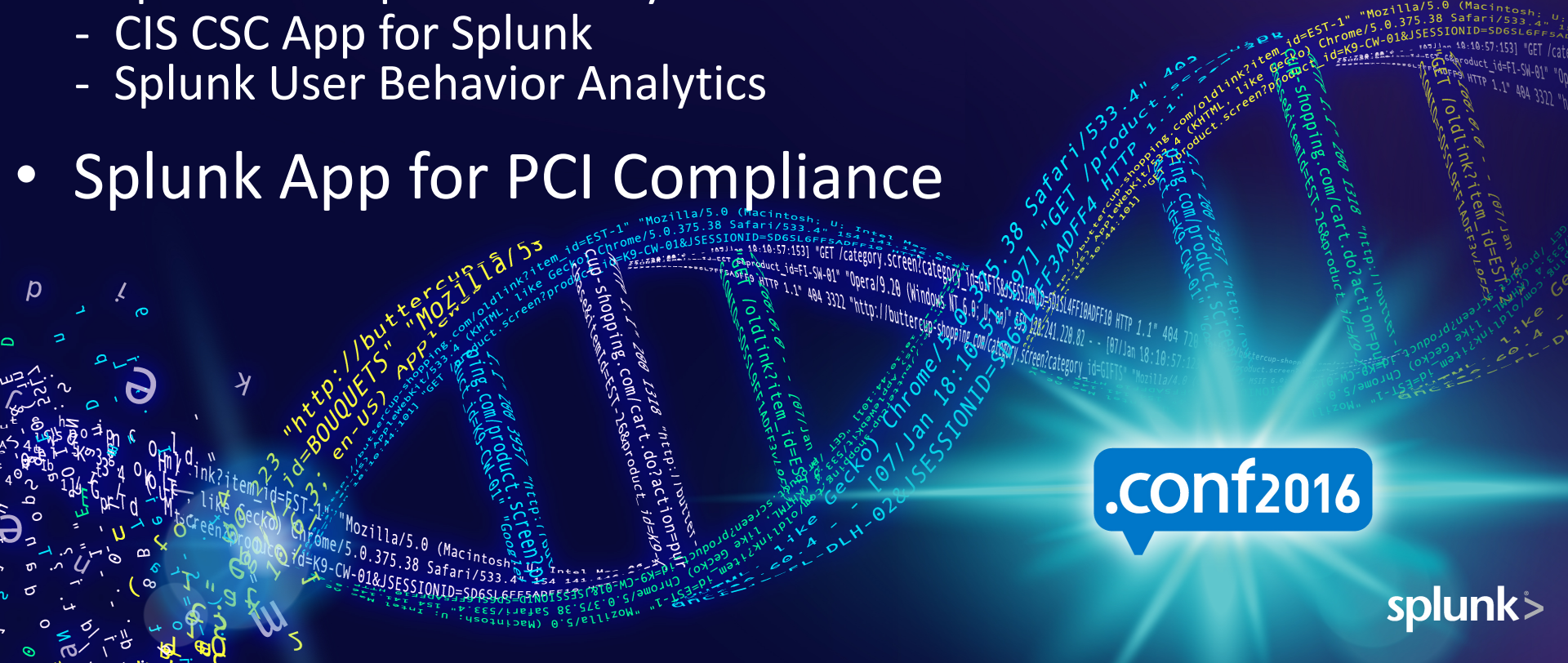
- **The Splunk way:** Better compliance, security, and operational efficiencies
  - Centralized logging of all required machine data and full visibility
  - Retain 300GB/day from 10k+ sources for 90 days
  - Fast searching, reporting, and analytics
  - Was able to retire multiple SIEMs
  - Use Splunk for security, IT ops, and business analytics

# Case Studies in Appendix


Cover HIPAA, NERC, SOX, ISO, SSAE 16

# Demos

- CIS Critical Security Controls mapped to:
  - Splunk Enterprise Security
  - CIS CSC App for Splunk
  - Splunk User Behavior Analytics
- Splunk App for PCI Compliance



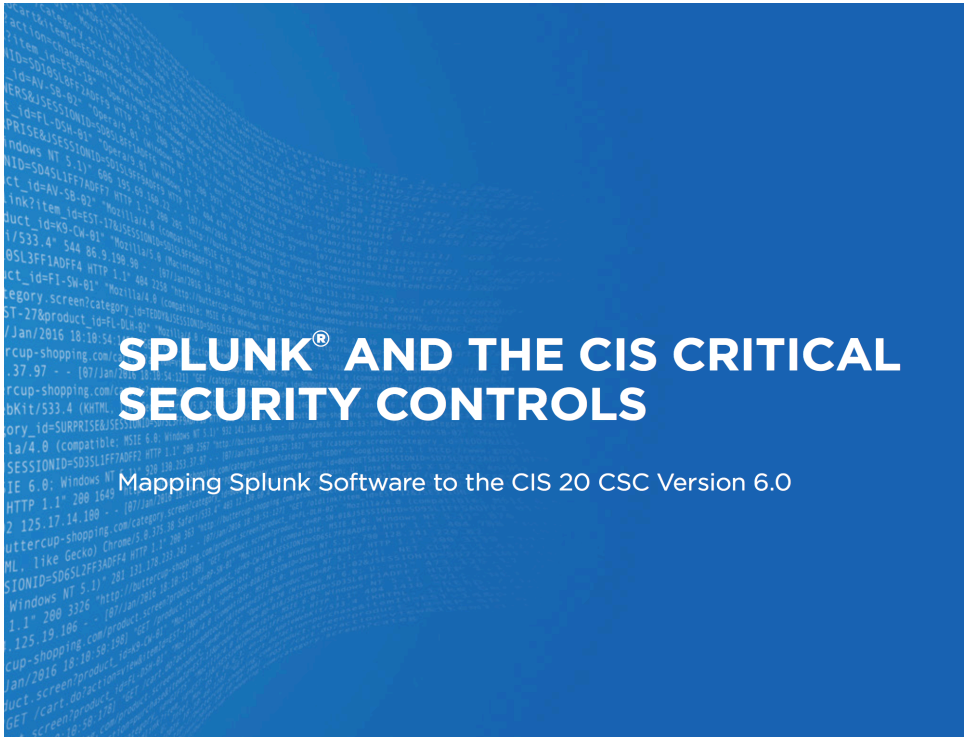
# Demo Time


Recorded demos of Splunk Enterprise Security and Splunk App for PCI Compliance:
Splunk.com > Videos > Apps

# Critical Security Controls: Formerly SANS 20

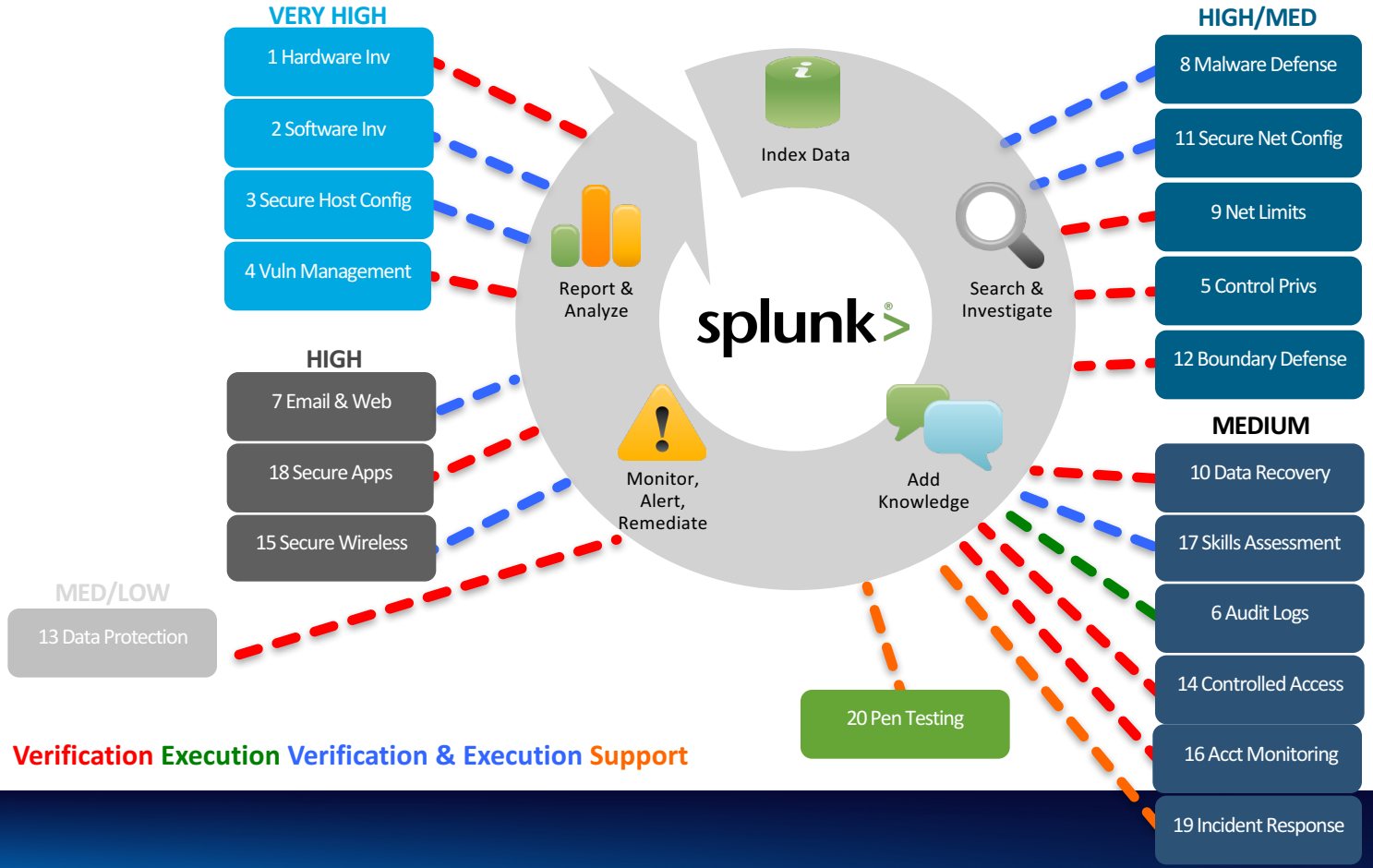
- Formerly maintained by NSA, consortium+SANS, and now Center for Internet Security (CIS)
- Why good?
  - Covers people, process, technology
  - Covers overall IT Security (not just specific industry or type of sensitive data)
  - Very specific/prescriptive and focuses on most critical controls
  - Real-world practitioners and the private sector helped write it
  - Kept up-to-date with the changing times!
- A great starting point for customer who is clueless about what they need to do for IT security or compliance

# We wrote a book…




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

# Splunk Helps You Meet All 20 of the CIS CSC



# Technical Best Practices

.conf2016

splunk>

# Splunk Best Practices Specific to Compliance

- Work closely with audit before starting
  - Measureable in machine data? > Determine data source > Write search/alert/report
  - Measure processes? (reviewing reports, closing incidents, etc)
- Data enrichment
  - External lookups of asset, identity and network information
  - Why? Narrow down searches and reports to in-scope, high-criticality employees/assets, etc
- Put text description of the control(s) at the top of the dashboard

# Splunk Best Practices Specific to Compliance cont.

- Use RBAC to control who can see/do what with machine data
- Configure data retention time per index for compliance requirements
- Consider a TSIDX retention policy to reduce storage space 33-66%
- Run searches on indexed data to ensure no PII or sensitive info
- Use data integrity control feature if data integrity is required

# Other Splunk Best Practices

- Use Tech Add-Ons on Splunkbase
- Try to use the Common Information Model
- Modularize components
  - Saved searches, macros, event types, tags
  - Why? Re-use (overlapping controls) and changes only made in one place

# Other Splunk Best Practices cont.

*For speed and scale use:*

- Scheduled searches
- Data summarization esp if search covers long time periods:
  - Report acceleration
  - Summary indexes
  - Data model acceleration (High Performance Analytics Store (HPAS)/TSIDX files))
- Key-Value (KV) Store
- See session PPT: David Veuve – How to Scale: _raw to tstats

For detail use Google: Splunk Docs & other info

# Popular Compliance Search

- *Detect when critical system stops sending logs > 60 min*

- Detail at Splunk.com > Solutions > Security, Compliance & Fraud > Security and Fraud Use Cases

1. Create Lookup File

A1 | Host_name

| | A | B | C | D |
|---|---|---|---|---|
| 1 | Host_name | | | |
| 2 | Server1 | | | |
| 3 | Server2 | | | |
| 4 | Firewall1 | | | |
| 5 | Activedirectory1 | | | |
| 6 | Datalossprevention1 | | | |
| 7 | | | | |

# Popular Compliance Search cont…

2. Add Lookup definition

## Add new

Lookups » Lookup definitions » Add new

Destination app *

search

Name *

critical_systems

Type *

File-based

Lookup file *

critical_systems

*Create and manage lookup table files.*

☐ Configure time-based lookup

☐ Advanced options

Cancel

Save

# Popular Compliance Search cont…

## 3. Search

```
| metadata type=hosts index=criticalsystems
| lookup critical_systems Host_name as host OUTPUT Host_name as host
| search host=*
|eval last60=relative_time(now(),”-60m@m")
```

## 4. Visualize

```
| convert ctime(lastTime) as LastTimeLogged
| where lastTime < last60
| table host, LastTimeLogged
| sort –LastTimeLogged
```

# Takeaways

- Log mgmt and review is typically required (Splunk!)
- Splunk enables faster, better, cheaper compliance
- Splunk is a single platform to help across multiple regulations

# What Now?

- App Showcase: “Splunk for Compliance & Anti-Fraud” booth
- Session: “Avoid Fines and Save Money! Automating Regulatory Compliance with Qmulos” Thurs, 2:35-3:20 PM
- Web site: Information, Solution Guide, CIS book, demo
  - Splunk.com > Solutions > Security, Compliance and Fraud > Compliance
- Contact sales team at Splunk.com > Contact Us

# Q&A

# THANK YOU


splunk>

# Appendix

.conf2016

splunk>

# External Compliance Regulations

| Reg | Type | Who Applies To | Protects | How | Penalties |
|---|---|---|---|---|---|
| **PCI** | Industry, Global | Every financial services firm, retailer, or service provider who issues, accepts, captures, stores, transmits, or processes credit card data | • Credit cardholder information<br>• Ex: CCN, magnetic stripe data | • 12 broad technical requirements, each with sub-reqs<br>• The most IT-specific regulation | • Fines up to $500k/violation<br>• Suspension of credit card capabilities<br>• Varies by brand |
| **HIPAA** | Govt, US | Any healthcare provider, hospital, company, or government agency that stores, manages or communicates any employee health related information | • Protected Health Information (PHI)<br>• Ex: medical records number, medical diagnosis of a condition, procedure codes on claim forms | • The "Security Rule" gives guidance<br>• Recommend NIST 800-66 | • Fines up to $1.5M per year per provision<br>• Possible criminal prosecution by DOJ |
| **GLBA** | Govt, US | Any company that provides a range of financial products and services to consumers (banks, brokerages, insurance, etc) | • Consumer's Personally Identifiable Information (PII)<br>• Examples: Full name, SSN, date & place of birth, drivers license | • The "Safeguards Rule" section of the Act<br>• ISO 27002 is often starting point | • Enforced by multiple federal agencies<br>• DOJ fine up to $100k per violation |
| **FISMA** | Govt, US | Federal agencies or any external agencies or contractors working on their behalf | Federal information and information systems | • NIST standards (esp 800 series). Also DIST and FIPS.<br>• Little of reg is directly applicable to IT | • Censure by Congress<br>• Negative publicity<br>• Reduced federal funding |

# External Compliance Regulations cont.

| Reg | Type | Who Applies To | Protects | How | Penalties |
|---|---|---|---|---|---|
| **Sarbanes-Oxley** | Govt, US | Publicly-traded company on U.S stock exchange | The accuracy and integrity of financial statements | • Few IT specifics. Sections 302 and 404 (internal system controls) are interpreted to apply to IT.<br>• Law does call out "timely monitoring and response" to issues and auditing access<br>• Many orgs use COBIT, COSO, and SAS 70 | • SEC fines up to $5M per person and higher per firm<br>• Imprisonment up to 20 years<br>• Loss of exchange listing |
| **NERC** | Industry, US / Canada | All electrical utilities in the U.S. and several provinces in Canada | The electrical grid | • Critical Infrastructure Protection (CIP) section of the standards | • NERC penalties up to $1M a day<br>• Must submit a mitigation plan and execute it |
| **EU Data Protection Directive / GDPR** | Govt, EU | All organizations doing business in the EU | Consumer privacy and Personally Identifiable Information (PII) | • Few IT specifics<br>• GDPR replaces EU Data Directive in ~2 yrs<br>• Articles on data security and breach notification | • GDPR: Fines up to greater of 4% of company's turnover or $20M EUR |

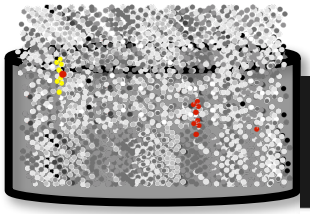
**Other US regs:** State Data Privacy laws (over 35 states), FERPA (student education records), OCC/OTS (banking)

# Frameworks / Standards

| | |
|---|---|
| **NIST 800** | Written by US govt, it is guidance on security topics to comply with FISMA. 9 steps. Also HIPAA guidance. |
| **COBIT** | Intl IT governance framework that emphasizes regulatory compliance. Written by ISACA. |
| **ISO 27000** | Intl best-practice recommendations on information security management. 12 sections. |
| **ITIL** | Intl set of concepts and best practices for IT service mgmt, dev, ops. Security based on ISO 27001. |
| **CIS Critical Security Controls** | Intl, independent list of top 20 security controls for effective cyber defense. Formerly SANS 20. |
| **SSAE 16** | U.S./AICPA guidance to auditors when assessing internal controls of a service/outsourcing organization. Type I and II. |
| **COSO** | Intl frameworks and guidance on enterprise risk management, internal control and fraud deterrence |
| **HITRUST CSF** | U.S. security framework for the healthcare industry. Leverages other regs/standards like HIPAA, NIST, ISO, PCI, COBIT. |

# Splunk Benefits vs Traditional SIEMs

*Better, faster, cheaper compliance*



Index any type of machine data from any source

All original/raw data indexed and searchable

eports), deep

time monitoring.

Extends into many use cases for strong ROI & improved collaboration

siliconANGLE

Cloud Mobile Social Big Data

## New Splunk release slashes machine data storage costs by up to 80 percent

by Maria Deutscher | Apr 5, 2016 | 0 comments

# Splunk Compliance/Security Use Cases

Splunk Can Complement OR Replace an Existing SIEM

Logging/
Ad-hoc Search/
Investigations

Compliance &
Security
Reporting

Monitoring/
Detection/
Alerting
(continuous monitoring)

splunk>

# Use Case 4 – Find Advanced, Hidden Threats

## *Sources*

## *Example Correlation - Spearphishing*

**Email Server**

2013-08-09T12:40:25.475Z,,exch-hub-den-01,,exch-mbx-cup-00,,,STOREDRIVER,DELIVER,79426,<20130809050115.18154.11234@acme.com>,johndoe@acme.com,685191,1,,,hacker@neverseenbefore.com, Please open this attachment with payroll information,, ,2013-08-

User Name

Rarely seen email domain

**Web Proxy**

Rarely visited web site

201 .29 98483 148 TCP_HIT 200 200 0 622 - - OBSERVED GET www.neverbeenseenbefore.com HTTP/1.1 0 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.1; MS-RTC LM 8; .NET CLR 1.1.4322; .NET CLR 3.0.4506.2152; ) User John Doe"

User Name

**Endpoint Logs**

User Name

08/09/2013 1 ent_status="(0)The operation completed successfully. "pid=1300 process_image="\John Doe\Device\HarddiskVolume1\Windows\System32\neverseenbefore.exe" registry_type="CreateKey"key_path="\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Printers Print\Providers\ John Doe-PC\Printers\{}\ NeverSeenbefore" data_type"

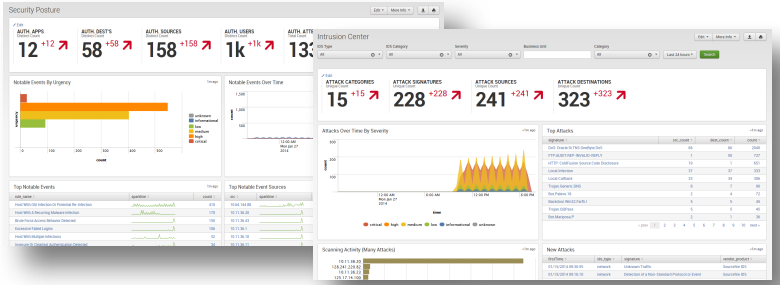
Rarely seen service

**Time Range**

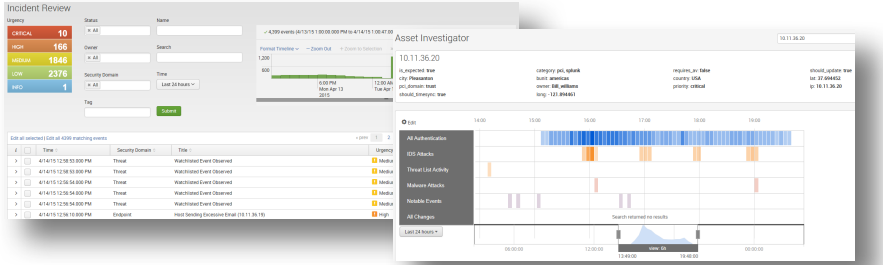
All three occurring within a 24-hour period

# Splunk App for Enterprise Security

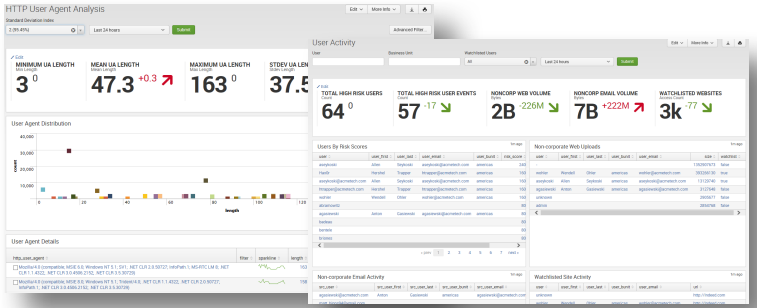
## Pre-built searches, alerts, reports, dashboards, workflow, and more



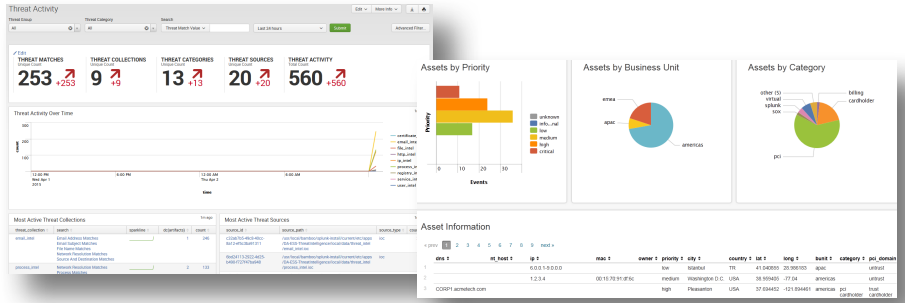

Alerts & Dashboards & Reports




Incident Investigations & Management



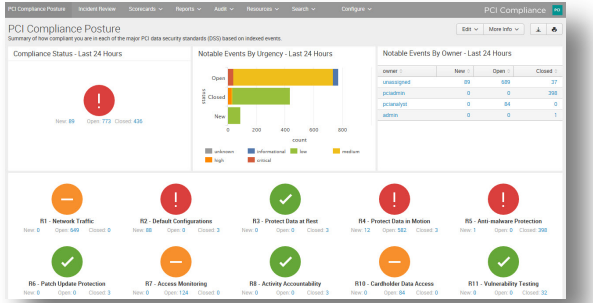

Statistical Outliers & Risk Scoring & User Activity



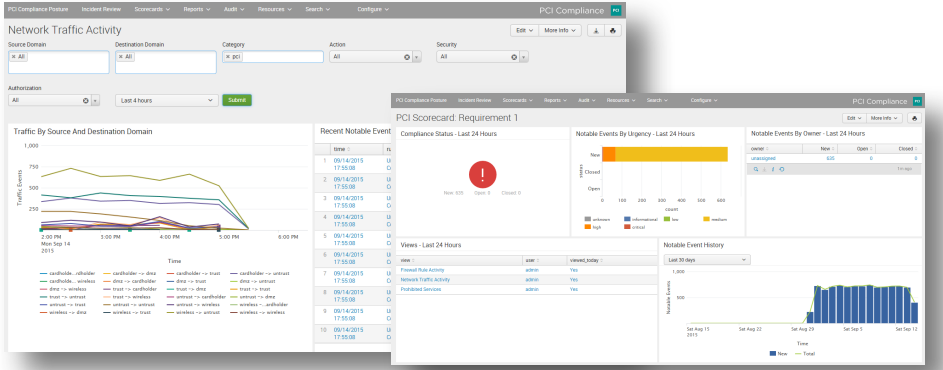

Threat Intel & Asset & Identity Integration

# Splunk App for PCI Compliance

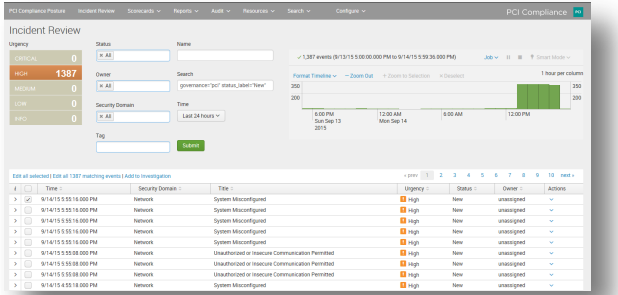
## Pre-built searches, alerts, reports, dashboards, workflow, and more

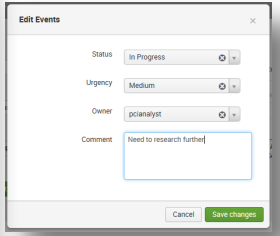



Compliance Overview

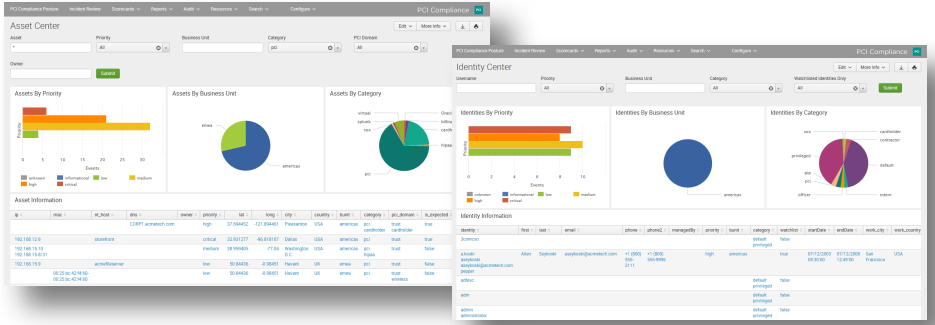



Scorecards and Reports




Incident Review and Management




Asset and Identity Aware

# Splunk Enterprise Security (ES) Helps. Big Time.

ES **Splunk Enterprise Security** DOWNLOAD

ADMINISTRATOR TOOLS: View App | View Analytics

OVERVIEW | DETAILS

Splunk Enterprise Security gives teams the insight to quickly detect and respond to internal and external attacks, to simplify threat management while minimizing risk. ES helps teams gain organization-wide visibility and security intelligence for continuous monitoring, incident response, SOC operations, and providing executives a window into business risk.

- Continuously Monitor: get a clear picture of security posture using pre-defined dashboards, key security and performance indicators, static & dynamic thresholds, and trending indicators
- Prioritize and Act: optimize incident response workflows with alerts, centralized logs, and pre-defined reports and correlations
- Conduct Rapid Investigations: use ad-hoc search and static, dynamic and visual correlations to detect malicious activities
- Handle Multi-step Investigations: trace activities associated with compromised systems and apply the kill-chain methodology to see the attack lifecycle

Splunk ES is a premium security solution requiring a paid license

Security Posture | Incident Review | Predictive Analytics | Event Investigators | Advanced Threat | Enterprise Security

Security Domains | Audit | Search | Configure

Security Posture — Edit | More Info

| INFECTED SYSTEMS (Percent) | AUTH. USERS (Distinct Count) | TOTAL INFECTIONS (Count) | TRAFFIC SOURCES (Unique Count) |
|---|---|---|---|
| 137 % -3.4 | 2k +136 | 126 -5 | 5k -267 |

SPLUNK CERTIFIED What's this?

72 ratings

Rate this app

Subscribe

Share this app

VERSION 4.1.1

Security, Fraud & Compliance

Splunk Enterprise

Splunk Cloud

App

Splunk 6.4, 6.3

Inputs

CIM 4.4

Splunk Software License Agreement

Platform Independent

SPLUNK SUPPORTED

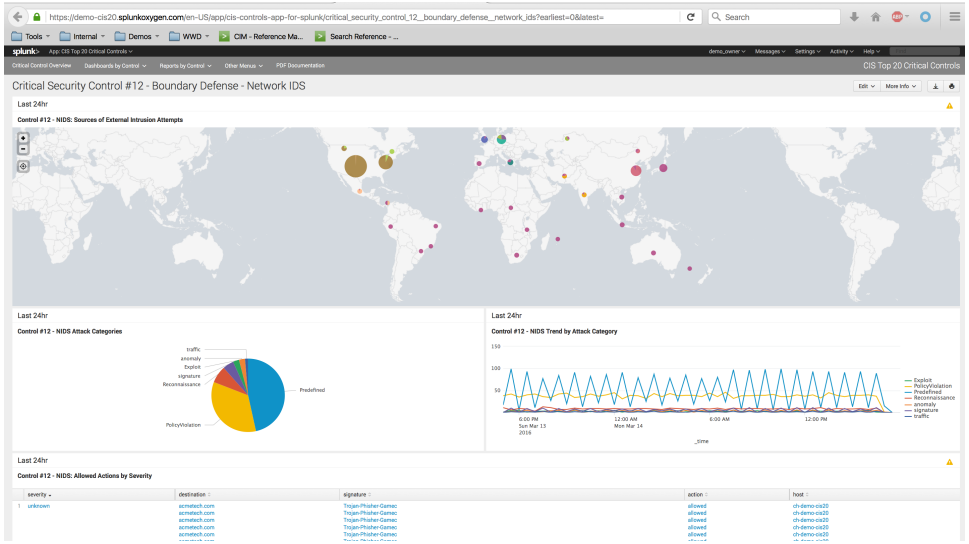
Questions on SplunkAnswers

File a case

Flag as inappropriate

BUILT BY SPLUNK INC.

# We have a free app for CIS

# PCI DSS v3.1: 12 Main Requirements

*Splunk directly does #10. Measures #1-8 and #10-11*

| | | |
|---|---|---|
| **Build and Maintain a Secure Network and Systems** | **1.** | Install and maintain a firewall configuration to protect cardholder data |
| | **2.** | Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | **3.** | Protect stored cardholder data |
| | **4.** | Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | **5.** | Protect all systems against malware and regularly update anti-virus software or programs |
| | **6.** | Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | **7.** | Restrict access to cardholder data by business need to know |
| | **8.** | Identify and authenticate access to system components |
| | **9.** | Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | **10.** | Track and monitor all access to network resources and cardholder data |
| | **11.** | Regularly test security systems and processes |
| **Maintain an Information Security Policy** | **12.** | Maintain a policy that addresses information security for all personnel |

# Leading Utility Complying with NERC and SOX

*Used compliance controls as driver for purchasing consolidated logging solution and charting advanced correlation*

## Splunk is the unified compliance platform

- Wanted one system for Windows, Linux, Cisco and logs
- Needed holistic view into all data
- With Splunk, easy to import obscure logs, flexible, RBAC
- Replaced multiple tools and reduced contractors needed

# Dignity Health Improves HIPAA Compliance


*"Splunk is the CHW standard for centralized event logging for HIPAA. It is a critical tool for monitoring access to information critical to our business, and most importantly to the privacy of our patients."*

## Splunk closes HIPAA compliance gaps

- Search data to instantly assess reports of ePHI leakage
- Meet HIPAA's explicit log collection and monitoring requirements
- Complete data visibility across systems to respond to patient complaints
- Reduce level of exposure and risk of violations

# Netsmart – ISO and SSAE 16

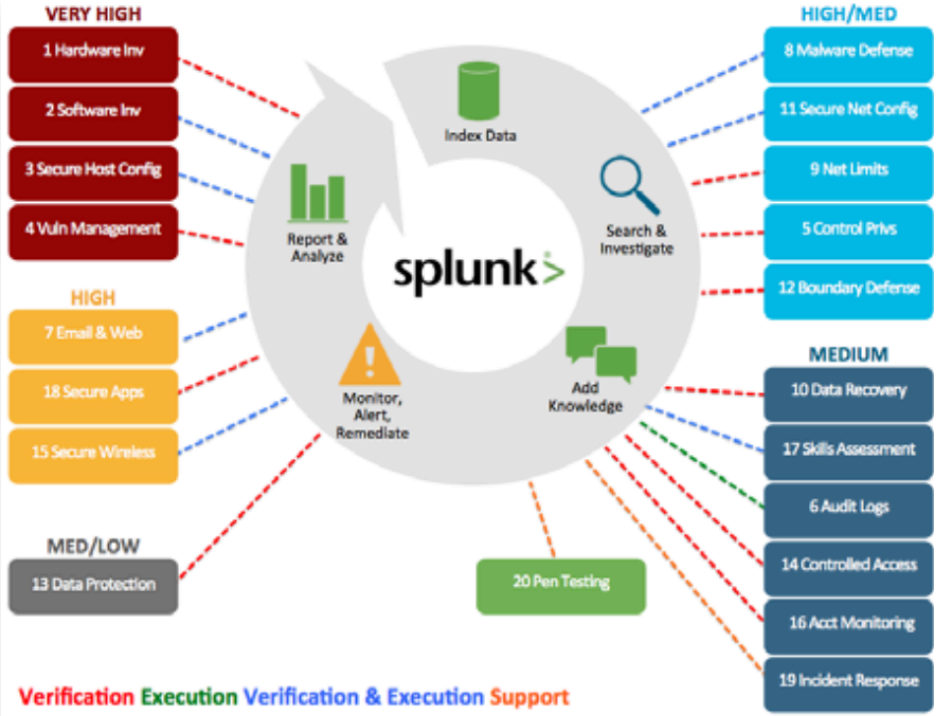

*"Splunk has enabled us to be more proactive in managing our IT environment"*

- Dir. Security & Compliance

- **The old way:** Slow, difficult compliance process
  - Netsmart is a SaaS provider to health care organizations
  - Siloed logs, no unified view, no easy way to investigate incidents or correlate
  - ISO and SSAE 16 compliance reporting was difficult
  - Managing appropriate log access for IT staff was tedious

- **The Splunk way:** Fast ISO and SSAE16 compliance
  - Troubleshooting, incident detection, and reporting requirements correlation, and reporting much faster
  - Use the Splunk App for Enterprise Security to automate ISO compliance
  - Comply with data retention & log review requirements

# Splunk Maps in Four Ways to Compliance




**VERIFICATION:** Ingest data from 3rd party sources, prove you are meeting this control

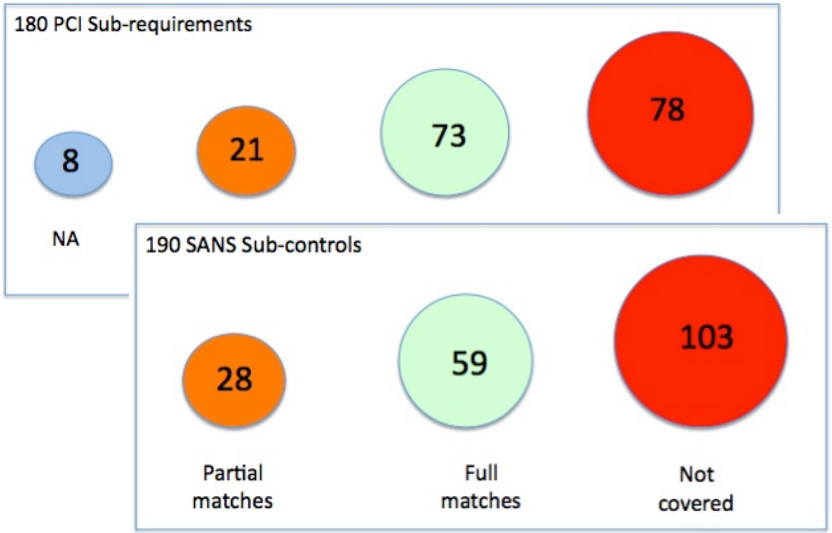
**EXECUTION:** Satisfy the control entirely with Splunk

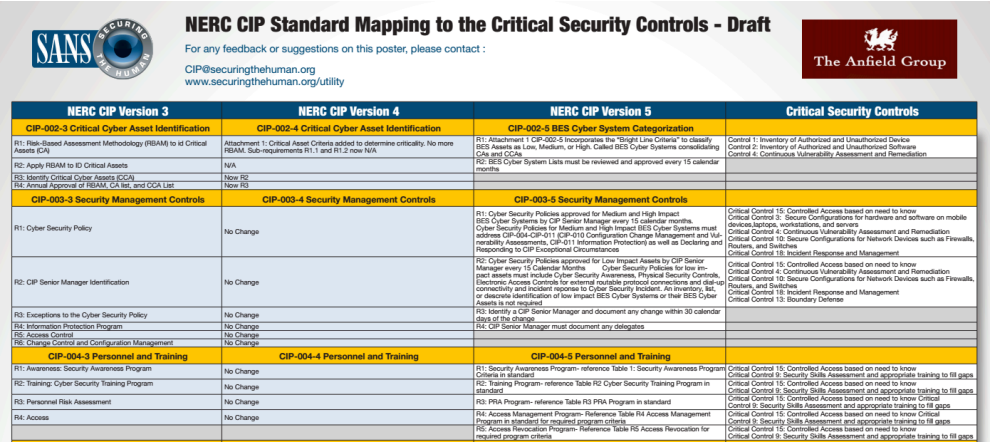
**VERIFICATION/EXECUTION:** Splunk cannot execute entirely, but can do some of it, still need ingest of 3rd party

**SUPPORT:** Usually policy or procedure, Splunk useful tool for staff.

# Can they help me become more “compliant”?

- There’s meaningful overlap. PCI and NERC-CIP are good examples…
- PCI: Malware. Default passwords. Audit logs.
- CIP: Known ports and services. Patch management. Security Event Monitoring.



SANS SECURING THE HUMAN

**NERC CIP Standard Mapping to the Critical Security Controls - Draft**

For any feedback or suggestions on this poster, please contact :

CIP@securingthehuman.org
www.securingthehuman.org/utility

The Anfield Group

| NERC CIP Version 3 | NERC CIP Version 4 | NERC CIP Version 5 | Critical Security Controls |
|---|---|---|---|
| **CIP-002-3 Critical Cyber Asset Identification** | **CIP-002-4 Critical Cyber Asset Identification** | **CIP-002-5 BES Cyber System Categorization** | |
| R1: Risk-Based Assessment Methodology (RBAM) to id Critical Assets (CA) | Attachment 1: Critical Asset Criteria added to determine criticality. No more RBAM. Sub-requirements R1.1 and R1.2 now N/A | R1: Attachment 1 CIP-002-5 Incorporates the “Bright Line Criteria” to classify BES Assets as Low, Medium, or High. Called BES Cyber Systems consolidating CAs and CCAs | Control 1: Inventory of Authorized and Unauthorized Device<br>Control 2: Inventory of Authorized and Unauthorized Software<br>Control 4: Continuous Vulnerability Assessment and Remediation |
| R2: Apply RBAM to ID Critical Assets | N/A | R2: BES Cyber System Lists must be reviewed and approved every 15 calendar months | |
| R3: Identify Critical Cyber Assets (CCA) | Now R2 | | |
| R4: Annual Approval of RBAM, CA list, and CCA List | Now R3 | | |
| **CIP-003-3 Security Management Controls** | **CIP-003-4 Security Management Controls** | **CIP-003-5 Security Management Controls** | |
| R1: Cyber Security Policy | No Change | R1: Cyber Security Policies approved for Medium and High Impact BES Cyber Systems by CIP Senior Manager every 15 calendar months. Cyber Security Policies for Medium and High Impact BES Cyber Systems must address CIP-004-CIP-011 (CIP-010 Configuration Change Management and Vulnerability Assessments, CIP-011 Information Protection) as well as Declaring and Responding to CIP Exceptional Circumstances | Critical Control 15: Controlled Access based on need to know<br>Critical Control 3: Secure Configurations for hardware and software on mobile devices,laptops, workstations, and servers<br>Critical Control 4: Continuous Vulnerability Assessment and Remediation<br>Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches<br>Critical Control 18: Incident Response and Management |
| R2: CIP Senior Manager Identification | No Change | R2: Cyber Security Policies approved for Low Impact Assets by CIP Senior Manager every 15 Calendar Months Cyber Security Policies for low impact assets must include Cyber Security Awareness, Physical Security Controls, Electronic Access Controls for external routable protocol connections and dial-up connectivity and incident reponse to Cyber Security Incident. An inventory, list, or descrete identification of low impact BES Cyber Systems or their BES Cyber Assets is not required | Critical Control 15: Controlled Access based on need to know<br>Critical Control 4: Continuous Vulnerability Assessment and Remediation<br>Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches<br>Critical Control 18: Incident Response and Management<br>Critical Control 13: Boundary Defense |
| R3: Exceptions to the Cyber Security Policy | No Change | R3: Identify a CIP Senior Manager and document any change within 30 calendar days of the change | |
| R4: Information Protection Program | No Change | R4: CIP Senior Manager must document any delegates | |
| R5: Access Control | No Change | | |
| R6: Change Control and Configuration Management | No Change | | |
| **CIP-004-3 Personnel and Training** | **CIP-004-4 Personnel and Training** | **CIP-004-5 Personnel and Training** | |
| R1: Awareness: Security Awareness Program | No Change | R1: Security Awareness Program- reference Table 1: Security Awareness Program Criteria in standard | Critical Control 15: Controlled Access based on need to know<br>Critical Control 9: Security Skills Assessment and appropriate training to fill gaps |
| R2: Training: Cyber Security Training Program | No Change | R2: Training Program- reference Table R2 Cyber Security Training Program in standard | Critical Control 15: Controlled Access based on need to know<br>Critical Control 9: Security Skills Assessment and appropriate training to fill gaps |
| R3: Personnel Risk Assessment | No Change | R3: PRA Program- reference Table R3 PRA Program in standard | Critical Control 15: Controlled Access based on need to know Critical Control 9: Security Skills Assessment and appropriate training to fill gaps |
| R4: Access | No Change | R4: Access Management Program- Reference Table R4 Access Management Program in standard for required program criteria | Critical Control 15: Controlled Access based on need to know Critical Control 9: Security Skills Assessment and appropriate training to fill gaps |
| | | R5: Access Revocation Program- Reference Table R5 Access Revocation for required program criteria | Critical Control 15: Controlled Access based on need to know<br>Critical Control 9: Security Skills Assessment and appropriate training to fill gaps |

splunk> App: Asset Discovery

Administrator | Messages | Settings | Activity | Help

Overview | Asset Details | Pivot | Reports | Alerts | Dashboards

Asset Discovery

# Overview

Edit | More Info

Today | Submit

## State Change: Up -> Down

<1m ago

| dest_ip | dest_host | states | _time |
|---|---|---|---|
| 192.168.10.158 | - | | 2014-09-04 16:43:07 |

## State Change: Down -> Up

<1m ago

| dest_ip | dest_host | states | _time |
|---|---|---|---|
| 192.168.10.154 | - | | 2014-09-04 16:43:07 |
| 192.168.10.157 | - | | 2014-09-04 16:43:07 |
| 192.168.10.175 | - | | 2014-09-04 16:43:07 |

## Scan Points

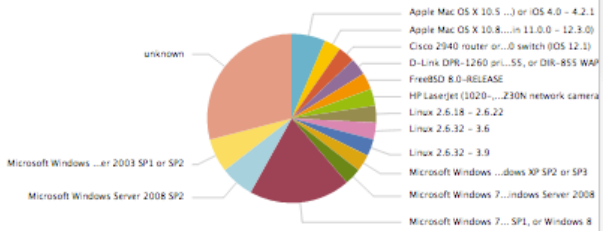
<1m ago

| | scan_point | scan_results | last_scan |
|---|---|---|---|
| 1 | airseabattle | 201255 | 2014-09-04 16:43:17 |

Recent scan activity

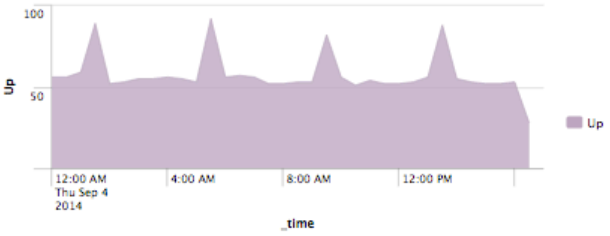
## Operating System Signatures

<1m ago




## Asset Availability

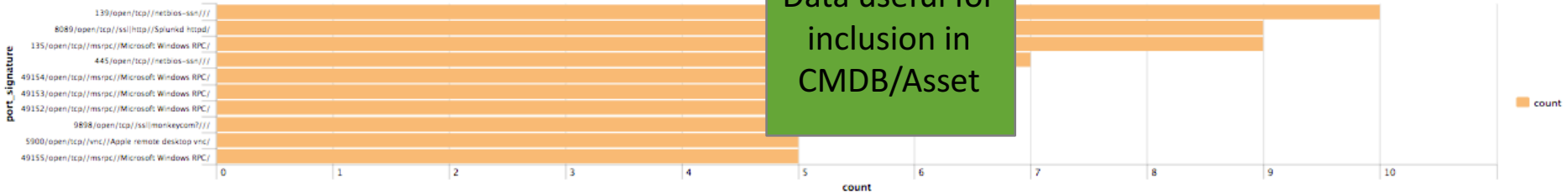
<1m ago




Data useful for inclusion in CMDB/Asset

## Top 10 Ports

<1m ago



splunk> App: Asset Discovery

Administrator | Messages | Settings | Activity | Help

Overview | Asset Details | Pivot | Reports | Alerts | Dashboards

Asset Discovery

# Host Overview

Edit | More Info

Host or IP: 192.168.10.91 | Today | Submit

## Host Overview

<1m ago

Distinct IPs available during timeframe: 1

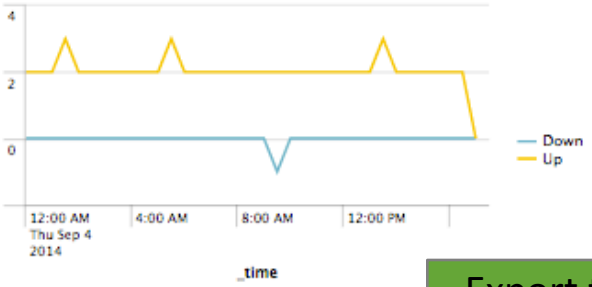
### Asset State

<1m ago

| dest_ip | dest_host | status | minutes_ago |
|---|---|---|---|
| 192.168.10.91 | | Up | 10 |

### Historical Availability

<1m ago




### Operating System Signatures

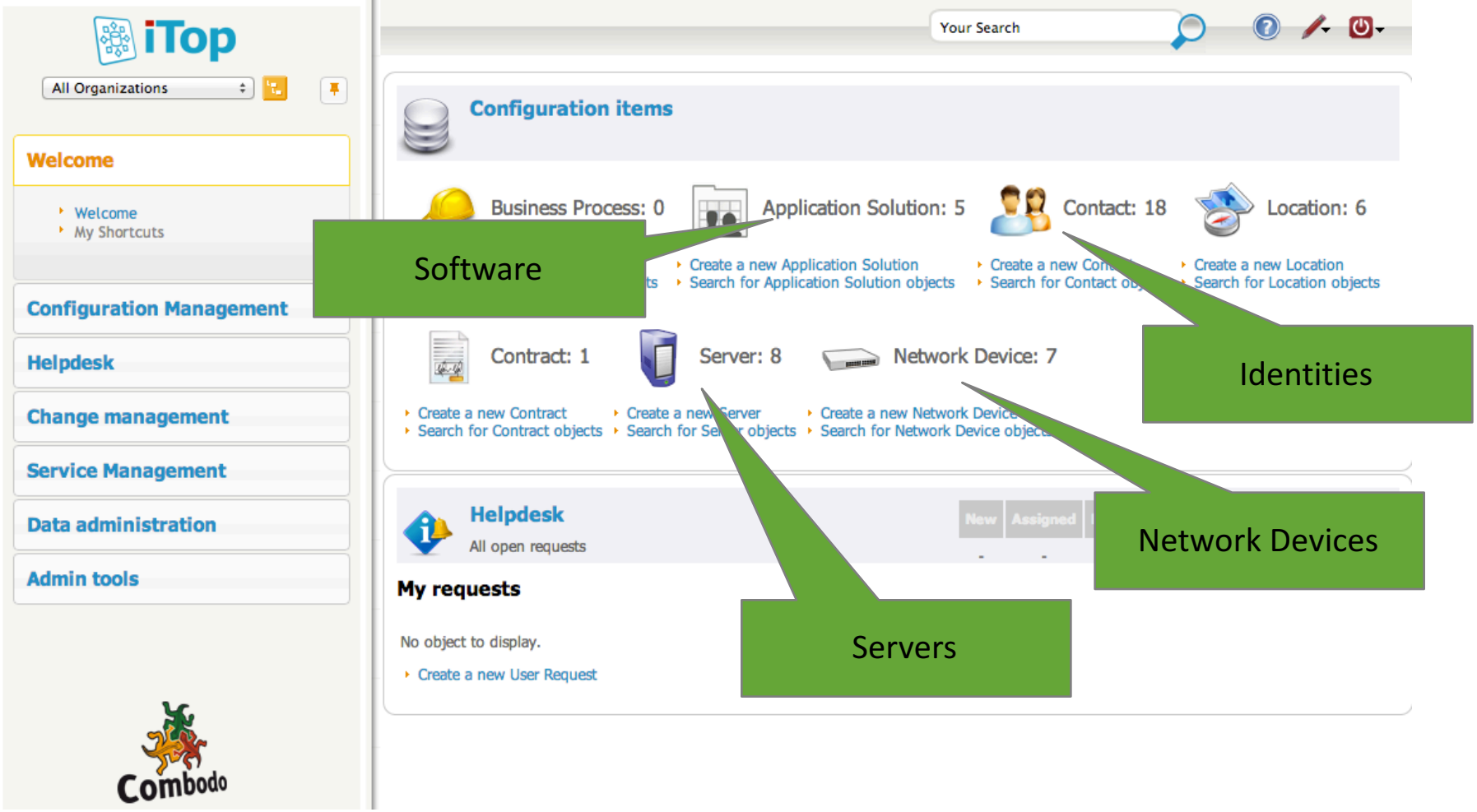
<1m ago


Export this data to asset/CMDB via DB Connect

### Host Details

<1m ago

| dest_ip | dest_host | os_signature | dest_port | transport | dest_port_state | app | app_version |
|---|---|---|---|---|---|---|---|
| 192.168.10.91 | | Linux 2.6.32 - 3.9 | 22 | tcp | open | ssh | OpenSSH 5.3 (protocol 2.0) |
| | | | 80 | tcp | open | http | Apache httpd 2.2.15 ((CentOS)) |
| | | | 111 | tcp | open | rpcbind | 2-4 (RPC #100000) |
| | | | 3306 | tcp | open | mysql | MySQL 5.1.73-log |
| | | | 8089 | tcp | open | ssl\|http | Splunkd httpd |


iTop
All Organizations
Welcome
Welcome
My Shortcuts
Configuration Management
Helpdesk
Change management
Service Management
Data administration
Admin tools
Combodo
Your Search
Configuration items
Business Process: 0
Application Solution: 5
Contact: 18
Location: 6
Create a new Application Solution
Search for Application Solution objects
Create a new Location
Search for Location objects
Contract: 1
Server: 8
Network Device: 7
Create a new Contract
Search for Contract objects
Helpdesk
All open requests
My requests
No object to display.
Create a new User Request
Software
Identities
Network Devices
Servers

# Connect to CMDB

splunk> App: Splunk DB Connect

Administrator | Messages | Settings | Activity | Help

Splunk DB Connect | Search | Database Info | Searches | Settings

Splunk DB Connect

Database Info | Actions

**Database Tables**

< 1m ago

Database: itop  Schema: All  Table name filter:

Fetch tables

304 tables

« prev 1 2 3 4 5 6 7 8 9 10 next »

| | table_name | schema | catalog | table_type |
|---|---|---|---|---|
| 1 | applicationsolution | | itop | TABLE |
| 2 | attachment | | itop | TABLE |
| 3 | brand | | itop | TABLE |
| 4 | businessprocess | | itop | TABLE |
| 5 | connectableci | | itop | TABLE |
| 6 | contact | | itop | TABLE |
| 7 | contacttype | | itop | TABLE |
| 8 | contract | | itop | TABLE |
| 9 | contracttype | | itop | TABLE |
| 10 | customercontract | | itop | TABLE |

splunk> App: CMDB

Administrator Messages Settings Activity Help

Search Pivot Reports Alerts Dashboards CMDB

# CMDB Updates

Edit More Info

All time

## Is CMDB Being Updated from Scans?

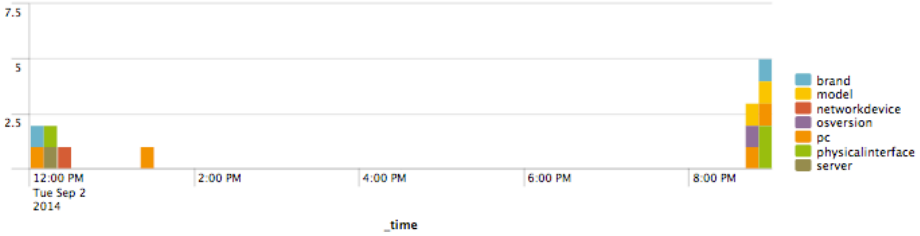
3h ago

**2014-09-02 12:20:45**
SERVER ASSETS LAST UPDATED

**2014-09-02 12:21:19**
NETWORK ASSETS LAST UPDATED

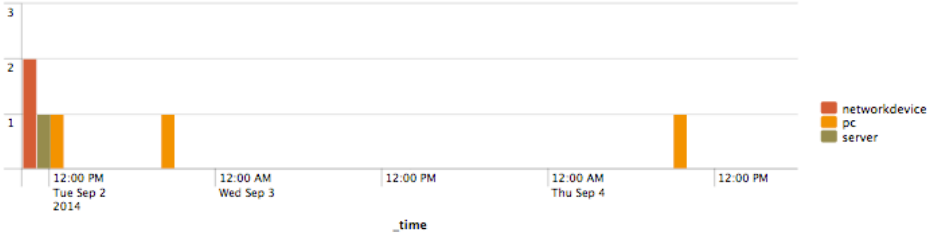
### New CIs Over Time via Discovery

3h ago




### Updated CIs Over Time via Discovery

3h ago




### New Devices Last 7 Days

3h ago

| name | business_criticity | location_name | status | brand_name | model_name | osfamily_name | osversion_name | cpu |
|---|---|---|---|---|---|---|---|---|
| android-367619d6ad65ff00 | low | Mobile | production | Samsung | | Android | | |
| android-bbe74d8e83da6ef6 | low | Mobile | production | HTC | One M7 | Android | 4.4.3 | |
| android-dba05e674aa98070 | low | Mobile | production | ASUS | | Android | 4.4.4 | |
| barnstorming | medium | Basement | production | HP | a6177 | Windows | 7 Enterprise | E6550 dual core |
| choppercommand | medium | Basement | production | Generic | | Windows | 7 Enterprise | Celeron G550 |

### Updated Devices Last 7 Days

3h ago

| name | business_criticity | location_name | status | brand_name | model_name | osfamily_name | osversion_name | cpu | ram |
|---|---|---|---|---|---|---|---|---|---|
| airseabattle | high | Basement | production | VMWare | | Linux | CentOS 6 64bit | 8 | 8GB |
| combat | low | Basement | obsolete | IBM | xSeries 330 | Linux | CentOS 5 32 bit | 2 | 4GB |
| esxy-5 | high | Basement | production | Generic | | VMware | ESXi 5.0 | AMD FX-8120 | 32GB |
| stream | medium | Basement | production | VirtualBox | | Linux | CentOS 6 64bit | 1 | 2GB |

splunk> App: Splunk DB Connect | Administrator | Messages | Settings | Activity | Help

Splunk DB Connect | Search | Database Info | Database Query | Searches | Settings

Splunk DB Connect

Database Info | Actions

Database Tables

< 1m ago

Database itop | Schema All | Table name filter: *physical*

Fetch tables

6 tables

| | table_name | schema | catalog | table_type |
|---|---|---|---|---|
| 1 | lnkphysicalinterfacetovlan | | itop | TABLE |
| 2 | physicaldevice | | itop | TABLE |
| 3 | physicalinterface | | itop | TABLE |
| 4 | view_PhysicalDevice | | itop | VIEW |
| 5 | view_PhysicalInterface | | itop | VIEW |
| 6 | view_lnkPhysicalInterfaceToVLAN | | itop | VIEW |

Correlate fields found in machine data with CMDB fields

14 columns in table view_PhysicalInterface

« prev 1 2 next »

| | column_name | type | | | rement | size | decimal_digits | radix | remarks |
|---|---|---|---|---|---|---|---|---|---|
| 1 | id | INT | NO | NO | | 10 | 0 | 10 | |
| 2 | name | VARCHAR | NO | NO | | 255 | 0 | 10 | |
| 3 | ipaddress | VARCHAR | YES | NO | | 255 | 0 | 10 | |
| 4 | macaddress | VARCHAR | YES | NO | | 255 | 0 | 10 | |
| 5 | comment | TEXT | YES | NO | | 65535 | 0 | 10 | |
| 6 | ipgateway | VARCHAR | YES | NO | | 255 | 0 | 10 | |
| 7 | ipmask | VARCHAR | YES | NO | | 255 | 0 | 10 | |
| 8 | speed | DECIMAL | YES | NO | | 12 | 2 | 10 | |
| 9 | connectableci_id | INT | NO | NO | | 10 | 0 | 10 | |
| 10 | connectableci_name | VARCHAR | NO | NO | | 255 | 0 | 10 | |

Show table contents...

New Search

Save As Close

index=tomato DHCPACK

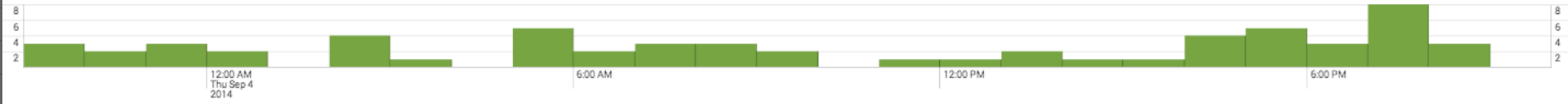
Last 24 hours

✓ 59 events (9/3/14 9:00:00.000 PM to 9/4/14 9:07:18.000 PM)

Job Verbose Mode

Events (59) Statistics Visualization

Format Timeline Zoom Out + Zoom to Selection × Deselect 1 hour per column




List Format 50 Per Page

Prev 1 2 Next

Hide Fields All Fields

Selected Fields
- a eventtype 1
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields
- # date_hour 21
- # date_mday 2
- # date_minute 35
- a date_month 1
- # date_second 37
- a date_wday 2
- # date_year 1
- a date_zone 1
- a dhcpack_ip 13
- a index 1
- # linecount 1
- a punct 2
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1

| i | Time | Event |
|---|---|---|
| > | 9/4/14 8:57:20.000 PM | Sep 4 20:57:20 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.170 24:77:03:34:ff:10 MMIL-6ZKP6R11<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 8:13:01.000 PM | Sep 4 20:13:01 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.159 28:cf:e9:55:3a:51 jbrodsky-mbp15<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 8:01:15.000 PM | Sep 4 20:01:15 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.158 e8:99:c4:83:da:54 android-bbe74d8e83da6ef6<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 7:56:41.000 PM | Sep 4 19:56:41 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.170 24:77:03:34:ff:10 MMIL-6ZKP6R11<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 7:56:40.000 PM | Sep 4 19:56:40 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.170 24:77:03:34:ff:10 MMIL-6ZKP6R11<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 7:29:48.000 PM | Sep 4 19:29:48 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.187 3c:15:c2:c1:2a:38 brodsky-mbp13<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 7:28:41.000 PM | Sep 4 19:28:41 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.158 e8:99:c4:83:da:54 android-bbe74d8e83da6ef6<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 7:23:22.000 PM | Sep 4 19:23:22 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.157 28:6a:ba:84:0e:0b pitfall<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 7:18:47.000 PM | Sep 4 19:18:47 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.156 00:d0:2d:29:25:57 Gateway292557<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |
| > | 9/4/14 7:10:22.000 PM | Sep 4 19:10:22 192.168.10.1 dnsmasq-dhcp[1153]: DHCPACK(br0) 192.168.10.169 00:21:00:73:67:51 kaboom<br>eventtype = nix-all-logs ¦ host = router ¦ source = /var/log/tomato ¦ sourcetype = tomato-router |

Put DHCP logs in Splunk, just like CSC 1 says. They have hostname, MAC, ipaddress…

# Passive Discovery - CSC 1 & 2

Edit | More Info

Last 7 days

## Approved DHCP Devices

24m ago

| hostname | src_mac_vendor | clientip | sparkline | count |
|---|---|---|---|---|
| DRAGSTER | vmware inc | 192.168.10.199 | | 1 |
| GWEN-ULTRABOOK | Unknown Vendor | 192.168.10.160 | | 1 |
| Gateway292557 | ademco | 192.168.10.156 | | 1 |
| MMIL-6ZKP6R11 | dell corporate | 192.168.10.170 | | 1 |
| android-367619d6ad65ff00 | Unknown Vendor | 192.168.10.174 | | 1 |
| android-bbe74d8e83da6ef6 | htc corporation | 192.168.10.158 | | 1 |
| android-dba05e674aa98070 | Unknown Vendor | 192.168.10.154 | | 1 |
| brodsky-mbp13 | Unknown Vendor | 192.168.10.187 | | 1 |
| jbrodsky-mbp15 | Unknown Vendor | 192.168.10.197 | | 1 |
| jbrodsky-mbp15 | apple computer inc | 192.168.10.159 | | 1 |

« prev 1 2 next »

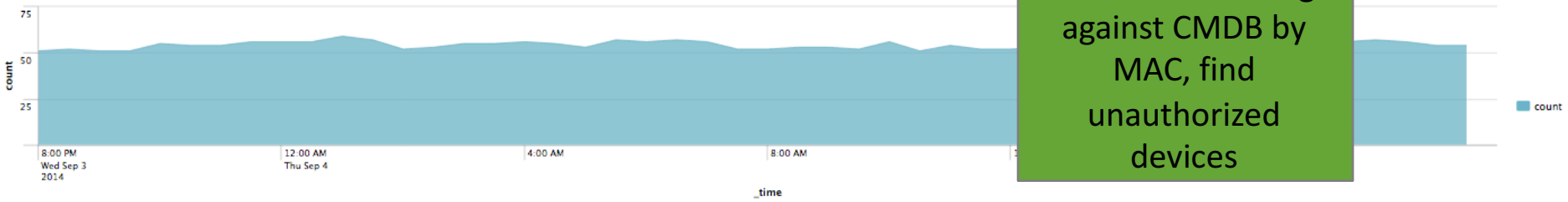
## Unapproved DHCP Devices

24m ago

| hostname | src_mac_vendor | clientip | sparkline | count |
|---|---|---|---|---|
| brodskys-iPod | apple computer inc | 192.168.10.161 | | 1 |

## Ping Scan Results

24m ago




Correlate DHCP logs against CMDB by MAC, find unauthorized devices

New Search

Save As Close

```
index=cloudmeter sourcetype="stream:http"  | eval macaddy=lower(src_mac)  | lookup cmdb_macaddress macaddress AS macaddy  | eval approved=if(isnull(friendlyname),"NO","YES")  | search approved="NO"  site="google.com" | stats  sparkline count by src_ip,src_mac,http_user_agent  | sort  -count
```

Last 24 hours

✓ 40 events (9/3/14 9:00:00.000 PM to 9/4/14 9:16:16.000 PM)

Job Verbose Mode

Events (40) Statistics (1) Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

1 hour per column

List Format 20 Per Page

Prev 1 2 Next

Hide Fields All Fields

Selected Fields
- a eventtype 2
- a host 1
- a source 1
- a sourcetype 1

Interesting Fields
- a action 1
- a approved 1
- # bytes 14
- # bytes_in 2
- # bytes_out 14
- a dest_ip 5
- a dest_mac 1
- # dest_port 1
- a http_comment 2
- # http_content_length 6
- a http_content_type 1
- a http_method 1
- a http_user_agent 1
- a index 1
- # linecount 1
- a macaddy 1
- a punct 1
- a server 1

| i | Time | Event |
|---|---|---|
| > | 9/4/14 8:44:53.000 PM | |

```
{ [-]
   bytes: 14461
   bytes_in: 326
   bytes_out: 14135
   dest_ip: 74.125.225.197
   dest_mac: 10:BF:48:E7:01:E1
   dest_port: 80
   http_comment: HTTP/1.1 206 Partial Content
   http_content_length: 21049653
   http_content_type: application/x-msdos-program
   http_method: GET
   http_user_agent: Google Update/1.3.24.15;winhttp
   server: downloads
   site: google.com
   src_ip: 192.168.10.115
   src_mac: 00:0C:29:D9:38:3A
   src_port: 61228
   status: 206
   time_taken: 109654
   timestamp: 2014-09-05T02:44:52.721937Z
   transport: tcp
   uri_path: /dl/chrome/win/2A4DAAA984C86D5B/37.0.2062.103_chrome_installer.exe
}
```

Show as raw text

eventtype = stream_network_traffic communicate network eventtype = stream_web web | host = stream64 | source = stream | sourcetype = stream:http

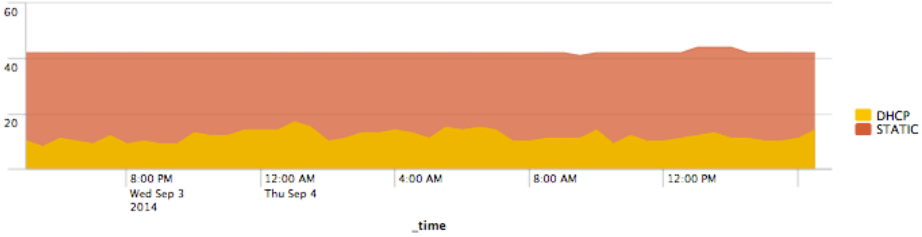
| | | |
|---|---|---|
| > | 9/4/14 8:44:53.000 PM | |

```
{ [-]
   bytes: 26066
   bytes_in: 326
   bytes_out: 25740
   dest_ip: 74.125.225.197
   dest_mac: 10:BF:48:E7:01:E1
   dest_port: 80
```

Stream data has ip, mac, useragent from devices seen on network

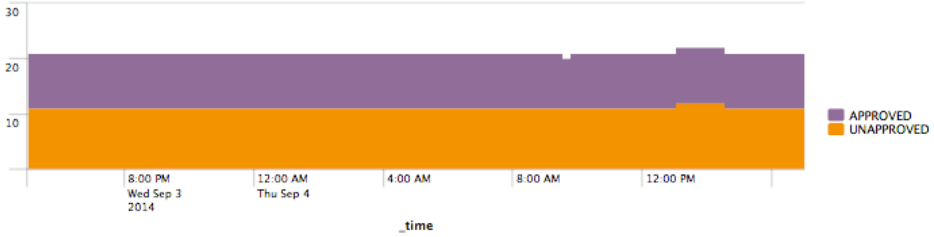
## Ping Count by DHCP Status

4h ago




## Static Addresses over Time

4h ago




## Approved Web Surfers

4h ago

| src_ip | src_mac | friendlyname | http_user_agent | sparkline | count |
|---|---|---|---|---|---|
| 192.168.10.197 | 10:DD:B1:B7:EB:A8 | en0 jbrodsky-mbp15 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36 | | 24953 |
| 192.168.10.197 | 10:DD:B1:B7:EB:A8 | en0 jbrodsky-mbp15 | Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:22.0) Gecko/20100101 Firefox/22.0 | | 6055 |
| 192.168.10.205 | BC:5F:F4:E6:49:2B | Local Area Connection fishingderby | Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36 | | 399 |
| 192.168.10.158 | EB:99:C4:83:DA:54 | eth0 android-bbe74d8e83da6ef6 | Lavf/55.19.104 | | 144 |
| 192.168.10.158 | EB:99:C4:83:DA:54 | eth0 android-bbe74d8e83da6ef6 | AirVideo/2.4.13 CFNetwork/548.1.4 Darwin/11.0.0 | | 92 |
| 192.168.10.158 | EB:99:C4:83:DA:54 | eth0 android-bbe74d8e83da6ef6 | Apache-HttpClient/UNAVAILABLE (java 1.4) | | 82 |
| 192.168.10.207 | 00:1B:FC:A5:18:AA | Local Area Connection barnstorming | Microsoft-Windows/6.1 UPnP/1.0 Windows-Media-Player-DMS/12.0.7601.17514 DLNADOC/1.50 | | 76 |
| 192.168.10.207 | 00:1B:FC:A5:18:AA | Local Area Connection barnstorming | Windows-Media-Player-DMS/12.0.7601.17514 | | 76 |
| 192.168.10.202 | 90:2B:34:34:23:DD | Local Area Connection choppercommand | Microsoft-Windows/6.1 UPnP/1.0 Windows-Media-Player-DMS/12.0.7601.17514 DLNADOC/1.50 | | 75 |
| 192.168.10.202 | 90:2B:34:34:23:DD | Local Area Connection | Windows-Media-Player-DMS/12.0.7601.17514 | | 75 |

## Unapproved Web Surfers

4h ago

| src_ip | src_mac | http_user_agent | sparkline | count |
|---|---|---|---|---|
| 192.168.10.115 | 00:0C:29:D9:38:3A | Google Update/1.3.24.15;winhttp | | 200 |
| 192.168.10.203 | 00:22:FA:F9:8E:04 | Microsoft-Windows/6.1 UPnP/1.0 Windows-Media-Player-DMS/12.0.7601.17514 DLNADOC/1.50 | | 46 |
| 192.168.10.203 | 00:22:FA:F9:8E:04 | Windows-Media-Player-DMS/12.0.7601.17514 | | 46 |
| 192.168.10.85 | 00:0C:29:C6:D2:37 | ip360 | | 24 |
| 192.168.10.112 | 00:0C:29:4E:7F:C2 | Windows-Update-Agent | | 16 |
| 192.168.10.115 | 00:0C:29:D9:38:3A | Microsoft-CryptoAPI/6.1 | | 10 |
| 192.168.10.85 | 00:0C:29:C6:D2:37 | Hewlett-Packard IPP | | 10 |
| 192.168.10.112 | 00:0C:29:4E:7F:C2 | Microsoft-CryptoAPI/6.1 | | 7 |
| 192.168.10.85 | 00:0C:29:C6:D2:37 | Mozilla/4.0 | | 6 |
| 192.168.10.113 | 00:0C:29:50:A7:43 | Windows-Update-Agent | | 5 |

« prev 1 2 next »

Use useragent data + ipaddress from Stream or proxy to find devices/browsers surfing that are not approved.

# Malware Center

Action: All | Business Unit: | Category: All | Last 24 hours | Submit

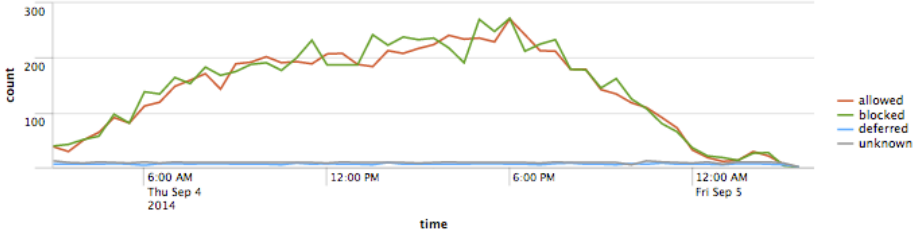
Edit

| NEW INFECTIONS | MULTIPLE INFECTIONS | UNIQUE MALWARE | INFECTED SYSTEMS | TOTAL INFECTIONS |
|---|---|---|---|---|
| Count | System Count | Unique Count | System Count | Count |
| 0 ↘ -3 | 31 ↗ +5 | 51 0 | 83 ↗ +1 | 131 ↗ +7 |

Track multiple vendors for malware defense, aggregate their information.

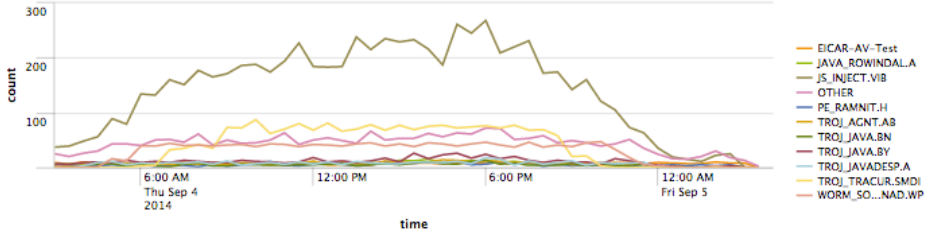
## Malware Activity Over Time By Action

<1m ago



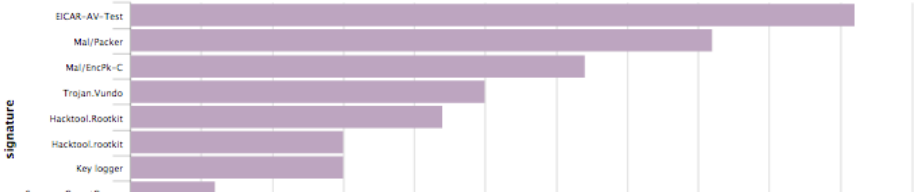

## Malware Activity Over Time By Signature

<1m ago




## Top Infections

<1m ago




## New Malware - Last 30 Days

<1m ago

No results found.

# Malware Search

Edit

| Action | Signature | File | Destination | User | | |
|---|---|---|---|---|---|---|
| All | | | | | Last 24 hours | Submit |

<1m ago

| _time | action | signature | file_name | dest | user | count |
|---|---|---|---|---|---|---|
| 2014-09-05 03:01:53 | blocked | JS_INJECT.VIB | 30A70787d01<br>Aqf4TvNf.zip.part<br>FedEx_Invoice.exe | ACME-12345 | unknown | 7083 |
| 2014-09-04 22:01:53 | allowed | TROJ_TRACUR.SMDI | DWrite32.dll<br>DevicePairingFolder32.dll<br>DevicePairingProxy32.dll<br>DevicePairingProxy32.dllabtrb6c32.dll<br>DevicePairingProxy32.dllabtrb6c32.dlluoi34rdh32.dll<br>DevicePairingProxy32.dllabtrb6c32.dlluoi34rdh32.dllznua5u32.dll<br>DevicePairingProxy32.dllabtrb6c32.dlluoi34rdh32.dllznua5u32.dll6zf1ucpq32.dll<br>devenum32.dll<br>dinput32.dll<br>dinput832.dll<br>divx32.dll<br>divx32.dll5uvhvf32.dll<br>divx32.dll5uvhvf32.dll8pe1jta56ztno32.dll<br>divx32.dll5uvhvf32.dll8pe1jta56ztno32.dll80uu732.dll<br>divx32.dll5uvhvf32.dll8pe1jta56ztno32.dll80uu732.dlldklmiigt32.dll<br>dui7032.dll<br>dui703232.dll<br>els32.dll<br>els3232.dll<br>elslad32.dll | KENNYPOWERS | SYSTEM | 1934 |
| 2014-09-05 00:02:06 | allowed | WORM_SOHANAD.WP | $$.exe<br>$OEM$.exe<br>0.0.0.1.exe<br>SCRIPTS.exe<br>SETUP.exe<br>_default.exe<br>base_images.exe<br>bitsextensions-server.exe<br>boot.exe<br>cable.exe<br>data.exe<br>dlmanifests.exe<br>efi.exe<br>en-us.exe<br>enterprise.exe<br>enterprisee.exe<br>enterprisen.exe<br>etwproviders.exe<br>fonts.exe<br>inf.exe | ACME-CA0382FD | SYSTEM | 1369 |

Drill down into specific malware found on endpoints or servers.

# Malware Operations

Edit

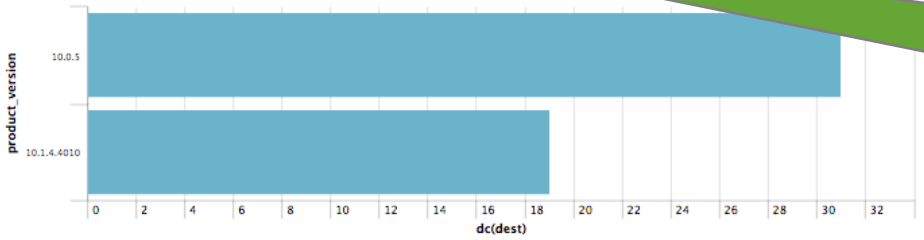
Business Unit | Category: All | Last 30 days | Submit

Edit

| MALWARE CLIENTS | OLD MALWARE DEFS | INFECTED SYSTEMS | AVG INFECTION LENGTH | OLDEST INFECTION |
|---|---|---|---|---|
| Client Count | Client Count | Percent | Days | Days |
| 59 0 | 62 0 | 141 % +1.7 | 233 +8.2 | 239 +1.1 |

## Clients By Product Version

<1m ago




## Clients By Signature Version

<1m ago

Understand when systems are not being updated with new malware signatures

## Repeat Infections

<1m ago

| signature | dest | action | day_count |
|---|---|---|---|
| Adware.Hotbar | 10.11.36.20 | deferred | 9 |
| EICAR-AV-Test | PROD-POS-005 | deferred | 9 |
| EICAR-AV-Test | ops-sys-002 | deferred | 9 |
| EICAR-AV-Test | ops-sys-004 | deferred | 9 |
| HIPS/IPConnect-002 | UK-GN-12345 | deferred | 9 |
| JS_INJECT.VIB | ACME-12345 | blocked | 9 |
| LeakTest | UK-GN-67890 | blocked | 9 |
| Mal/EncPk-C | SE-001 | deferred | 9 |
| Mal/Packer | HOST-001 | deferred | 9 |
| Sus/ComPack-C | ACME-1386 | unknown | 9 |

## Oldest Infections

<1m ago

| firstTime | lastTime | signature | dest | days_active |
|---|---|---|---|---|
| 01/08/2014 22:05:36 | 09/04/2014 23:24:05 | ADW_FAM_000006a.TOMA | D8Q8XM51 | 240 |
| 01/08/2014 22:21:38 | 09/05/2014 02:02:05 | Adware.Hotbar | 10.11.36.20 | 240 |
| 01/08/2014 23:29:49 | 09/05/2014 01:41:55 | EICAR-AV-Test | ACME-001 | 240 |
| 01/08/2014 22:07:09 | 09/05/2014 02:07:58 | EICAR-AV-Test | COREDEV-003 | 240 |
| 01/08/2014 22:54:41 | 09/05/2014 00:59:39 | EICAR-AV-Test | HOST-002 | 240 |
| 01/09/2014 00:15:47 | 09/05/2014 02:23:26 | EICAR-AV-Test | PROD-MFS-004 | 240 |
| 01/08/2014 22:16:25 | 09/04/2014 23:03:46 | EICAR-AV-Test | PROD-MFS-005 | 240 |
| 01/08/2014 22:00:42 | 09/05/2014 02:51:15 | EICAR-AV-Test | TELE-PC | 240 |
| 01/08/2014 22:00:04 | 09/05/2014 02:34:52 | EICAR-AV-Test | de-gn-12345 | 240 |
| 01/08/2014 22:17:52 | 09/05/2014 01:18:53 | EICAR-AV-Test | ops-sys-002 | 240 |

# Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report.
Open the report in Pivot or Search to refine the parameters or further explore the data.

28 Reports

All | Yours | This App's | malware

| i | Title | Actions | | Owner | App | Sharing | Embedding |
|---|---|---|---|---|---|---|---|
| > | Malware - Activity Over Time | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Activity Over Time By Action | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Activity Over Time By Infection | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Average Infection Length | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Average Infection Length Over Time | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Clients By Product Version | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Clients By Signature Version | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Clients Not Updating Signatures | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Infected System Count | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Multiple Infections | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - New Infections | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - New Malware | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Old Malware Defintions | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Oldest Infection | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Oldest Infections | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Percent Of Systems Infected | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Repeat Infections | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Systems With Anti-Malware | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Top 10 Infected Domains | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Top 10 Infected Systems | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Top 10 Infections | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Top Infected Domain | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Top Infected System | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Top Infection | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Total Infection Count | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Unique Infected Systems | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Unique Infections | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |
| > | Malware - Unique Malware Count | Open in Search | Edit | admin | DA-ESS-EndpointProtecti... | Global | Disabled |

We don't talk about the ES reports enough…check out all of these malware reports…

# Malware - Clients Not Updating Signatures

Edit | More Info | Add to Dashboard

✓ 0 events (1/1/70 12:00:00.000 AM to 9/5/14 3:47:38.000 AM)

Job

63 results 20 per page

Prev 1 2 3 4 Next

| _time | dest | dest_nt_domain | product_version | signature_version | vendor_product | dayDiff |
|---|---|---|---|---|---|---|
| 2014-01-08 20:10:38 | COREDEV-006 | DS | 10.1.4.4010 | 4.78G | Symantec Antivirus | 239.32 |
| 2014-01-08 20:27:26 | BUSDEV-002 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.31 |
| 2014-01-08 20:33:10 | BUSDEV-007 | WORKGROUP | 10.1.4.4010 | 4.78G | Symantec Antivirus | 239.30 |
| 2014-01-08 21:13:16 | PROD-POS-004 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.27 |
| 2014-01-08 21:20:02 | HAMSANDWICH | ENG | 8.7 | None | McAfee VirusScan Enterprise | 239.27 |
| 2014-01-08 21:24:58 | ACME-003 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.27 |
| 2014-01-08 21:47:26 | COREDEV-002 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.25 |
| 2014-01-08 21:56:24 | SE-005 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.24 |
| 2014-01-08 21:59:16 | COREDEV-005 | WORKGROUP | 10.1.4.4010 | 4.78G | Symantec Antivirus | 239.24 |
| 2014-01-08 22:00:45 | ops-sys-001 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.24 |
| 2014-01-08 22:14:34 | HOST-006 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.23 |
| 2014-01-08 22:16:19 | SE-001 | WORKGROUP | 10.1.4.4010 | 4.78G | Symantec Antivirus | 239.23 |
| 2014-01-08 22:18:31 | BUSDEV-003 | DS | 10.1.4.4010 | 4.78G | Symantec Antivirus | 239.23 |
| 2014-01-08 22:20:09 | SERVER2 | unknown | | 120429c | Symantec Antivirus | 239.23 |
| 2014-01-08 22:23:31 | JANETLWIN704 | WORKGROUP | 8.7 | 5400.1158 | McAfee VirusScan Enterprise | 239.23 |
| 2014-01-08 22:24:38 | SERVER3 | unknown | | 120429c | Symantec Antivirus | 239.22 |
| 2014-01-08 22:46:37 | SE-003 | DS | 10.1.4.4010 | 4.78G | Symantec Antivirus | 239.21 |
| 2014-01-08 22:50:33 | PROD-MFS-006 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.21 |
| 2014-01-08 23:00:41 | ACME-006 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.20 |
| 2014-01-08 23:20:22 | PROD-MFS-001 | INTRANET | 10.0.5 | 4.78G | Sophos Endpoint Protection | 239.19 |

Here's all the clients that need attention. Check out the four different vendors on one report…

# CSC 5 “Execution” Example

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor

Set that to “4” to disable USB.

```
[WinRegMon://hklm_usb]
disabled=0
hive =
\\REGISTRY\\MACHINE\\SYSTEM\\CurrentControlSet\\Services\\UsbStor\\.*
proc = .*
type = set|create|delete|rename
```

USB ports are a common malware threat vector. Have the forwarder watch this entry for changes…

# CSC 5 “Execution” Example

```
# Gather data on USB activity levels every 10 seconds.  Store this data in the default index.

[perfmon://USBChanges]
interval = 10
object = USB
counters = Usb Control Data Bytes/Sec
instances = *
disabled = 0
```

…look for USB activity where there shouldn’t be.

https://demo-cis20.splunkoxygen.com/en-US/app/cis-controls-app-for-splunk/control-1?earliest=0&latest=

Tools | Internal | Demos | WWD | CIM - Reference Ma... | Search Reference - ...

splunk> App: CIS Top 20 Critical Controls | demo_owner | Messages | Settings | Activity | Help | Find

Critical Control Overview | Dashboards by Control | Reports by Control | Other Menus | PDF Documentation | CIS Top 20 Critical Controls

# Critical Security Control #01 - Inventory of Authorized and Unauthorized Devices

Inventory of Authorized and Unauthorized Devices

Edit | More Info

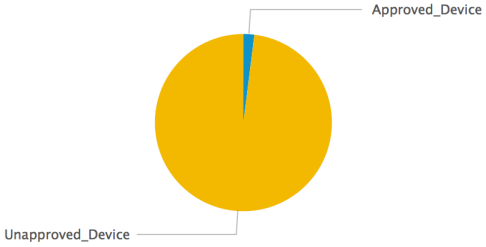
Last 60min

**Control #1 - Inventory of Authorized Devices - Count**

1

Last 60min

**Control #1 - Inventory of Authorized and Unauthorized Devices - Chart**




Last 60min

**Control #1 - Inventory of Unauthorized Devices - Count**

49

Last 60min

**Control #1 - Inventory of Authorized and Unauthorized Devices**

| | dest_mac | asset_owner | clientip | department | is_approved | machine_name | personal | portable | purpose |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 92:90:55:51:61:31 | perez_anthony | 10.11.36.20 | engineering | 1 | cis_dev_test_box | 0 | 0 | development |
| 2 | 01:30:f9:d0:79:13 | | | | | | | | |
| 3 | 03:53:39:5b:ed:ab | | | | | | | | |
| 4 | 04:83:e5:65:6b:2c | | | | | | | | |

https://demo-cis20.splunkoxygen.com/en-US/app/cis-controls-app-for-splunk/critical_security_control_12__boundary_defense__network_ids?earliest=0&latest=

Tools | Internal | Demos | WWD | CIM - Reference Ma... | Search Reference - ...

splunk> App: CIS Top 20 Critical Controls | demo_owner | Messages | Settings | Activity | Help

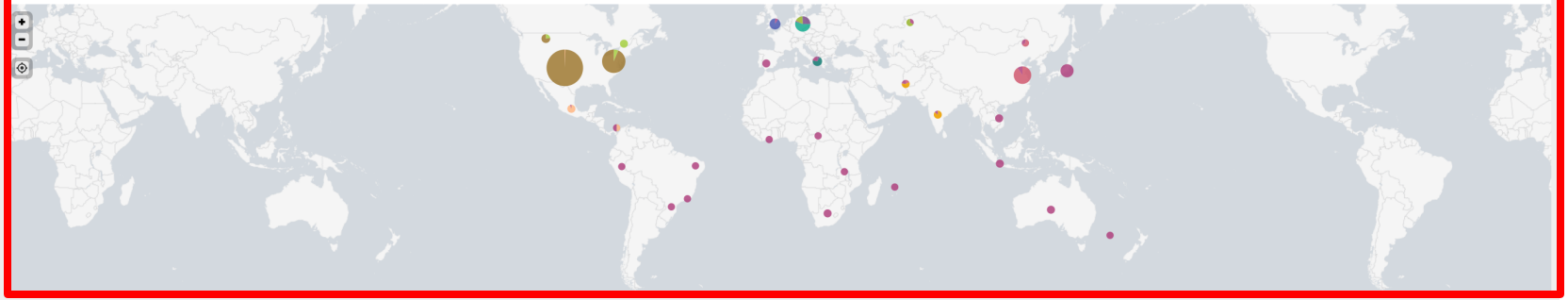
Critical Control Overview | Dashboards by Control | Reports by Control | Other Menus | PDF Documentation | CIS Top 20 Critical Controls

# Critical Security Control #12 - Boundary Defense - Network IDS

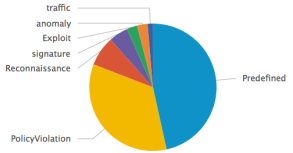
Edit | More Info

Last 24hr

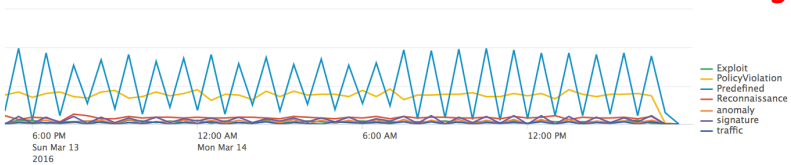
**Control #12 - NIDS: Sources of External Intrusion Attempts** 1



**Control #12 - NIDS Attack Categories** 2




**Control #12 - NIDS Trend by Attack Category** 3




Last 24hr

**Control #12 - NIDS: Allowed Actions by Severity** 4

| | severity | destination | signature | action | host |
|---|---|---|---|---|---|
| 1 | unknown | acmetech.com | Trojan-Phisher-Gamec | allowed | ch-demo-cis20 |
| | | acmetech.com | Trojan-Phisher-Gamec | allowed | ch-demo-cis20 |
| | | acmetech.com | Trojan-Phisher-Gamec | allowed | ch-demo-cis20 |
| | | acmetech.com | Trojan-Phisher-Gamec | allowed | ch-demo-cis20 |
| | | acmetech.com | Trojan-Phisher-Gamec | allowed | ch-demo-cis20 |

# Splunk App for PCI Compliance

- Measures effectiveness and status of PCI compliance technical controls
- Meets PCI requirements around log retention/review, and continuous monitoring
- Fast ability to get to cause of non-compliance or answer auditor data requests
- Covers up to PCI DSS v3.1 standards
- Built, tested, documented, and supported by Splunk; not a free app

# PCI DSS v3.1: 12 Main Requirements

*Splunk directly does #10. Measures #1-8 and #10-11*

| | | |
|---|---|---|
| **Build and Maintain a Secure Network and Systems** | **1.** | Install and maintain a firewall configuration to protect cardholder data |
| | **2.** | Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | **3.** | Protect stored cardholder data |
| | **4.** | Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | **5.** | Protect all systems against malware and regularly update anti-virus software or programs |
| | **6.** | Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | **7.** | Restrict access to cardholder data by business need to know |
| | **8.** | Identify and authenticate access to system components |
| | **9.** | Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | **10.** | Track and monitor all access to network resources and cardholder data |
| | **11.** | Regularly test security systems and processes |
| **Maintain an Information Security Policy** | **12.** | Maintain a policy that addresses information security for all personnel |

# Splunk FISMA App

splunk> FISMA

Administrator | App | Manager | Alerts | Jobs | Logout

Search | Overview | Investigate a Control | Searches & Reports | About

Actions

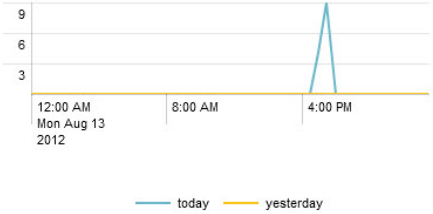
## Overview

Components

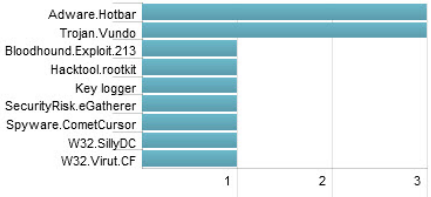
Accounts | Audit | Logins | Malware | Network | Updates | Vulnerabilities

**Today's Malware Events**


**Malware Event Trends**




**Top 10 Malware Event Signatures**




Configure Gauge Thresholds

**Sources (≥ 73)**

« prev 1 2 3 4 5 6 7 8 next »

| | source | Count | Last Update |
|---|---|---|---|
| 1 | WMI:LocalProcesses | 275,958 | 08/13/2012 17:52:52 |
| 2 | WMI:LocalNetwork | 61,297 | 08/13/2012 17:52:59 |
| 3 | WinEventLog:System | 55,140 | 08/13/2012 17:52:20 |