Your Very Own Splunk ES Sandbox!

James Brodsky

Staff Sales Eng/Security SME

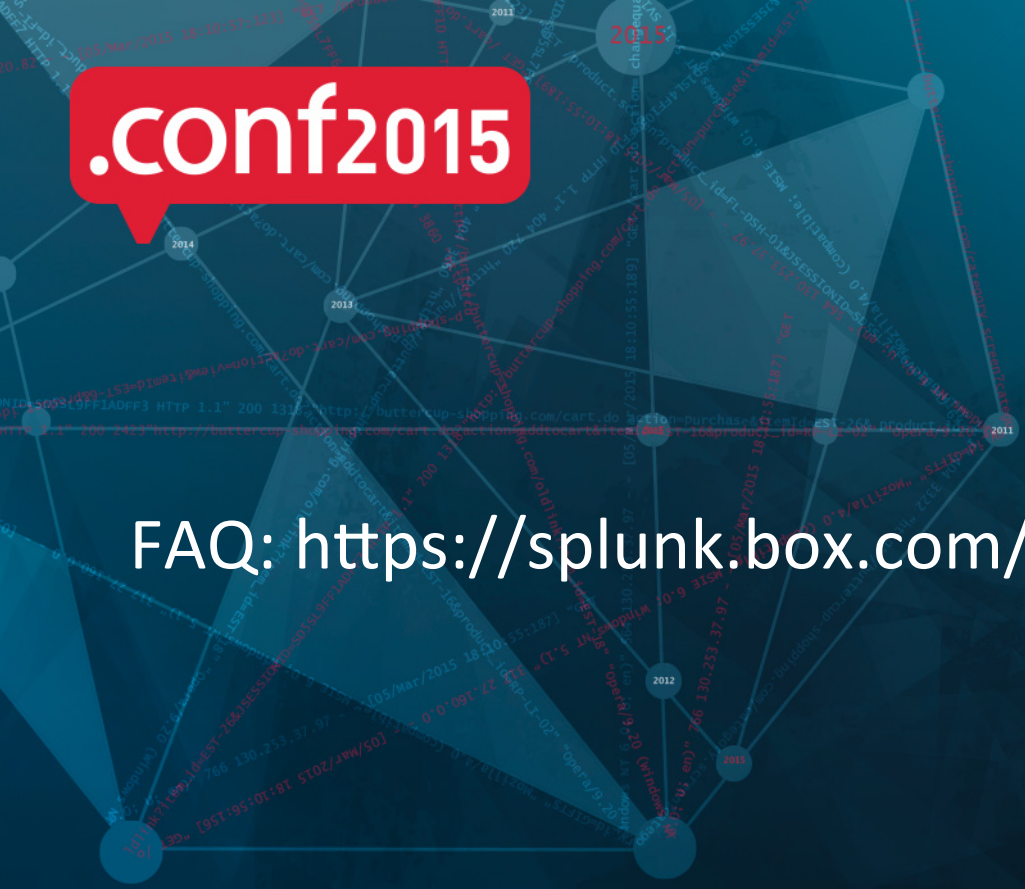
brodsky@splunk.com

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.

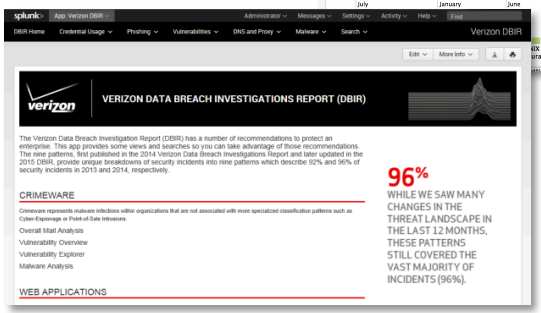


FAQ: https://splunk.box.com/es-sandbox-questions

splunk>

About Me

splunk> 2 Years+



What's a sandbox?

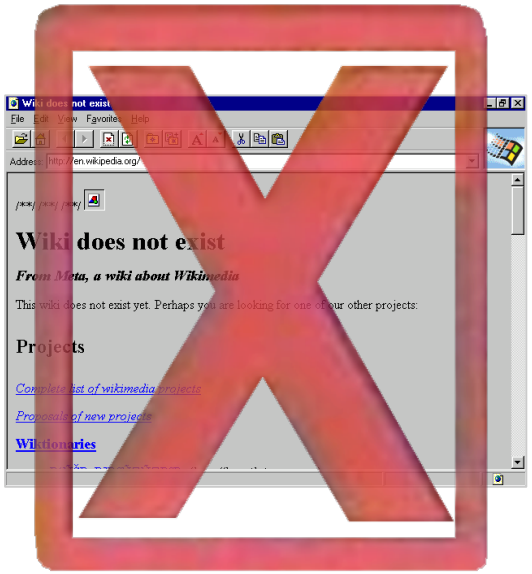
What's a sandbox?

- A **100% free**, fully featured 15 day trial of Splunk products: Cloud, Light, or ES
- Hosted in AWS
- Authenticates off of your Splunk account
- Has sample data for you to play with
- Supports onboard of your own data

Today's session: A hands-on activity with your very own Enterprise Security sandbox!

*** This is a hands-on session ***

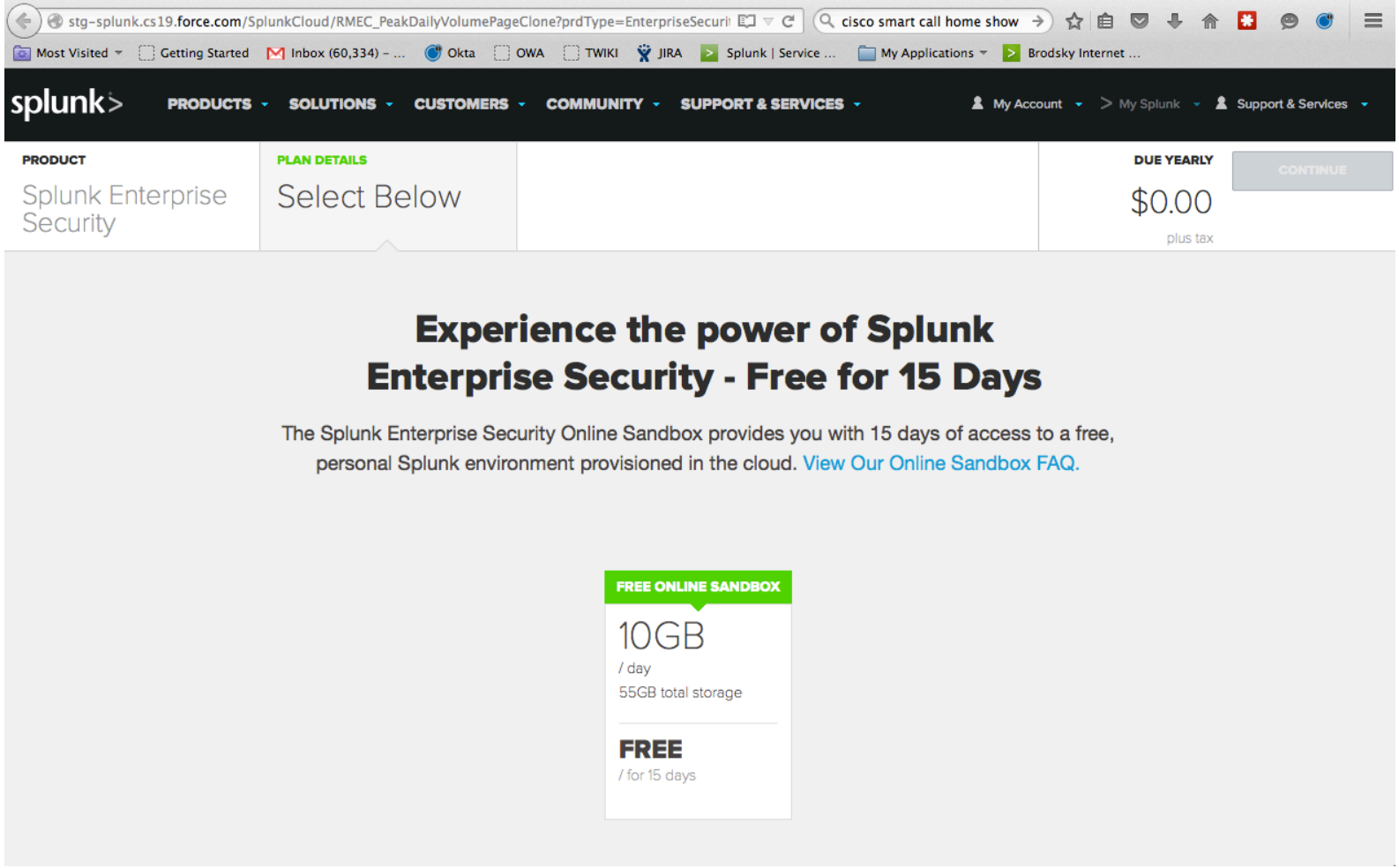
Please use your personal ES Sandbox.

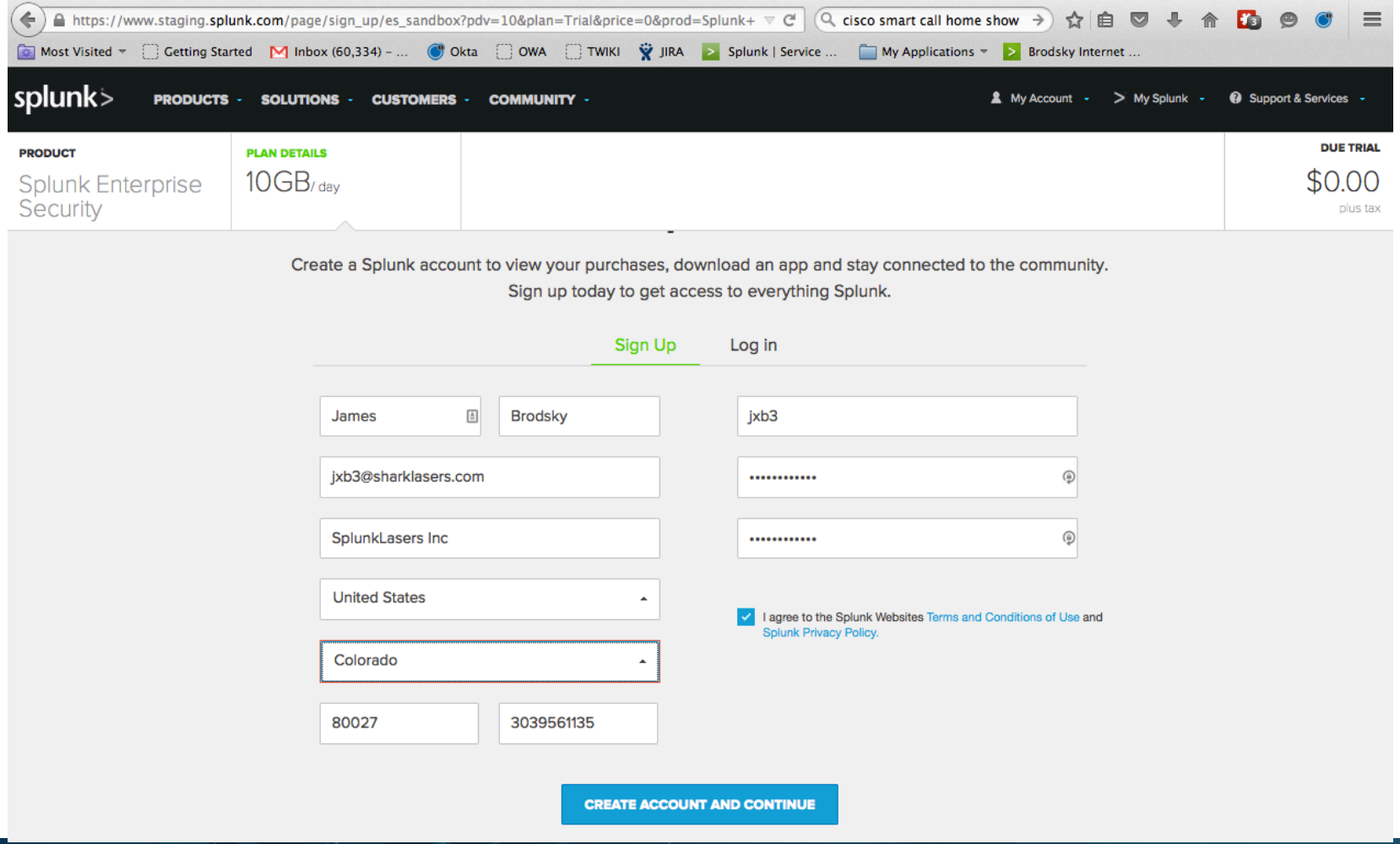


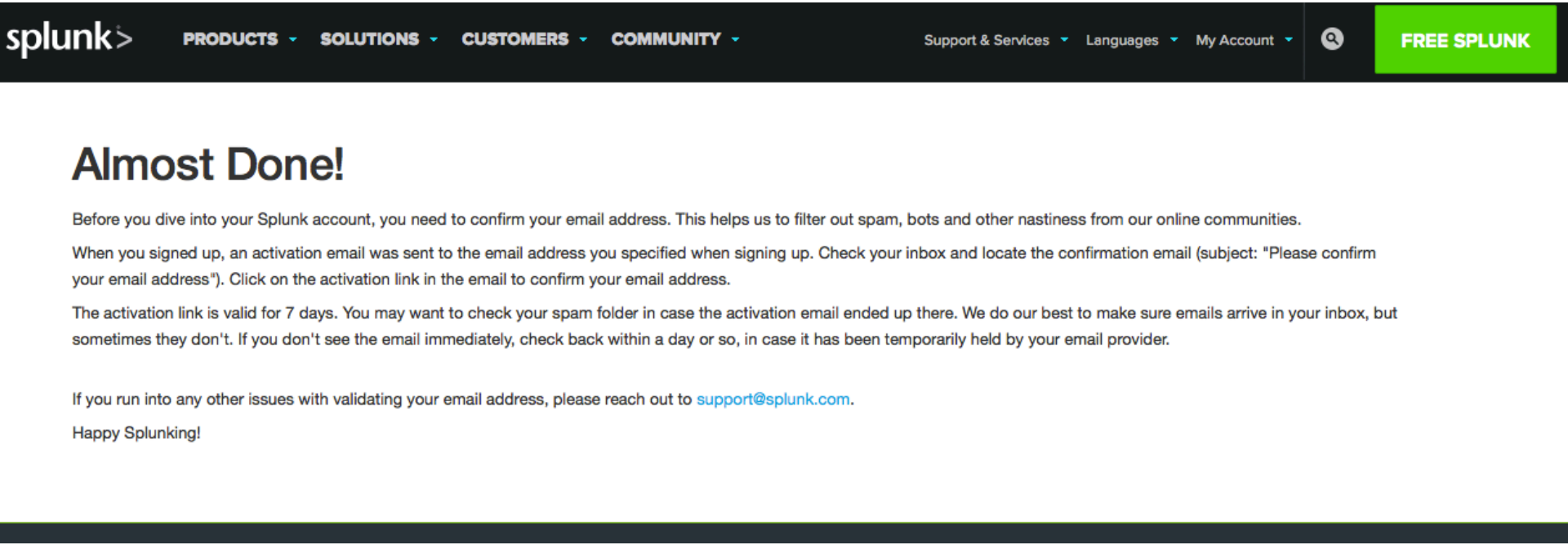
Let’s create a sandbox

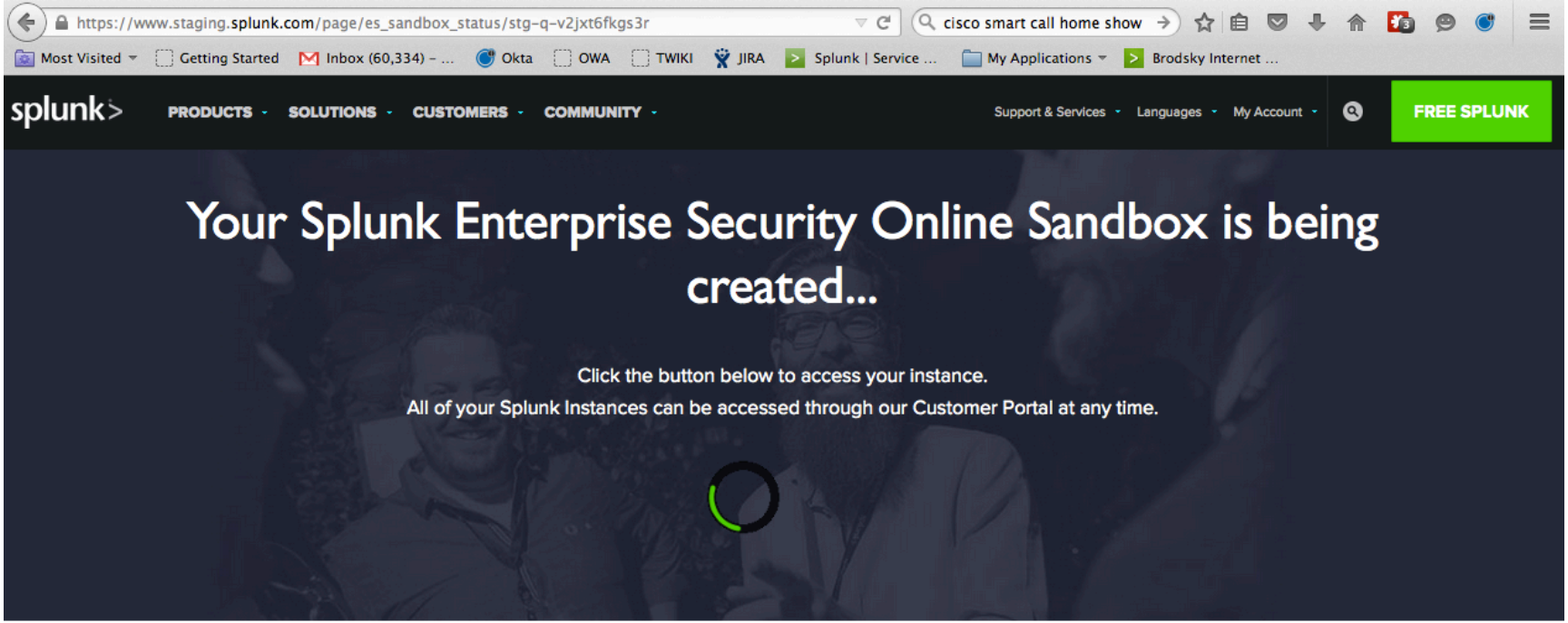
splunk>

https://www.splunk.com/getsplunk/es_sandbox


stg-splunk.cs19.force.com/SplunkCloud/RMEC_PeakDailyVolumePageClone?prdType=EnterpriseSecuri
cisco smart call home show
Most Visited
Getting Started
Inbox (60,334) - ...
Okta
OWA
TWIKI
JIRA
Splunk | Service ...
My Applications
Brodsky Internet ...
splunk>
PRODUCTS
SOLUTIONS
CUSTOMERS
COMMUNITY
SUPPORT & SERVICES
My Account
My Splunk
Support & Services
PRODUCT
Splunk Enterprise Security
PLAN DETAILS
Select Below
DUE YEARLY
$0.00
plus tax
CONTINUE
Experience the power of Splunk Enterprise Security - Free for 15 Days
The Splunk Enterprise Security Online Sandbox provides you with 15 days of access to a free, personal Splunk environment provisioned in the cloud. View Our Online Sandbox FAQ.
FREE ONLINE SANDBOX
10GB
/ day
55GB total storage
FREE
/ for 15 days

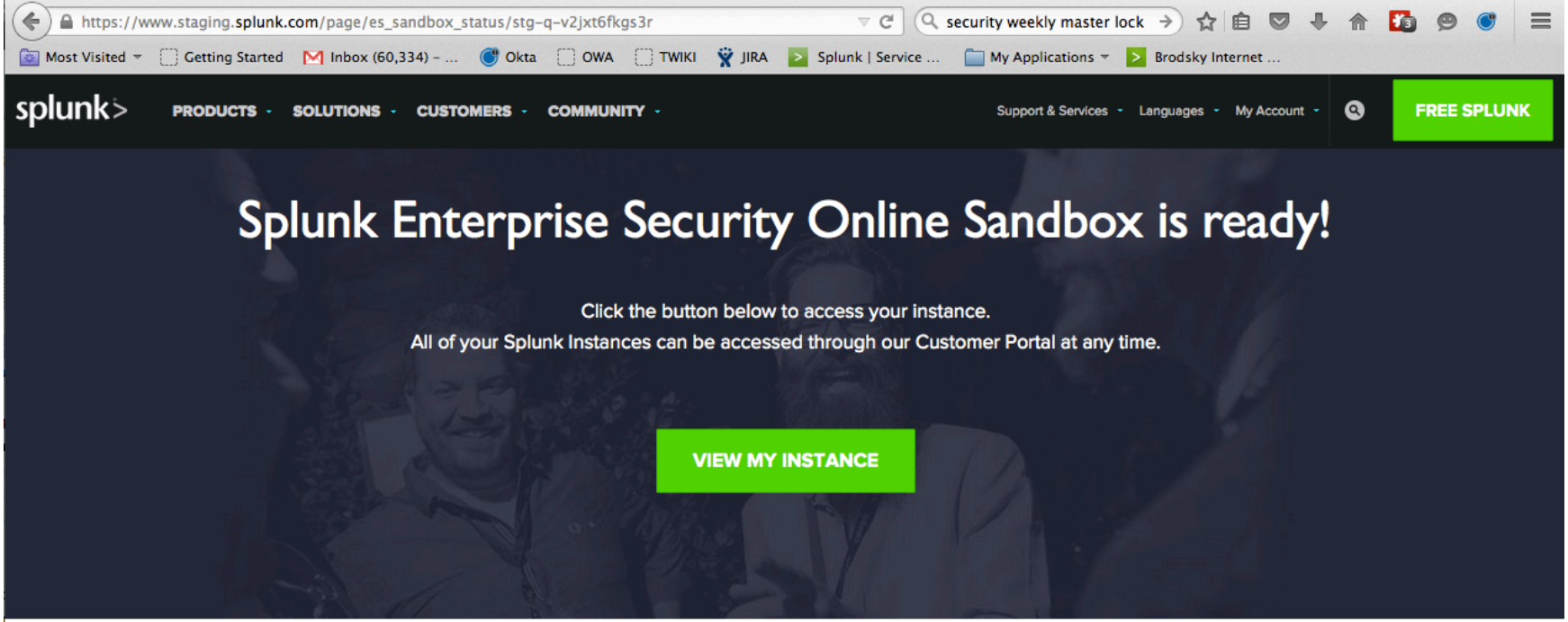

https://www.staging.splunk.com/page/sign_up/es_sandbox?pdv=10&plan=Trial&price=0&prod=Splunk+
cisco smart call home show
Most Visited
Getting Started
Inbox (60,334) - ...
Okta
OWA
TWIKI
JIRA
Splunk | Service ...
My Applications
Brodsky Internet ...
splunk>
PRODUCTS
SOLUTIONS
CUSTOMERS
COMMUNITY
My Account
My Splunk
Support & Services
PRODUCT
Splunk Enterprise Security
PLAN DETAILS
10GB/ day
DUE TRIAL
$0.00
plus tax
Create a Splunk account to view your purchases, download an app and stay connected to the community.
Sign up today to get access to everything Splunk.
Sign Up
Log in
James
Brodsky
jxb3
jxb3@sharklasers.com
SplunkLasers Inc
United States
Colorado
80027
3039561135
I agree to the Splunk Websites Terms and Conditions of Use and Splunk Privacy Policy.
CREATE ACCOUNT AND CONTINUE


splunk>
PRODUCTS
SOLUTIONS
CUSTOMERS
COMMUNITY
Support & Services
Languages
My Account
FREE SPLUNK
Almost Done!
Before you dive into your Splunk account, you need to confirm your email address. This helps us to filter out spam, bots and other nastiness from our online communities.
When you signed up, an activation email was sent to the email address you specified when signing up. Check your inbox and locate the confirmation email (subject: "Please confirm your email address"). Click on the activation link in the email to confirm your email address.
The activation link is valid for 7 days. You may want to check your spam folder in case the activation email ended up there. We do our best to make sure emails arrive in your inbox, but sometimes they don't. If you don't see the email immediately, check back within a day or so, in case it has been temporarily held by your email provider.
If you run into any other issues with validating your email address, please reach out to support@splunk.com.
Happy Splunking!

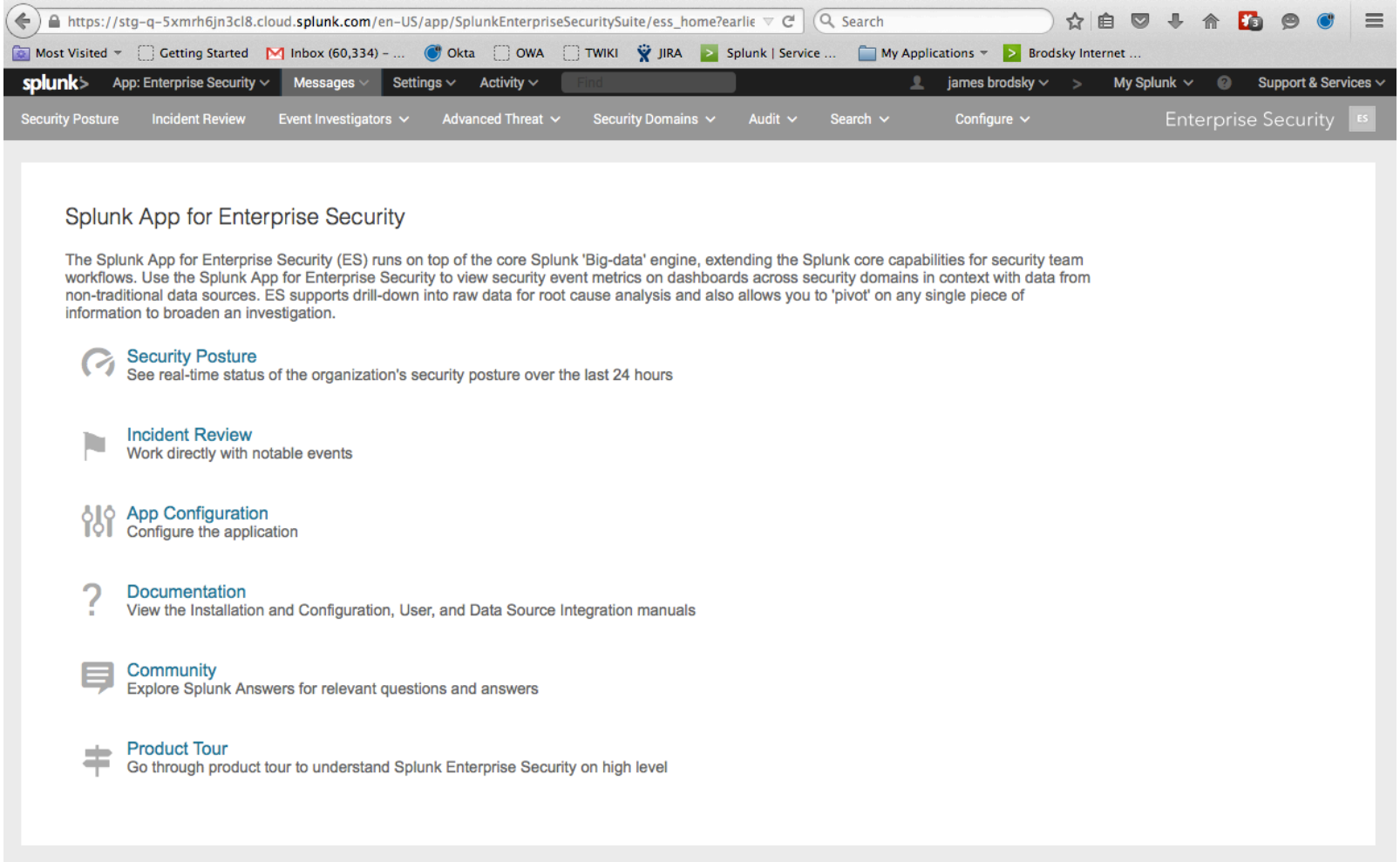


Welcome to the Splunk Community

The Splunk community is here for you! Ask a question, download an app, join a user group and more.
You can access our resources anytime by clicking on the dropdown above. Get your Splunk on!

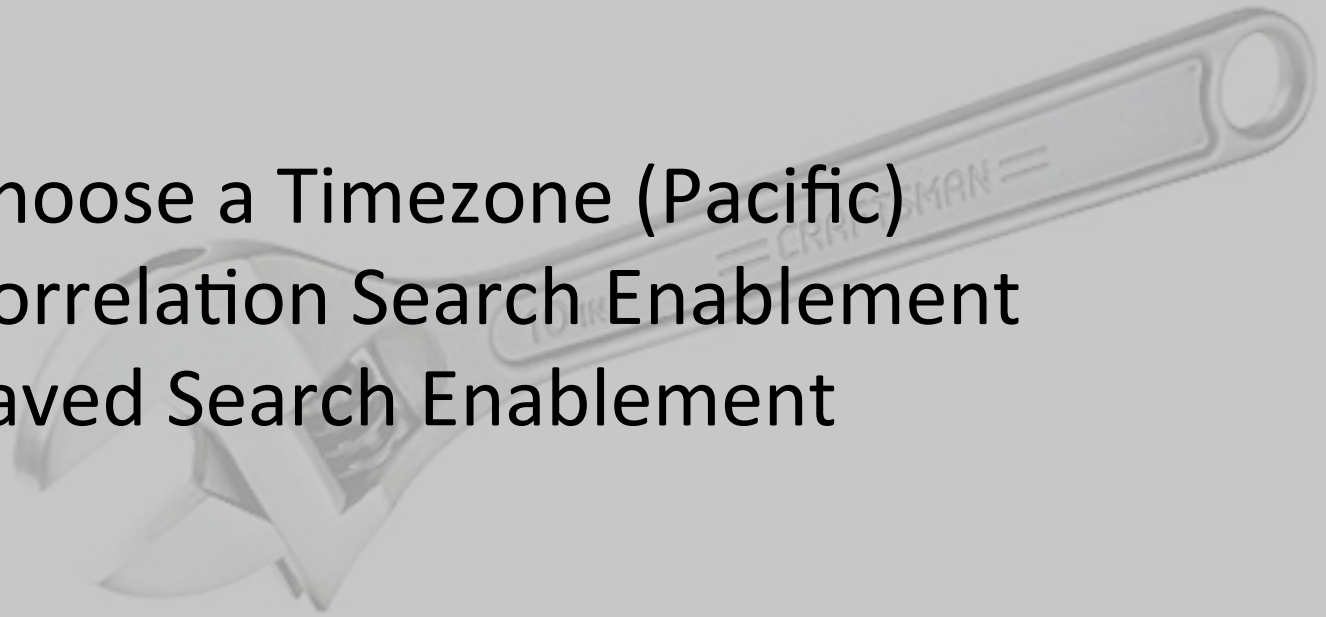

https://www.staging.splunk.com/page/es_sandbox_status/stg-q-v2jxt6fkgs3r
security weekly master lock
Most Visited
Getting Started
Inbox (60,334) - ...
Okta
OWA
TWIKI
JIRA
Splunk | Service ...
My Applications
Brodsky Internet ...
splunk>
PRODUCTS
SOLUTIONS
CUSTOMERS
COMMUNITY
Support & Services
Languages
My Account
FREE SPLUNK
Splunk Enterprise Security Online Sandbox is ready!
Click the button below to access your instance.
All of your Splunk Instances can be accessed through our Customer Portal at any time.
VIEW MY INSTANCE
Welcome to the Splunk Community
The Splunk community is here for you! Ask a question, download an app, join a user group and more.
You can access our resources anytime by clicking on the dropdown above. Get your Splunk on!


https://stg-q-5xmrh6jn3cl8.cloud.splunk.com/en-US/account/status?samlstatus=c3RhdHVzU3RyPSAmc3
Search
Most Visited
Getting Started
Inbox (60,334) - ...
Okta
OWA
TWIKI
JIRA
Splunk | Service ...
My Applications
Brodsky Internet ...
splunk>cloud
Terms of Service
Splunk Cloud Terms of Service
These Splunk Cloud Terms of Service ("TOS") between you ("Customer") and Splunk Inc. ("Splunk"), as updated from time to time, and together with the documents and policies referred to herein (collectively, the "Agreement"), govern Customer's access to and use of any Splunk Cloud Service, the Splunk Software, the Splunk Applications and the Splunk Content. By accessing or using a Splunk Cloud Service in any manner, Customer is agreeing to the Agreement. Section 15 contains definitions of certain terms that are capitalized in these TOS.
1- SPLUNK CLOUD SERVICE.
1.1 Splunk Cloud Service Subscriptions. Subject to Customer's continuing compliance with this Agreement, Splunk will make the applicable Splunk Cloud Services available to Customer during the Subscription Term identified on the Order. Unless indicated otherwise in the Order, the Subscription Term and the Agreement will automatically renew for: an additional period of time equal to the length of the
Click here to accept the terms:
Ok
© 2005-2015 Splunk Inc. Splunk 6.3.0 build 1b982fb0e4c5

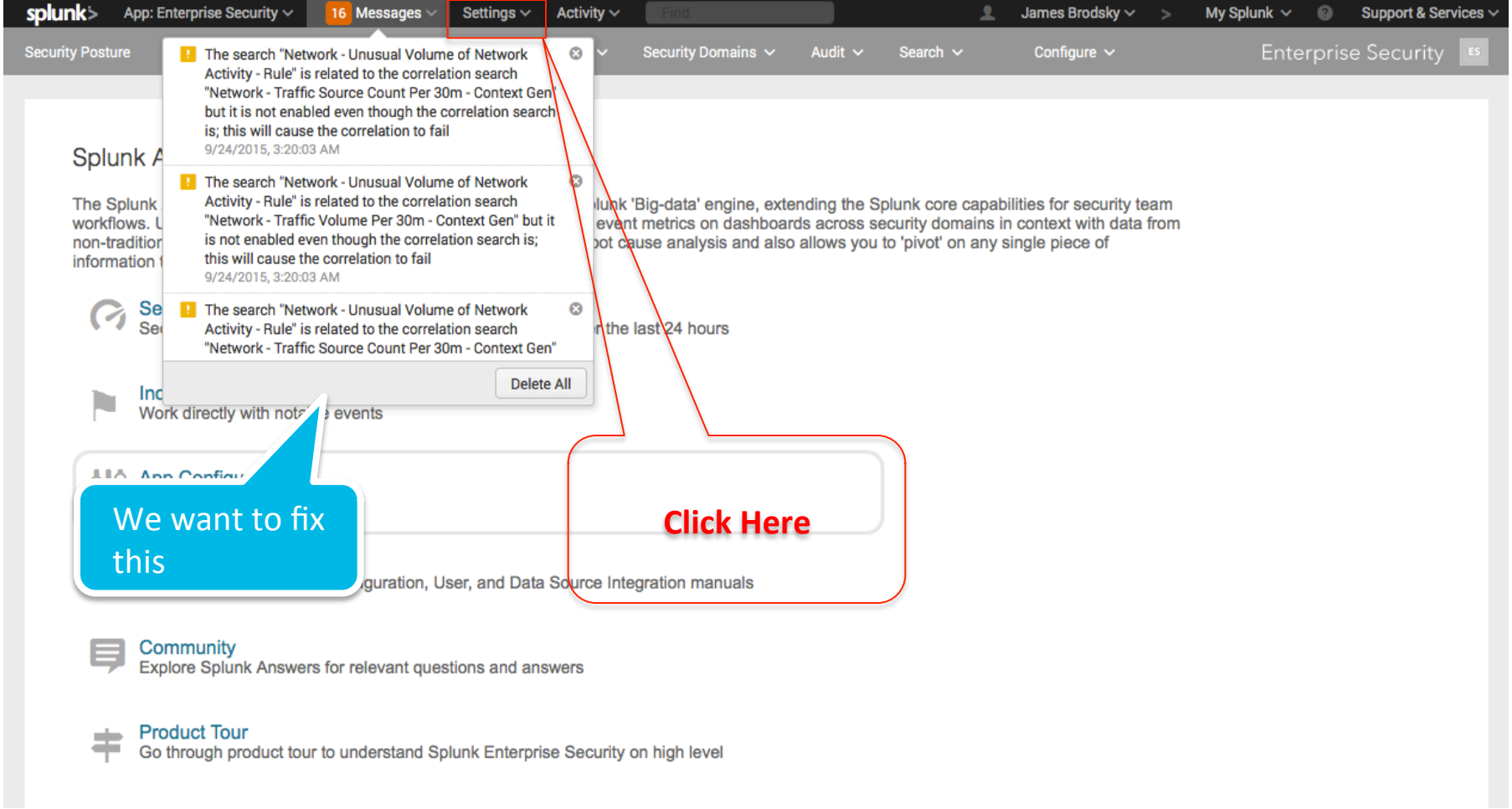

https://stg-q-5xmrh6jn3cl8.cloud.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/ess_home?earlie
Search
Most Visited
Getting Started
Inbox (60,334) - ...
Okta
OWA
TWIKI
JIRA
Splunk | Service ...
My Applications
Brodsky Internet ...
splunk>
App: Enterprise Security
Messages
Settings
Activity
Find
james brodsky
My Splunk
Support & Services
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
ES
Splunk App for Enterprise Security
The Splunk App for Enterprise Security (ES) runs on top of the core Splunk 'Big-data' engine, extending the Splunk core capabilities for security team workflows. Use the Splunk App for Enterprise Security to view security event metrics on dashboards across security domains in context with data from non-traditional data sources. ES supports drill-down into raw data for root cause analysis and also allows you to 'pivot' on any single piece of information to broaden an investigation.
Security Posture
See real-time status of the organization's security posture over the last 24 hours
Incident Review
Work directly with notable events
App Configuration
Configure the application
Documentation
View the Installation and Configuration, User, and Data Source Integration manuals
Community
Explore Splunk Answers for relevant questions and answers
Product Tour
Go through product tour to understand Splunk Enterprise Security on high level

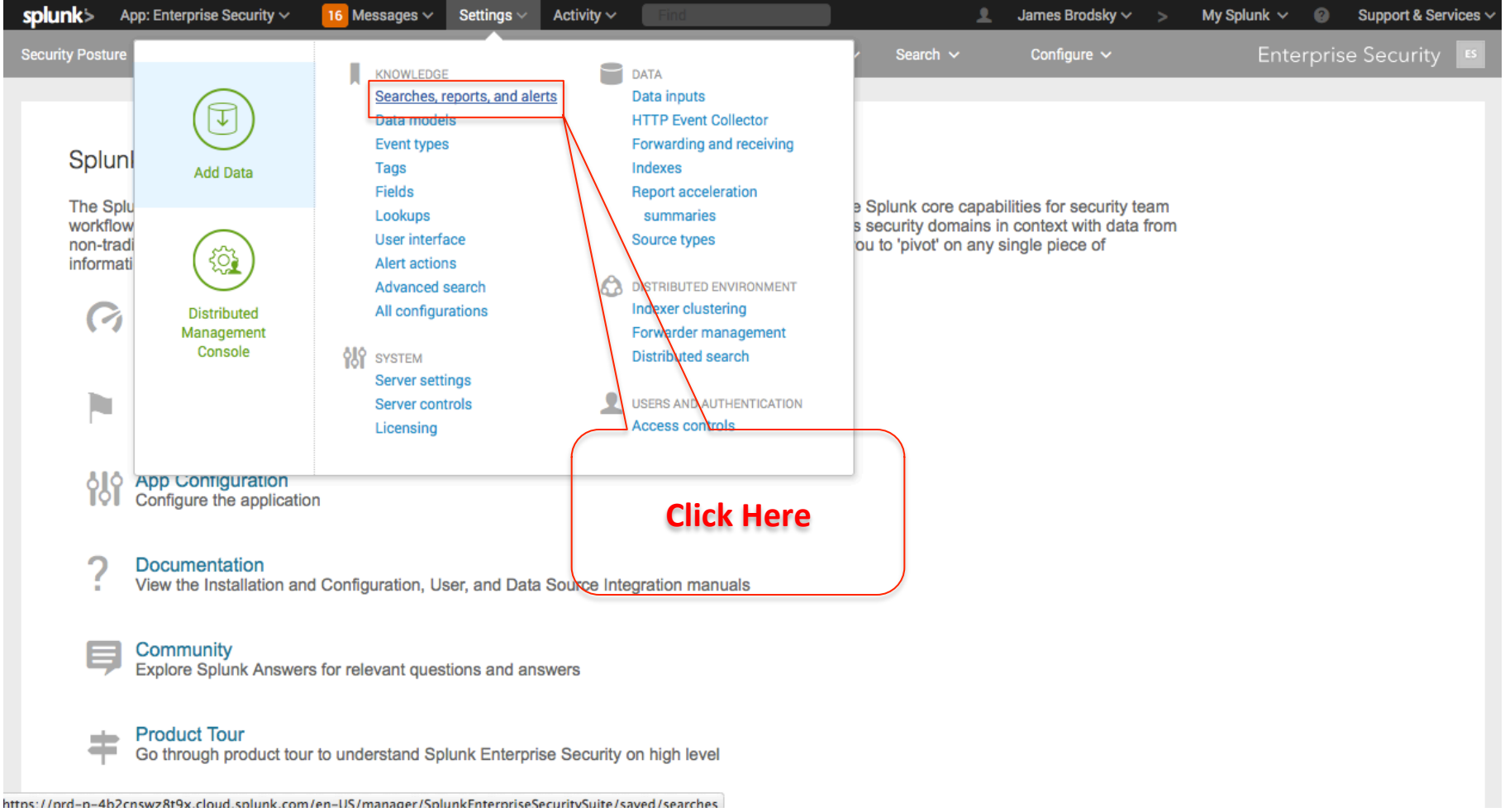
Let’s fix a few things!

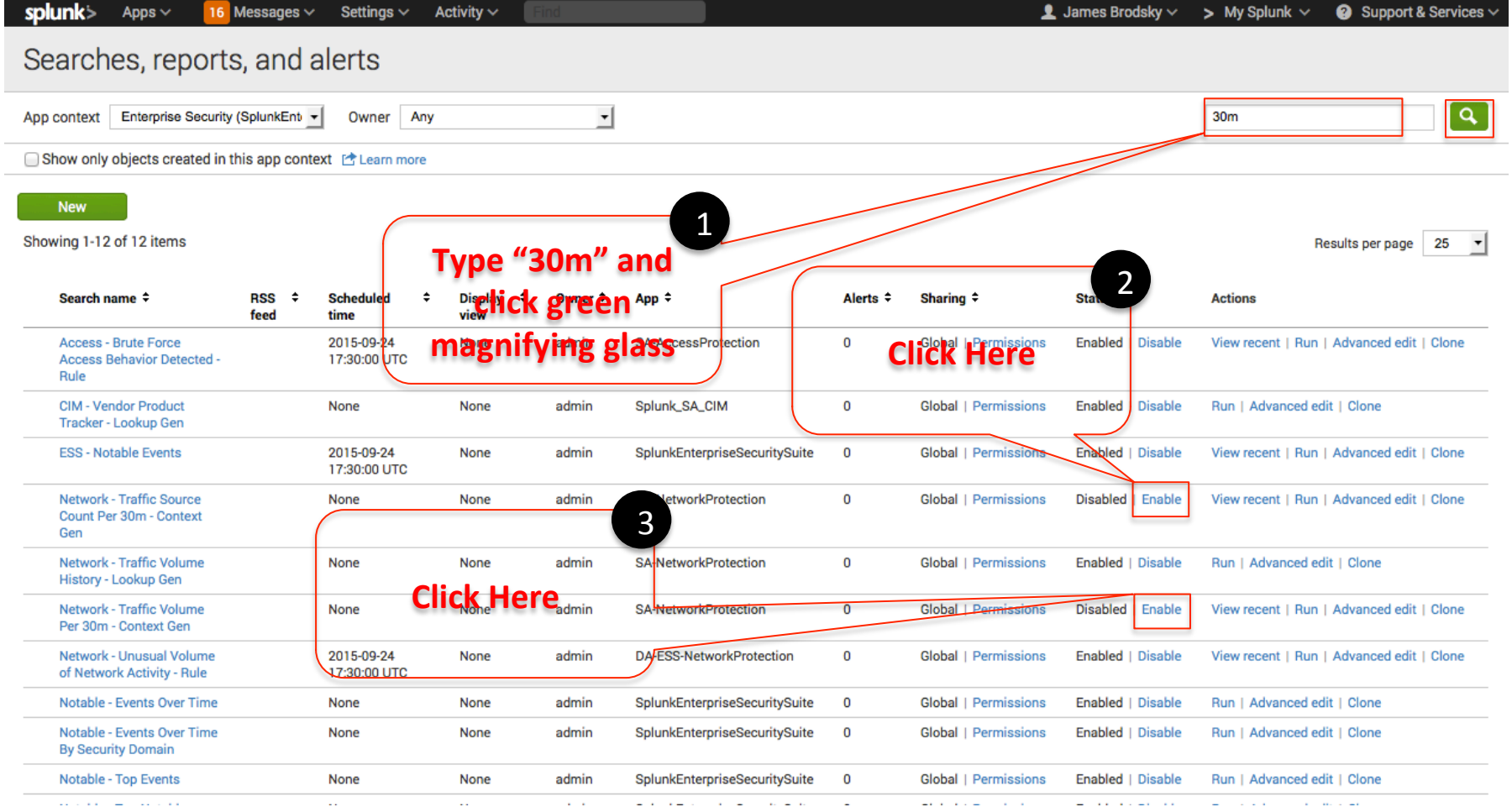
Let's fix a few things!

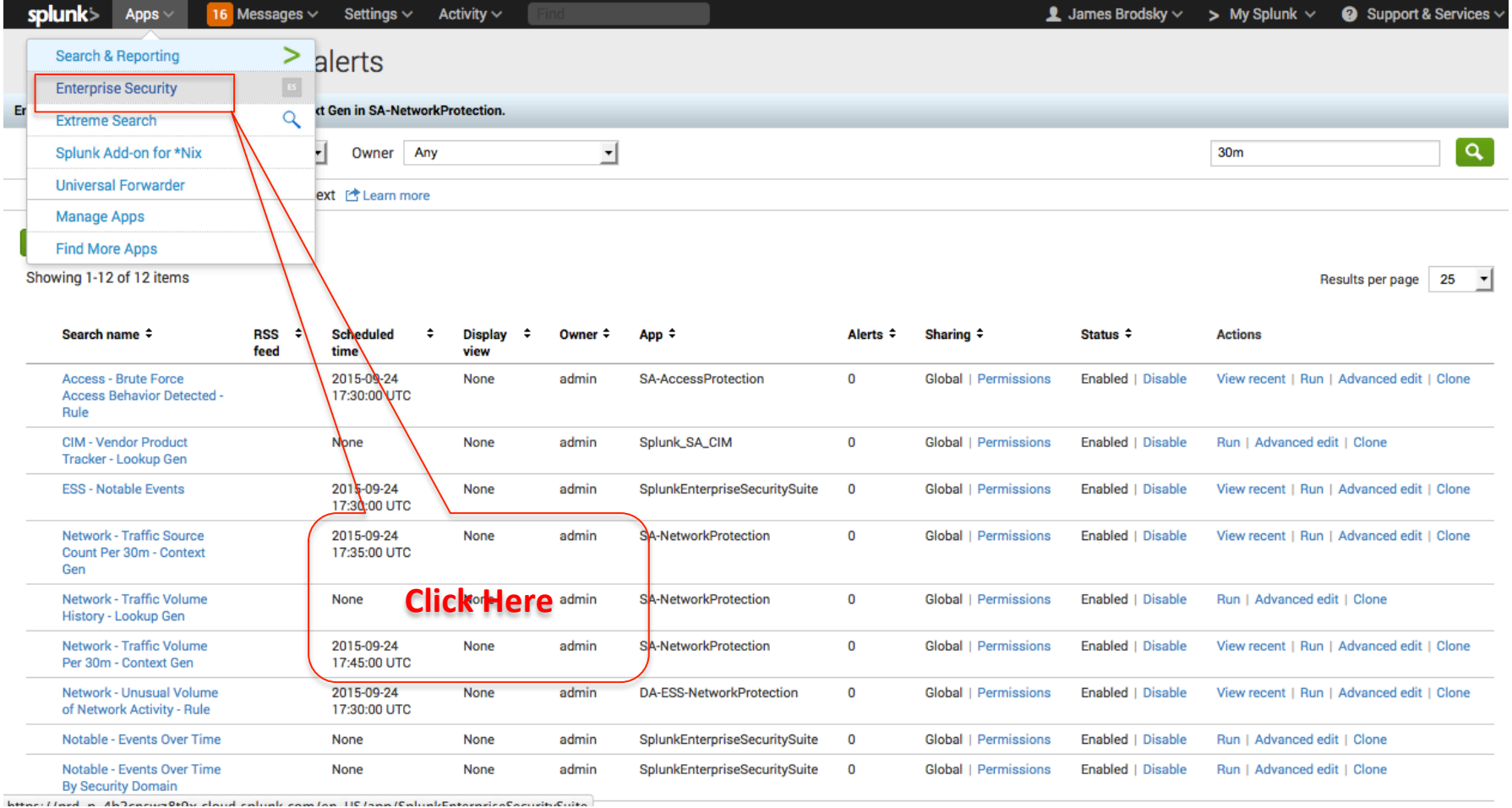


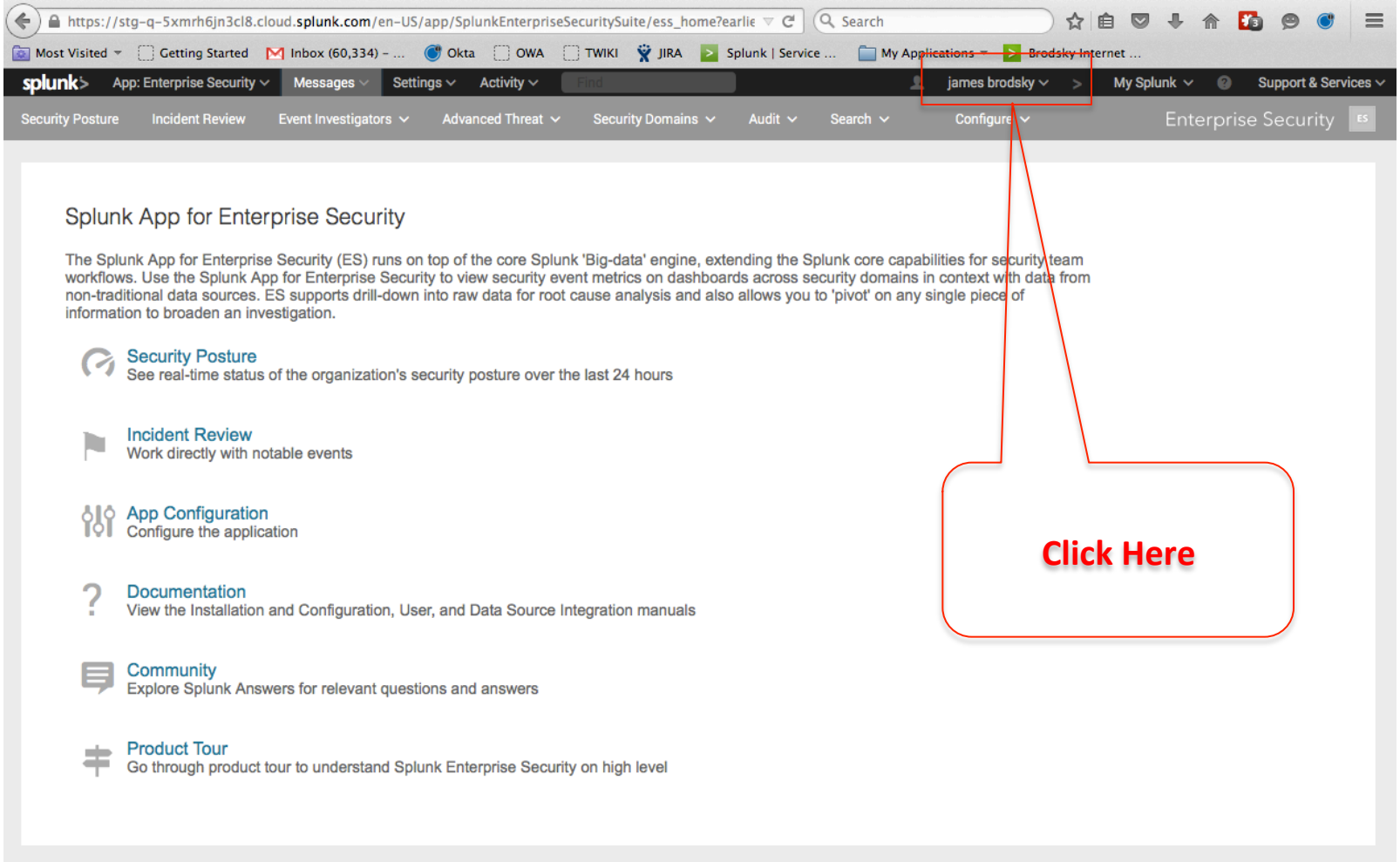
- Choose a Timezone (Pacific)
- Correlation Search Enablement
- Saved Search Enablement

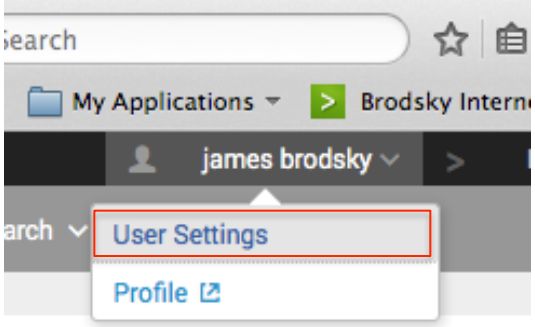

splunk> App: Enterprise Security
16 Messages
Settings
Activity
James Brodsky
My Splunk
Support & Services
Security Posture
Security Domains
Audit
Search
Configure
Enterprise Security
The search "Network - Unusual Volume of Network Activity - Rule" is related to the correlation search "Network - Traffic Source Count Per 30m - Context Gen" but it is not enabled even though the correlation search is; this will cause the correlation to fail
9/24/2015, 3:20:03 AM
The search "Network - Unusual Volume of Network Activity - Rule" is related to the correlation search "Network - Traffic Volume Per 30m - Context Gen" but it is not enabled even though the correlation search is; this will cause the correlation to fail
9/24/2015, 3:20:03 AM
The search "Network - Unusual Volume of Network Activity - Rule" is related to the correlation search "Network - Traffic Source Count Per 30m - Context Gen"
Delete All
Splunk A
The Splunk
workflows.
non-traditio
information
unk 'Big-data' engine, extending the Splunk core capabilities for security team
event metrics on dashboards across security domains in context with data from
ot cause analysis and also allows you to 'pivot' on any single piece of
the last 24 hours
Work directly with not events
We want to fix this
Click Here
guration, User, and Data Source Integration manuals
Community
Explore Splunk Answers for relevant questions and answers
Product Tour
Go through product tour to understand Splunk Enterprise Security on high level


splunk>
App: Enterprise Security
16 Messages
Settings
Activity
Find
James Brodsky
My Splunk
Support & Services
Security Posture
Search
Configure
Enterprise Security
ES
Add Data
Distributed Management Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Licensing
DATA
Data inputs
HTTP Event Collector
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
USERS AND AUTHENTICATION
Access controls
Splunk core capabilities for security team
security domains in context with data from
ou to 'pivot' on any single piece of
App Configuration
Configure the application
Documentation
View the Installation and Configuration, User, and Data Source Integration manuals
Community
Explore Splunk Answers for relevant questions and answers
Product Tour
Go through product tour to understand Splunk Enterprise Security on high level
Click Here

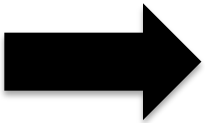

splunk> Apps 16 Messages Settings Activity James Brodsky > My Splunk Support & Services
Searches, reports, and alerts
App context Enterprise Security (SplunkEnt Owner Any
30m
Show only objects created in this app context Learn more
New
Showing 1-12 of 12 items
Results per page 25
Search name RSS feed Scheduled time Display view Owner App Alerts Sharing Status Actions
Access - Brute Force Access Behavior Detected - Rule 2015-09-24 17:30:00 UTC 0 Global | Permissions Enabled Disable View recent | Run | Advanced edit | Clone
CIM - Vendor Product Tracker - Lookup Gen None None admin Splunk_SA_CIM 0 Global | Permissions Enabled Disable Run | Advanced edit | Clone
ESS - Notable Events 2015-09-24 17:30:00 UTC None admin SplunkEnterpriseSecuritySuite 0 Global | Permissions Enabled Disable View recent | Run | Advanced edit | Clone
Network - Traffic Source Count Per 30m - Context Gen None None admin 0 Global | Permissions Disabled Enable View recent | Run | Advanced edit | Clone
Network - Traffic Volume History - Lookup Gen None None admin SA-NetworkProtection 0 Global | Permissions Enabled Disable Run | Advanced edit | Clone
Network - Traffic Volume Per 30m - Context Gen None None admin SA-NetworkProtection 0 Global | Permissions Disabled Enable View recent | Run | Advanced edit | Clone
Network - Unusual Volume of Network Activity - Rule 2015-09-24 17:30:00 UTC None admin DA-ESS-NetworkProtection 0 Global | Permissions Enabled Disable View recent | Run | Advanced edit | Clone
Notable - Events Over Time None None admin SplunkEnterpriseSecuritySuite 0 Global | Permissions Enabled Disable Run | Advanced edit | Clone
Notable - Events Over Time By Security Domain None None admin SplunkEnterpriseSecuritySuite 0 Global | Permissions Enabled Disable Run | Advanced edit | Clone
Notable - Top Events None None admin SplunkEnterpriseSecuritySuite 0 Global | Permissions Enabled Disable Run | Advanced edit | Clone
1
Type "30m" and click green magnifying glass
2
Click Here
3
Click Here

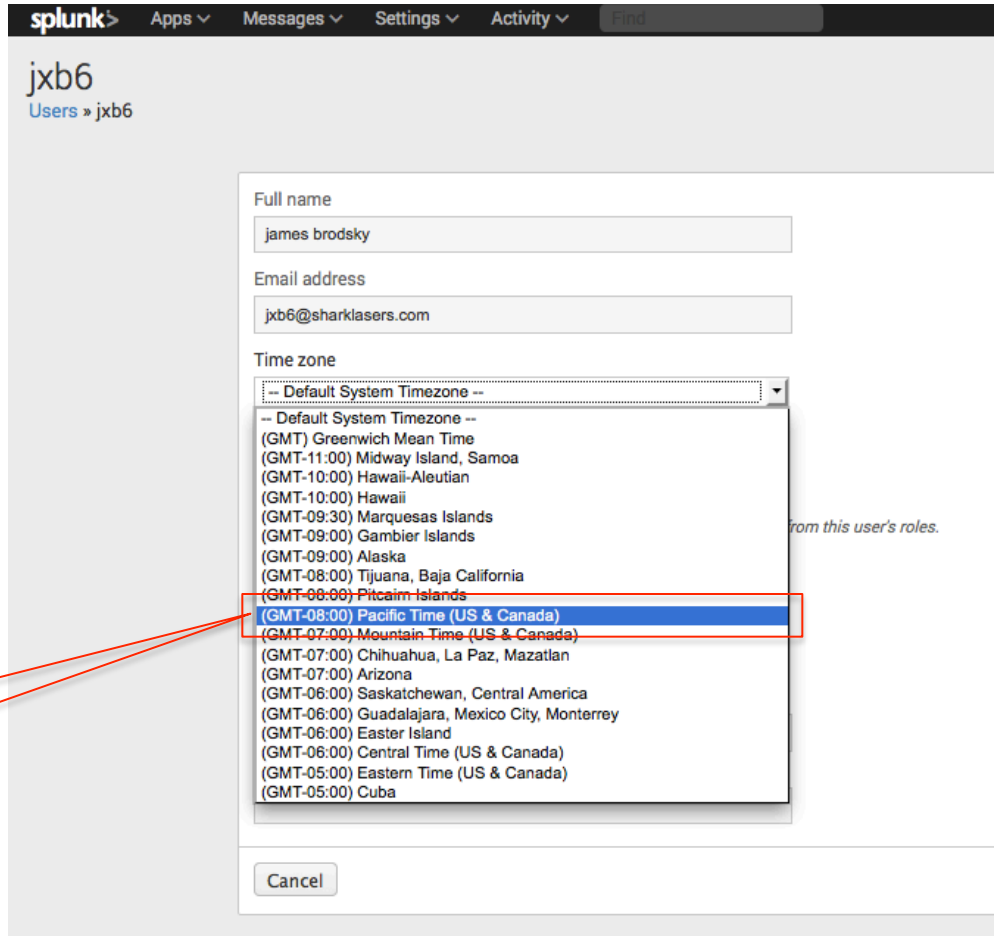

splunk>
Apps
16 Messages
Settings
Activity
James Brodsky
My Splunk
Support & Services
Search & Reporting
Enterprise Security
Extreme Search
Splunk Add-on for *Nix
Universal Forwarder
Manage Apps
Find More Apps
alerts
Owner
Any
30m
Learn more
Showing 1-12 of 12 items
Results per page
25
Search name
RSS feed
Scheduled time
Display view
Owner
App
Alerts
Sharing
Status
Actions
Access - Brute Force Access Behavior Detected - Rule
2015-09-24 17:30:00 UTC
None
admin
SA-AccessProtection
0
Global | Permissions
Enabled | Disable
View recent | Run | Advanced edit | Clone
CIM - Vendor Product Tracker - Lookup Gen
None
None
admin
Splunk_SA_CIM
0
Global | Permissions
Enabled | Disable
Run | Advanced edit | Clone
ESS - Notable Events
2015-09-24 17:30:00 UTC
None
admin
SplunkEnterpriseSecuritySuite
0
Global | Permissions
Enabled | Disable
View recent | Run | Advanced edit | Clone
Network - Traffic Source Count Per 30m - Context Gen
2015-09-24 17:35:00 UTC
None
admin
SA-NetworkProtection
0
Global | Permissions
Enabled | Disable
View recent | Run | Advanced edit | Clone
Network - Traffic Volume History - Lookup Gen
None
admin
SA-NetworkProtection
0
Global | Permissions
Enabled | Disable
Run | Advanced edit | Clone
Network - Traffic Volume Per 30m - Context Gen
2015-09-24 17:45:00 UTC
None
admin
SA-NetworkProtection
0
Global | Permissions
Enabled | Disable
View recent | Run | Advanced edit | Clone
Network - Unusual Volume of Network Activity - Rule
2015-09-24 17:30:00 UTC
None
admin
DA-ESS-NetworkProtection
0
Global | Permissions
Enabled | Disable
View recent | Run | Advanced edit | Clone
Notable - Events Over Time
None
None
admin
SplunkEnterpriseSecuritySuite
0
Global | Permissions
Enabled | Disable
Run | Advanced edit | Clone
Notable - Events Over Time By Security Domain
None
None
admin
SplunkEnterpriseSecuritySuite
0
Global | Permissions
Enabled | Disable
Run | Advanced edit | Clone
Click Here


https://stg-q-5xmrh6jn3cl8.cloud.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/ess_home?earlie
Search
Most Visited
Getting Started
Inbox (60,334) - ...
Okta
OWA
TWIKI
JIRA
Splunk | Service ...
My Applications
Brodsky Internet ...
splunk>
App: Enterprise Security
Messages
Settings
Activity
Find
james brodsky
My Splunk
Support & Services
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
ES
Splunk App for Enterprise Security
The Splunk App for Enterprise Security (ES) runs on top of the core Splunk 'Big-data' engine, extending the Splunk core capabilities for security team workflows. Use the Splunk App for Enterprise Security to view security event metrics on dashboards across security domains in context with data from non-traditional data sources. ES supports drill-down into raw data for root cause analysis and also allows you to 'pivot' on any single piece of information to broaden an investigation.
Security Posture
See real-time status of the organization's security posture over the last 24 hours
Incident Review
Work directly with notable events
App Configuration
Configure the application
Documentation
View the Installation and Configuration, User, and Data Source Integration manuals
Community
Explore Splunk Answers for relevant questions and answers
Product Tour
Go through product tour to understand Splunk Enterprise Security on high level
Click Here

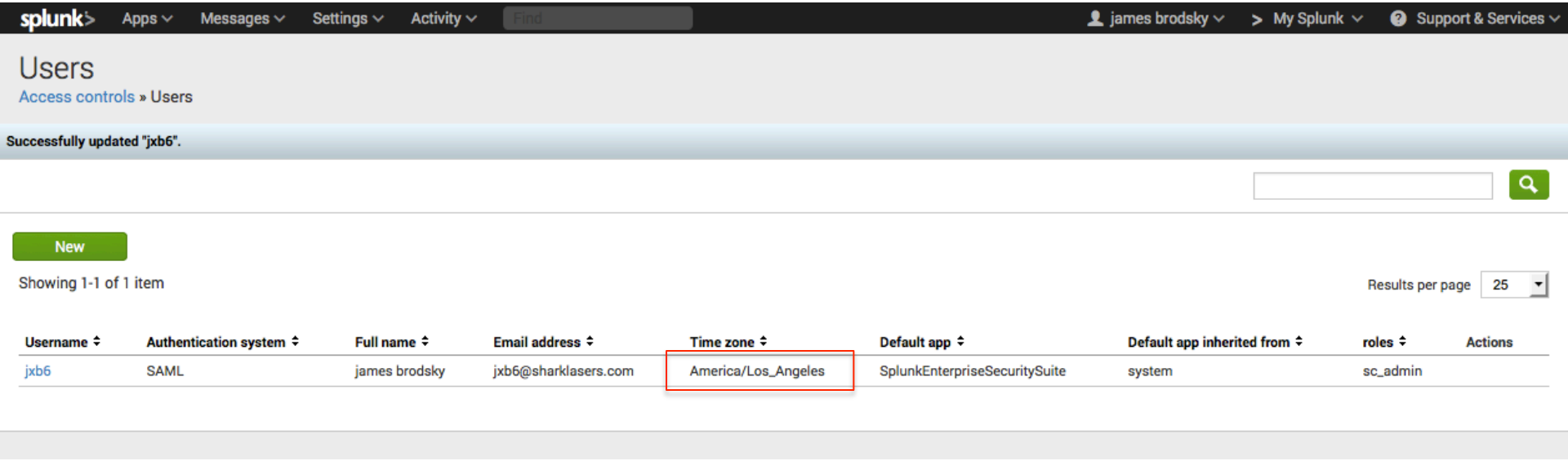


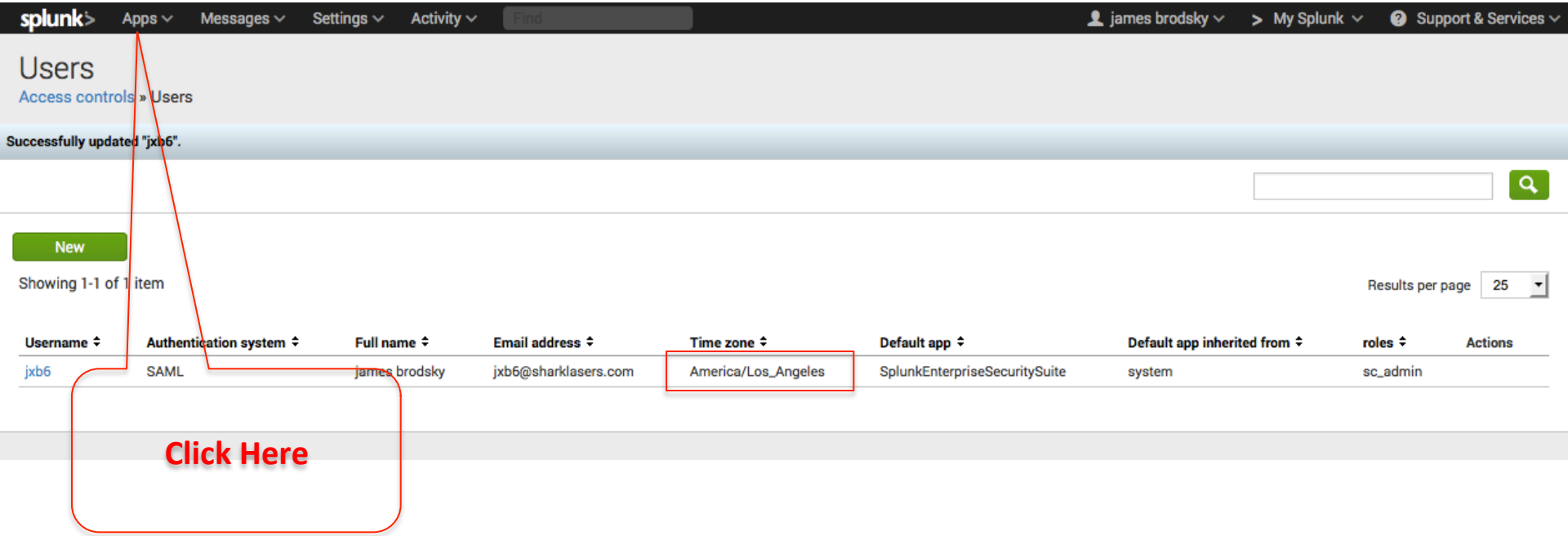
k core capabilities for security team
y domains in context with data from
vot' on any single piece of

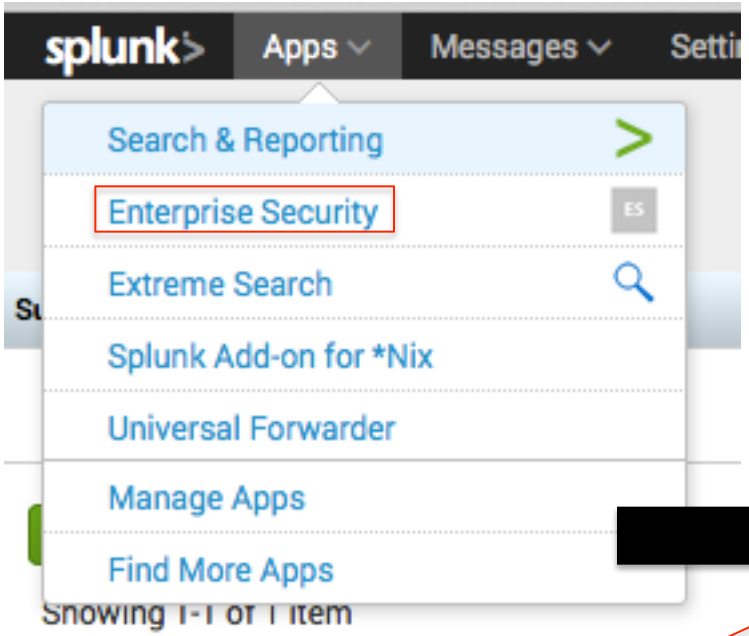


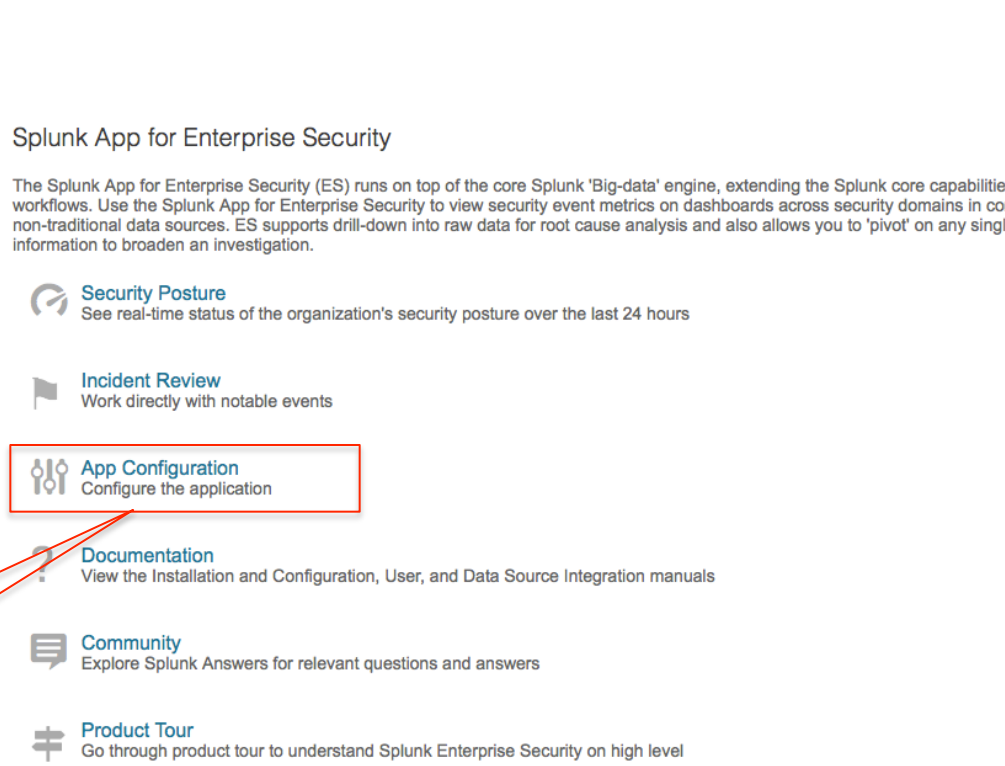


Pick “Pacific”, and save

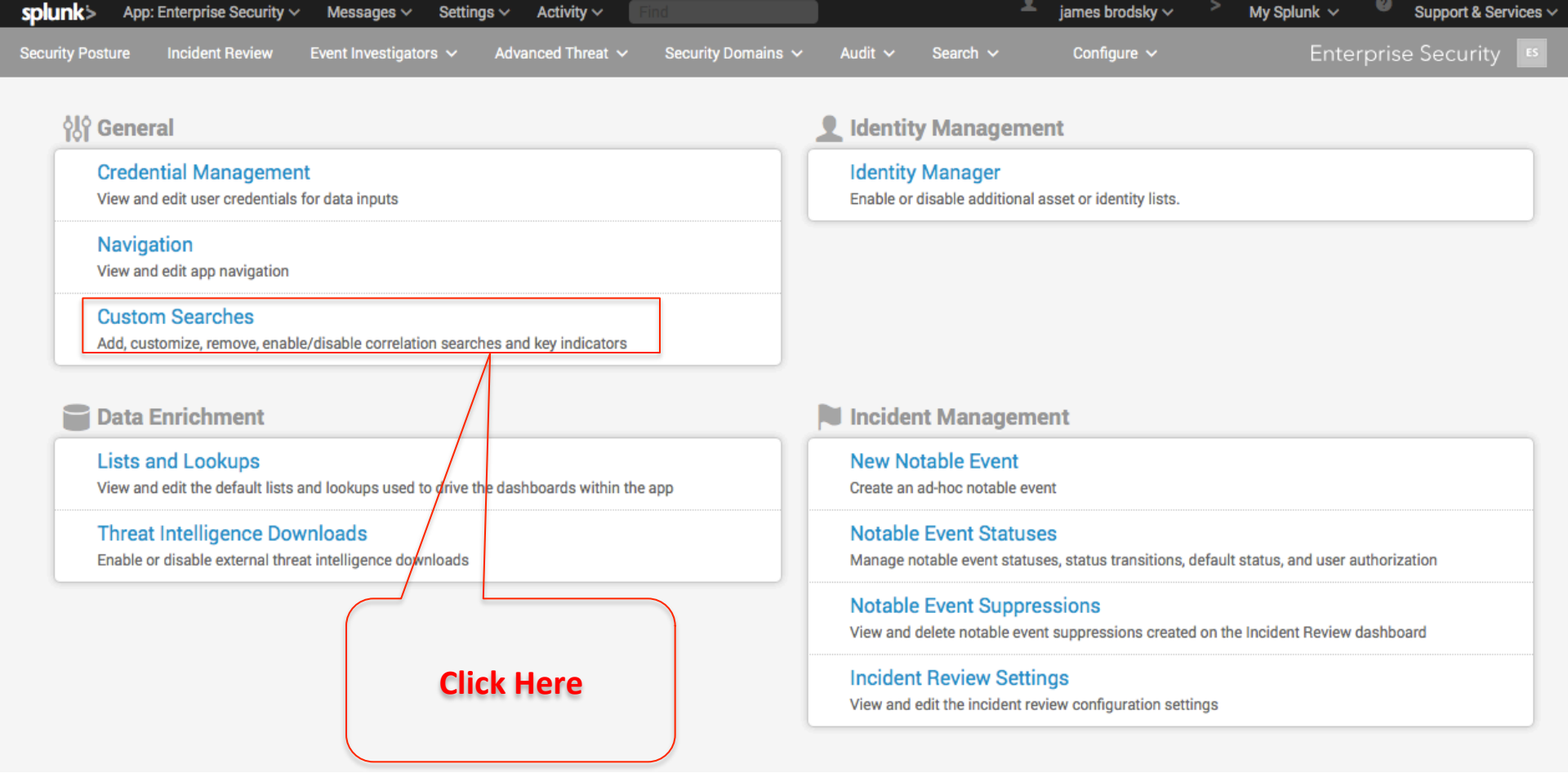

splunk>
Apps
Messages
Settings
Activity
Find
james brodsky
My Splunk
Support & Services
Users
Access controls » Users
Successfully updated "jxb6".
New
Showing 1-1 of 1 item
Results per page
25
Username
Authentication system
Full name
Email address
Time zone
Default app
Default app inherited from
roles
Actions
jxb6
SAML
james brodsky
jxb6@sharklasers.com
America/Los_Angeles
SplunkEnterpriseSecuritySuite
system
sc_admin

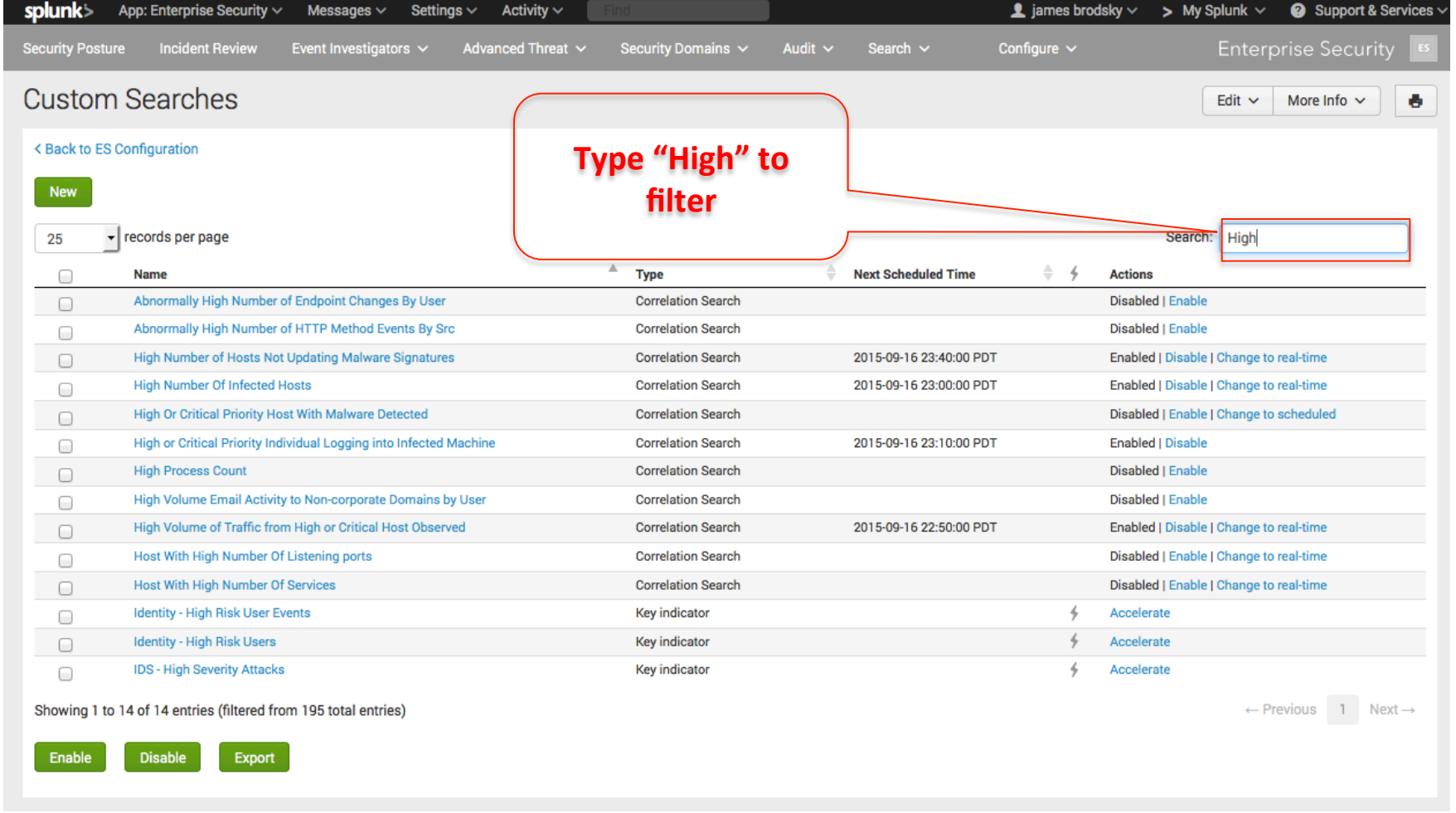

splunk>
Apps
Messages
Settings
Activity
Find
james brodsky
My Splunk
Support & Services
Users
Access controls » Users
Successfully updated "jxb6".
New
Showing 1-1 of 1 item
Results per page
25
Username
Authentication system
Full name
Email address
Time zone
Default app
Default app inherited from
roles
Actions
jxb6
SAML
james brodsky
jxb6@sharklasers.com
America/Los_Angeles
SplunkEnterpriseSecuritySuite
system
sc_admin
Click Here

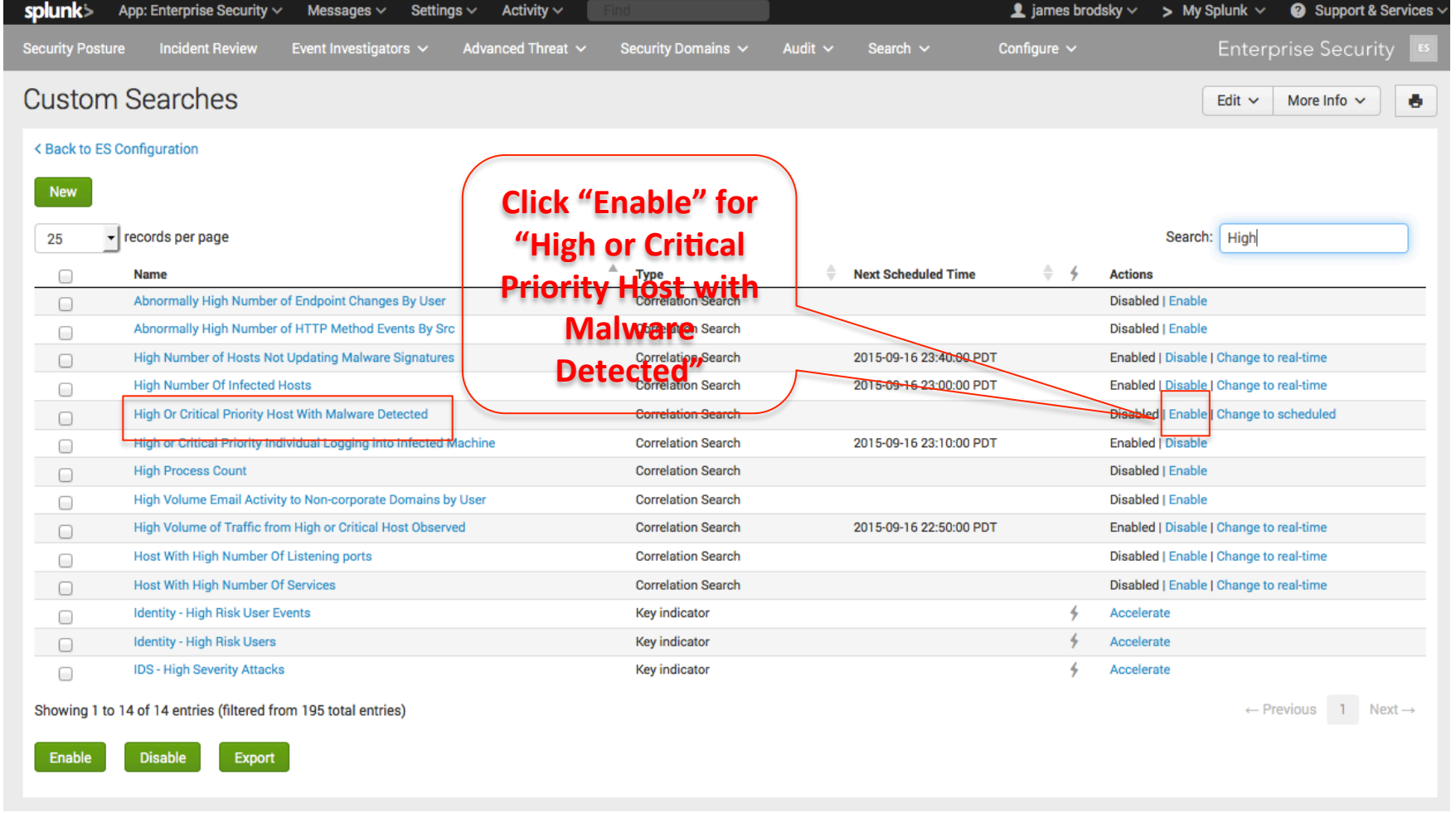

splunk>
Apps
Messages
Setti
Search & Reporting
Enterprise Security
ES
Extreme Search
Splunk Add-on for *Nix
Universal Forwarder
Manage Apps
Find More Apps
Showing 1-1 of 1 item

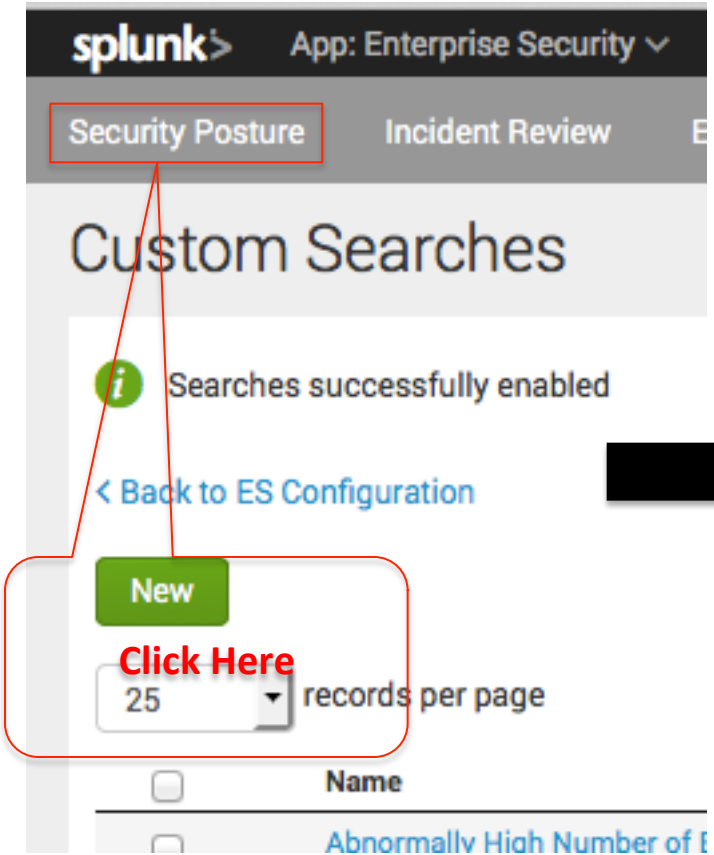

Splunk App for Enterprise Security
The Splunk App for Enterprise Security (ES) runs on top of the core Splunk 'Big-data' engine, extending the Splunk core capabilitie
workflows. Use the Splunk App for Enterprise Security to view security event metrics on dashboards across security domains in co
non-traditional data sources. ES supports drill-down into raw data for root cause analysis and also allows you to 'pivot' on any singl
information to broaden an investigation.
Security Posture
See real-time status of the organization's security posture over the last 24 hours
Incident Review
Work directly with notable events
App Configuration
Configure the application
Documentation
View the Installation and Configuration, User, and Data Source Integration manuals
Community
Explore Splunk Answers for relevant questions and answers
Product Tour
Go through product tour to understand Splunk Enterprise Security on high level

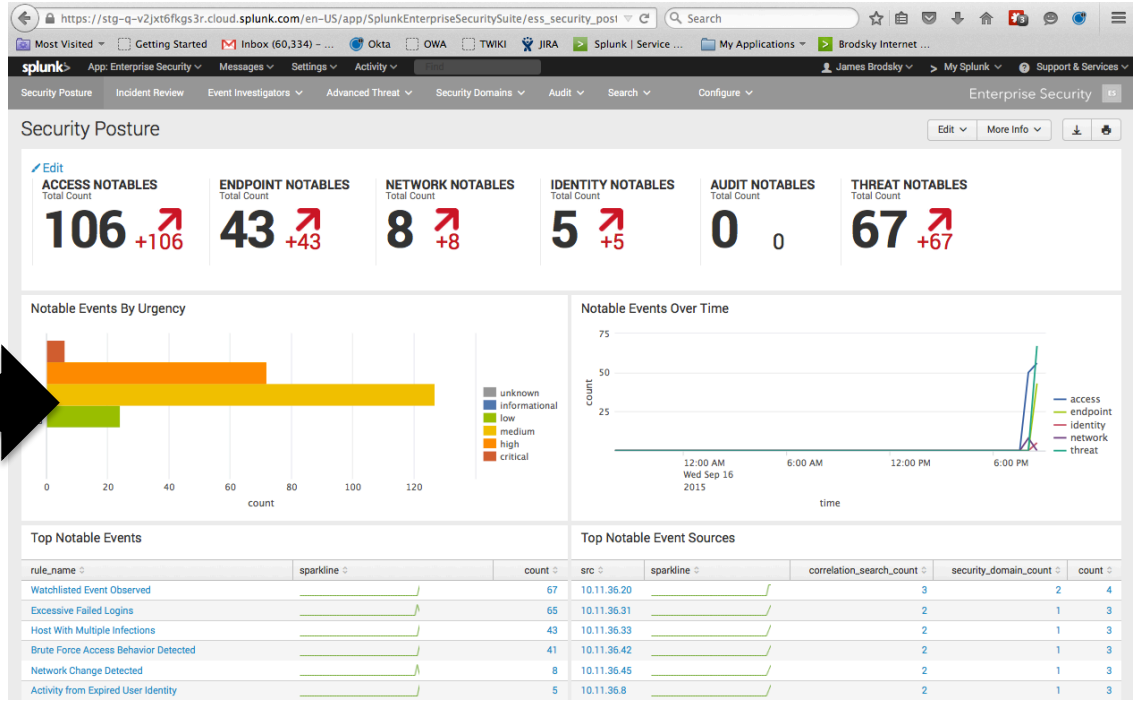
Click Here


splunk> App: Enterprise Security Messages Settings Activity Find james brodsky My Splunk Support & Services
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure Enterprise Security ES
General
Credential Management
View and edit user credentials for data inputs
Navigation
View and edit app navigation
Custom Searches
Add, customize, remove, enable/disable correlation searches and key indicators
Identity Management
Identity Manager
Enable or disable additional asset or identity lists.
Data Enrichment
Lists and Lookups
View and edit the default lists and lookups used to drive the dashboards within the app
Threat Intelligence Downloads
Enable or disable external threat intelligence downloads
Incident Management
New Notable Event
Create an ad-hoc notable event
Notable Event Statuses
Manage notable event statuses, status transitions, default status, and user authorization
Notable Event Suppressions
View and delete notable event suppressions created on the Incident Review dashboard
Incident Review Settings
View and edit the incident review configuration settings
Click Here


splunk> App: Enterprise Security Messages Settings Activity Find james brodsky > My Splunk Support & Services
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure Enterprise Security ES
Custom Searches
Edit More Info
Back to ES Configuration
New
Type “High” to filter
25 records per page
Search: High
Name Type Next Scheduled Time Actions
Abnormally High Number of Endpoint Changes By User Correlation Search Disabled | Enable
Abnormally High Number of HTTP Method Events By Src Correlation Search Disabled | Enable
High Number of Hosts Not Updating Malware Signatures Correlation Search 2015-09-16 23:40:00 PDT Enabled | Disable | Change to real-time
High Number Of Infected Hosts Correlation Search 2015-09-16 23:00:00 PDT Enabled | Disable | Change to real-time
High Or Critical Priority Host With Malware Detected Correlation Search Disabled | Enable | Change to scheduled
High or Critical Priority Individual Logging into Infected Machine Correlation Search 2015-09-16 23:10:00 PDT Enabled | Disable
High Process Count Correlation Search Disabled | Enable
High Volume Email Activity to Non-corporate Domains by User Correlation Search Disabled | Enable
High Volume of Traffic from High or Critical Host Observed Correlation Search 2015-09-16 22:50:00 PDT Enabled | Disable | Change to real-time
Host With High Number Of Listening ports Correlation Search Disabled | Enable | Change to real-time
Host With High Number Of Services Correlation Search Disabled | Enable | Change to real-time
Identity - High Risk User Events Key indicator Accelerate
Identity - High Risk Users Key indicator Accelerate
IDS - High Severity Attacks Key indicator Accelerate
Showing 1 to 14 of 14 entries (filtered from 195 total entries)
← Previous 1 Next →
Enable Disable Export


splunk> App: Enterprise Security Messages Settings Activity Find james brodsky My Splunk Support & Services
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure Enterprise Security ES
Custom Searches
Edit More Info
Back to ES Configuration
New
Click "Enable" for "High or Critical Priority Host with Malware Detected"
25 records per page
Search: High
Name Type Next Scheduled Time Actions
Abnormally High Number of Endpoint Changes By User Correlation Search Disabled | Enable
Abnormally High Number of HTTP Method Events By Src Correlation Search Disabled | Enable
High Number of Hosts Not Updating Malware Signatures Correlation Search 2015-09-16 23:40:00 PDT Enabled | Disable | Change to real-time
High Number Of Infected Hosts Correlation Search 2015-09-16 23:00:00 PDT Enabled | Disable | Change to real-time
High Or Critical Priority Host With Malware Detected Correlation Search Disabled | Enable | Change to scheduled
High or Critical Priority Individual Logging into Infected Machine Correlation Search 2015-09-16 23:10:00 PDT Enabled | Disable
High Process Count Correlation Search Disabled | Enable
High Volume Email Activity to Non-corporate Domains by User Correlation Search Disabled | Enable
High Volume of Traffic from High or Critical Host Observed Correlation Search 2015-09-16 22:50:00 PDT Enabled | Disable | Change to real-time
Host With High Number Of Listening ports Correlation Search Disabled | Enable | Change to real-time
Host With High Number Of Services Correlation Search Disabled | Enable | Change to real-time
Identity - High Risk User Events Key indicator Accelerate
Identity - High Risk Users Key indicator Accelerate
IDS - High Severity Attacks Key indicator Accelerate
Showing 1 to 14 of 14 entries (filtered from 195 total entries)
← Previous 1 Next →
Enable Disable Export


splunk> App: Enterprise Security
Security Posture
Incident Review
Custom Searches
Searches successfully enabled
< Back to ES Configuration
New
Click Here
25
records per page
Name


Security Posture
Edit
More Info
ACCESS NOTABLES
Total Count
106 +106
ENDPOINT NOTABLES
Total Count
43 +43
NETWORK NOTABLES
Total Count
8 +8
IDENTITY NOTABLES
Total Count
5 +5
AUDIT NOTABLES
Total Count
0 0
THREAT NOTABLES
Total Count
67 +67
Notable Events By Urgency
unknown
informational
low
medium
high
critical
count
Notable Events Over Time
count
access
endpoint
identity
network
threat
time
Top Notable Events
rule_name
sparkline
count
Watchlisted Event Observed 67
Excessive Failed Logins 65
Host With Multiple Infections 43
Brute Force Access Behavior Detected 41
Network Change Detected 8
Activity from Expired User Identity 5
Top Notable Event Sources
src
sparkline
correlation_search_count
security_domain_count
count
10.11.36.20 3 2 4
10.11.36.31 2 1 3
10.11.36.33 2 1 3
10.11.36.42 2 1 3
10.11.36.45 2 1 3
10.11.36.8 2 1 3

What's ES anyway?

splunk>

Machine data contains a definitive record of all interactions

Human  Machine

Machine  Machine

Splunk is a very effective platform to collect, store, and analyze all of that data

Splunk Solutions > Easy to Adopt

Across Data Sources, Use Cases & Consumption Models

Splunk Premium Apps

- ES — Security
- MINT — Mobile Intel
- VM — VMware
- EX — Exchange
- PCI — PCI

Rich Ecosystem of Apps

splunk>enterprise | splunk>cloud | splunk>light | Hunk

splunk> Platform for Machine Data

Forwarders | Syslog / TCP / Other | Wire Data | Relational Databases | Mobile | Sensors & Control Systems | Mainframe Data

Rapid Ascent in the Gartner SIEM Magic Quadrant*

2015 Leader and the only vendor to improve its visionary position

2014 Leader

2013 Leader

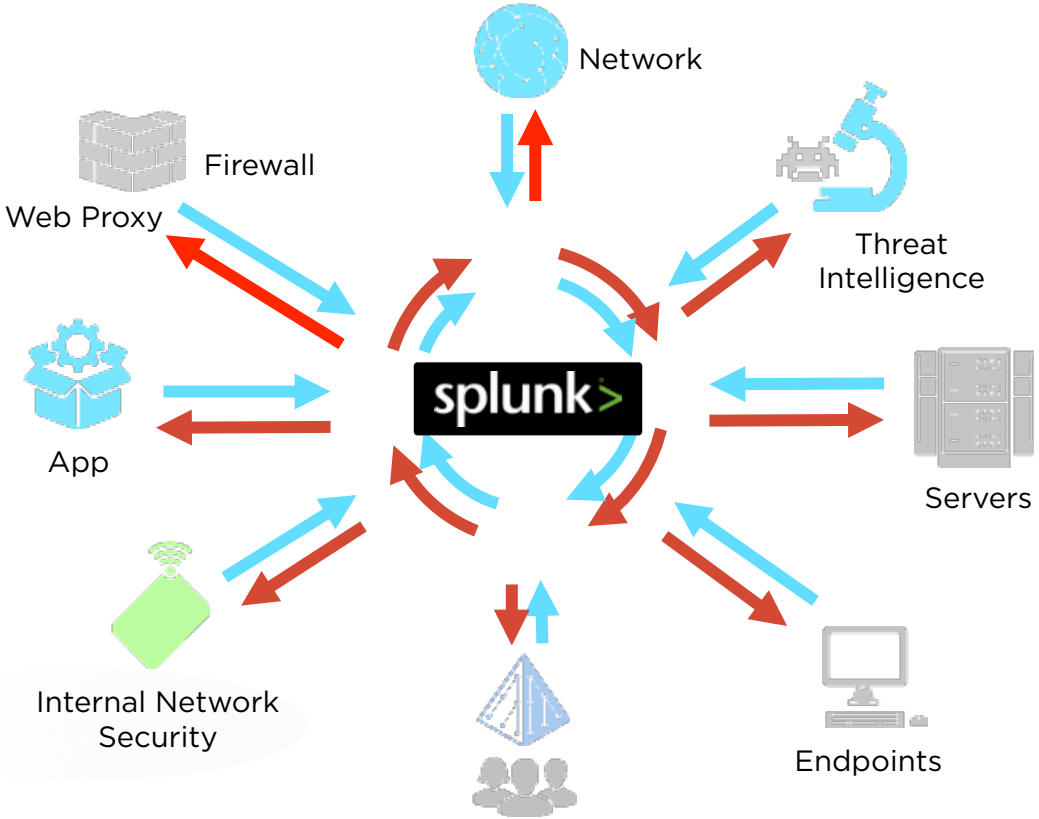
2012 Challenger

2011 Niche Player

*Gartner, Inc., SIEM Magic Quadrant 2011-2015. Gartner does not endorse any vendor, product or service depicted in its research publication and not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

2015

Splunk as the Security Nerve Center



ES Fast Facts

4.0 not in sandbox…yet

- Current version: 3.3, 4.0 just announced yesterday!
- Two releases per year
- Content comes from industry experts, market analysis, but most importantly YOU
- The best of Splunk carries through to ES – flexible, scalable, fast, and customizable
- ES has its own development team, dedicated support, services practice, and training courses

WARNING: It’s really rich!

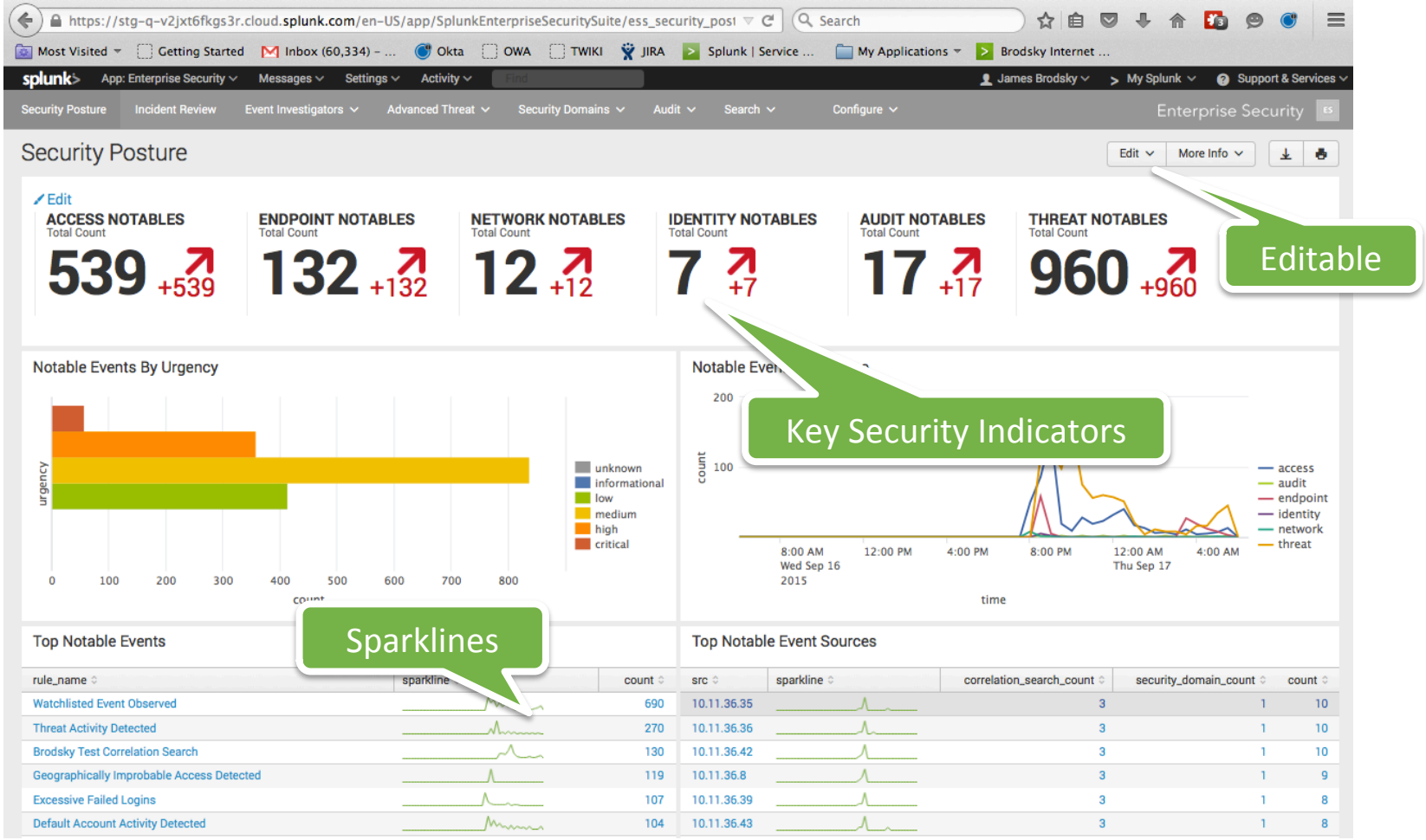
You can’t eat all of ES in one sitting, so we won’t.

Security Posture

splunk>

Security Posture

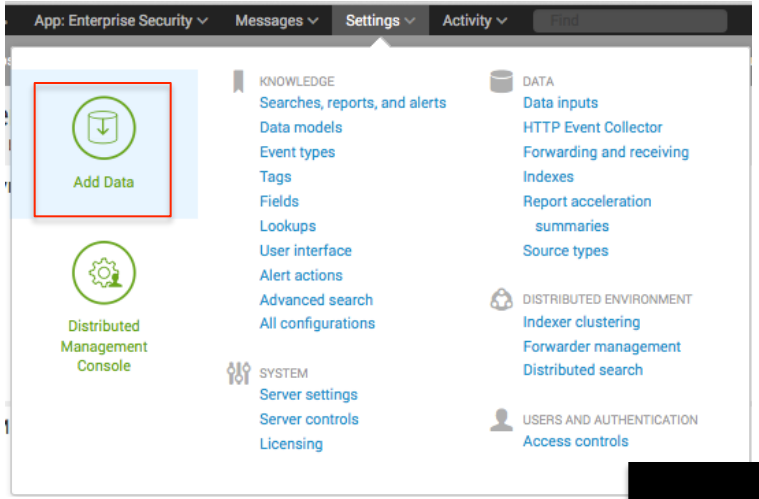
How do you start and end your day?


Security Posture
Edit
More Info
Edit
ACCESS NOTABLES
Total Count
539 +539
ENDPOINT NOTABLES
Total Count
132 +132
NETWORK NOTABLES
Total Count
12 +12
IDENTITY NOTABLES
Total Count
7 +7
AUDIT NOTABLES
Total Count
17 +17
THREAT NOTABLES
Total Count
960 +960
Editable
Key Security Indicators
Notable Events By Urgency
urgency
unknown
informational
low
medium
high
critical
0
100
200
300
400
500
600
700
800
count
Notable Event
200
100
count
access
audit
endpoint
identity
network
threat
8:00 AM
Wed Sep 16
2015
12:00 PM
4:00 PM
8:00 PM
12:00 AM
Thu Sep 17
4:00 AM
time
Sparklines
Top Notable Events
rule_name
sparkline
count
Watchlisted Event Observed 690
Threat Activity Detected 270
Brodsky Test Correlation Search 130
Geographically Improbable Access Detected 119
Excessive Failed Logins 107
Default Account Activity Detected 104
Top Notable Event Sources
src
sparkline
correlation_search_count
security_domain_count
count
10.11.36.35 3 1 10
10.11.36.36 3 1 10
10.11.36.42 3 1 10
10.11.36.8 3 1 9
10.11.36.39 3 1 8
10.11.36.43 3 1 8

How do we get data in?

splunk>

Data comes from…



upload
files from my computer

Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

forward
data from Splunk forwarder

Files - TCP/UDP - Scripts
Help me install the universal forwarder

Splunk can index any machine data. Common data sources are:

STRUCTURED DATA
CSV
JSON
XML

MICROSOFT INFRASTRUCTURE
Exchange
Active Directory
Sharepoint

NETWORK & SECURITY
Syslog & SNMP
Cisco Devices
Snort

WEB SERVICES
Apache
IIS

DATABASE SERVICES
Oracle
MySQL
Microsoft SQL Server

CLOUD
AWS Cloudtrail
Amazon S3
Azure

IT OPERATIONS
Nagios
NetApp
Cisco UCS

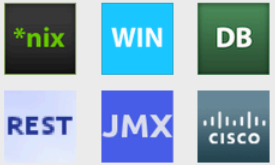
VIRTUALIZATION
VMWare
Xen Desktop
XenApp
Hyper-V

APPLICATION SERVICES
JMX & JMS
WebLogic
WebSphere
Tomcat

Featured apps

Many Splunk apps and add-ons will add data for you

See more Splunk Apps



Did you know?

You can index just about anything with Splunk.

Learn More

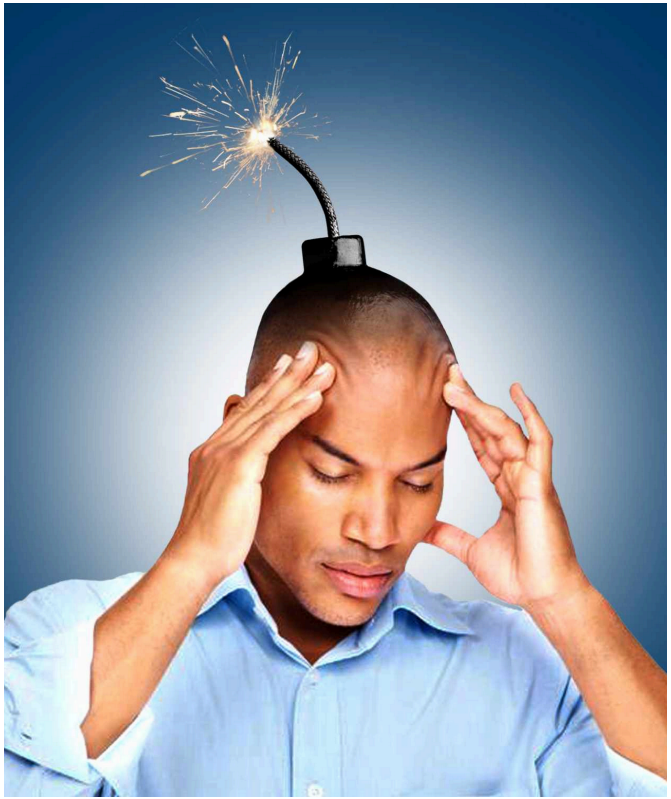
Having trouble finding data you added in Splunk?

Learn More

You can actually do this in the sandbox, if you want.

Data Ingest + Common Information Model

- You've got a bunch of systems…
- How to bring in:
  - Network AV
  - Windows + OS X AV
  - PCI-zone Linux AV
  - Network Sandboxing
  - APT Protection
- CIM = Data **Normalization**

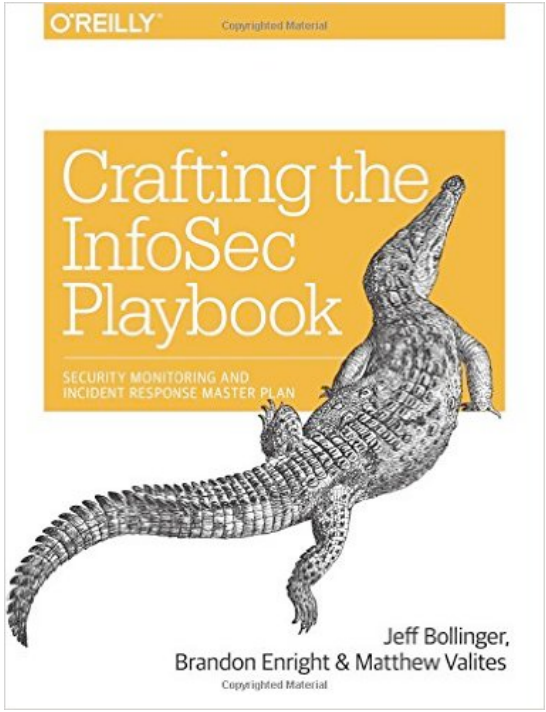



NORMALIZATION?!?

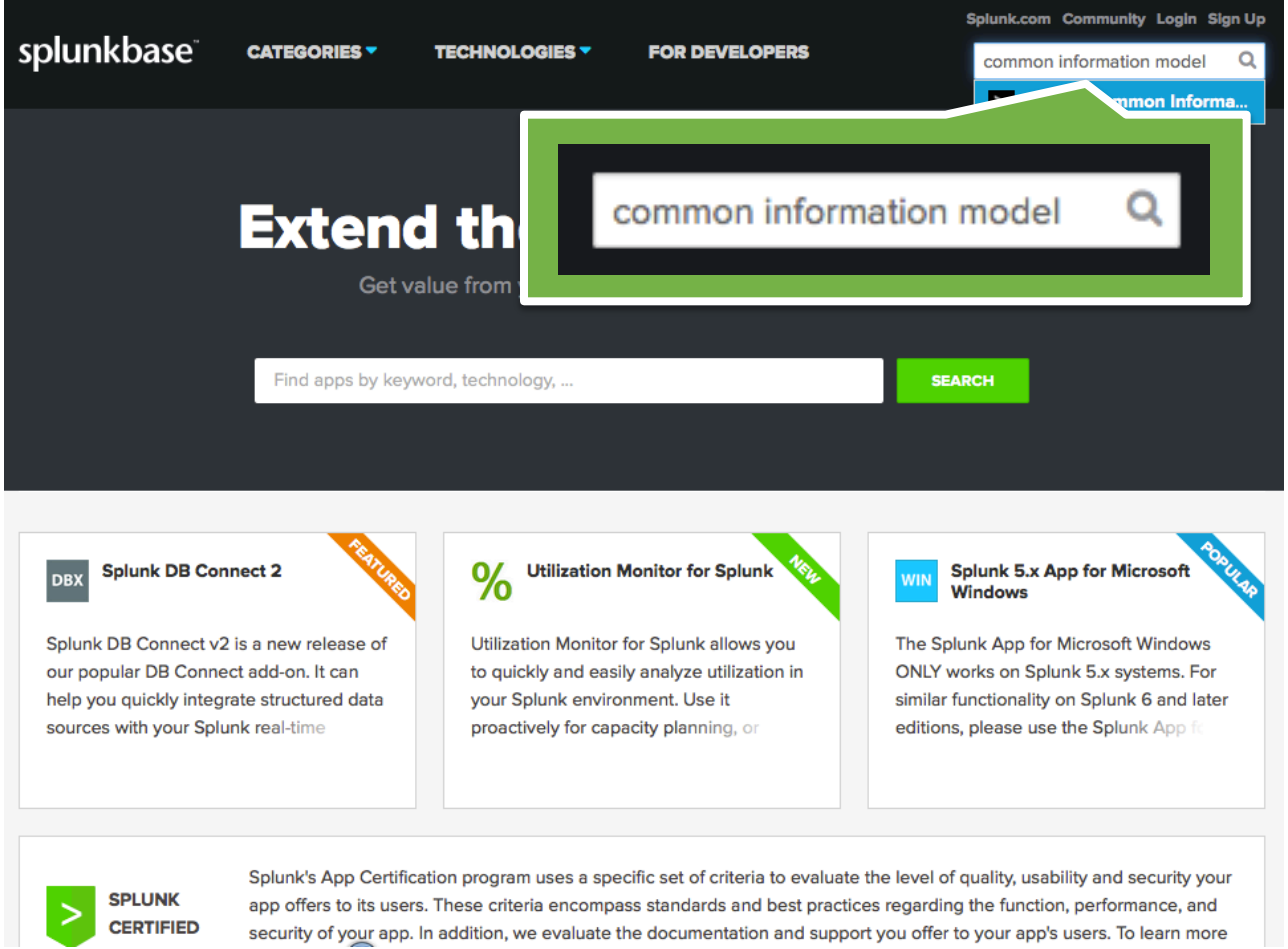

Relax. This is
splunk>
therefore, CIM gets applied at SEARCH TIME.
NORMALIZATION?!?

Data Normalization is Mandatory for your SOC

"The organization consuming the data must develop and consistently use a standard format for log normalization." – Jeff Bollinger et. al., Cisco CSIRT



Your fields don't match? Good luck creating investigative queries


splunkbase
CATEGORIES
TECHNOLOGIES
FOR DEVELOPERS
Splunk.com Community Login Sign Up
common information model
common information model
Extend th
Get value from
Find apps by keyword, technology, ...
SEARCH
DBX
Splunk DB Connect 2
FEATURED
Splunk DB Connect v2 is a new release of our popular DB Connect add-on. It can help you quickly integrate structured data sources with your Splunk real-time
%
Utilization Monitor for Splunk
NEW
Utilization Monitor for Splunk allows you to quickly and easily analyze utilization in your Splunk environment. Use it proactively for capacity planning, or
WIN
Splunk 5.x App for Microsoft Windows
POPULAR
The Splunk App for Microsoft Windows ONLY works on Splunk 5.x systems. For similar functionality on Splunk 6 and later editions, please use the Splunk App
SPLUNK CERTIFIED
Splunk's App Certification program uses a specific set of criteria to evaluate the level of quality, usability and security your app offers to its users. These criteria encompass standards and best practices regarding the function, performance, and security of your app. In addition, we evaluate the documentation and support you offer to your app's users. To learn more

Free.
Supported.
Fully documented.

splunkbase CATEGORIES TECHNOLOGIES FOR DEVELOPERS

Splunk.com Community Login Sign Up

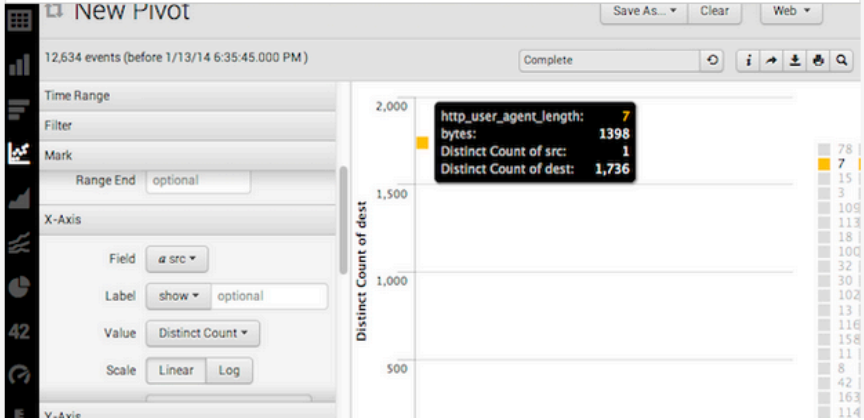
Search apps...

Splunk Common Information Model

LOGIN TO DOWNLOAD

OVERVIEW | DOCUMENTATION

The Common Information Model is a set of field names and tags which are expected to define the least common denominator of a domain of interest. It is implemented as documentation on the Splunk docs website and JSON data model files in this add-on. Use the CIM add-on when modeling data or building apps to ensure compatibility between apps, or to just take advantage of these data models to pivot and report.



6 ratings

Rate this app

7,297 downloads
Subscribe
Share this app

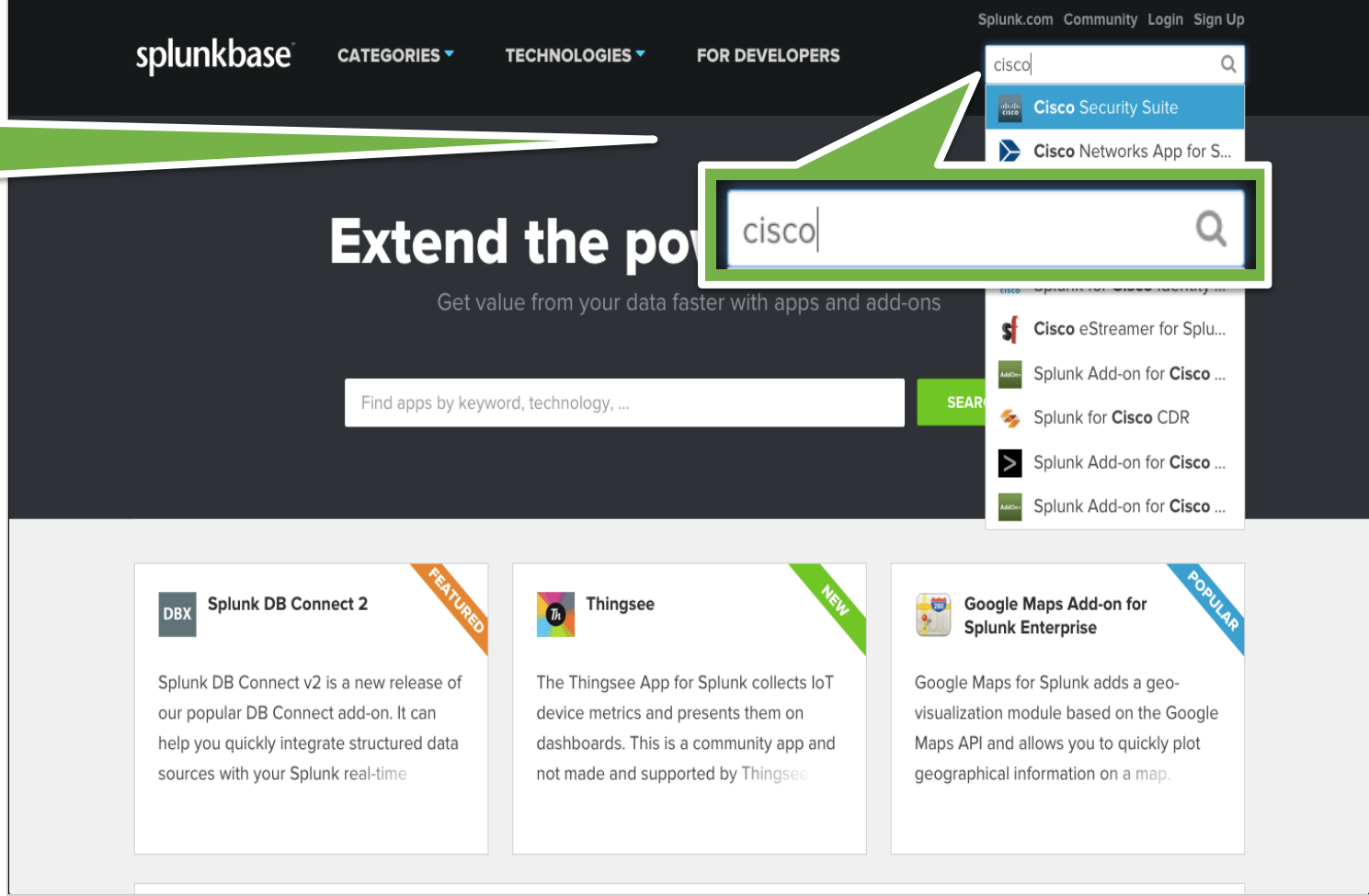
VERSION 4.2.0

Utilities
Cool Stuff
Enterprise
Add-on
Splunk 6.2, 6.1, 6.0
Splunk Software License Agreement
Platform Independent

SPLUNK SUPPORTED

Questions on SplunkAnswers
File a case
Flag as inappropriate

Lots of apps support CIM.



splunkbase CATEGORIES TECHNOLOGIES FOR DEVELOPERS

Splunk.com Community Login Sign Up

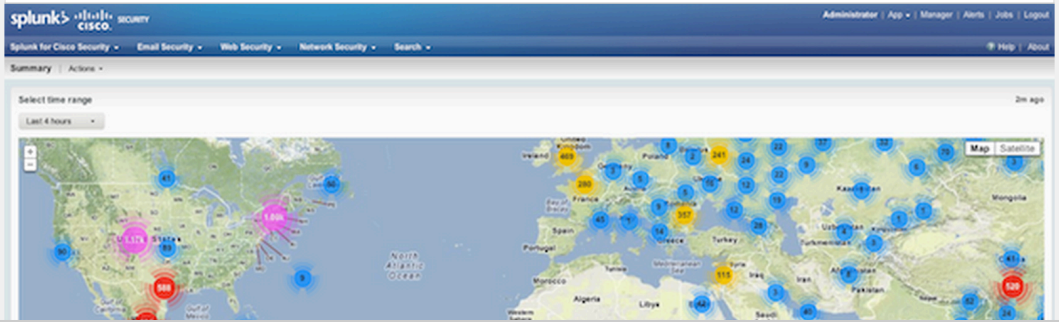
Search apps...

Cisco Security Suite

LOGIN TO DOWNLOAD

OVERVIEW | DOCUMENTATION

The Cisco Security Suite provides a single pane of glass interface into Cisco security data. It supports Cisco ASA and PIX firewall appliances, the FWSM firewall services module, Cisco IPS, Cisco Web Security Appliance (WSA), Cisco Email Security Appliance (ESA), Cisco Identity Services Engine (ISE), pxGrid, and Cisco Advanced Malware Protection / Sourcefire.



★★★★☆ 18 ratings

Rate this app

29,594 downloads

Subscribe

Share this app

CIM Compliant!

VERSION 3.1.1

Security and Compli

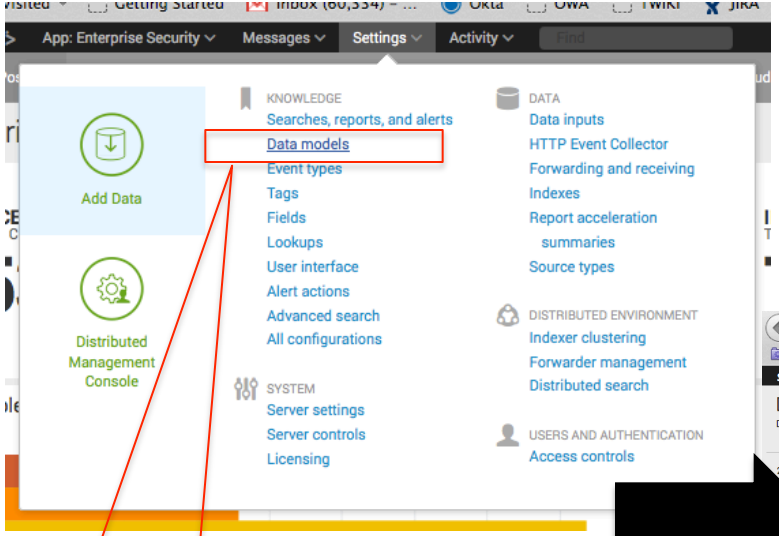
Add-on

Splunk 6.2, 6.1, 6.0

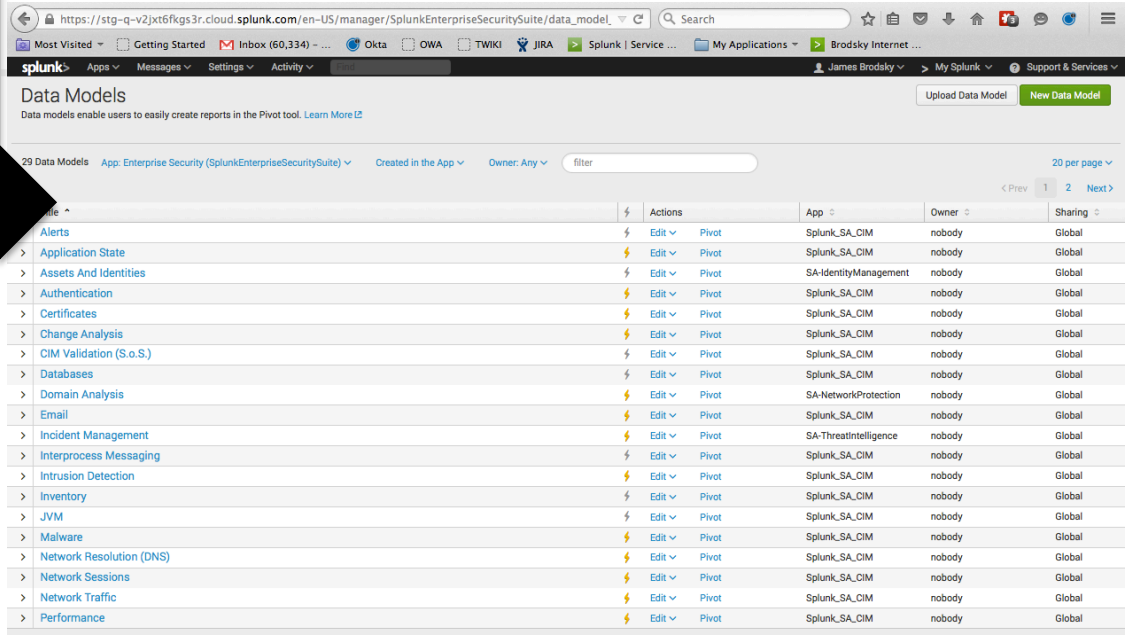
CIM 4.1, 4.0, 3.0

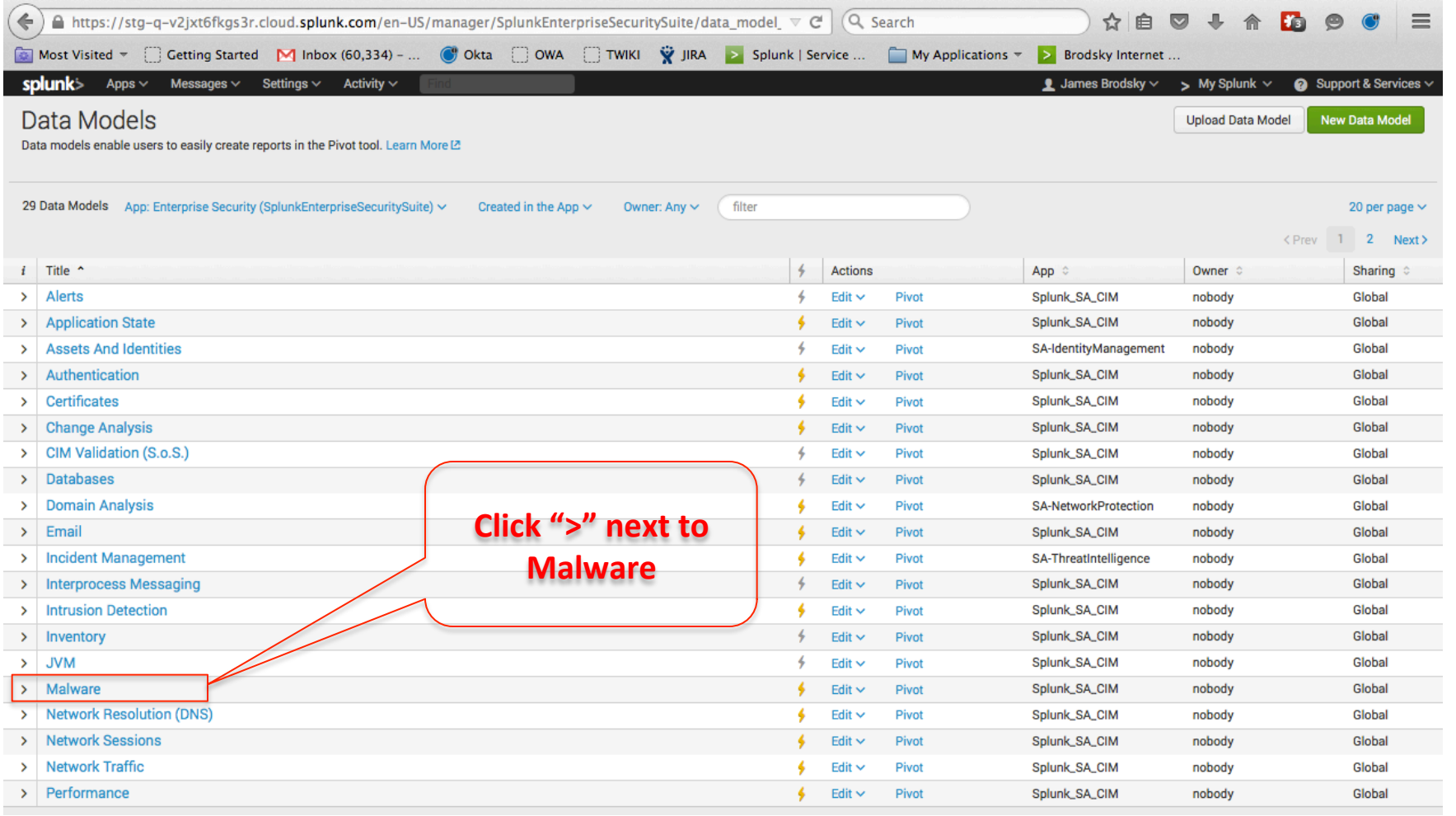
Splunk Software License Agreement

Platform Independent

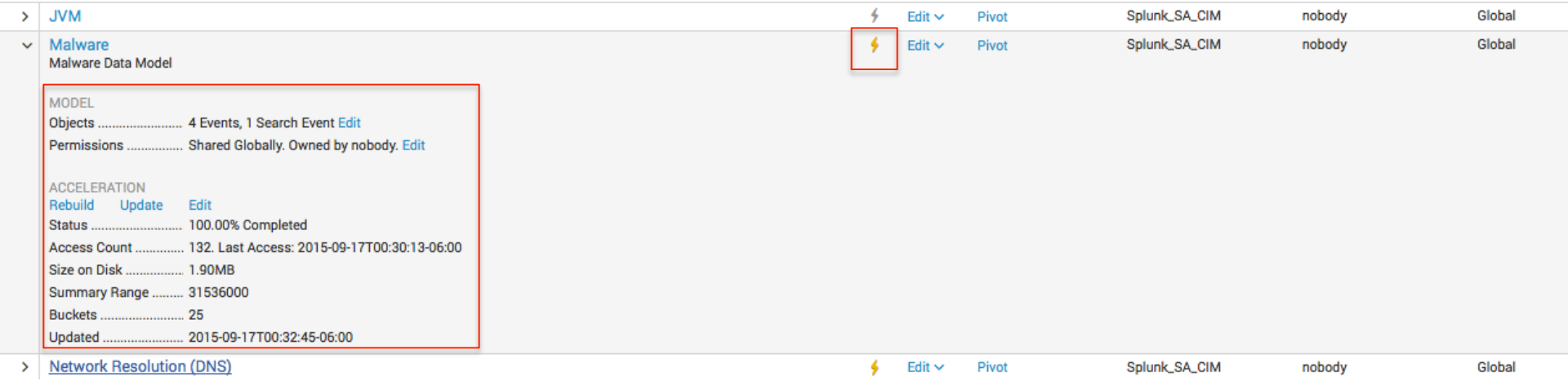


Click "Data models" under settings

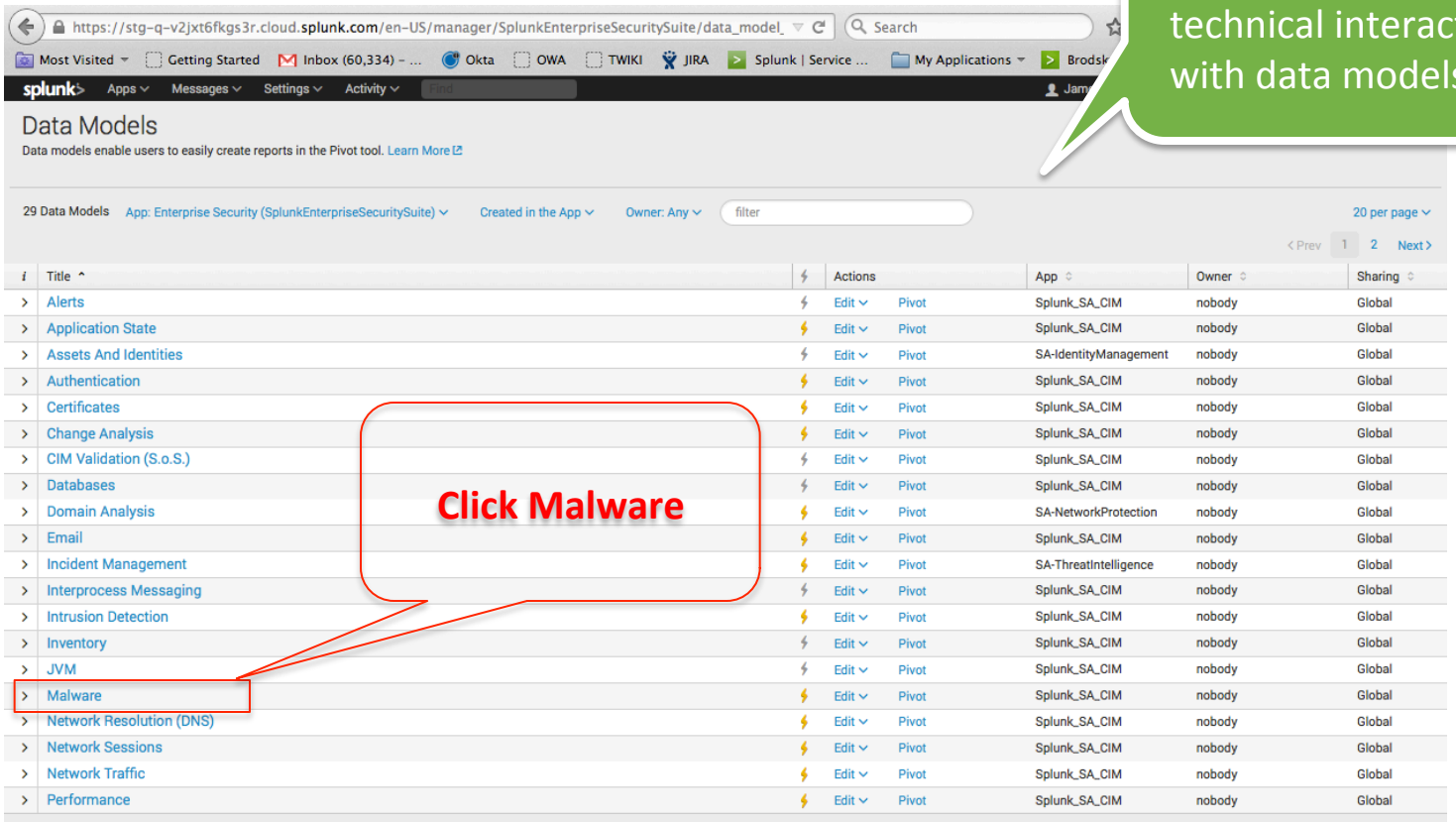



https://stg-q-v2jxt6fkgs3r.cloud.splunk.com/en-US/manager/SplunkEnterpriseSecuritySuite/data_model_
Search
Most Visited
Getting Started
Inbox (60,334) - ...
Okta
OWA
TWIKI
JIRA
Splunk | Service ...
My Applications
Brodsky Internet ...
splunk>
Apps
Messages
Settings
Activity
Find
James Brodsky
My Splunk
Support & Services
Data Models
Data models enable users to easily create reports in the Pivot tool. Learn More
Upload Data Model
New Data Model
29 Data Models
App: Enterprise Security (SplunkEnterpriseSecuritySuite)
Created in the App
Owner: Any
filter
20 per page
Prev
1
2
Next
i
Title
Actions
App
Owner
Sharing
Alerts Edit Pivot Splunk_SA_CIM nobody Global
Application State Edit Pivot Splunk_SA_CIM nobody Global
Assets And Identities Edit Pivot SA-IdentityManagement nobody Global
Authentication Edit Pivot Splunk_SA_CIM nobody Global
Certificates Edit Pivot Splunk_SA_CIM nobody Global
Change Analysis Edit Pivot Splunk_SA_CIM nobody Global
CIM Validation (S.o.S.) Edit Pivot Splunk_SA_CIM nobody Global
Databases Edit Pivot Splunk_SA_CIM nobody Global
Domain Analysis Edit Pivot SA-NetworkProtection nobody Global
Email Edit Pivot Splunk_SA_CIM nobody Global
Incident Management Edit Pivot SA-ThreatIntelligence nobody Global
Interprocess Messaging Edit Pivot Splunk_SA_CIM nobody Global
Intrusion Detection Edit Pivot Splunk_SA_CIM nobody Global
Inventory Edit Pivot Splunk_SA_CIM nobody Global
JVM Edit Pivot Splunk_SA_CIM nobody Global
Malware Edit Pivot Splunk_SA_CIM nobody Global
Network Resolution (DNS) Edit Pivot Splunk_SA_CIM nobody Global
Network Sessions Edit Pivot Splunk_SA_CIM nobody Global
Network Traffic Edit Pivot Splunk_SA_CIM nobody Global
Performance Edit Pivot Splunk_SA_CIM nobody Global
Click “>” next to Malware

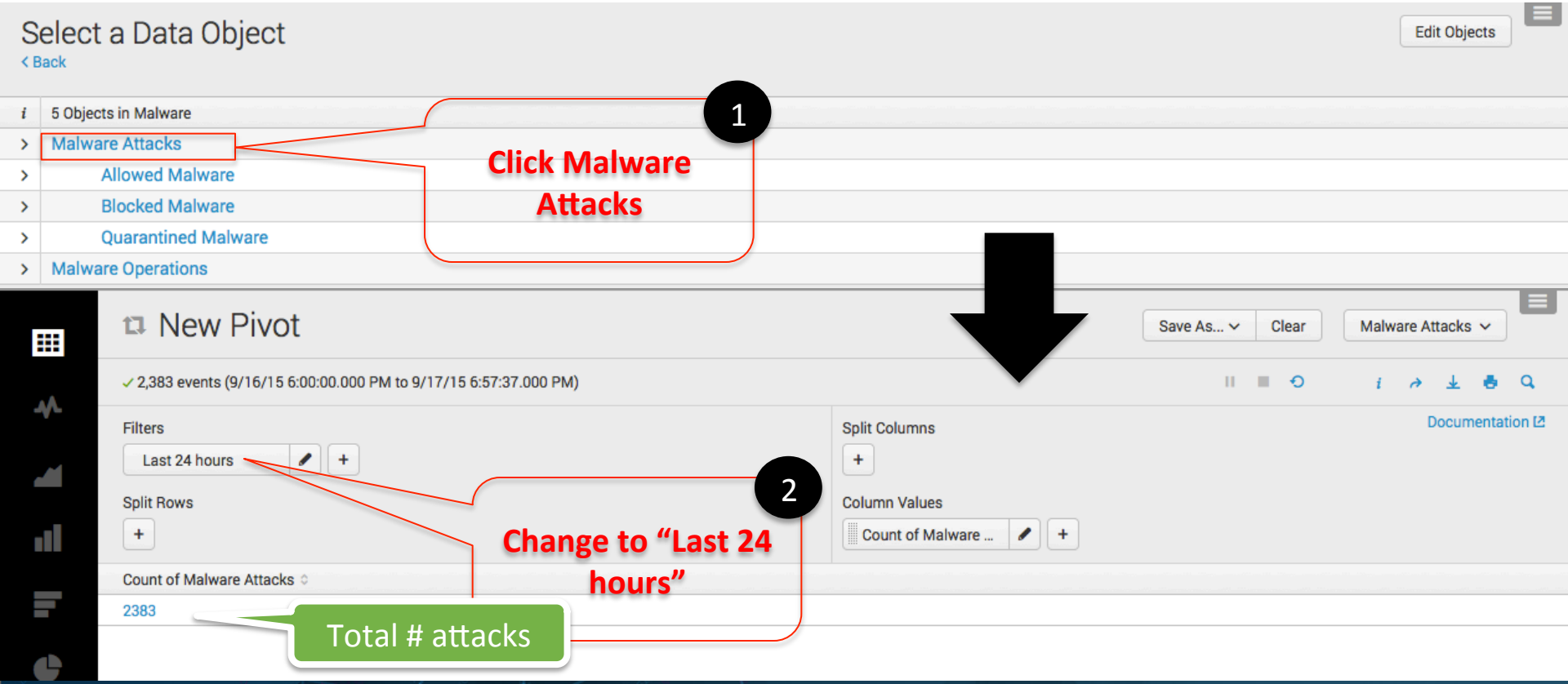
Data Models are Accelerated



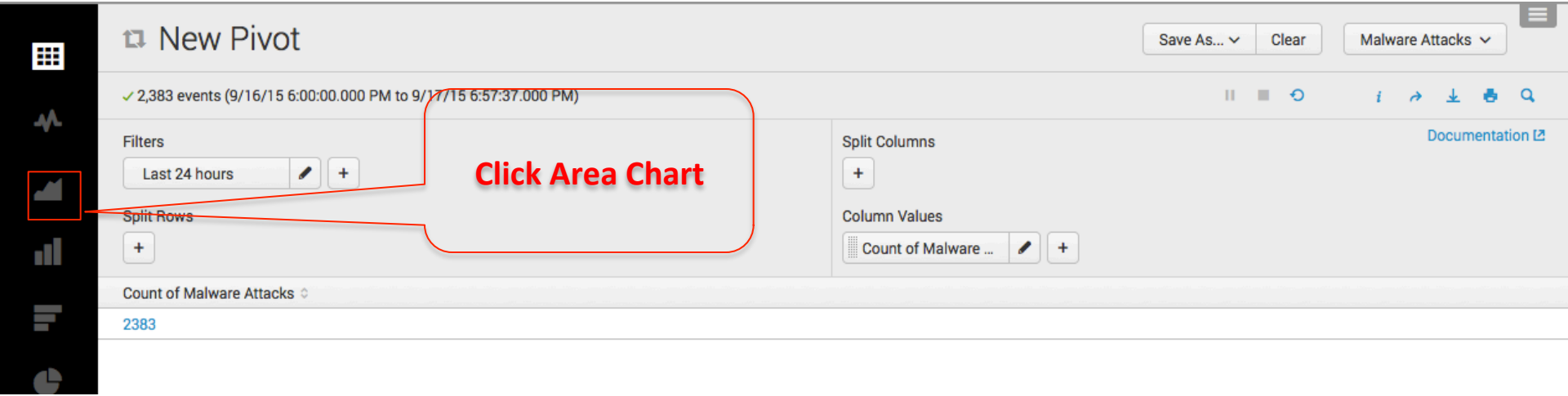
Let's Pivot!


Pivot allows non-technical interaction with data models.
Click Malware
Data Models
Data models enable users to easily create reports in the Pivot tool. Learn More
29 Data Models
App: Enterprise Security (SplunkEnterpriseSecuritySuite)
Created in the App
Owner: Any
filter
20 per page
Prev 1 2 Next
Title
Actions
App
Owner
Sharing
Alerts Edit Pivot Splunk_SA_CIM nobody Global
Application State Edit Pivot Splunk_SA_CIM nobody Global
Assets And Identities Edit Pivot SA-IdentityManagement nobody Global
Authentication Edit Pivot Splunk_SA_CIM nobody Global
Certificates Edit Pivot Splunk_SA_CIM nobody Global
Change Analysis Edit Pivot Splunk_SA_CIM nobody Global
CIM Validation (S.o.S.) Edit Pivot Splunk_SA_CIM nobody Global
Databases Edit Pivot Splunk_SA_CIM nobody Global
Domain Analysis Edit Pivot SA-NetworkProtection nobody Global
Email Edit Pivot Splunk_SA_CIM nobody Global
Incident Management Edit Pivot SA-ThreatIntelligence nobody Global
Interprocess Messaging Edit Pivot Splunk_SA_CIM nobody Global
Intrusion Detection Edit Pivot Splunk_SA_CIM nobody Global
Inventory Edit Pivot Splunk_SA_CIM nobody Global
JVM Edit Pivot Splunk_SA_CIM nobody Global
Malware Edit Pivot Splunk_SA_CIM nobody Global
Network Resolution (DNS) Edit Pivot Splunk_SA_CIM nobody Global
Network Sessions Edit Pivot Splunk_SA_CIM nobody Global
Network Traffic Edit Pivot Splunk_SA_CIM nobody Global
Performance Edit Pivot Splunk_SA_CIM nobody Global

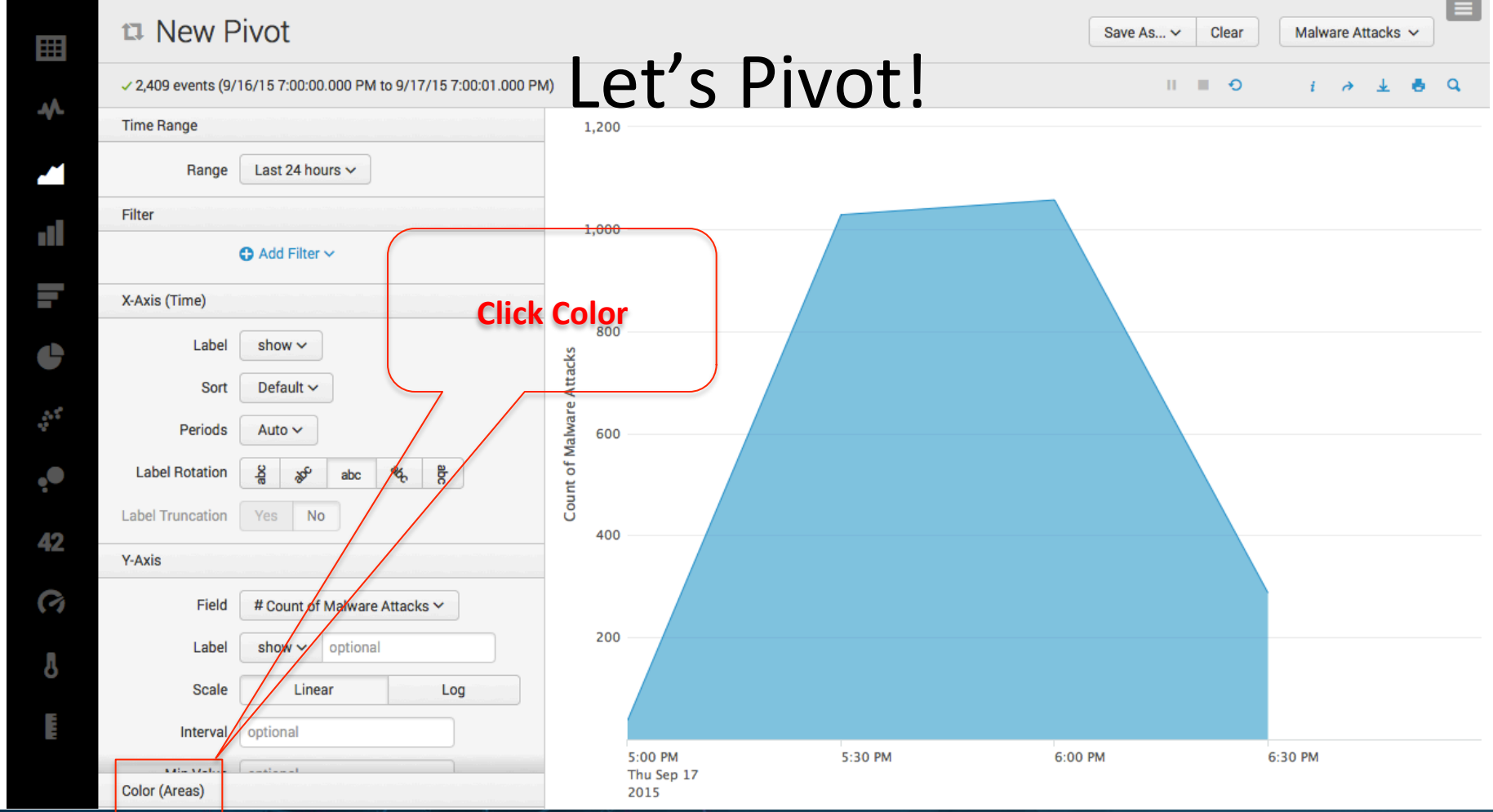
Let’s Pivot!

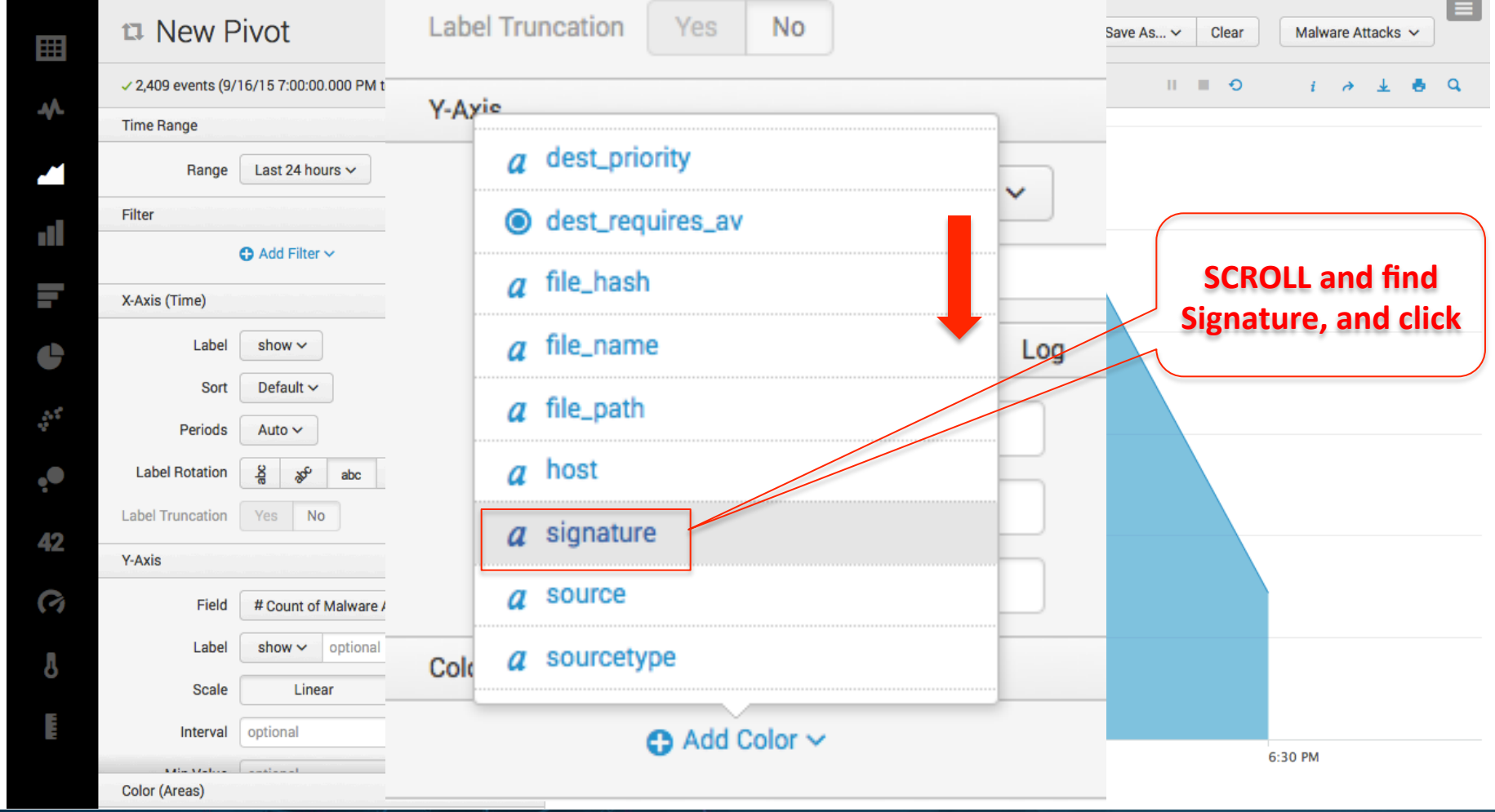

Select a Data Object
Back
Edit Objects
5 Objects in Malware
Malware Attacks
Allowed Malware
Blocked Malware
Quarantined Malware
Malware Operations
1
Click Malware Attacks
New Pivot
Save As...
Clear
Malware Attacks
2,383 events (9/16/15 6:00:00.000 PM to 9/17/15 6:57:37.000 PM)
Filters
Last 24 hours
Split Rows
Split Columns
Column Values
Count of Malware ...
Documentation
2
Change to “Last 24 hours”
Count of Malware Attacks
2383
Total # attacks

Let’s Pivot!


New Pivot
Save As...
Clear
Malware Attacks
2,383 events (9/16/15 6:00:00.000 PM to 9/17/15 6:57:37.000 PM)
Filters
Last 24 hours
Split Rows
Click Area Chart
Split Columns
Column Values
Count of Malware ...
Documentation
Count of Malware Attacks
2383

Let's Pivot!


New Pivot
Save As...
Clear
Malware Attacks
2,409 events (9/16/15 7:00:00.000 PM to 9/17/15 7:00:01.000 PM)
Time Range
Range
Last 24 hours
Filter
Add Filter
X-Axis (Time)
Label
show
Sort
Default
Periods
Auto
Label Rotation
Label Truncation
Yes
No
Y-Axis
Field
Count of Malware Attacks
Label
show
optional
Scale
Linear
Log
Interval
optional
Color (Areas)
Click Color
1,200
1,000
800
600
400
200
Count of Malware Attacks
5:00 PM
Thu Sep 17
2015
5:30 PM
6:00 PM
6:30 PM


New Pivot
2,409 events (9/16/15 7:00:00.000 PM t
Time Range
Range
Last 24 hours
Filter
Add Filter
X-Axis (Time)
Label
show
Sort
Default
Periods
Auto
Label Rotation
abc
Label Truncation
Yes
No
Y-Axis
Field
Count of Malware A
Label
show
optional
Scale
Linear
Interval
optional
Color (Areas)
Label Truncation
Yes
No
Y-Axis
dest_priority
dest_requires_av
file_hash
file_name
file_path
host
signature
source
sourcetype
Add Color
Save As...
Clear
Malware Attacks
Log
SCROLL and find Signature, and click
6:30 PM

New Pivot

Save As... | Clear | Malware Attacks

✓ 2,435 events (9/16/15 7:00:00.000 PM to 9/17/15 7:02:22.000 PM)

Time Range

Filter

X-Axis (Time)

Label Truncation: Yes | No

Y-Axis

Field: # Count of Malware Attacks

Label: show | optional

Scale: Linear | Log

Interval: optional

Min Value: optional

Max Value: optional

Color (Areas)

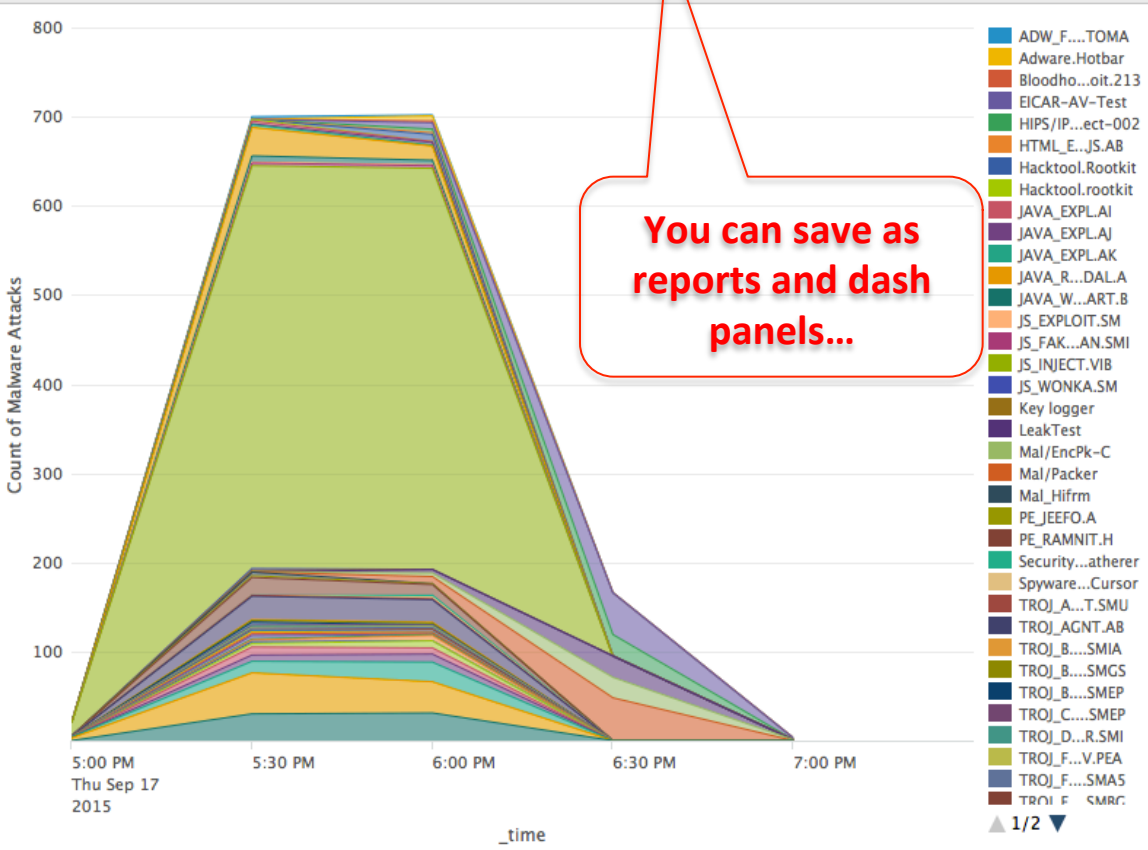
Field: a signature

Max Areas: 100 | Group Others

Legend Position: Right

Legend Truncation: A... | A...Z | ...Z

General



You can save as reports and dash panels…

New Pivot

Save As... | Clear | Malware Attacks

✓ 2,435 events (9/16/15 7:00:00.000 PM to 9/17/15 7:02:22.000 PM)

Time Range

Filter

X-Axis (Time)

Label Truncation: Yes | No

Y-Axis

Field: # Count of Malware Attacks

Label: show | optional

Scale: Linear | Log

Interval: optional

Min Value: optional

Max Value: optional

Color (Areas)

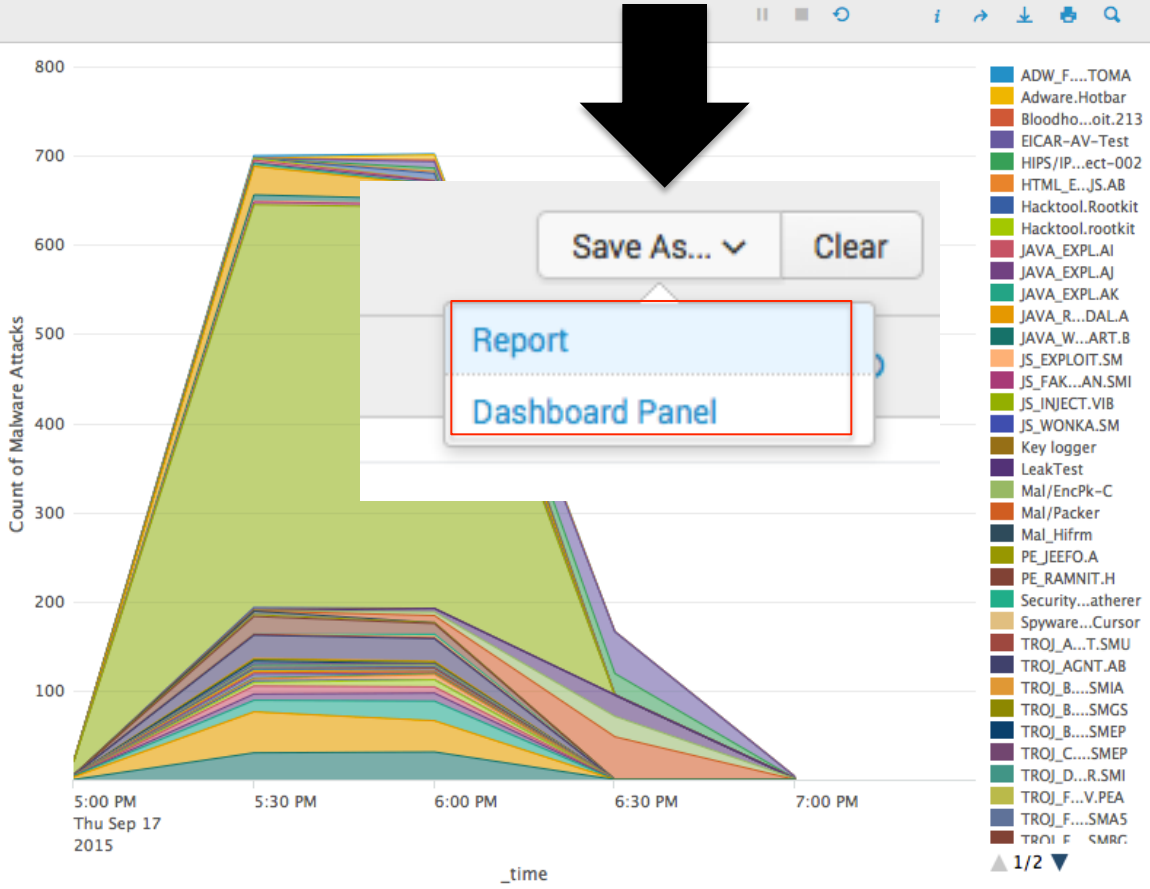
Field: a signature

Max Areas: 100 | Group Others

Legend Position: Right

Legend Truncation: A... | A...Z | ...Z

General



New Pivot

Save As... | Clear | Malware Attacks

✓ 2,513 events (9/16/15 7:00:00.000 PM to 9/17/15 7:09:09.000 PM)

Time Range

Filter

X-Axis (Time)

Label Truncation: Yes | No

Y-Axis

Field: # Count of Malware Attacks

Label: show | optional

Scale: Linear | Log

Interval: optional

Min Value: optional

Max Value: optional

Color (Areas)

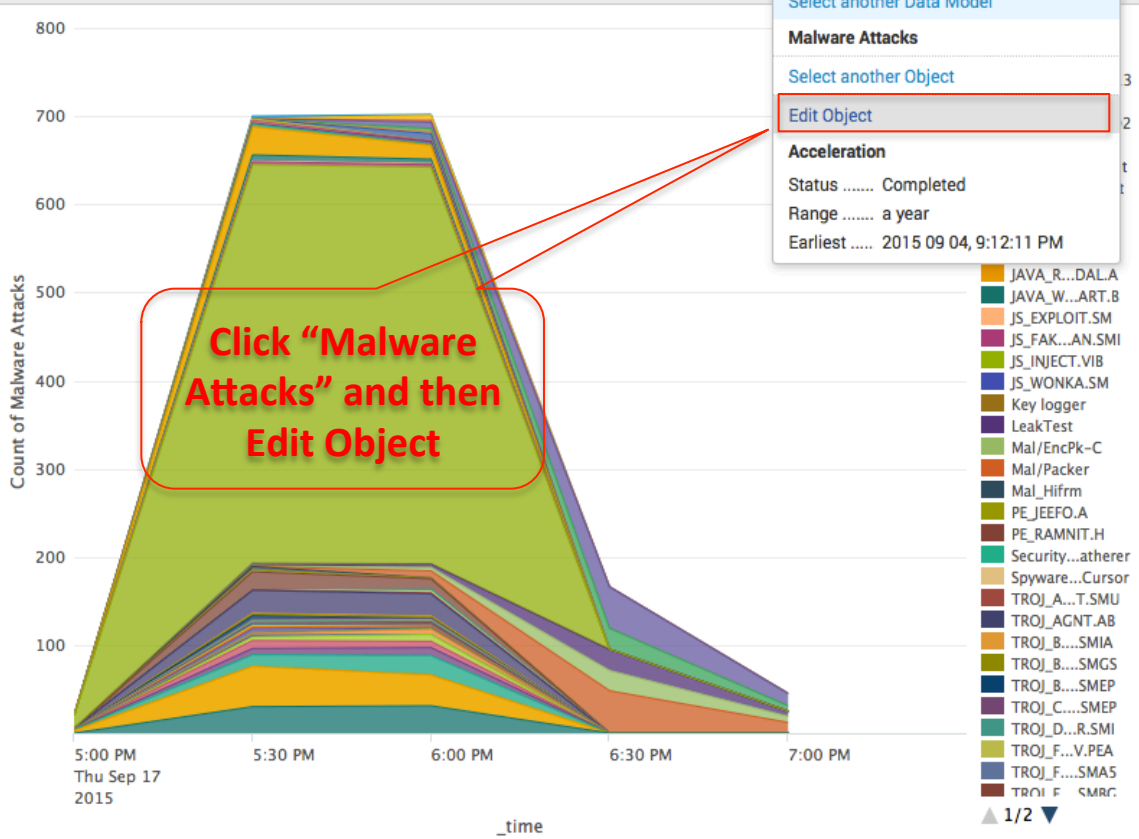
Field: a signature

Max Areas: 100 | Group Others

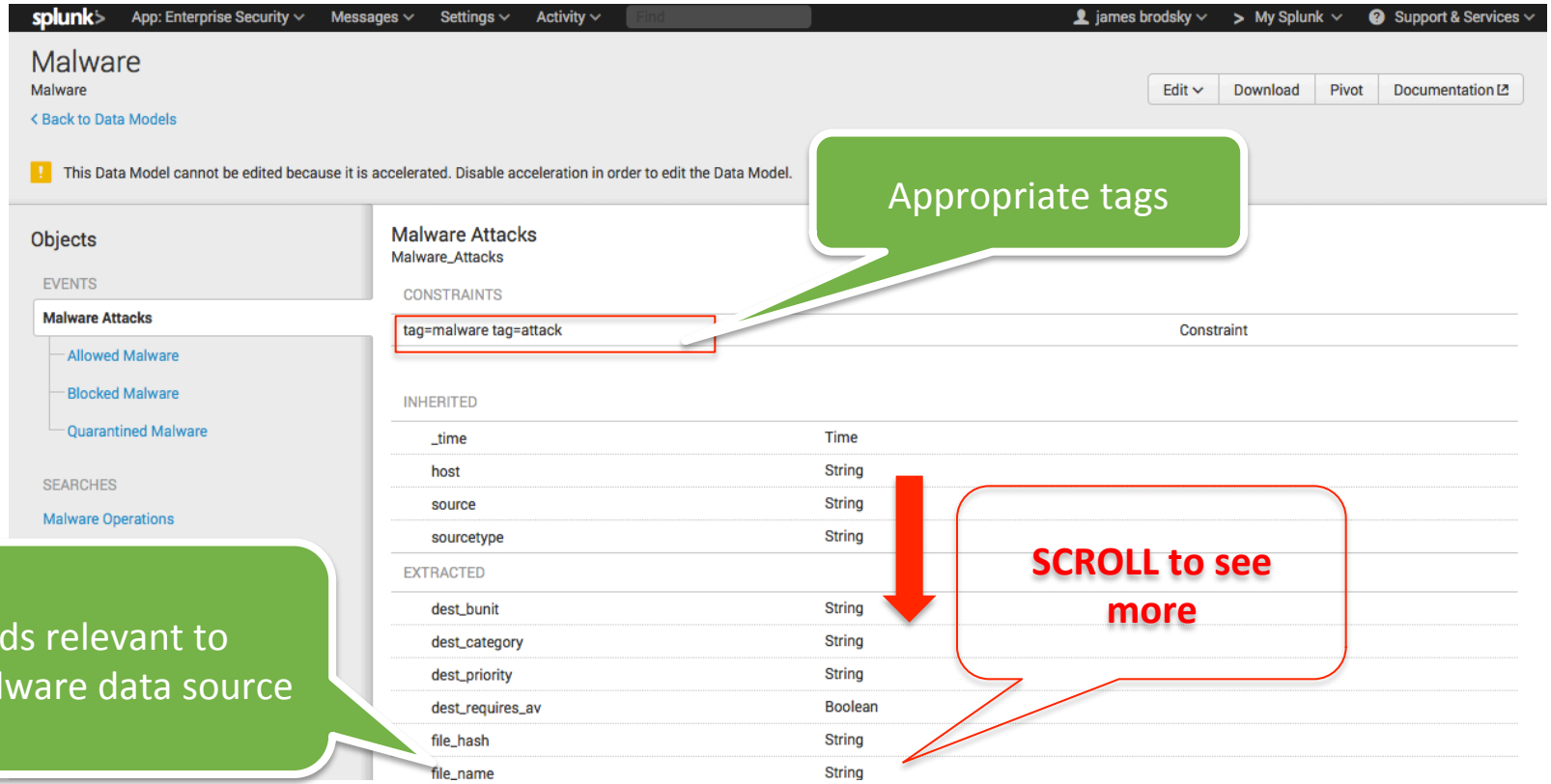
Legend Position: Right

Legend Truncation: A... | A...Z | ...Z

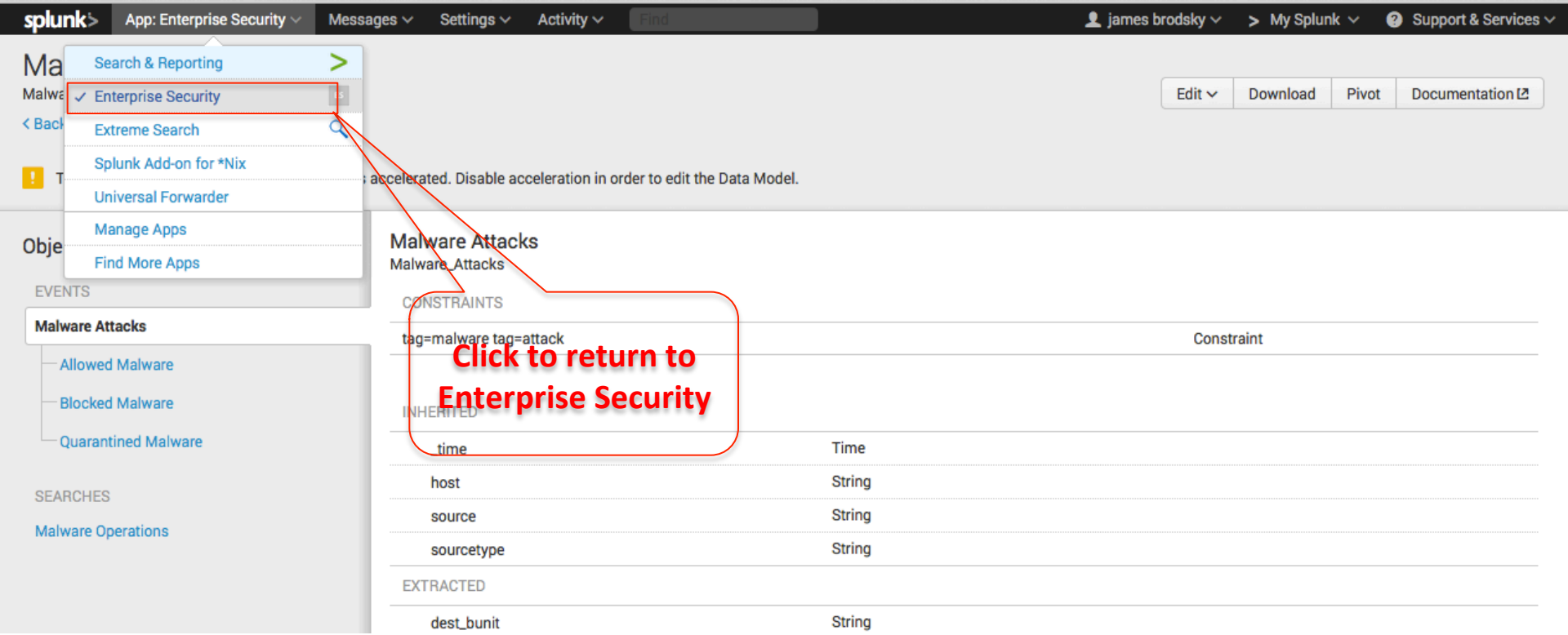
General



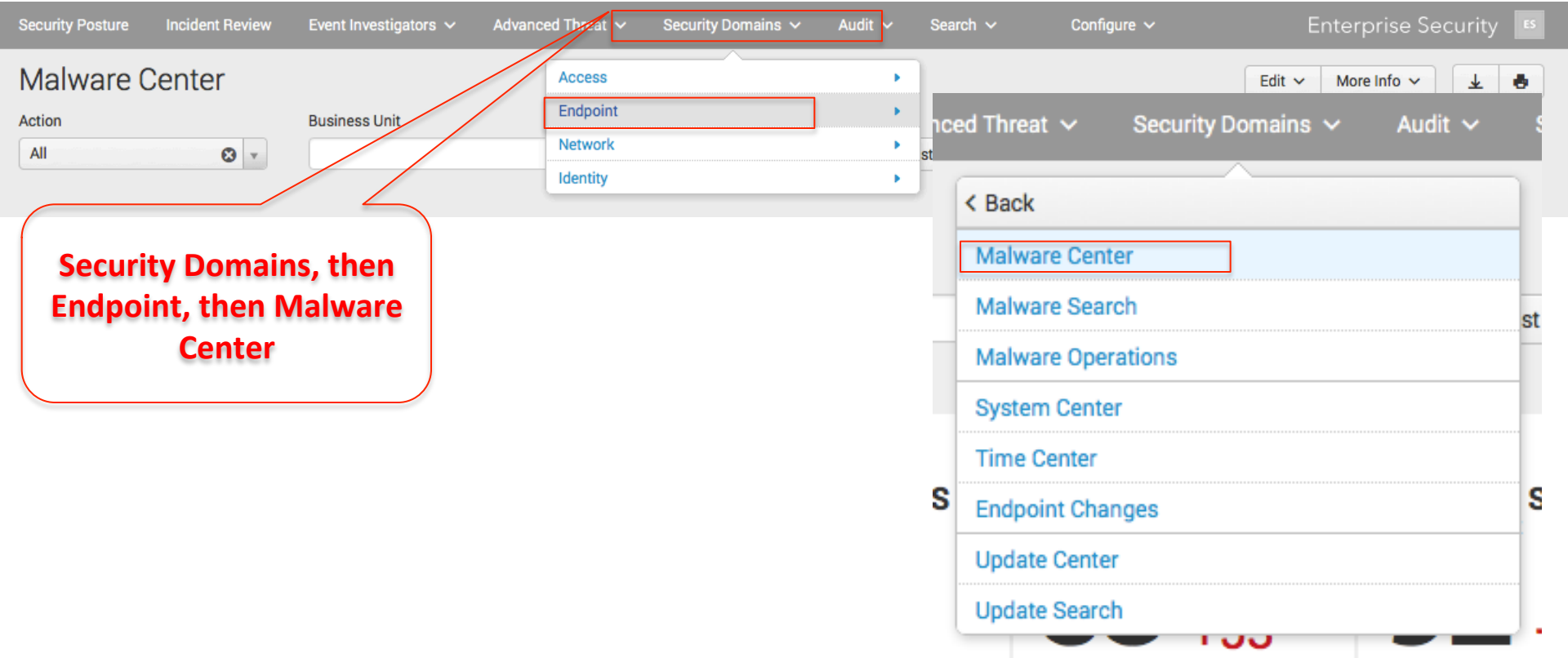
Data Models map to CIM-compliant tagged data



So what?


splunk>
App: Enterprise Security
Messages
Settings
Activity
james brodsky
My Splunk
Support & Services
Search & Reporting
Enterprise Security
Extreme Search
Splunk Add-on for *Nix
Universal Forwarder
Manage Apps
Find More Apps
Edit
Download
Pivot
Documentation
accelerated. Disable acceleration in order to edit the Data Model.
Malware Attacks
Malware_Attacks
CONSTRAINTS
tag=malware tag=attack
Constraint
Click to return to Enterprise Security
INHERITED
time
Time
host
String
source
String
sourcetype
String
EXTRACTED
dest_bunit
String
EVENTS
Malware Attacks
Allowed Malware
Blocked Malware
Quarantined Malware
SEARCHES
Malware Operations

So what?


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Malware Center
Action
All
Business Unit
Access
Endpoint
Network
Identity
Edit
More Info
Security Domains
Audit
Back
Malware Center
Malware Search
Malware Operations
System Center
Time Center
Endpoint Changes
Update Center
Update Search
Security Domains, then Endpoint, then Malware Center

Security Posture | Incident Review | Event Investigators | Advanced Threat | Security Domains | Audit | Search | Configure | Enterprise Security

Malware Center

Edit | More Info

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

KSI specific to malware

Edit

NEW INFECTIONS
Count
302 +302

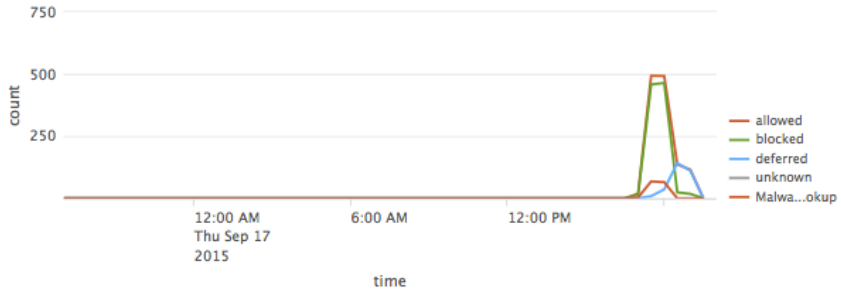
MULTIPLE INFECTIONS
System Count
20 +20

UNIQUE MALWARE
Unique Count
53 +53

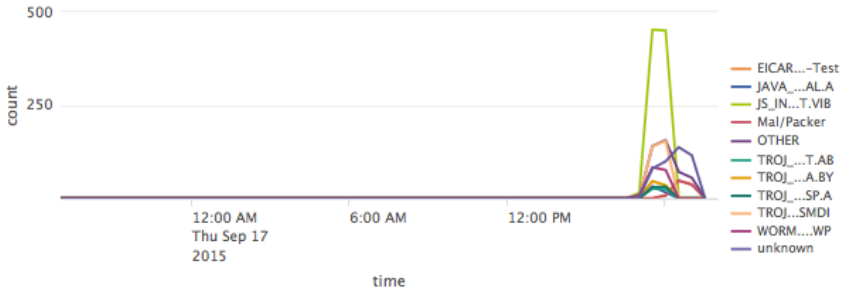
INFECTED SYSTEMS
System Count
92 +92

TOTAL INFECTIONS
Count
extreme
Currently is: 124
increasing extreme

Malware Activity Over Time By Action



Malware Activity Over Time By Signature

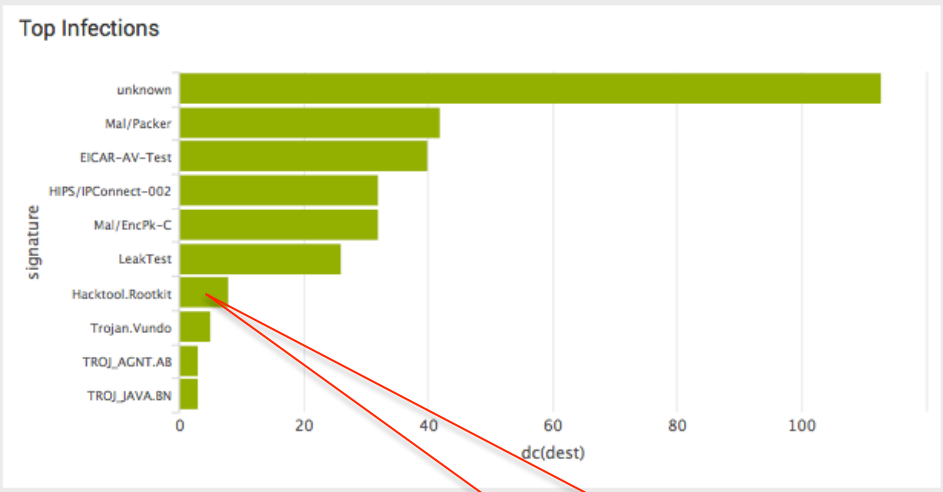


Top Infections

New Malware - Last 30 Days

firstTime	signature	dc(dest)
09/17/2015 18:28:12	Adware.Hotbar	1
09/17/2015 18:28:11	Hacktool.Rootkit	8
09/17/2015 18:28:06	Bloodhound.Exploit.213	2

Let’s drill into two examples



New Malware - Last 30 Days

firstTime	signature	dc(dest)
09/17/2015 18:28:12	Adware.Hotbar	1
09/17/2015 18:28:11	Hacktool.Rootkit	8
09/17/2015 18:28:06	Bloodhound.Exploit.213	2
09/17/2015 18:28:06	SecurityRisk.eGatherer	2
09/17/2015 18:28:06	Spyware.CometCursor	2
09/17/2015 18:28:06	W32.SillyDC	2
09/17/2015 18:28:06	W32.Virut.CF	2
09/17/2015 18:27:01	PE_JEEFO.A	1
09/17/2015 18:26:43	LeakTest	19
09/17/2015 18:26:30	EICAR-AV-Test	33

« prev 1 2 3 4 5 6 next »

Click “Hacktool.Rootkit” bar

Malware Search

Edit | More Info

Action: All

Signature: Hacktool.Rootkit

File:

Destination:

User:

Date time range | Submit

Normalized fields to CIM from Symantec

_time	action	signature	file_name	dest	user	count
2015-09-17 18:28:36	blocked	Hacktool.Rootkit	phqghume.sys	BUSDEV-001	rosher	1
2015-09-17 18:28:36	blocked	Hacktool.Rootkit	sysret.dat	BUSDEV-003	housner	1
2015-09-17 18:28:11	blocked	Hacktool.Rootkit	sysret.dat	BUSDEV-007	chan	1
2015-09-17 18:28:11	allowed	Hacktool.Rootkit	vga.sys	COREDEV-001	kraut	1
2015-09-17 18:28:11	allowed	Hacktool.Rootkit	uackdujoewm.sys	COREDEV-005	zellefrow	1

« prev 1 2 3 next »

i	Time	Event
>	9/17/15 7:03:06.000 PM	Sep 17 19:03:06 acmesep01.acmetech.com Sep 17 19:16:18 SymantecServer acmesep01: Virus found,Computer name: PROD-POS-002,Source: Real Time Scan,Risk name: Hacktool.rootkit,Occurrences: 1,C:/Documents and Settings/smithe/Local Settings/Temp/evil.tmp,""",Actual action: Quarantined,Requested action: Cleaned,Secondary action: Quarantined,Event time: 2009-01-23 03:19:12,Inserted: 2009-01-23 03:20:12,End: 2009-01-23 03:19:12,Domain: Default,Group: My Company\ACME Remote,Server: acmesep01,User: smithe,Source computer: ,Source IP: 0.0.0.0 action = blocked action = blocked | dest = PROD-POS-002 | file_name = evil.tmp | signature = Hacktool.rootkit | user = smithe | vendor_product = Symantec Endpoint Protection
>	9/17/15 7:02:38.000 PM	Sep 17 19:02:38 acmesep01.acmetech.com Sep 17 18:32:34 SymantecServer acmesep01: Virus found,Computer name: COREDEV-006,Source: Real Time Scan,Risk name: Hacktool.rootkit,Occurrences: 1,C:/Documents and Settings/smithe/Local Settings/Temp/evil.tmp,""",Actual action: Quarantined,Requested action: Cleaned,Secondary action: Quarantined,Event time: 2009-01-23 03:19:12,Inserted: 2009-01-23 03:20:12,End: 2009-01-23 03:19:12,Domain: Default,Group: My Company\ACME Remote,Server: acmesep01,User: smithe,Source computer: ,Source IP: 0.0.0.0 action = blocked action = blocked | dest = COREDEV-006 | file_name = evil.tmp | signature = Hacktool.rootkit | user = smithe | vendor_product = Symantec Endpoint Protection
>	9/17/15 6:28:36.000 PM	270114042E1D,5,1,131174,BUSDEV-003,housner,Hacktool.Rootkit,C:\sysret.dat,5,3,3,256,1128288324,"",0,,0,201 4 4 0 1 5 1 6 0 0 0,0,16268,0,1,0,0,0,0,,0,2,5,0,WMSMSUSNY001002,{833A9787-5752-43D3-A0CC-698B7015DA3A},,(IP)-10.11.36.48,SAV.acmetech.COM_USEAST,WORKGROUP,92:90:55:51:61:31,10.1.4.4010,,,,,,,,,,,,,,,0,5D95444F36C24748BF07752CD14A2311,b70d284e-2dd1-4b7a-b090-84e0a28cd582,0,ACMETECH-F1794C05 action = blocked | dest = BUSDEV-003 | file_name = sysret.dat | signature = Hacktool.Rootkit | user = housner | vendor_product = Symantec Antivirus
>	9/17/15 6:28:36.000 PM	27011408303A,46,1,589926,PROD-POS-004,yeboah,Hacktool.Rootkit,c:\windows\system32\drivers\vga.sys,5,1,4,256,1124073476,"",1235141220,,0,101 {53DED684-5935-45D1-AE83-4FB12099303A} 0 2 Hacktool.Rootkit 2;0;13 0 0 ,0,16268,0,0,0,0,0,0,,0,0,4,0,WMSMSUSNY001002,{ACF89A3D-D154-46C2-

Malware Search

Edit | More Info

Action: All

Signature: Hacktool.Rootkit

File:

Destination:

User:

Date time range | Submit

_time	action	signature	file_name	dest	user	count
2015-09-17 18:28:36	blocked	Hacktool.Rootkit	phqghume.sys	BUSDEV-001	rosher	1
2015-09-17 18:28:36	blocked	Hacktool.Rootkit	sysret.dat	BUSDEV-003	housner	1
2015-09-17 18:28:11	blocked	Hacktool.Rootkit	sysret.dat	BUSDEV-007	chan	1
2015-09-17 18:28:11	allowed	Hacktool.Rootkit	vga.sys	COREDEV-001	kraut	1
2015-09-17 18:28:11	allowed	Hacktool.Rootkit	uackdujoewm.sys	COREDEV-005	zellefrow	1

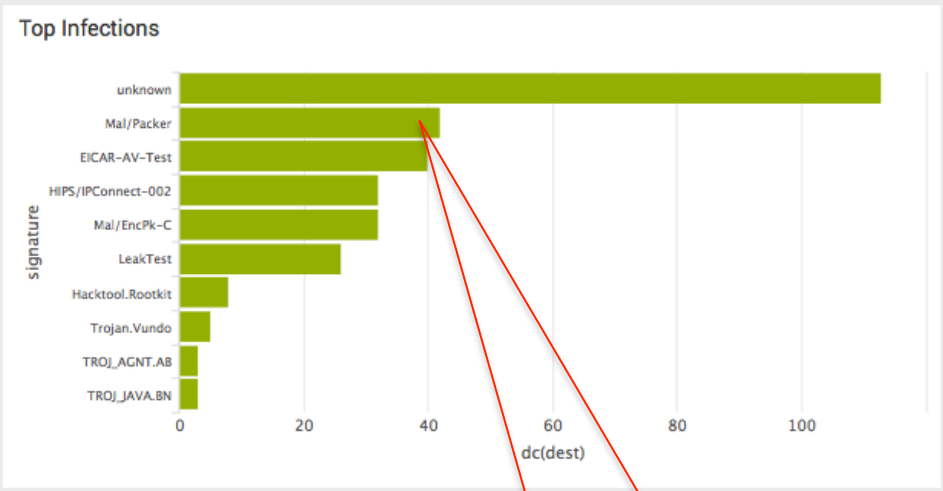
1 2 3 next »

Click browser back button…

We know about this.

i	Time	Event
>	9/17/15 7:03:06.000 PM	Sep 17 19:03:06 acmesep01.acmetech.com Sep 17 19:16:18 SymantecServer acmesep01: Virus found,Computer name: PROD-POS-002,Source: Real Time Scan,Risk name: Hacktool.rootkit,Occurrences: 1,C:/Documents and Settings/smithe/Local Settings/Temp/evil.tmp,""",Actual action: Quarantined,Requested action: Cleaned,Secondary action: Quarantined,Event time: 2009-01-23 03:19:12,Inserted: 2009-01-23 03:20:12,End: 2009-01-23 03:19:12,Domain: Default,Group: My Company\ACME Remote,Server: acmesep01,User: smithe,Source computer: ,Source IP: 0.0.0.0 action = blocked action = blocked | dest = PROD-POS-002 | file_name = evil.tmp | signature = Hacktool.rootkit | user = smithe | vendor_product = Symantec Endpoint Protection
>	9/17/15 7:02:38.000 PM	Sep 17 19:02:38 acmesep01.acmetech.com Sep 17 18:32:34 SymantecServer acmesep01: Virus found,Computer name: COREDEV-006,Source: Real Time Scan,Risk name: Hacktool.rootkit,Occurrences: 1,C:/Documents and Settings/smithe/Local Settings/Temp/evil.tmp,""",Actual action: Quarantined,Requested action: Cleaned,Secondary action: Quarantined,Event time: 2009-01-23 03:19:12,Inserted: 2009-01-23 03:20:12,End: 2009-01-23 03:19:12,Domain: Default,Group: My Company\ACME Remote,Server: acmesep01,User: smithe,Source computer: ,Source IP: 0.0.0.0 action = blocked action = blocked | dest = COREDEV-006 | file_name = evil.tmp | signature = Hacktool.rootkit | user = smithe | vendor_product = Symantec Endpoint Protection
>	9/17/15 6:28:36.000 PM	270114042E1D,5,1,131174,BUSDEV-003,housner,Hacktool.Rootkit,C:\sysret.dat,5,3,3,256,1128288324,"",0,,0,201 4 4 0 1 5 1 6 0 0 0,0,16268,0,1,0,0,0,0,,0,2,5,0,WMSMSUSNY001002,{833A9787-5752-43D3-A0CC-698B7015DA3A},,(IP)-10.11.36.48,SAV.acmetech.COM_USEAST,WORKGROUP,92:90:55:51:61:31,10.1.4.4010,,,,,,,,,,,,,,,0,5D95444F36C24748BF07752CD14A2311,b70d284e-2dd1-4b7a-b090-84e0a28cd582,0,ACMETECH-F1794C05 action = blocked | dest = BUSDEV-003 | file_name = sysret.dat | signature = Hacktool.Rootkit | user = housner | vendor_product = Symantec Antivirus
>	9/17/15 6:28:36.000 PM	27011408303A,46,1,589926,PROD-POS-004,yeboah,Hacktool.Rootkit,c:\windows\system32\drivers\vga.sys,5,1,4,256,1124073476,"",1235141220,,0,101 {53DED684-5935-45D1-AE83-4FB12099303A} 0 2 Hacktool.Rootkit 2;0;13 0 0 ,0,16268,0,0,0,0,0,0,,0,0,4,0,WMSMSUSNY001002,{ACF89A3D-D154-46C2-

Second example

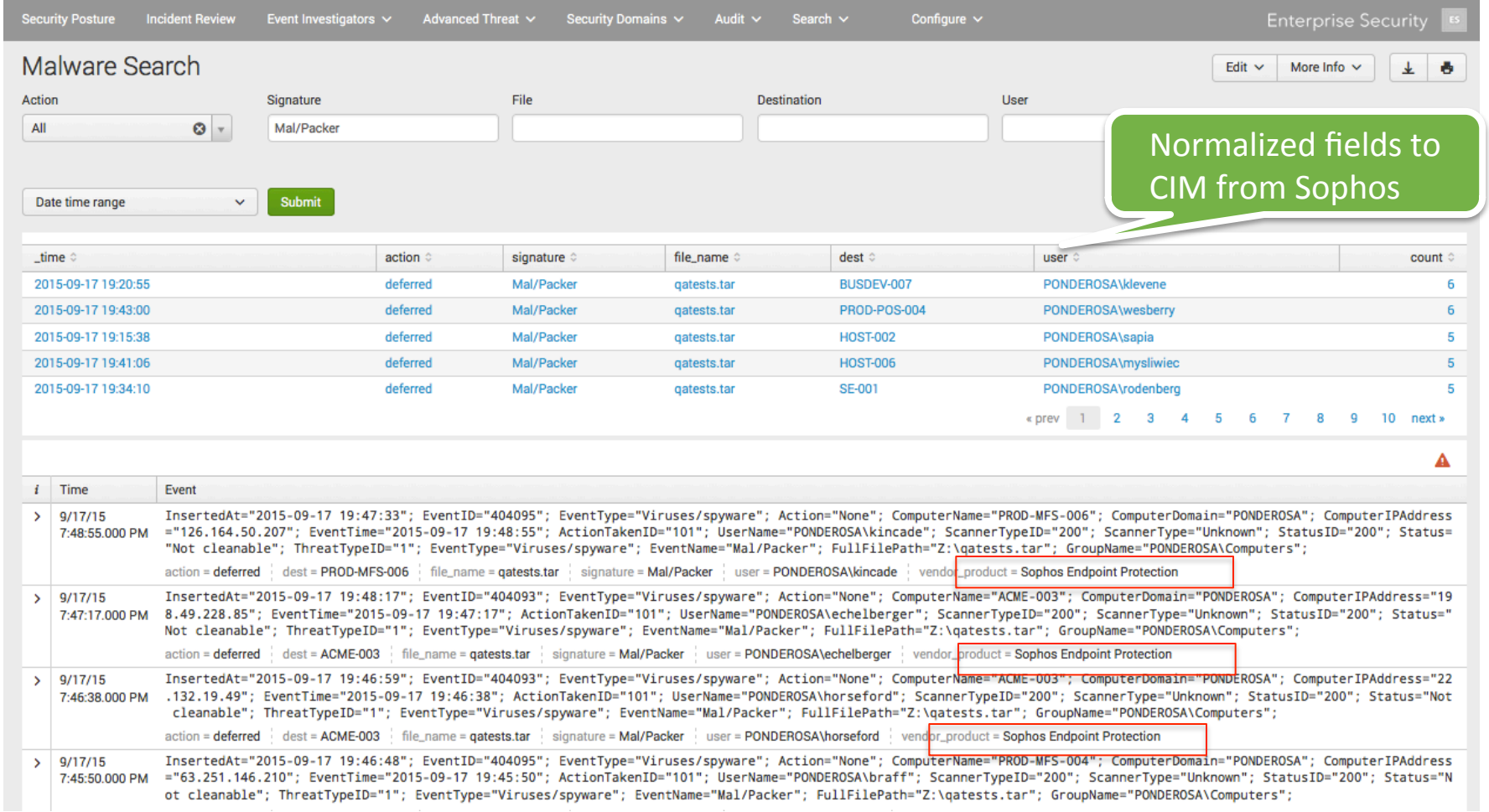


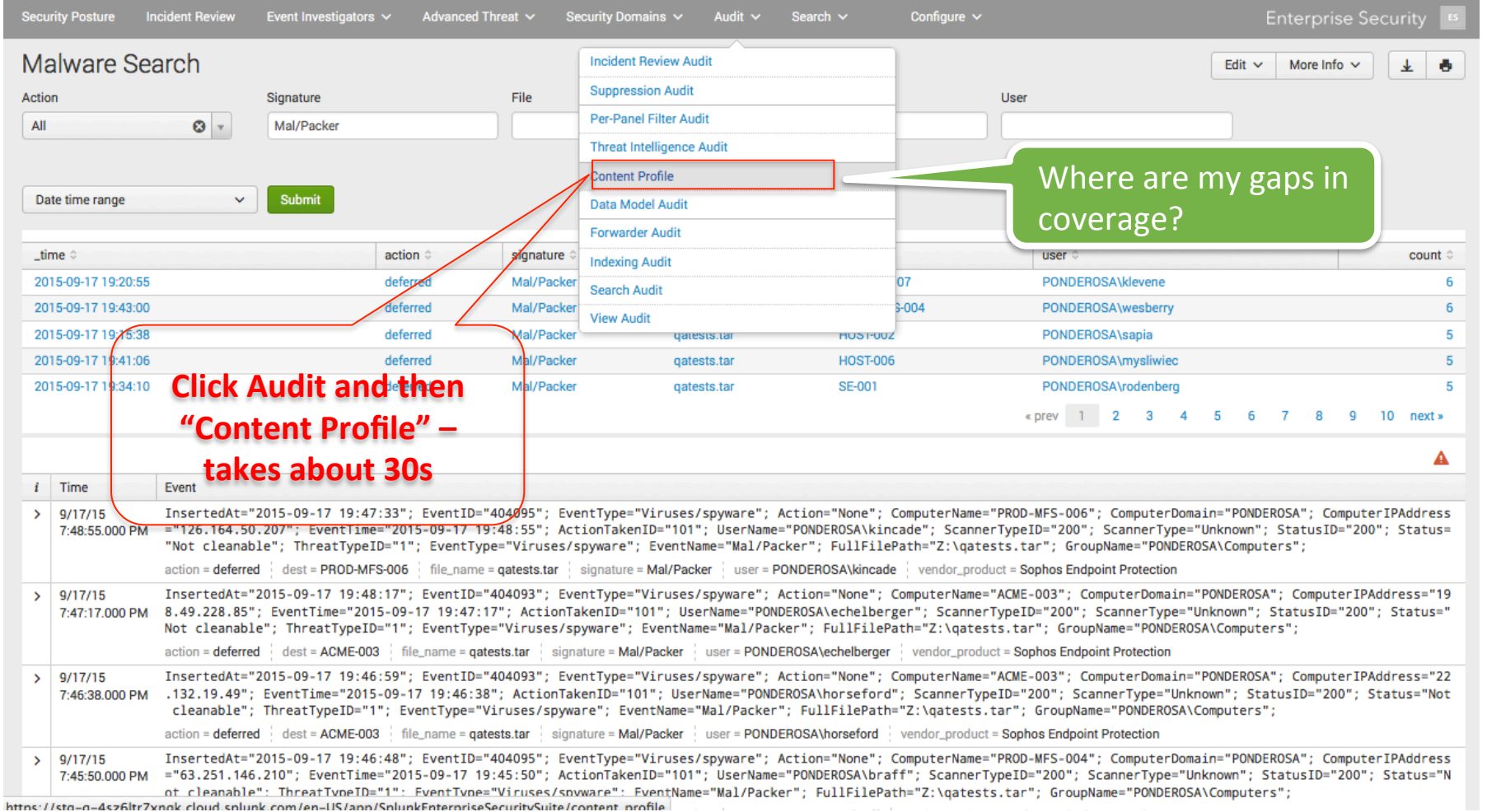
New Malware - Last 30 Days

firstTime	signature	dc(dest)
09/17/2015 18:28:12	Adware.Hotbar	1
09/17/2015 18:28:11	Hacktool.Rootkit	8
09/17/2015 18:28:06	Bloodhound.Exploit.213	2
09/17/2015 18:28:06	SecurityRisk.eGatherer	2
09/17/2015 18:28:06	Spyware.CometCursor	2
09/17/2015 18:28:06	W32.SillyDC	2
09/17/2015 18:28:06	W32.Virut.CF	2
09/17/2015 18:27:01	PE_JEEFO.A	1
09/17/2015 18:26:43	LeakTest	19
09/17/2015 18:26:30	EICAR-AV-Test	33

« prev 1 2 3 4 5 6 next »

Click “Mal/Packer” bar


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Malware Search
Edit
More Info
Action
All
Signature
Mal/Packer
File
Destination
User
Date time range
Submit
Normalized fields to CIM from Sophos
_time
action
signature
file_name
dest
user
count
2015-09-17 19:20:55 deferred Mal/Packer qatests.tar BUSDEV-007 PONDEROSA\klevene 6
2015-09-17 19:43:00 deferred Mal/Packer qatests.tar PROD-POS-004 PONDEROSA\wesberry 6
2015-09-17 19:15:38 deferred Mal/Packer qatests.tar HOST-002 PONDEROSA\sapia 5
2015-09-17 19:41:06 deferred Mal/Packer qatests.tar HOST-006 PONDEROSA\mysliwiec 5
2015-09-17 19:34:10 deferred Mal/Packer qatests.tar SE-001 PONDEROSA\rodenberg 5
« prev 1 2 3 4 5 6 7 8 9 10 next »
Time
Event
9/17/15 7:48:55.000 PM
InsertedAt="2015-09-17 19:47:33"; EventID="404095"; EventType="Viruses/spyware"; Action="None"; ComputerName="PROD-MFS-006"; ComputerDomain="PONDEROSA"; ComputerIPAddress="126.164.50.207"; EventTime="2015-09-17 19:48:55"; ActionTakenID="101"; UserName="PONDEROSA\kincade"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="200"; Status="Not cleanable"; ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="Mal/Packer"; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Computers";
action = deferred | dest = PROD-MFS-006 | file_name = qatests.tar | signature = Mal/Packer | user = PONDEROSA\kincade | vendor_product = Sophos Endpoint Protection
9/17/15 7:47:17.000 PM
InsertedAt="2015-09-17 19:48:17"; EventID="404093"; EventType="Viruses/spyware"; Action="None"; ComputerName="ACME-003"; ComputerDomain="PONDEROSA"; ComputerIPAddress="198.49.228.85"; EventTime="2015-09-17 19:47:17"; ActionTakenID="101"; UserName="PONDEROSA\echelberger"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="200"; Status="Not cleanable"; ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="Mal/Packer"; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Computers";
action = deferred | dest = ACME-003 | file_name = qatests.tar | signature = Mal/Packer | user = PONDEROSA\echelberger | vendor_product = Sophos Endpoint Protection
9/17/15 7:46:38.000 PM
InsertedAt="2015-09-17 19:46:59"; EventID="404093"; EventType="Viruses/spyware"; Action="None"; ComputerName="ACME-003"; ComputerDomain="PONDEROSA"; ComputerIPAddress="22.132.19.49"; EventTime="2015-09-17 19:46:38"; ActionTakenID="101"; UserName="PONDEROSA\horseford"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="200"; Status="Not cleanable"; ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="Mal/Packer"; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Computers";
action = deferred | dest = ACME-003 | file_name = qatests.tar | signature = Mal/Packer | user = PONDEROSA\horseford | vendor_product = Sophos Endpoint Protection
9/17/15 7:45:50.000 PM
InsertedAt="2015-09-17 19:46:48"; EventID="404095"; EventType="Viruses/spyware"; Action="None"; ComputerName="PROD-MFS-004"; ComputerDomain="PONDEROSA"; ComputerIPAddress="63.251.146.210"; EventTime="2015-09-17 19:45:50"; ActionTakenID="101"; UserName="PONDEROSA\braff"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="200"; Status="Not cleanable"; ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="Mal/Packer"; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Computers";


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Malware Search
Edit
More Info
Action
All
Signature
Mal/Packer
File
User
Incident Review Audit
Suppression Audit
Per-Panel Filter Audit
Threat Intelligence Audit
Content Profile
Data Model Audit
Forwarder Audit
Indexing Audit
Search Audit
View Audit
Where are my gaps in coverage?
Date time range
Submit
_time
action
signature
user
count
2015-09-17 19:20:55
deferred
Mal/Packer
PONDEROSA\klevene
6
2015-09-17 19:43:00
deferred
Mal/Packer
PONDEROSA\wesberry
6
2015-09-17 19:15:38
deferred
Mal/Packer
qatests.tar
PONDEROSA\sapia
5
2015-09-17 19:41:06
deferred
Mal/Packer
qatests.tar
HOST-006
PONDEROSA\mysliwiec
5
2015-09-17 19:34:10
deferred
Mal/Packer
qatests.tar
SE-001
PONDEROSA\rodenberg
5
« prev
1
2
3
4
5
6
7
8
9
10
next »
Click Audit and then "Content Profile" – takes about 30s
i
Time
Event
9/17/15 7:48:55.000 PM
InsertedAt="2015-09-17 19:47:33"; EventID="404095"; EventType="Viruses/spyware"; Action="None"; ComputerName="PROD-MFS-006"; ComputerDomain="PONDEROSA"; ComputerIPAddress="126.164.50.207"; EventTime="2015-09-17 19:48:55"; ActionTakenID="101"; UserName="PONDEROSA\kincade"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="200"; Status="Not cleanable"; ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="Mal/Packer"; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Computers";
action = deferred | dest = PROD-MFS-006 | file_name = qatests.tar | signature = Mal/Packer | user = PONDEROSA\kincade | vendor_product = Sophos Endpoint Protection
9/17/15 7:47:17.000 PM
InsertedAt="2015-09-17 19:48:17"; EventID="404093"; EventType="Viruses/spyware"; Action="None"; ComputerName="ACME-003"; ComputerDomain="PONDEROSA"; ComputerIPAddress="198.49.228.85"; EventTime="2015-09-17 19:47:17"; ActionTakenID="101"; UserName="PONDEROSA\echelberger"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="200"; Status="Not cleanable"; ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="Mal/Packer"; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Computers";
action = deferred | dest = ACME-003 | file_name = qatests.tar | signature = Mal/Packer | user = PONDEROSA\echelberger | vendor_product = Sophos Endpoint Protection
9/17/15 7:46:38.000 PM
InsertedAt="2015-09-17 19:46:59"; EventID="404093"; EventType="Viruses/spyware"; Action="None"; ComputerName="ACME-003"; ComputerDomain="PONDEROSA"; ComputerIPAddress="22.132.19.49"; EventTime="2015-09-17 19:46:38"; ActionTakenID="101"; UserName="PONDEROSA\horseford"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="200"; Status="Not cleanable"; ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="Mal/Packer"; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Computers";
action = deferred | dest = ACME-003 | file_name = qatests.tar | signature = Mal/Packer | user = PONDEROSA\horseford | vendor_product = Sophos Endpoint Protection
9/17/15 7:45:50.000 PM
InsertedAt="2015-09-17 19:46:48"; EventID="404095"; EventType="Viruses/spyware"; Action="None"; ComputerName="PROD-MFS-004"; ComputerDomain="PONDEROSA"; ComputerIPAddress="63.251.146.210"; EventTime="2015-09-17 19:45:50"; ActionTakenID="101"; UserName="PONDEROSA\braff"; ScannerTypeID="200"; ScannerType="Unknown"; StatusID="200"; Status="Not cleanable"; ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="Mal/Packer"; FullFilePath="Z:\qatests.tar"; GroupName="PONDEROSA\Computers";
https://sto-g-4sz6ltr7xnqk.cloud.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/content_profile

Content Profile

ES Content profile and completeness

Deployment Completeness

You can use **99%** of knowledge objects

Unused Data Models

1

Unused Knowledge Objects

2

Data Model Info

i	datamodel	readiness
>	Application_State	✓
>	Authentication	✓
>	Certificates	✓
>	Change_Analysis	✓
>	Domain_Analysis	✓
>	Email	✓
>	Incident_Management	✓
>	Intrusion_Detection	✓
>	Malware	✓
>	Network_Resolution	✓
>	Network_Sessions	✓
>	Network_Traffic	✓
>	Performance	✓
>	Risk	✓
>	Splunk_Audit	✓
>	Threat_Intelligence	✓
>	Ticket_Management	⚠
>	Updates	✓
>	Vulnerabilities	✓
>	Web	✓

Which models could I be using, but I'm not?

Questions on CIM/Data Models?

splunk>

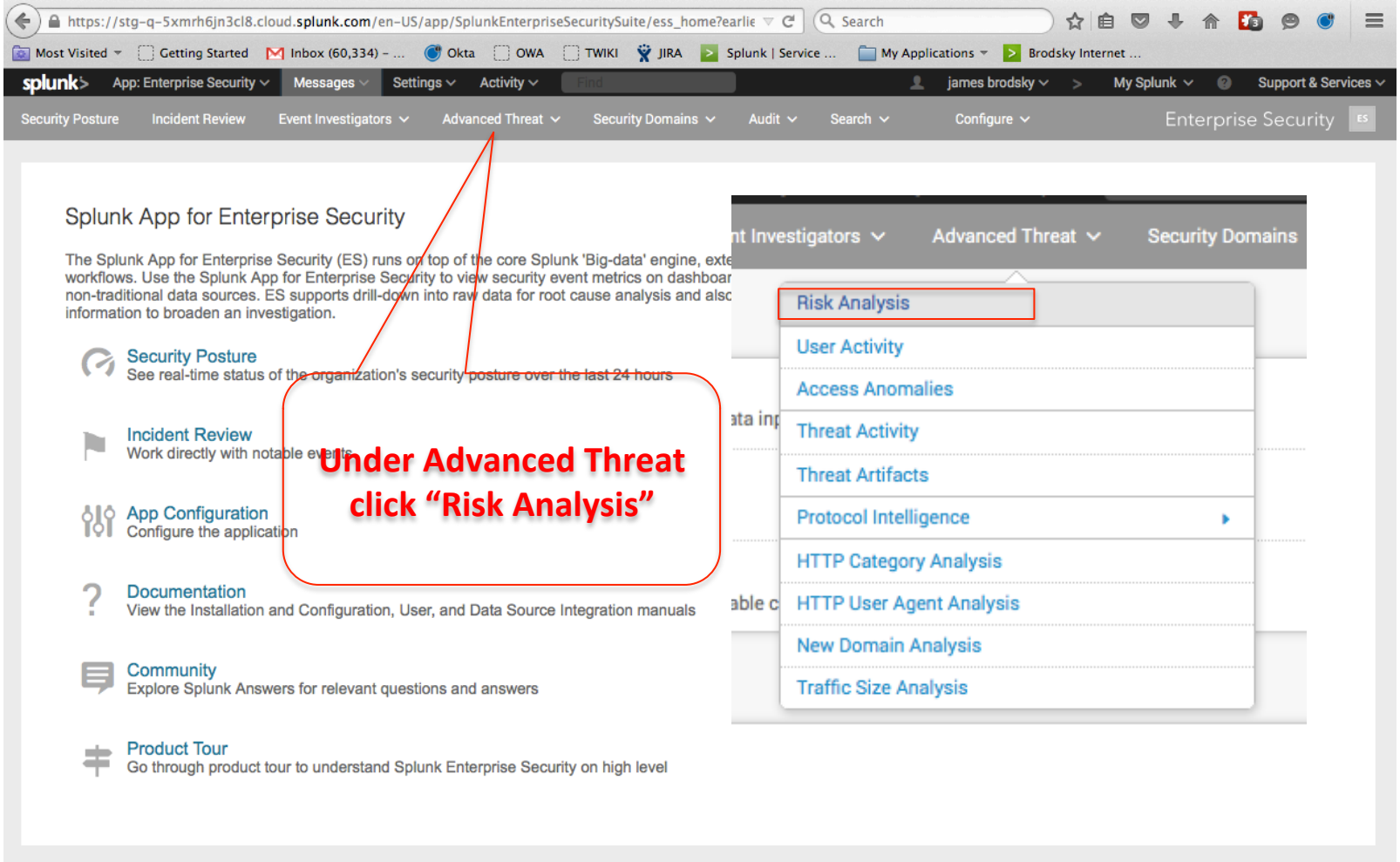
Risk Analysis

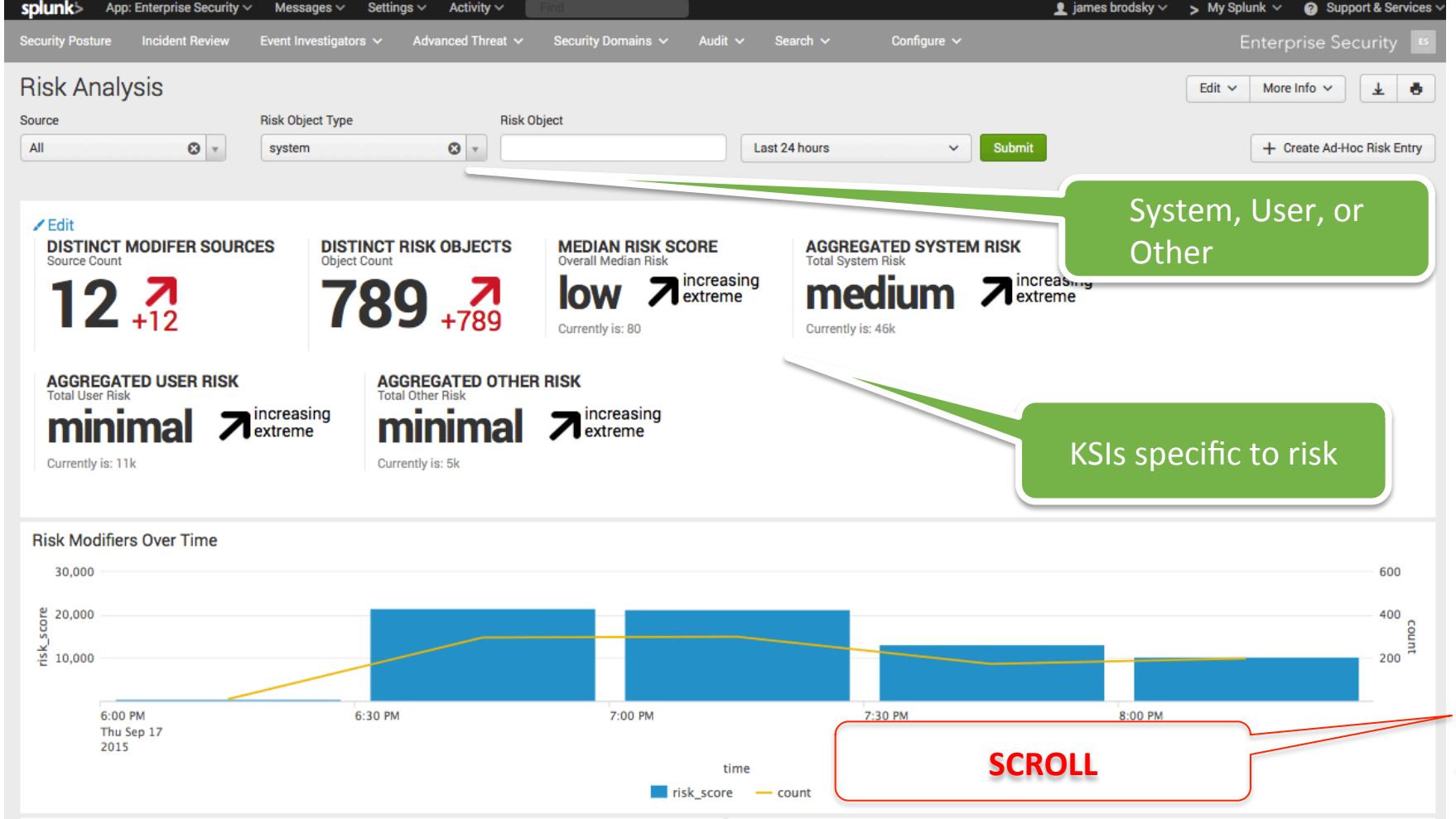
splunk>

What To Do First?

- Risk provides context
- Risk helps direct analysts

"Risk Analysis is my favorite dashboard for my SOC analysts!"


https://stg-q-5xmrh6jn3cl8.cloud.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/ess_home?earlie
Search
Most Visited
Getting Started
Inbox (60,334) - ...
Okta
OWA
TWIKI
JIRA
Splunk | Service ...
My Applications
Brodsky Internet ...
splunk>
App: Enterprise Security
Messages
Settings
Activity
james brodsky
My Splunk
Support & Services
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
ES
Splunk App for Enterprise Security
The Splunk App for Enterprise Security (ES) runs on top of the core Splunk 'Big-data' engine, exte
workflows. Use the Splunk App for Enterprise Security to view security event metrics on dashboar
non-traditional data sources. ES supports drill-down into raw data for root cause analysis and alsc
information to broaden an investigation.
Security Posture
See real-time status of the organization's security posture over the last 24 hours
Incident Review
Work directly with notable events
App Configuration
Configure the application
Documentation
View the Installation and Configuration, User, and Data Source Integration manuals
Community
Explore Splunk Answers for relevant questions and answers
Product Tour
Go through product tour to understand Splunk Enterprise Security on high level
Under Advanced Threat
click “Risk Analysis”
nt Investigators
Advanced Threat
Security Domains
Risk Analysis
User Activity
Access Anomalies
Threat Activity
Threat Artifacts
Protocol Intelligence
HTTP Category Analysis
HTTP User Agent Analysis
New Domain Analysis
Traffic Size Analysis


splunk> App: Enterprise Security Messages Settings Activity james brodsky My Splunk Support & Services
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure Enterprise Security
Risk Analysis
Edit More Info
Source
All
Risk Object Type
system
Risk Object
Last 24 hours
Submit
Create Ad-Hoc Risk Entry
System, User, or Other
Edit
DISTINCT MODIFER SOURCES
Source Count
12 +12
DISTINCT RISK OBJECTS
Object Count
789 +789
MEDIAN RISK SCORE
Overall Median Risk
low increasing extreme
Currently is: 80
AGGREGATED SYSTEM RISK
Total System Risk
medium increasing extreme
Currently is: 46k
AGGREGATED USER RISK
Total User Risk
minimal increasing extreme
Currently is: 11k
AGGREGATED OTHER RISK
Total Other Risk
minimal increasing extreme
Currently is: 5k
KSIs specific to risk
Risk Modifiers Over Time
30,000
20,000
10,000
risk_score
600
400
200
count
6:00 PM
Thu Sep 17
2015
6:30 PM
7:00 PM
7:30 PM
8:00 PM
time
risk_score
count
SCROLL

Risk Score By Object

risk_object	risk_object_type	risk_score	source_count	count
127.0.0.1	system	1720	1	43
10.11.36.20	system	420	4	7
ip-192-168-156-162	system	360	2	7
aseykoski	user	320	3	4
GH4-FGT300A	system	300	1	5
10.11.36.10	system	200	2	3
10.11.36.11	system	200	2	3
10.11.36.14	system	200	2	3
10.11.36.16	system	200		3
10.11.36.18	system	200		

« prev 1 2 3 4 5

Most Active Sources

source	risk_score	risk_objects	count
Threat - Watchlisted Events - Rule	35680	445	446
Threat - Threat List Activity - Rule	7320	178	183
Access - Geographically Improbable Access Detected - Rule	9440	118	118
Access - Excessive Failed Logins - Rule	4920	57	82
Endpoint - Host With Multiple Infections - Rule	4960	62	62
Access - Brute Force Access Behavior Detected - Rule	4480	56	56
Access - Default Account Usage - Rule	2080	5	52
Access - Insecure Or Cleartext Authentication - Rule	1520	18	19
Network - Policy Or Configuration Change - Rule	480	3	8
from Expired User Identity - Rule	560	7	7

« prev 1 2 next »

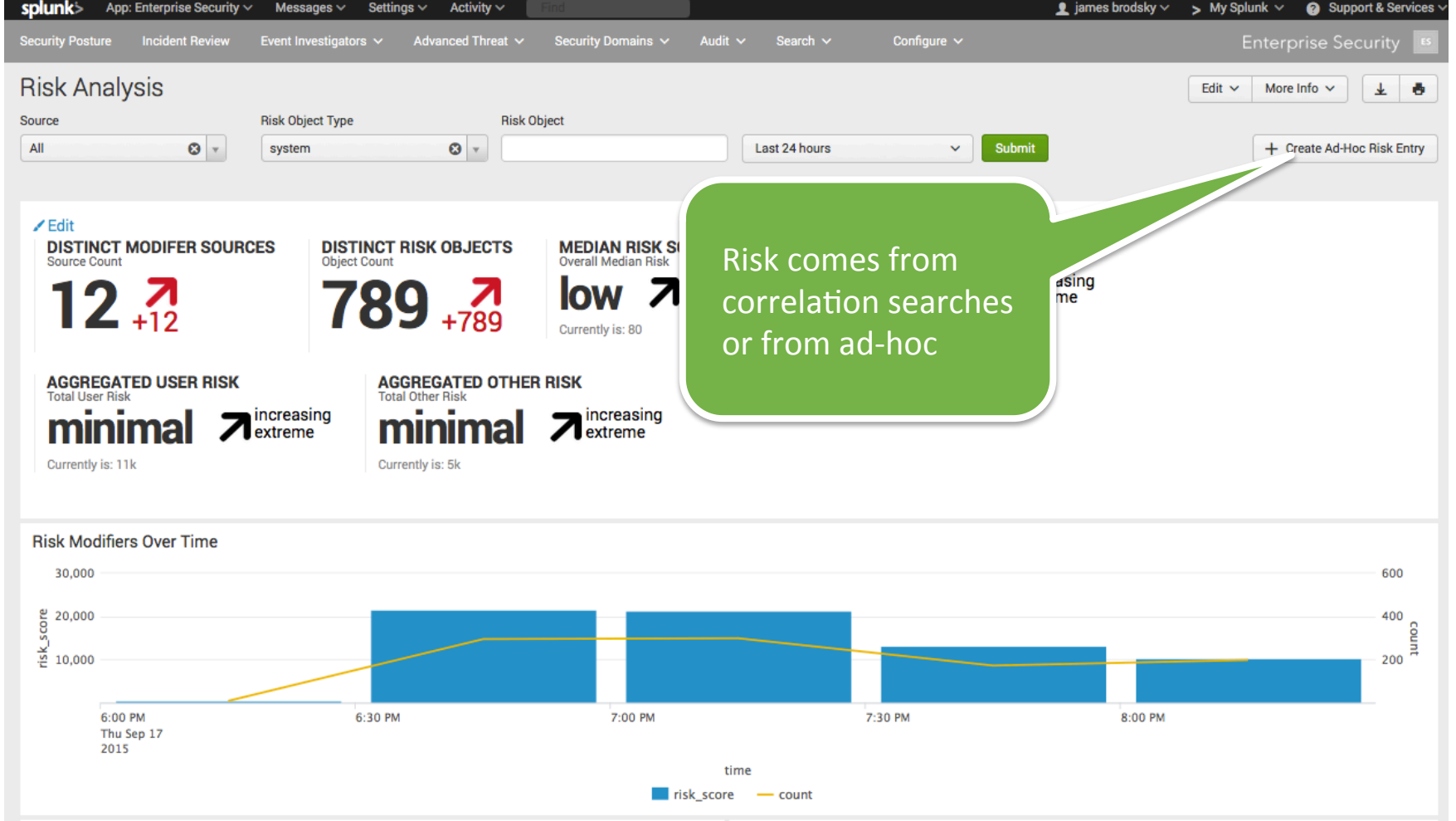
The score per object

The source of risk score

Recent Risk Modifiers

_time	risk_object	risk_object_type	source	description	
2015-09-17 20:44:57	127.0.0.1	system	Access - Default Account Usage - Rule	Discovers use of default accounts (such as admin, administrator, etc.). Default accounts ha commonly targeted by attackers using brute force attack tools.	
2015-09-17 20:44:57	127.0.0.1	system	Access - Default Account Usage - Rule	Discovers use of default accounts (such as admin, administrator, etc.). Default accounts have default passwords and are therefore commonly targeted by attackers using brute force attack tools.	40
2015-09-17 20:44:57	127.0.0.1	system	Access - Default Account Usage - Rule	Discovers use of default accounts (such as admin, administrator, etc.). Default accounts have default passwords and are therefore commonly targeted by attackers using brute force attack tools.	40
2015-09-17 20:44:57	127.0.0.1	system	Access - Default Acc Usage - Rule	Discovers use of default accounts (such as admin, administrator, etc.). Default accounts have default passwords and are therefore ted by attackers using brute force attack tools.	40
2015-09-17 20:44:57	127.0.0.1	system	Access - Default Account Usage - Rule	Discovers use of default accounts (such as admin, administrator, etc.). Default accounts have default passwords and are therefore commonly targeted by attackers using brute	40
2015-09-17 20:44:57	127.0.0.1	system	Access - Default Account Usage - Rule	Discovers use of default accounts (such as admin, administrator, etc.). commonly targeted by attackers using brute force attack tools.	40
2015-09-17 20:44:57	127.0.0.1	system	Access - Default Account Usage - Rule	Discovers use of default accounts (such as admin, administrator, etc.). Defau commonly targeted by attackers using brute force attack tools.	40

The details


splunk> App: Enterprise Security Messages Settings Activity
james brodsky My Splunk Support & Services
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Risk Analysis
Edit More Info
Source
All
Risk Object Type
system
Risk Object
Last 24 hours
Submit
Create Ad-Hoc Risk Entry
Edit
DISTINCT MODIFER SOURCES
Source Count
12 +12
DISTINCT RISK OBJECTS
Object Count
789 +789
MEDIAN RISK S
Overall Median Risk
low
Currently is: 80
Risk comes from correlation searches or from ad-hoc
AGGREGATED USER RISK
Total User Risk
minimal
increasing extreme
Currently is: 11k
AGGREGATED OTHER RISK
Total Other Risk
minimal
increasing extreme
Currently is: 5k
Risk Modifiers Over Time
30,000
20,000
10,000
risk_score
600
400
200
count
6:00 PM
Thu Sep 17
2015
6:30 PM
7:00 PM
7:30 PM
8:00 PM
time
risk_score
count

Questions on Risk Analysis?

splunk>

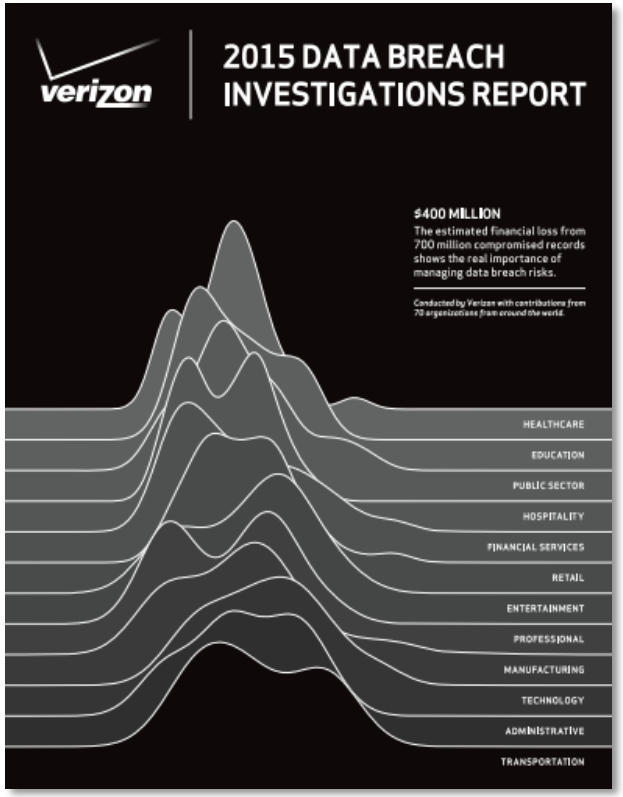
Threat Intelligence

splunk>

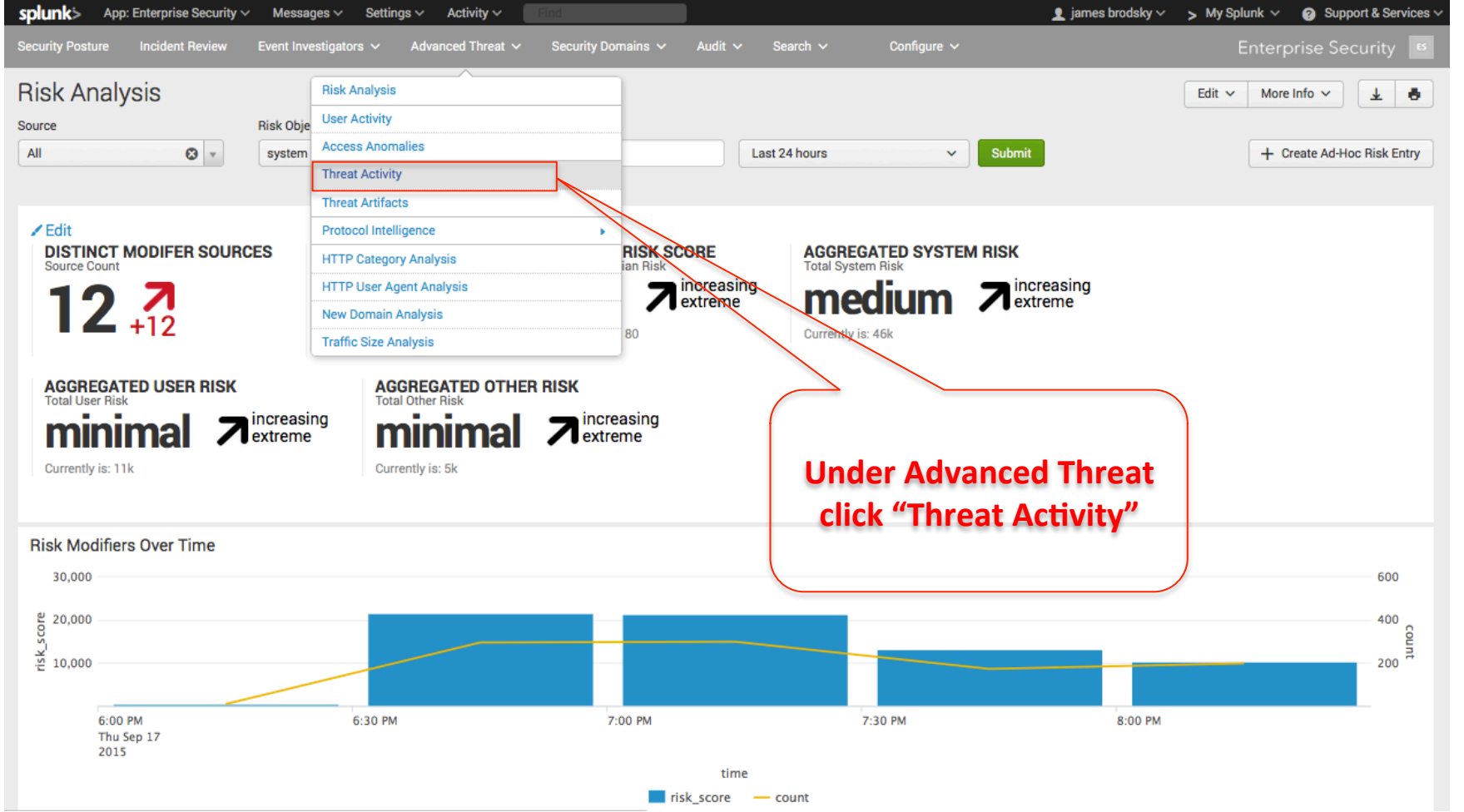

The Challenge:
• Industry says Threat Intel is key to APT Protection
• Management wants all threat intel checked against every system, constantly
• Don’t forget to keep your 15+ threat feeds updated
The Solution:
splunk>
NORSE Attack Map

Verizon 2015 DBIR

“”…the percentage of indicators unique to only one (outbound destination) feed…is north of 97% for the feeds we have sampled…”



Threat list aggregation = more complete intelligence


splunk> App: Enterprise Security Messages Settings Activity Find
james brodsky My Splunk Support & Services
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Risk Analysis
Edit More Info
Source
All
Risk Obje
system
Last 24 hours
Submit
Create Ad-Hoc Risk Entry
Risk Analysis
User Activity
Access Anomalies
Threat Activity
Threat Artifacts
Protocol Intelligence
HTTP Category Analysis
HTTP User Agent Analysis
New Domain Analysis
Traffic Size Analysis
Edit
DISTINCT MODIFER SOURCES
Source Count
12
+12
RISK SCORE
increasing extreme
80
AGGREGATED SYSTEM RISK
Total System Risk
medium
increasing extreme
Currently is: 46k
AGGREGATED USER RISK
Total User Risk
minimal
increasing extreme
Currently is: 11k
AGGREGATED OTHER RISK
Total Other Risk
minimal
increasing extreme
Currently is: 5k
Under Advanced Threat click “Threat Activity”
Risk Modifiers Over Time
30,000
20,000
10,000
risk_score
600
400
200
count
6:00 PM Thu Sep 17 2015
6:30 PM
7:00 PM
7:30 PM
8:00 PM
time
risk_score
count

Security Posture | Incident Review | Event Investigators | Advanced Threat | Security Domains | Audit | Search | Configure | Enterprise Security

Threat Activity

Edit | More Info

Threat Group: All

Threat Category: All

Search: Threat Match Value | Last 24 hours | Submit

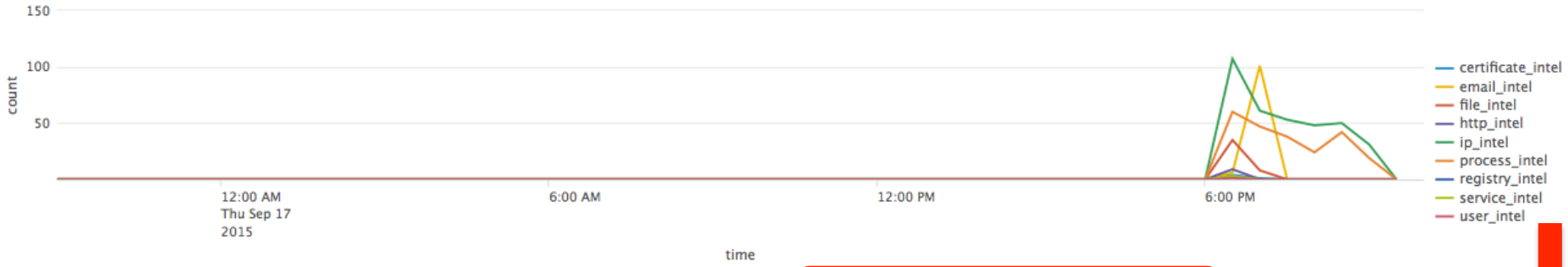
Advanced Filter...

Edit

THREAT MATCHES	THREAT COLLECTIONS	THREAT CATEGORIES	THREAT SOURCES	THREAT ACTIVITY
Unique Count	Unique Count	Unique Count	Unique Count	Total Count
221 +221	9 +9	13 +13	18 +18	750 +750

KSIs specific to threat

Threat Activity Over Time



SCROLL

Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches …rk Resolution Matches Sou… Destination Matches		12	350
process_intel	Process Ma… Source And Desti… …tches		2	230
email_intel	Email Address Matches File Name Matches Network Resolution Matches Source And Destination Matches		1	107
file_intel	File Hash Matches File Name Matches		24	43
http_intel	HTTP User Agent Matches Network Resolution Matches Source And Destination Matches URL Matches		1	9
certificate_intel	Certificate Common Name Matches Certificate Organization Matches Certificate Serial Matches Certificate Unit Matches Email Address Matches			
service_intel	Service Matches		2	3
registry_intel	Registry Path Matches Registry Value Text Matches		1	2
user_intel	User Matches		1	1

4m ago

Most Active Threat Sources

source_id	source_path	source_type	count
fc2d3e44-80a6-4add-ad94-de9f289e62ff	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc	ioc	270
6bd24113-2922-4d25-b490-f727f47ba948	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	229
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	107
iblocklist_logmein	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	csv	70
mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_G_IOCs_No_OpenIOC.xml	stix	39
…-4cd8-9a9e-	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc	ioc	9
…-lcfe-…49	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_F_SSLCertificates.xml	stix	5
…ins	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/malware_domains.csv	csv	4
0c7c902c-61f8-479c-9f44-4d985106365a	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.1.ioc	ioc	3
0c7c902c-67f8-479c-9f44-4d985106365a	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local	ioc	3

« prev 1 2 next »

Threat categories

Threat specifics

Threat Activity Details

_time	threat_match_field	threat_match_value	filter	sourcetype	src	dest	threat_collection	threat_group	threat_category
2015-9-17 15:15:00	dest	166.48.67.28		stream:http	65.101.44.34	166.48.67.28	ip_intel	iblocklist_spyware	threatlist
2015-9-17 15:15:00	dest	25.136.23.240		stream:http	183.202.198.58	25.136.23.240	ip_intel	iblocklist_logmein	threatlist
2015-9-17 15:15:00	dest	25.146.122.133		stream:http	137.218.114.121	25.146.122.133	ip_intel	iblocklist_logmein	threatlist
2015-9-17 15:15:00	dest	25.150.140.217		stream:http	33.32.189.211	25.150.140.217	ip_intel	iblocklist_logmein	threatlist
2015-9-17 15:15:00	src	10.11.36.20		bluecoat bro_conn bro_http	10.11.36.20	10.11.36.1 10.11.36.10 10.11.36.11	ip_intel	IP APT	IP Utility

Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		12	350
process_intel	Process Matches Source And Destination Matches		2	230
email_intel	Email Address Matches File Name Matches Network Resolution Matches Source And Destination Matches		1	107
file_intel	File Hash Matches File Name Matches		24	43
http_intel	HTTP User Agent Matches Network Resolution Matches Source And Destination Matches URL Matches		1	9
certificate_intel	Certificate Common Name Matches Certificate Organization Matches Certificate Serial Matches Certificate Unit Matches Email Address Matches		4	5
service_intel	Service Matches		2	3
registry_intel	Registry Path Matches Registry Value Text Matches		1	2
user_intel	User Matches		1	1

4m ago

Most Active Threat Sources

source_id	source_path	source_type	count
fc2d3e44-80a6-4add-ad94-de9f289e62ff	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc	ioc	270
6bd24113-2922-4d25-b490-f727f47ba948	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	229
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	107
iblocklist_logmein	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	csv	70
mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_G_IOCs_No_OpenIOC.xml	stix	39
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc	ioc	9
mandiant:package-190593d6-1861-4cfe-b212-c016fce1e249	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_F_SSLCertificates.xml	stix	5
malware_domains	/opt/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/malware_domains.csv	csv	4
0c7c902c-61f8-479c-9f44-4d985106365a	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.1.ioc	ioc	3
0c7c902c-67f8-479c-9f44-4d985106365a	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel.ioc	ioc	3

« prev 1 2 next »

We know about this.
Let me tell you the fix.

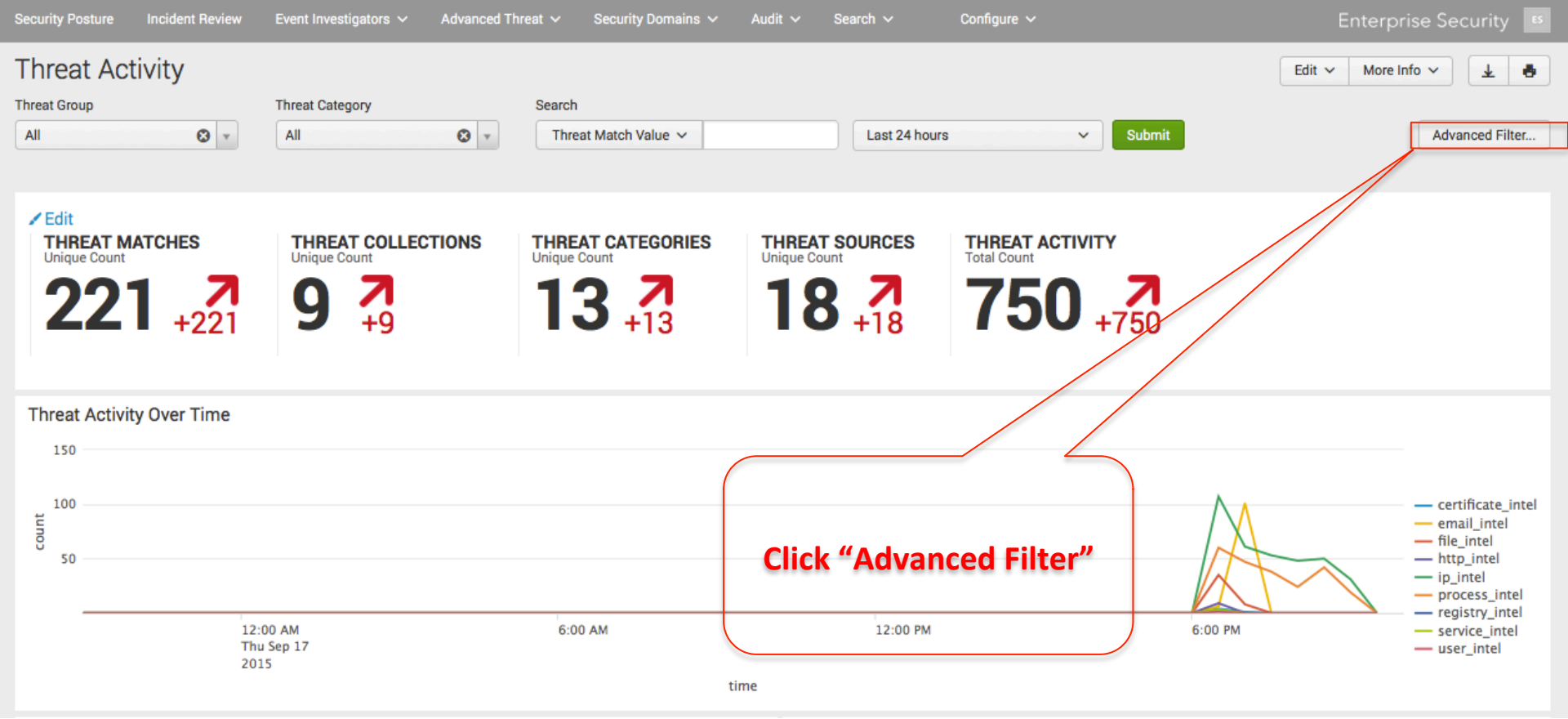
Threat Activity Details

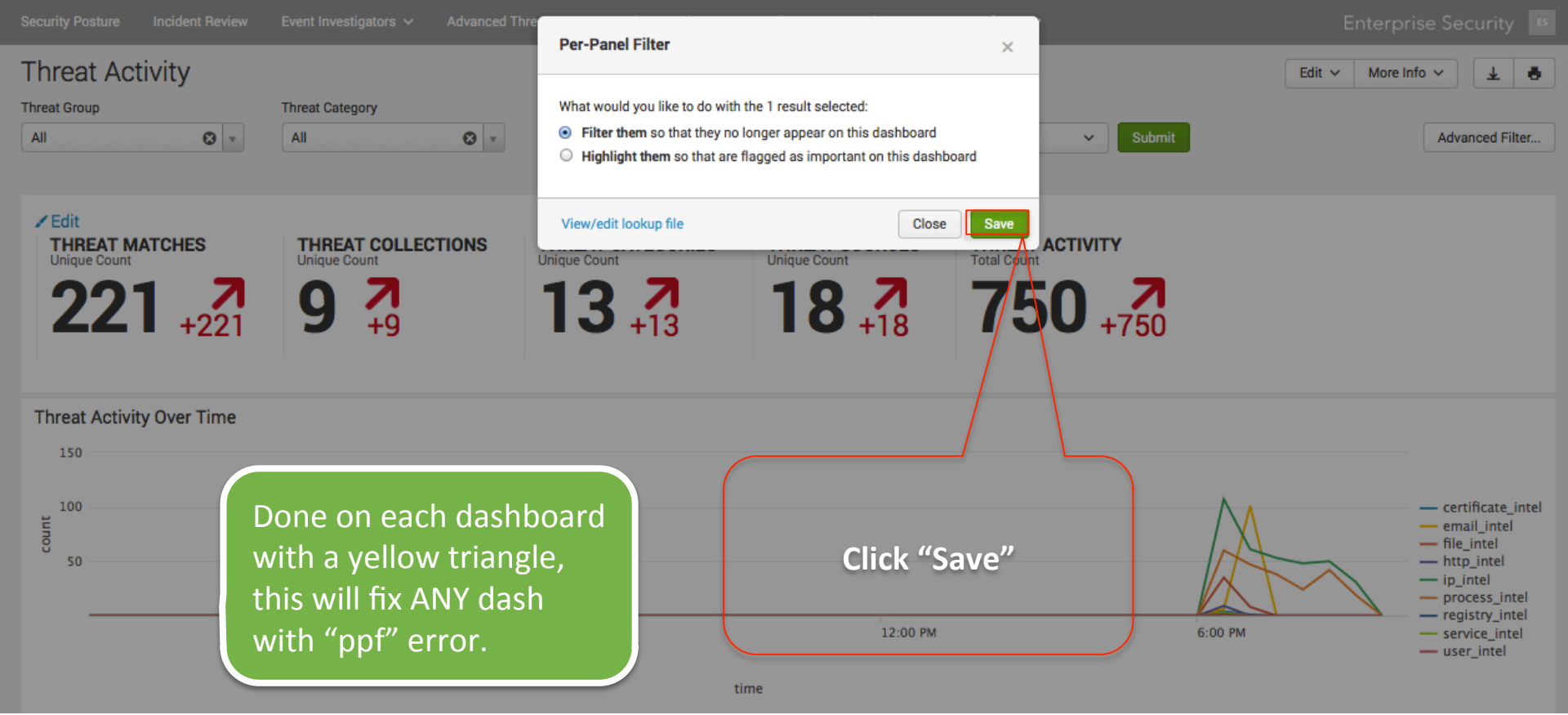
_time	threat_match_field	threat_match_value	filter	sourcetype	src	dest			threat_category
2015-9-17 15:15:00	dest	166.48.67.28		stream:http	65.101.44.34	166.48.67.28	ip_intel	iblocklist_spyware	threatlist
2015-9-17 15:15:00	dest	25.136.23.240		stream:http	183.202.198.58	25.136.23.240	ip_intel	iblocklist_logmein	threatlist
2015-9-17 15:15:00	dest	25.146.122.133		stream:http	137.218.114.121	25.146.122.133	ip_intel	iblocklist_logmein	threatlist
2015-9-17 15:15:00	dest	25.150.140.217		stream:http	33.32.189.211	25.150.140.217	ip_intel	iblocklist_logmein	threatlist
2015-9-17 15:15:00	src	10.11.36.20		bluecoat bro_conn bro_http	10.11.36.20	10.11.36.1 10.11.36.10 10.11.36.11	ip_intel	IP APT	IP Utility

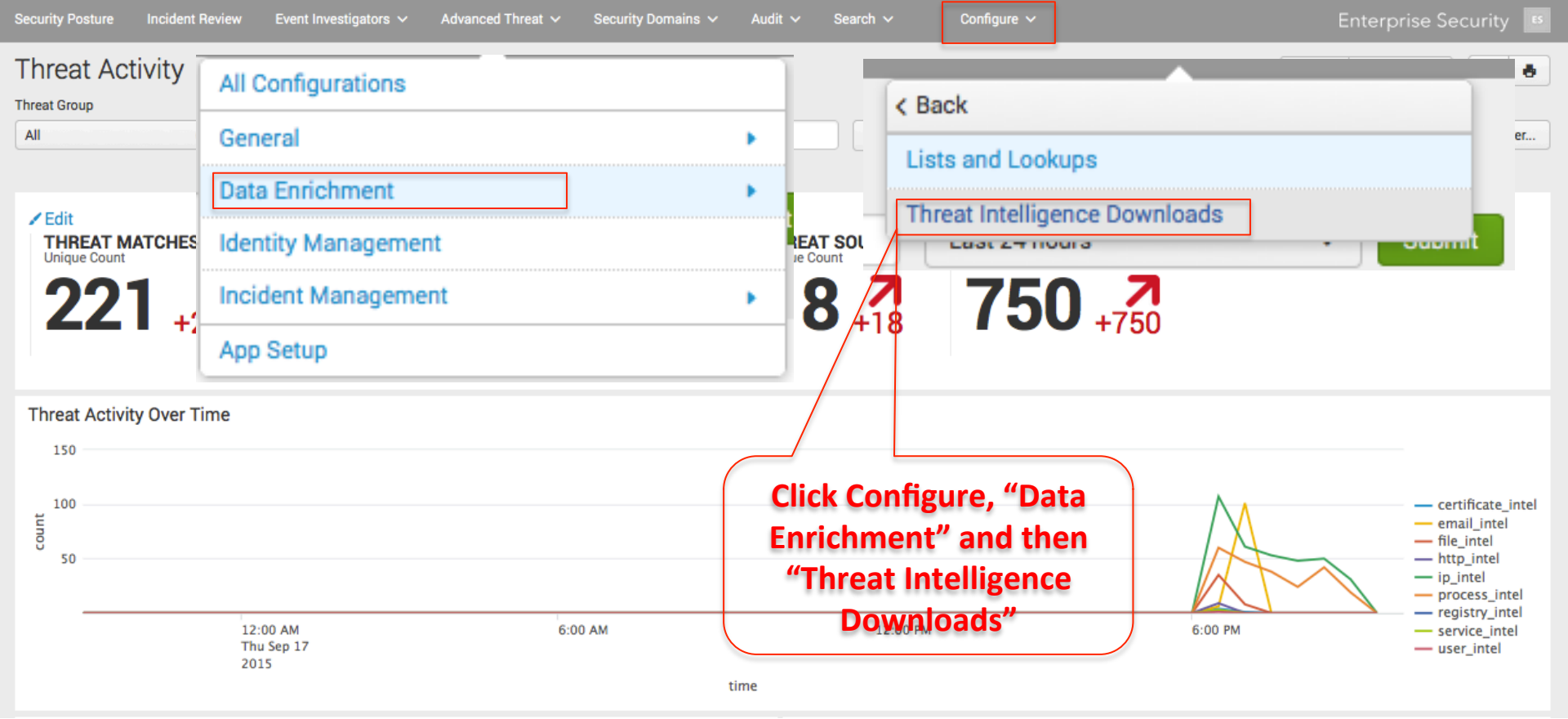
Threat Activity Details

_time	threat_match_field	threat_match_value	filter	sourcetype	src	dest	threat_collection	threat_group	threat_category
2015-9-17 15:15:00	dest	166.48.67.28		stream:http	65.101.44.34	166.48.67.28	ip_intel	iblocklist_spyware	threatlist
2015-9-17 15:15:00	dest	25.136.23.240		stream:http	183.202.198.58	25.136.23.240	ip_intel	iblocklist_logmein	threatlist
2015-9-17 15:15:00	dest	25.146.122.133		stream:http	137.218.114.121	25.146.122.133	ip_intel	iblocklist_logmein	threatlist
2015-9-17 15:15:00	dest	25.150.140.217		stream:http	33.32.189.211	25.150.140.217	ip_intel	iblocklist_logmein	threatlist

Checkbox any line in the "Threat Activity Details"


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Threat Activity
Edit
More Info
Threat Group
All
Threat Category
All
Search
Threat Match Value
Last 24 hours
Submit
Advanced Filter...
Edit
THREAT MATCHES
Unique Count
221 +221
THREAT COLLECTIONS
Unique Count
9 +9
THREAT CATEGORIES
Unique Count
13 +13
THREAT SOURCES
Unique Count
18 +18
THREAT ACTIVITY
Total Count
750 +750
Threat Activity Over Time
150
100
50
count
12:00 AM
Thu Sep 17
2015
6:00 AM
12:00 PM
6:00 PM
time
certificate_intel
email_intel
file_intel
http_intel
ip_intel
process_intel
registry_intel
service_intel
user_intel
Click “Advanced Filter”


Security Posture
Incident Review
Event Investigators
Enterprise Security
Threat Activity
Edit
More Info
Threat Group
All
Threat Category
All
Submit
Advanced Filter...
Per-Panel Filter
What would you like to do with the 1 result selected:
Filter them so that they no longer appear on this dashboard
Highlight them so that are flagged as important on this dashboard
View/edit lookup file
Close
Save
Edit
THREAT MATCHES
Unique Count
221 +221
THREAT COLLECTIONS
Unique Count
9 +9
Unique Count
13 +13
Unique Count
18 +18
Total Count
750 +750
Threat Activity Over Time
150
100
50
count
12:00 PM
6:00 PM
time
certificate_intel
email_intel
file_intel
http_intel
ip_intel
process_intel
registry_intel
service_intel
user_intel
Done on each dashboard with a yellow triangle, this will fix ANY dash with “ppf” error.
Click “Save”


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Threat Activity
Threat Group
All
All Configurations
General
Data Enrichment
Identity Management
Incident Management
App Setup
Back
Lists and Lookups
Threat Intelligence Downloads
Edit
THREAT MATCHES
Unique Count
221
8
+18
750
+750
Threat Activity Over Time
150
100
50
count
12:00 AM
Thu Sep 17
2015
6:00 AM
6:00 PM
time
certificate_intel
email_intel
file_intel
http_intel
ip_intel
process_intel
registry_intel
service_intel
user_intel
Click Configure, “Data Enrichment” and then “Threat Intelligence Downloads”

Threat Intelligence Downloads

Data inputs » Threat Intelligence Downloads

Various community threat lists

TAXII support

Local ones too

New

Showing 1-25 of 25 items

Results per page 25

Name	Type	Description	URL	Weight	App	Status	Actions
alexa_top_one_million_sites	alexa	Alexa Top 1 Million Sites, copyright 2014, Alexa Internet (www.alexa.com)	...onaws.com/alexa-static/top-1m.csv.zip	1	SA-ThreatIntelligence	Enabled | Disable	Clone
emerging_threats_compromised_ip_blocklist	threatlist	Emerging Threats compromised ...	http://rules.emergingthreats.net/blockrules/compromised-ips.txt	1	SA-ThreatIntelligence	Disabled | Enable	Clone
emerging_threats_ip_blocklist	threatlist	Em... ...hreats fwip rules	http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt	1	SA-ThreatIntelligence	Disabled | Enable	Clone
hailataxii_malware	taxii	Hail a TAXII.com malware domain host list	http://hailataxii.com/taxii-data	1	DA-ESS-ThreatIntelligence	Disabled | Enable	Clone
iblocklist_logmein	threatlist	Addresses that are used by the LogMeIn product to enable unauthorized remote access	http://list.iblocklist.com/?list=logmein	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_piratebay	threatlist	Addresses that are commonly associated with known PirateBay sites	http://list.iblocklist.com/?list=nzldzlpkgrcncdomnttb	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_proxy	threatlist	Addresses that are commonly associated with known traffic-proxy sites	http://list.iblocklist.com/?list=bt_pr...			Enabled | Disable	Clone
iblocklist_rapidshare	threatlist	Addresses that are commonly associated with known RapidShare sites	http://list.iblocklist.com/?list=zfucv...			Enabled | Disable	Clone
iblocklist_spyware	threatlist	Addresses that are commonly associated with known spyware sites	http://list.iblocklist.com/?list=bt_sp...			Enabled | Disable	Clone
iblocklist_tor	threatlist	Addresses that are commonly associated with known Tor sites	http://list.iblocklist.com/?list=tor	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_web_attacker	threatlist	Addresses that are commonly associated with known malicious attacker sites	http://list.iblocklist.com/?list=ghlzqtqxnzc...	1	SA-ThreatIntelligence	Enabled | Disable	Clone
icaan_top_level_domain_list	tld	ICAAN Top-level Domains List	http://data.iana.org/TLD/tlds-alpha-by-d...xt	1	SA-ThreatIntelligence	Enabled | Disable	Clone
local_threatlist	threatlist	Custom list of threat IP addresses	lookup://local_threatlist	1	SA-ThreatIntelligence	Enabled | Disable	Clone
local_threatlist_domains	threatlist_domain	Custom list of threat domains	lookup://local_threatlist_domains	1	SA-ThreatIntelligence	Enabled | Disable	Clone
local_threatlist_urls	threatlist_url	Custom list of threat urls	lookup://local_threatlist_urls	1	SA-ThreatIntelligence	Enabled | Disable	Clone
malware_domains	threatlist_domain	Malware Domain Blocklist	http://mirror1.malwaredomains.com/files/domains.txt	1	SA-ThreatIntelligence	Enabled | Disable	Clone

Threat Intelligence Downloads

Data inputs » Threat Intelligence Downloads

New

Showing 1-25 of 25 items

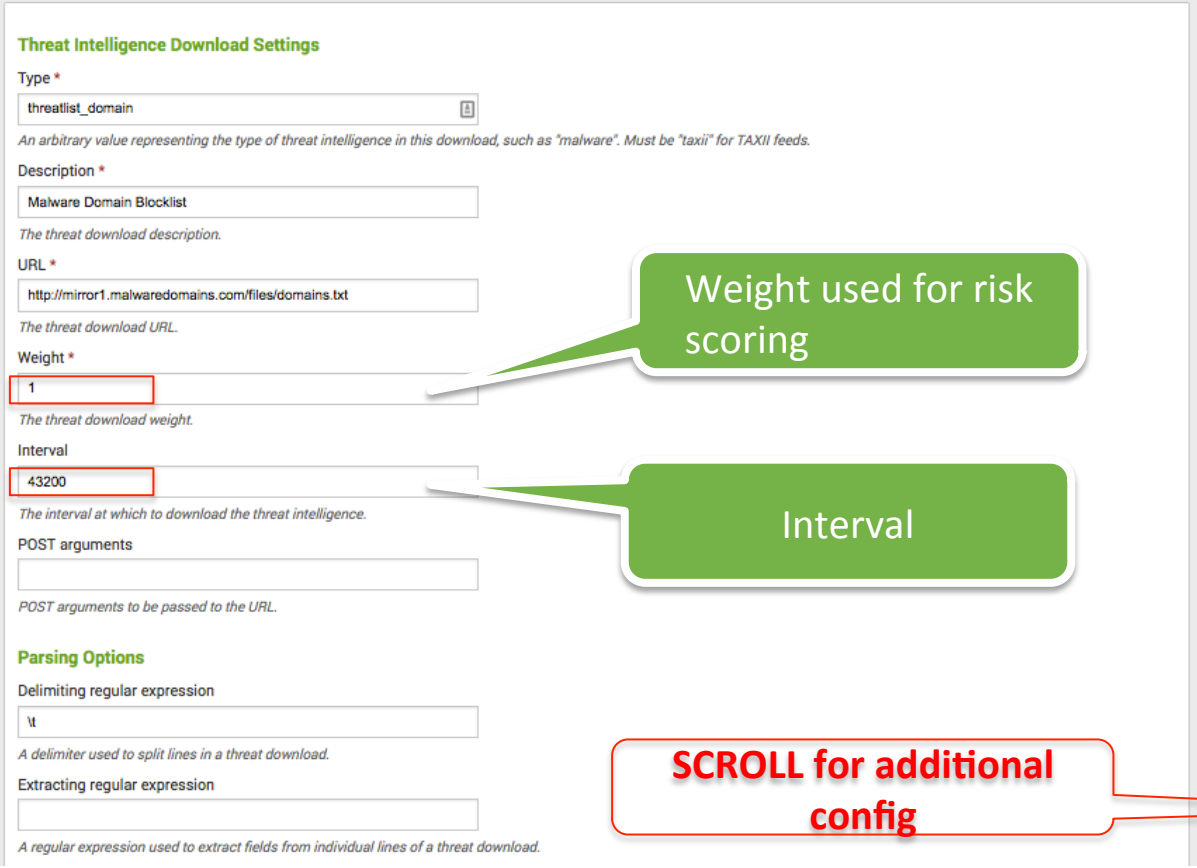
Results per page 25

Name	Type	Description	URL	Weight	App	Status	Actions
alexa_top_one_million_sites	alexa	Alexa Top 1 Million Sites, copyright 2014, Alexa Internet (www.alexa.com)	http://s3.amazonaws.com/alexa-static/top-1m.csv.zip	1	SA-ThreatIntelligence	Enabled | Disable	Clone
emerging_threats_compromised_ip_blocklist	threatlist	Emerging Threats compromised IPs blocklist	http://rules.emergingthreats.net/blockrules/compromised-ips.txt	1	SA-ThreatIntelligence	Disabled | Enable	Clone
emerging_threats_ip_blocklist	threatlist	Emerging Threats fwip rules	http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt	1	SA-ThreatIntelligence	Disabled | Enable	Clone
hailataxii_malware	taxii	Hail a TAXII.com malware domain host list	http://hailataxii.com/taxii-data	1	DA-ESS-ThreatIntelligence	Disabled | Enable	Clone
iblocklist_logmein	threatlist	Addresses that are used by the LogMeIn product to enable unauthorized remote access	http://list.iblocklist.com/?list=logmein	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_piratebay	threatlist	Addresses that are commonly associated with known PirateBay sites	http://list.iblocklist.com/?list=nzldzlpkgrcncdomnttb	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_proxy	threatlist	Addresses that are commonly associated with known traffic-proxy sites	http://list.iblocklist.com/?list=bt_proxy	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_rapidshare	threatlist	Addresses that are commonly associated with known RapidShare sites	http://list.iblocklist.com/?list=zfucwtikfwkalytktyiw	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_spyware	threatlist	Addresses that are commonly associated with known spyware sites	http://list.iblocklist.com/?list=bt_spyware	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_tor	threatlist	Addresses that are commonly associated with known Tor sites	http://list.iblocklist.com/?list=tor	1	SA-ThreatIntelligence	Enabled | Disable	Clone
iblocklist_web_attacker	threatlist	Addresses that are commonly associated with known malicious attacker sites	http://list.iblocklist.com/?list=ghlzqtqxnzctvvajwwag	1	SA-ThreatIntelligence	Enabled | Disable	Clone
icaan_top_level_domain_list	tld	ICAAN Top-level Domains List	http://data.iana.org/TLD/tlds-alpha-by-domain.txt	1	SA-ThreatIntelligence	Enabled | Disable	Clone
local_threatlist	threatlist	Custom list of threat IP addresses	lookup://local_threatlist	1	SA-ThreatIntelligence	Enabled | Disable	Clone
local_threatlist_domains	threatlist_domain	Custom list of threat domains	lookup://local_threatlist_domains	1	SA-ThreatIntelligence	Enabled | Disable	Clone
local_threatlist_urls	threatlist_url	Custom list of threat urls	lookup://local_threatlist_urls	1	SA-ThreatIntelligence	Enabled | Disable	Clone
malware_domains	threatlist_domain	Malware Domain Blocklist	http://mirror1.malwaredomains.com/files/domains.txt	1	SA-ThreatIntelligence	Enabled | Disable	Clone

Click "Malware Domains"

malware_domains

Data inputs » Threat Intelligence Downloads » malware_domains



malware_domains

Data inputs » Threat Intelligence Downloads » malware_domains

Threat Intelligence Download Settings

Type *

threatlist_domain

An arbitrary value representing the type of threat intelligence in this download, such as "malware". Must be "taxii" for TAXII feeds.

Description *

Malware Domain Blocklist

The threat download description.

URL *

http://mirror1.malwaredomains.com/files/domains.txt

The threat download URL.

Weight *

1

The threat download weight.

Interval

43200

The interval at which to download the threat intelligence.

POST arguments

POST arguments to be passed to the URL.

Parsing Options

Delimiting regular expression

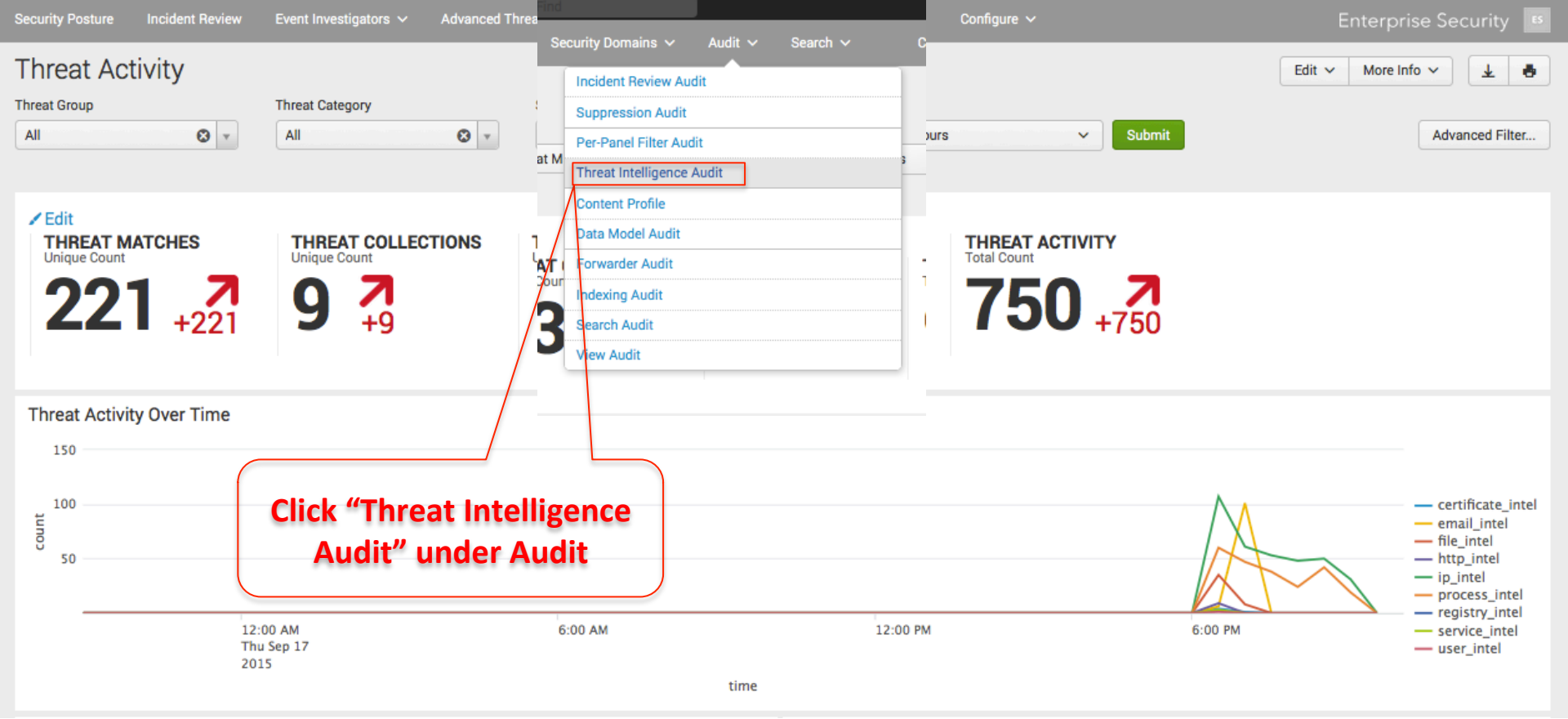
\t

A delimiter used to split lines in a threat download.

Extracting regular expression

A regular expression used to extract fields from individual lines of a threat download.

Hit "back" button twice


Security Posture
Incident Review
Event Investigators
Advanced Threa
Configure
Enterprise Security
Security Domains
Audit
Search
Incident Review Audit
Suppression Audit
Per-Panel Filter Audit
Threat Intelligence Audit
Content Profile
Data Model Audit
Forwarder Audit
Indexing Audit
Search Audit
View Audit
Threat Activity
Edit
More Info
Threat Group
All
Threat Category
All
Submit
Advanced Filter...
Edit
THREAT MATCHES
Unique Count
221
+221
THREAT COLLECTIONS
Unique Count
9
+9
THREAT ACTIVITY
Total Count
750
+750
Threat Activity Over Time
150
100
50
count
12:00 AM
Thu Sep 17
2015
6:00 AM
12:00 PM
6:00 PM
time
certificate_intel
email_intel
file_intel
http_intel
ip_intel
process_intel
registry_intel
service_intel
user_intel
Click “Threat Intelligence Audit” under Audit

Threat Intelligence Audit

Details regarding updates to ES Threat Intelligence

Edit | More Info

Download Enabled/Disabled: Enabled

Download Location: All

Status of downloads

Threat Intelligence Downloads

_time	stanza	disabled	type	url	weight	exit_status	download_status	run_duration
	alexa_top_one_million_sites	0	alexa	http://s3.amazonaws.com/alexa-static/top-1m.csv.zip	1	0	threat list downloaded	
	iblocklist_logmein	0	threatlist	http://list.iblocklist.com/?list=logmein	1	0	threat list downloaded	
	iblocklist_piratebay	0	threatlist	http://list.iblocklist.com/?list=nzldzlpkgrcncdomnttb	1	0	threat list downloaded	
	iblocklist_proxy	0	threatlist	http://list.iblocklist.com/?list=bt_proxy	1	0	threat list downloaded	
	iblocklist_rapidshare	0	threatlist	http://list.iblocklist.com/?list=zfucwtjkfwkalytktyiw	1	0	threat list downloaded	
	iblocklist_spyware	0	threatlist	http://list.iblocklist.com/?list=bt_spyware	1	0	threat list downloaded	
	iblocklist_tor	0	threatlist	http://list.iblocklist.com/?list=tor	1	0	threat list downloaded	
	iblocklist_web_attacker	0	threatlist	http://list.iblocklist.com/?list=ghlzqtqxnzctvvajwwag	1	0	threat list downloaded	
	icaan_top_level_domain_list	0	tld	http://data.iana.org/TLD/tlds-alpha-by-domain.txt	1	0	threat list downloaded	
	local_threatlist	0	threatlist	lookup://local_threatlist	1	0		

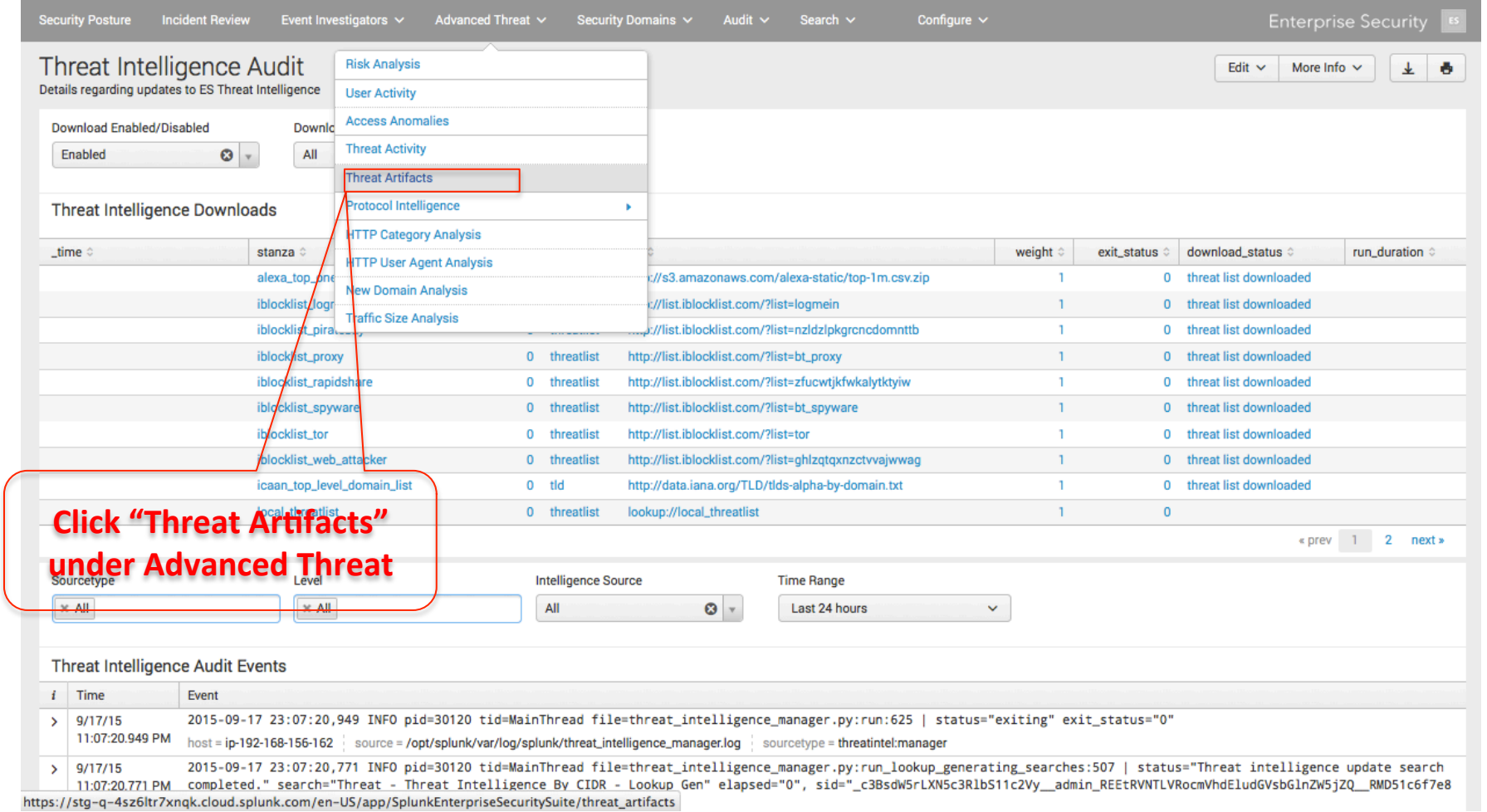
« prev 1 2 next »

Sourcetype: All | Level: All | Intelligence Source: All | Time Range: Last 24 hours

Details including errors

Threat Intelligence Audit Events

i	Time	Event
>	9/17/15 11:07:20.949 PM	2015-09-17 23:07:20,949 INFO pid=30120 tid=MainThread file=threat_intelligence_manager.py:run:625 | status="exiting" exit_status="0" host = ip-192-168-156-162 | source = /opt/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager
>	9/17/15 11:07:20.771 PM	2015-09-17 23:07:20,771 INFO pid=30120 tid=MainThread file=threat_intelligence_manager.py:run_lookup_generating_searches:507 | status="Threat intelligence update search completed." search="Threat - Threat Intelligence By CIDR - Lookup Gen" elapsed="0", sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_REEtRVNTLVRocmVhdEludGVsbGlnZW5jZQ__RMD51c6f7e87b9cc2578_at_1442531236_2565"


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Risk Analysis
User Activity
Access Anomalies
Threat Activity
Threat Artifacts
Protocol Intelligence
HTTP Category Analysis
HTTP User Agent Analysis
New Domain Analysis
Traffic Size Analysis
Threat Intelligence Audit
Details regarding updates to ES Threat Intelligence
Edit
More Info
Download Enabled/Disabled
Enabled
All
Threat Intelligence Downloads
_time
stanza
weight
exit_status
download_status
run_duration
threat list downloaded
Click "Threat Artifacts" under Advanced Threat
Sourcetype
Level
Intelligence Source
Time Range
Last 24 hours
Threat Intelligence Audit Events
Time
Event
9/17/15 11:07:20.949 PM
2015-09-17 23:07:20,949 INFO pid=30120 tid=MainThread file=threat_intelligence_manager.py:run:625 | status="exiting" exit_status="0"
host = ip-192-168-156-162 source = /opt/splunk/var/log/splunk/threat_intelligence_manager.log sourcetype = threatintel:manager
9/17/15 11:07:20.771 PM
2015-09-17 23:07:20,771 INFO pid=30120 tid=MainThread file=threat_intelligence_manager.py:run_lookup_generating_searches:507 | status="Threat intelligence update search completed." search="Threat - Threat Intelligence By CIDR - Lookup Gen" elapsed="0", sid="_c3BsdW5rLXN5c3RlbS11c2Vy__admin_REEtRVNTLVRocmVhdEludGVsbGlnZW5jZQ__RMD51c6f7e8
https://stg-q-4sz6ltr7xnqk.cloud.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/threat_artifacts

Threat Artifacts

Edit | More Info

Threat Artifact: Threat ID | Threat Category: All | Threat Group: All | Malware Alias | Intel Source ID

Intel Source Path | Submit

STIX/TAXII feed

Threat Overview | Network | Endpoint | Certificate | Email

Threat Overview

source_id	source_path	ource_type	threat_group	threat_category	malware_alias	c
0c7c902c-67f8-479c-9f44-4d985106365a	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel.ioc	oc	APT	Utility		5
0c7c902c-61f8-479c-9f44-4d985106365a	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.1.ioc	oc	APT1.1	Utility1.1		5
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	oc	Email APT	Email Utility		6
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F (and 6 more)	APT (and 2 more)		5
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc	ioc	HTTP APT	HTTP Utility		1
fc2d3e44-80a6-4add-ad94-de9f289e62ff	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc	ioc	IP APT	IP Utility		9
6bd24113-2922-4d25-b490-f727f47ba948	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	Process APT	Process Backdoor		1
4a2c5f60-f4c0-4844-ba1f-a14dac9fa36c	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/registry_intel.ioc	ioc	Registry APT	Registry Backdoor		9
7f9a6986-f00a-4071-99d3-484c9158beba	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/service_intel.ioc	ioc	Service APT	Service Backdoor		6
e651c4e4-6cce-4cfc-8bd4-ebc203907ef4	/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/user_intel.ioc	ioc	User APT	User Utility		2

« prev 1 2 3 next »

Browse through the tabs…

Endpoint Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
file_intel	stix	undefined	undefined		1356
file_intel	stix	F	APT		194
file_intel	stix	admin338	APT		194

Network Artifacts

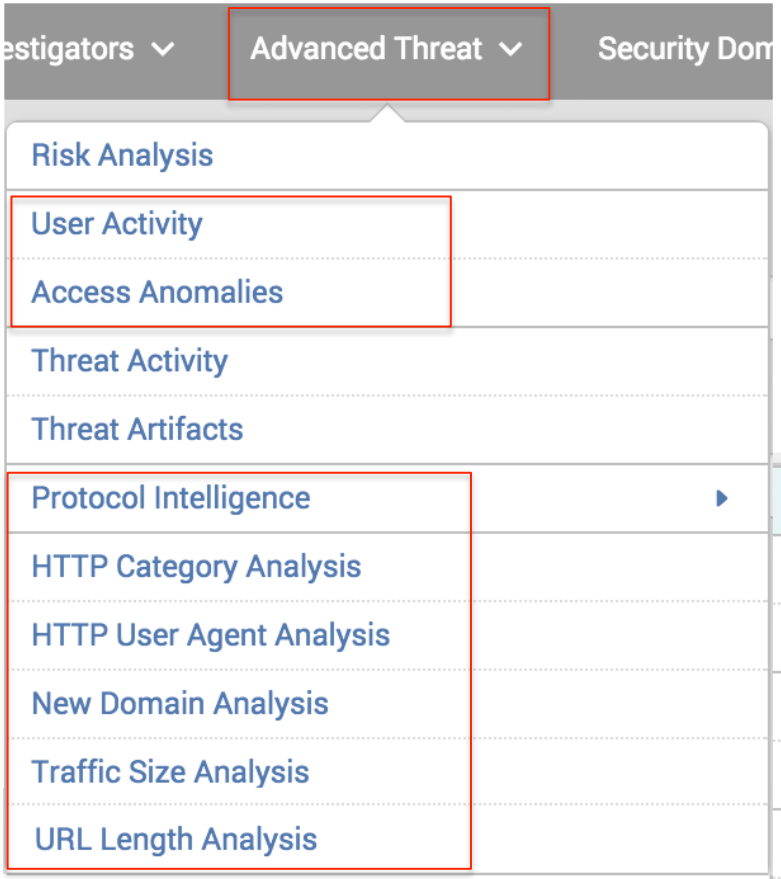
threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_categ
ip_intel	csv	0	10589	0	0	10589	malware_domains	threatlist_dor
ip_intel	csv	6203	0	0	0	6203	iblocklist_tor	threatlist
ip_intel	csv	5817	0	0	0	5817	iblocklist_proxy	threatlist

Questions on Threat Intelligence?

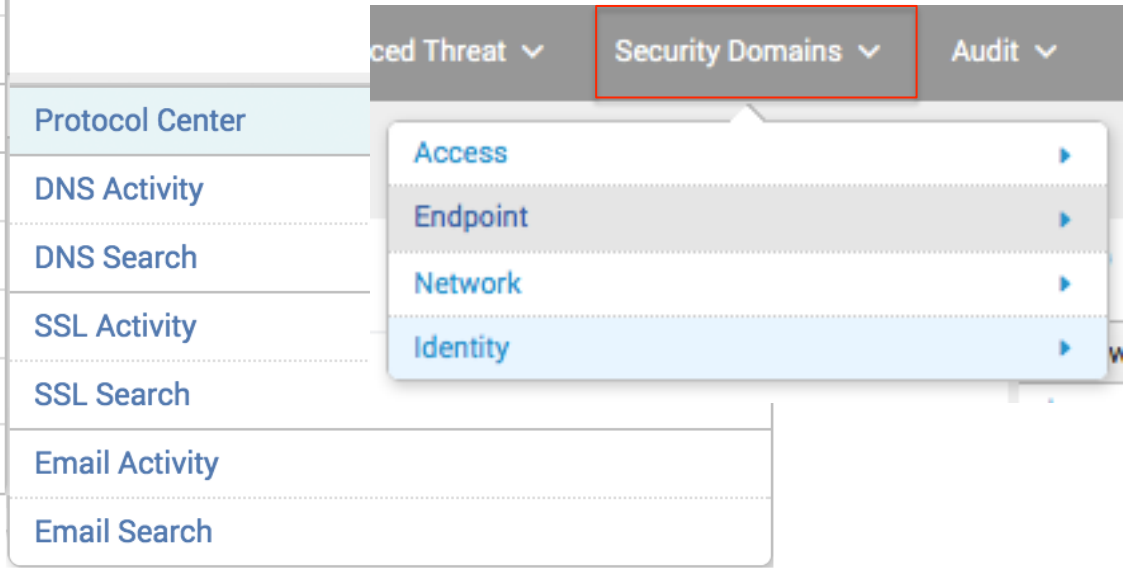
splunk>

More Advanced Threat

splunk>



Investigate on your own time: Advanced Threat capabilities worth your while…and all areas under Security Domains



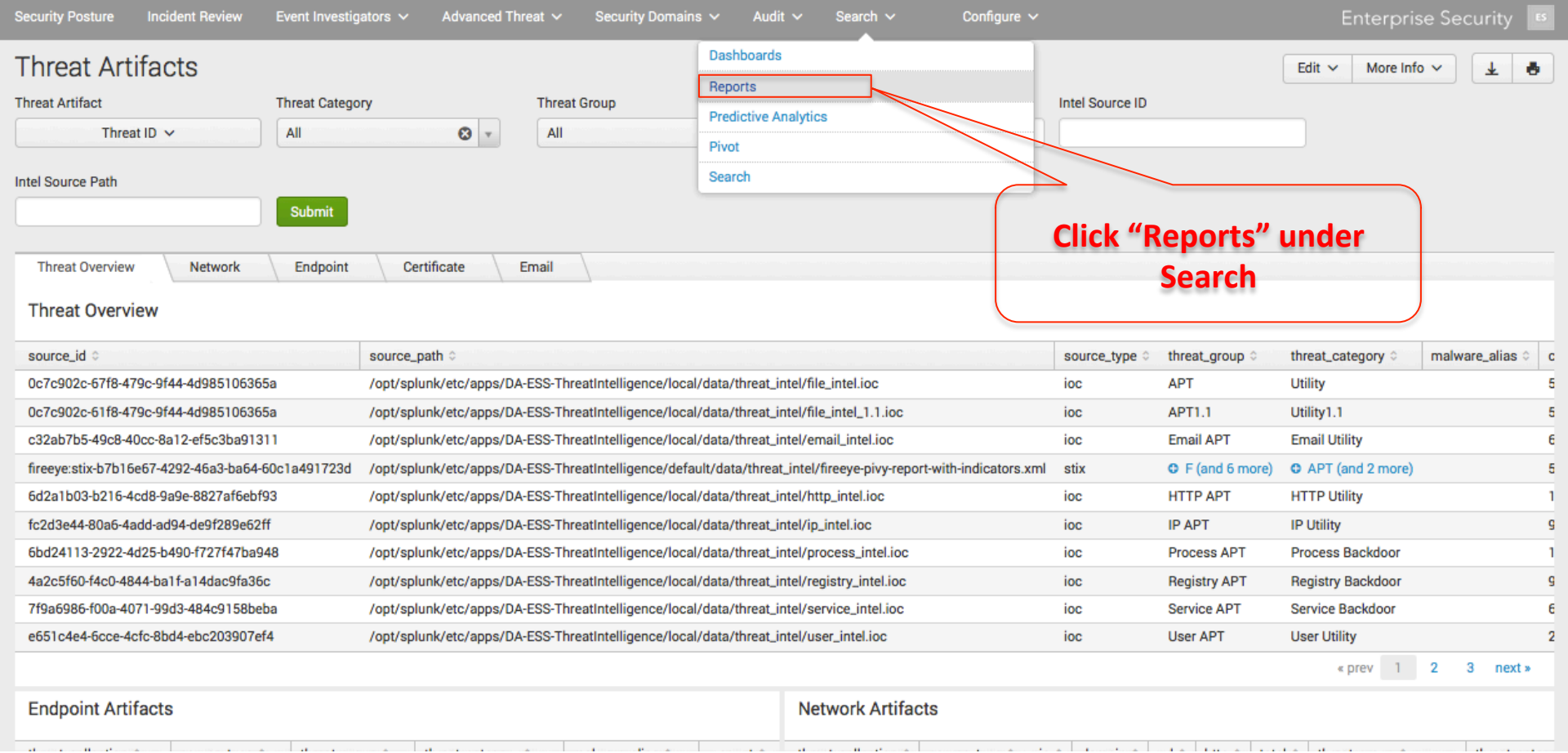
Additional Reports

splunk>

Auditors / Management / Compliance Says…

- Can you show me <Typical Report>?

- Reporting is easy in Splunk
- But we have more than 300 standard reports too


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Dashboards
Reports
Predictive Analytics
Pivot
Search
Threat Artifacts
Edit
More Info
Threat Artifact
Threat ID
Threat Category
All
Threat Group
All
Intel Source ID
Intel Source Path
Submit
Click “Reports” under Search
Threat Overview
Network
Endpoint
Certificate
Email
Threat Overview
source_id
source_path
source_type
threat_group
threat_category
malware_alias
0c7c902c-67f8-479c-9f44-4d985106365a
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel.ioc
ioc
APT
Utility
0c7c902c-61f8-479c-9f44-4d985106365a
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.1.ioc
ioc
APT1.1
Utility1.1
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc
ioc
Email APT
Email Utility
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml
stix
F (and 6 more)
APT (and 2 more)
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc
ioc
HTTP APT
HTTP Utility
fc2d3e44-80a6-4add-ad94-de9f289e62ff
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc
ioc
IP APT
IP Utility
6bd24113-2922-4d25-b490-f727f47ba948
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc
ioc
Process APT
Process Backdoor
4a2c5f60-f4c0-4844-ba1f-a14dac9fa36c
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/registry_intel.ioc
ioc
Registry APT
Registry Backdoor
7f9a6986-f00a-4071-99d3-484c9158beba
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/service_intel.ioc
ioc
Service APT
Service Backdoor
e651c4e4-6cce-4cfc-8bd4-ebc203907ef4
/opt/splunk/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/user_intel.ioc
ioc
User APT
User Utility
« prev
1
2
3
next »
Endpoint Artifacts
Network Artifacts

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.

328 Reports | All | Yours | This App's | filter | < Prev 1 2 3 4 Next >

i	Title	Actions	Owner	App	Sharing	Embedding
>	Access - Access Over Time	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Access Over Time By	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Access Over Time By App	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Account Usage For Expired Id	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Default Account Usage Over Time	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Default Account Usage Over Time By	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Default Accounts In Use	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Default Local Accounts	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Distinct Apps	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Distinct Destinations	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Distinct Sources	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Distinct Users	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - First Time Account Access	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - First Time Account Access Over Time	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Inactive Account Usage	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Inactive Accounts	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Notable Access Events	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Number Of Default Accounts In Use	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Privileged Account Usage Over Time	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Privileged Accounts In Use	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Top Access By Destination	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Top Access By Source	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled
>	Access - Total Access Attempts	Open in Search Edit	admin	DA-ESS-AccessProtection	Global	Disabled

Almost 330 reports to use/customize

Incident Response Workflow

splunk>

Security Posture | Incident Review | Event Investigators | Advanced Threat | Security Domains | Audit | Search | Configure | Enterprise Security

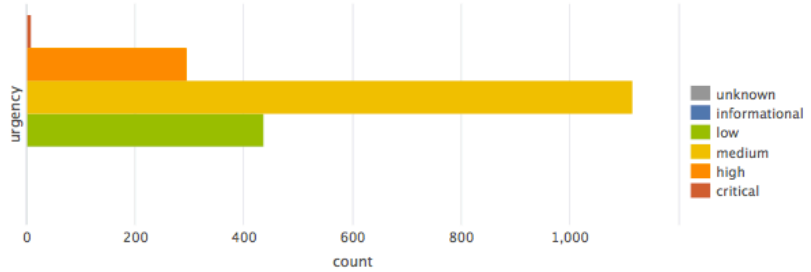
Security Posture

Edit | More Info

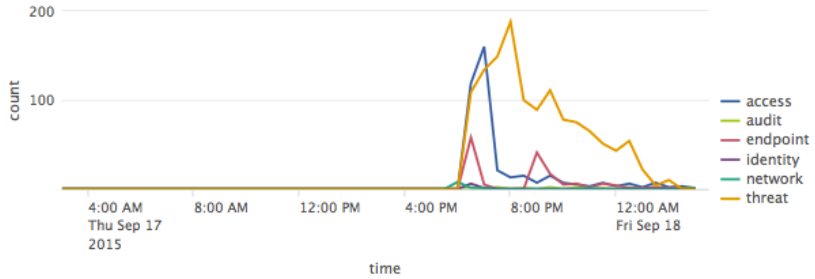
Edit

ACCESS NOTABLES	ENDPOINT NOTABLES	NETWORK NOTABLES	IDENTITY NOTABLES	AUDIT NOTABLES	THREAT NOTABLES
Total Count	Total Count	Total Count	Total Count	Total Count	Total Count
396 +396	150 +150	12 +12	7 +7	15 +15	1k +1k

Notable Events By Urgency



Notable Events Over Time



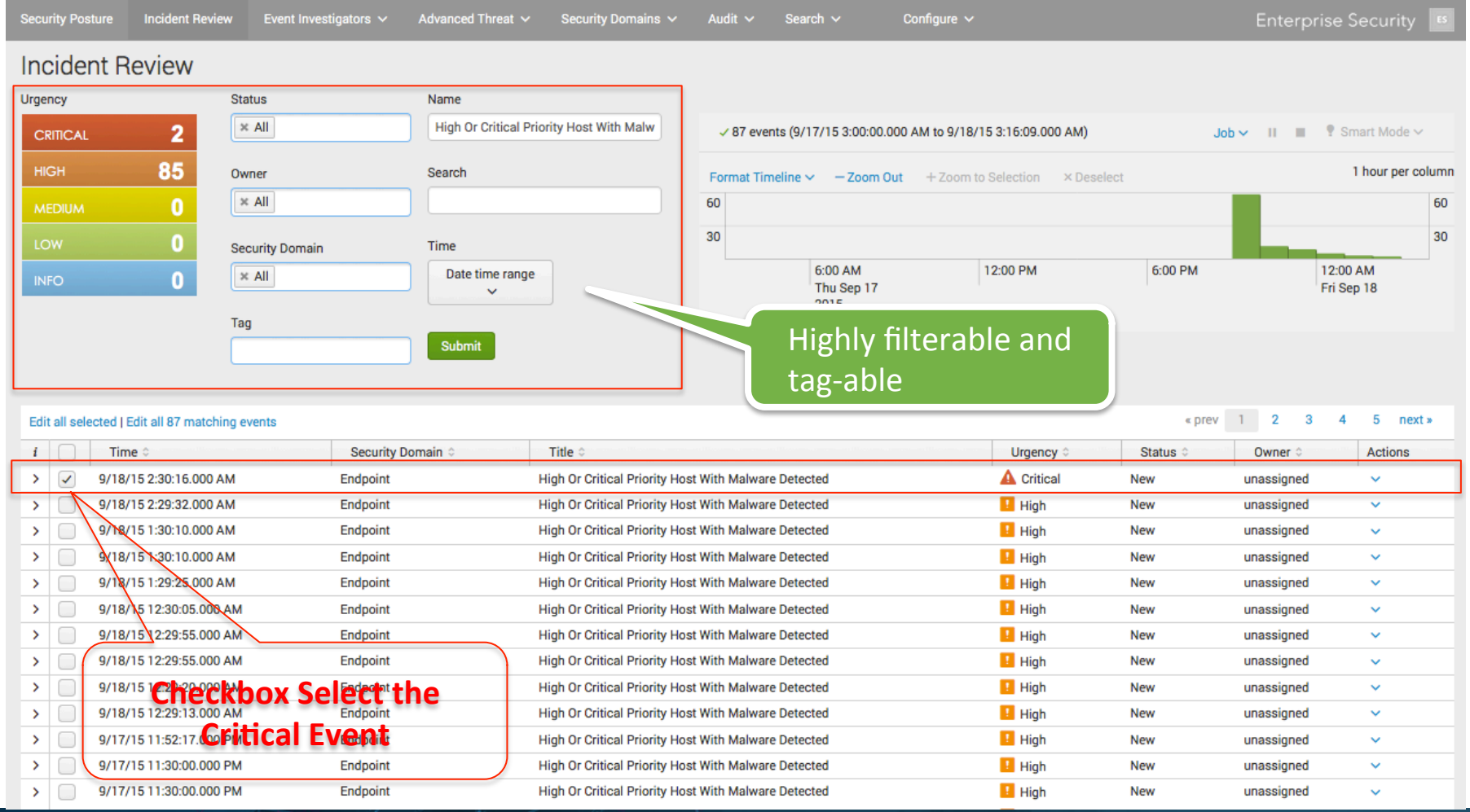
Top Notable Events

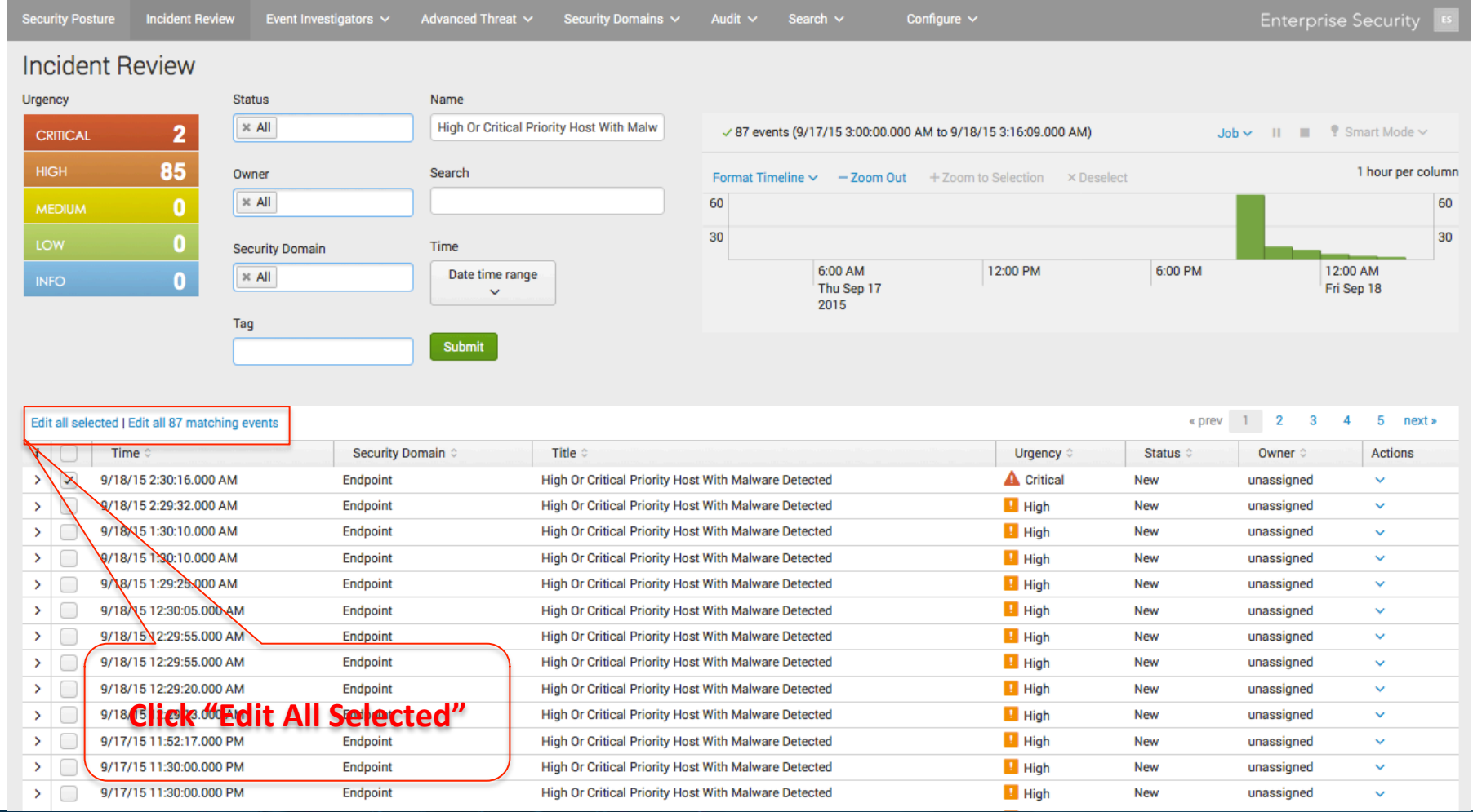
rule_name	sparkline	count
Watchlisted Event Observed		985
Threat Activity Detected		297
Geographically Improbable Access Detected		118
Default Account Activity Detected		101
Excessive Failed Logins		97
High Or Critical Priority Host With Malware Detected		87
Host With Multiple Infections		62

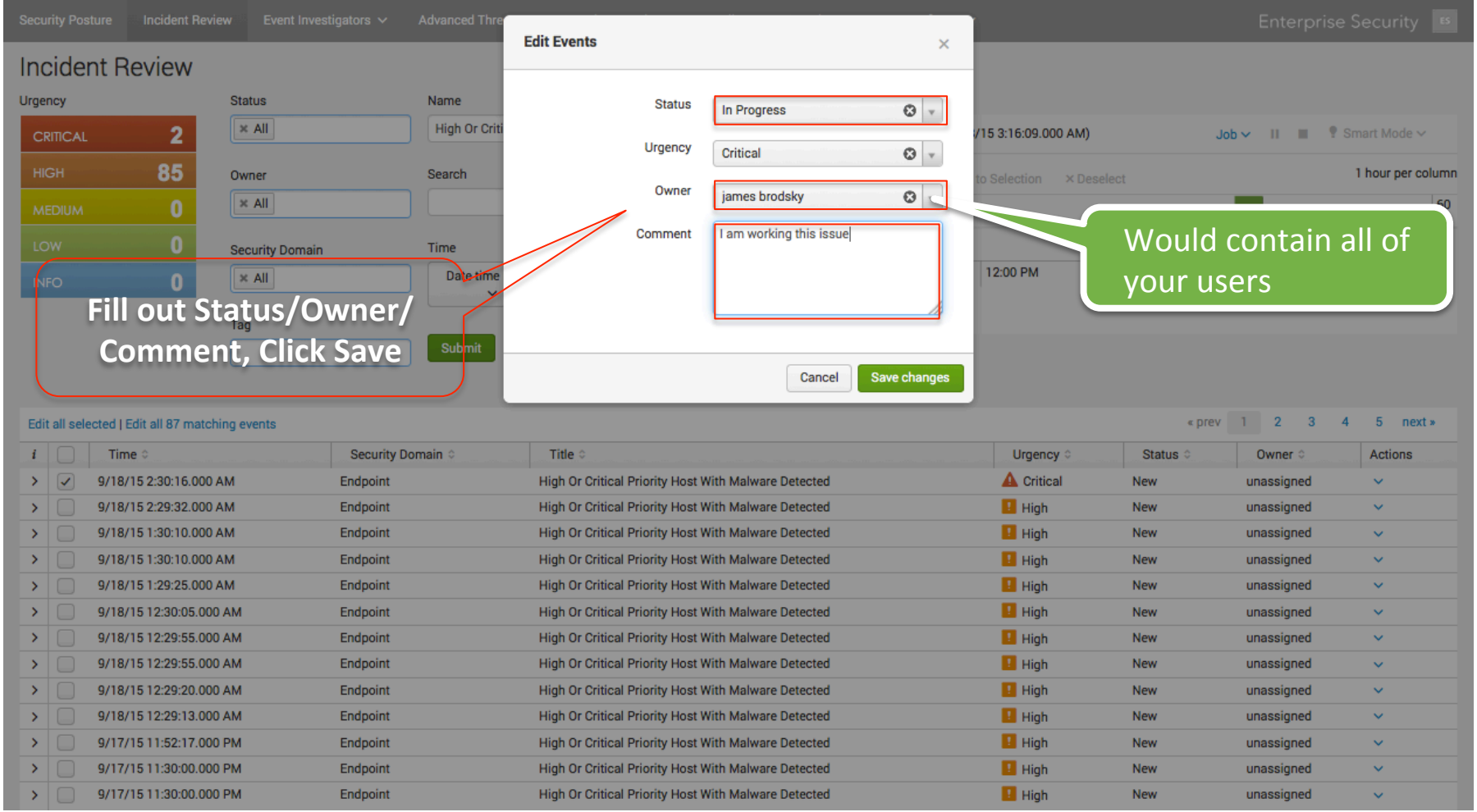
Top Notable Event Sources

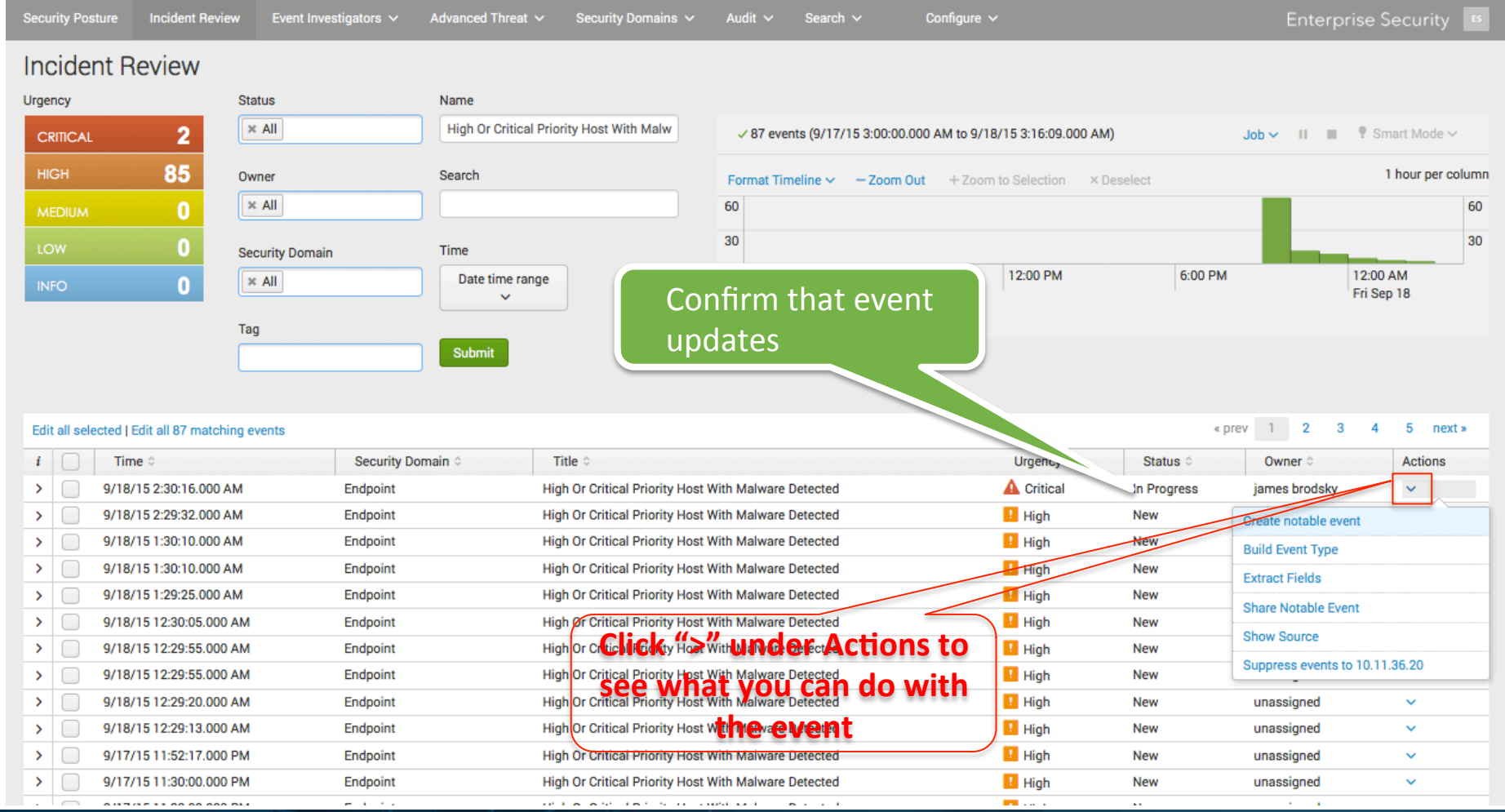
src	sparkline	correlation_search_count	security_domain_count	count
10.64.144.88		1	1	14
10.11.36.40		4	2	10
10.11.36.41		3	1	10
10.11.36.45		3	1	10
10.11.36.3		3	1	9
10.11.36.34		3	1	9
10.11.36.6		3	1	9

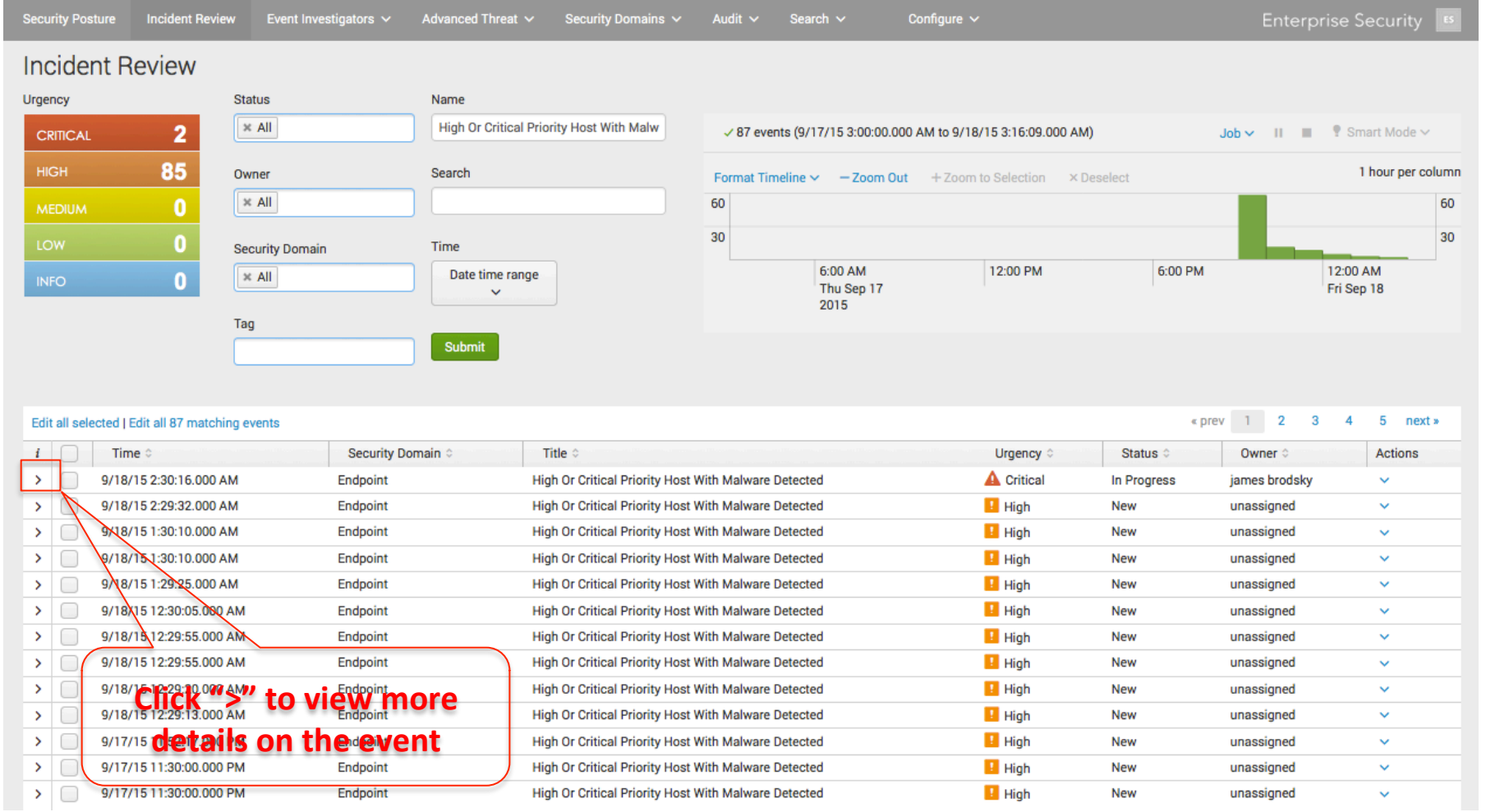
Click “High or Critical Priority Host with Malware Detected”

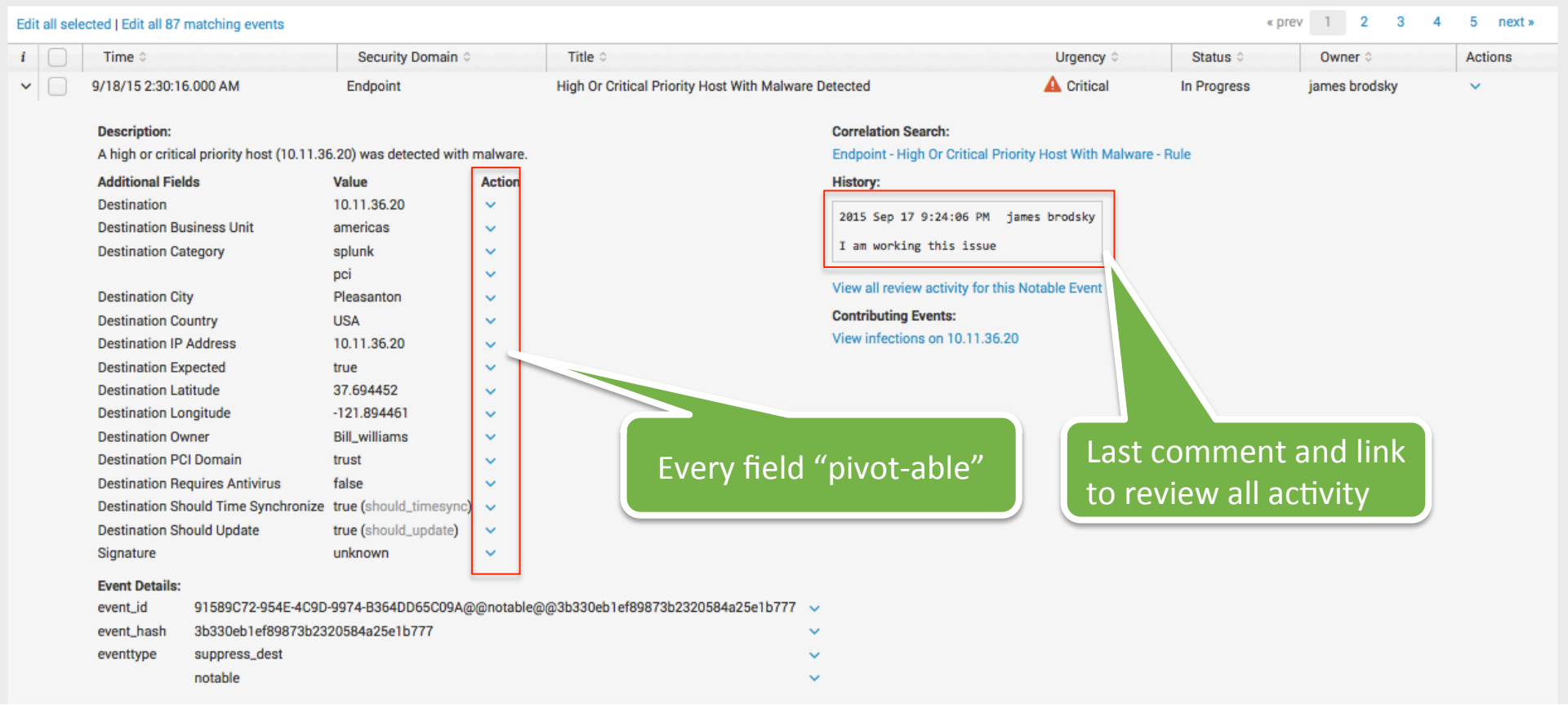

Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Incident Review
Urgency
CRITICAL 2
HIGH 85
MEDIUM 0
LOW 0
INFO 0
Status
All
Name
High Or Critical Priority Host With Malw
Owner
All
Search
Security Domain
All
Time
Date time range
Tag
Submit
87 events (9/17/15 3:00:00.000 AM to 9/18/15 3:16:09.000 AM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
60
30
6:00 AM Thu Sep 17
12:00 PM
6:00 PM
12:00 AM Fri Sep 18
Highly filterable and tag-able
Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM Endpoint High Or Critical Priority Host With Malware Detected Critical New unassigned
9/18/15 2:29:32.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:29:25.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:30:05.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:30.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:13.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:52:17.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
Checkbox Select the Critical Event

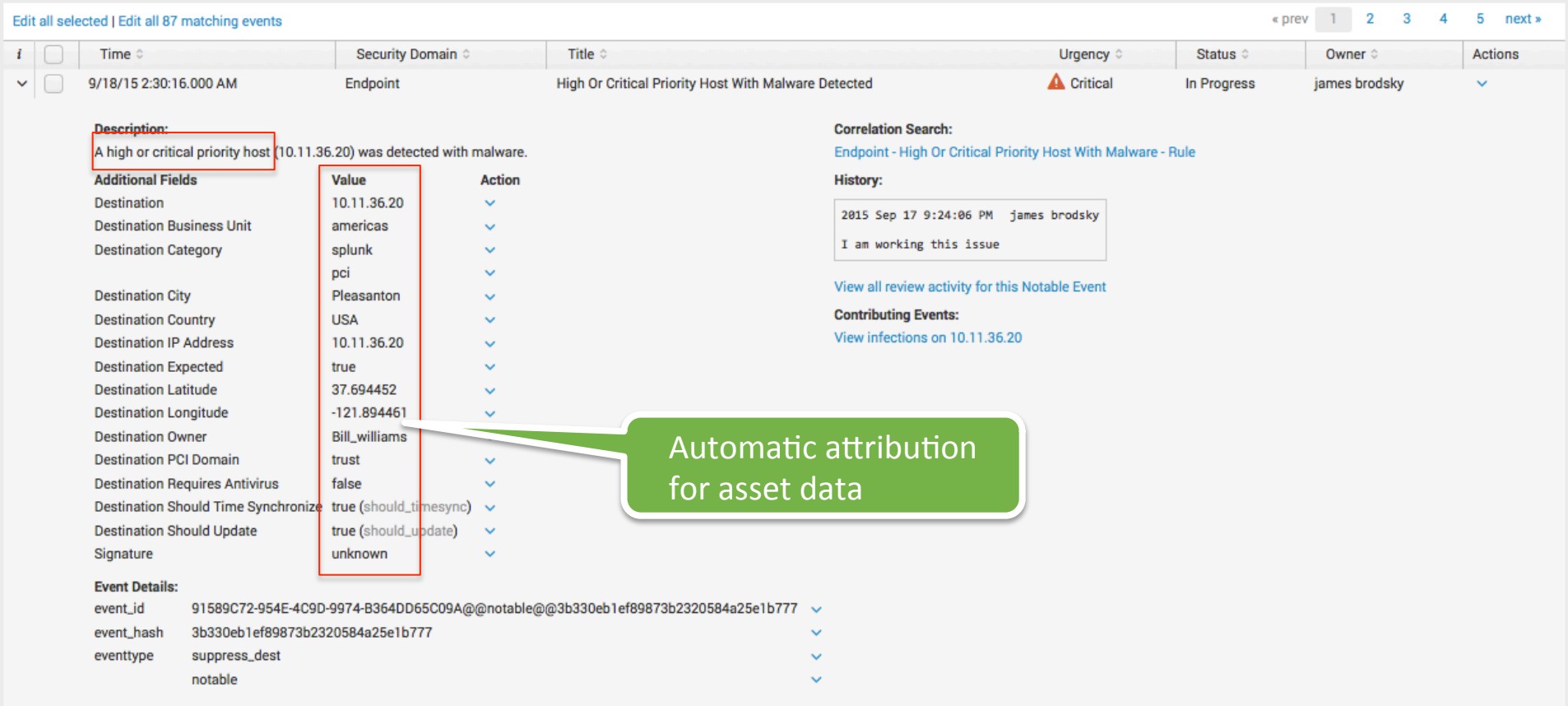

Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Incident Review
Urgency
CRITICAL 2
HIGH 85
MEDIUM 0
LOW 0
INFO 0
Status
All
Name
High Or Critical Priority Host With Malw
Owner
All
Search
Security Domain
All
Time
Date time range
Tag
Submit
87 events (9/17/15 3:00:00.000 AM to 9/18/15 3:16:09.000 AM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
60
30
6:00 AM Thu Sep 17 2015
12:00 PM
6:00 PM
12:00 AM Fri Sep 18
Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM Endpoint High Or Critical Priority Host With Malware Detected Critical New unassigned
9/18/15 2:29:32.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:29:25.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:30:05.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:20.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:03.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:52:17.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
Click “Edit All Selected”

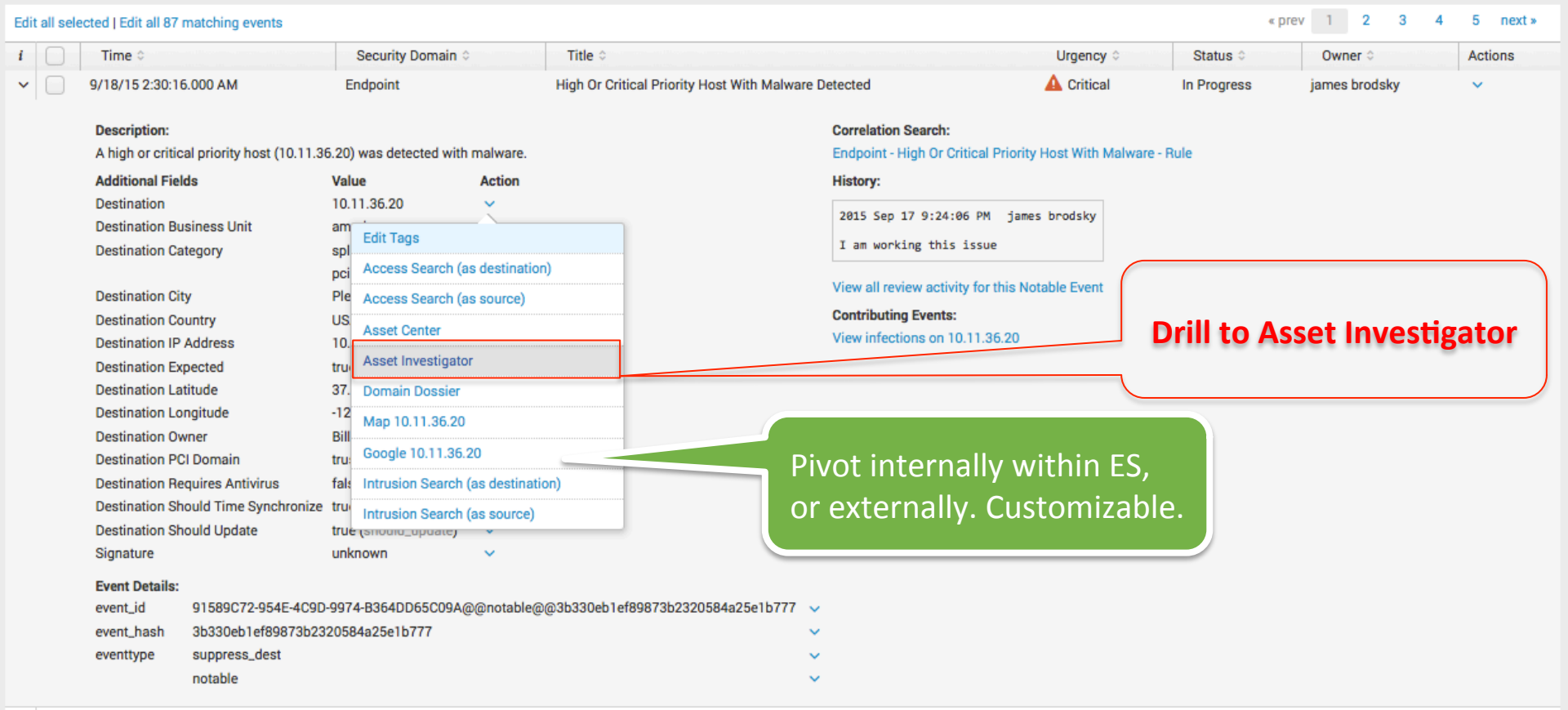

Security Posture
Incident Review
Event Investigators
Advanced Thre
Enterprise Security
Incident Review
Urgency
CRITICAL 2
HIGH 85
MEDIUM 0
LOW 0
INFO 0
Status
All
Owner
All
Security Domain
All
Name
High Or Criti
Search
Time
Date time
Tag
Submit
Edit Events
Status
In Progress
Urgency
Critical
Owner
james brodsky
Comment
I am working this issue
Cancel
Save changes
Fill out Status/Owner/ Comment, Click Save
Would contain all of your users
Job
Smart Mode
1 hour per column
12:00 PM
Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM Endpoint High Or Critical Priority Host With Malware Detected Critical New unassigned
9/18/15 2:29:32.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:29:25.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:30:05.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:20.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:13.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:52:17.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Incident Review
Urgency
CRITICAL 2
HIGH 85
MEDIUM 0
LOW 0
INFO 0
Status
All
Name
High Or Critical Priority Host With Malw
Owner
All
Search
Security Domain
All
Time
Date time range
Tag
Submit
87 events (9/17/15 3:00:00.000 AM to 9/18/15 3:16:09.000 AM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
60
30
12:00 PM
6:00 PM
12:00 AM
Fri Sep 18
Confirm that event updates
Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM Endpoint High Or Critical Priority Host With Malware Detected Critical In Progress james brodsky
9/18/15 2:29:32.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New
9/18/15 1:29:25.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New
9/18/15 12:30:05.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New
9/18/15 12:29:20.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:13.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:52:17.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
Create notable event
Build Event Type
Extract Fields
Share Notable Event
Show Source
Suppress events to 10.11.36.20
Click “>” under Actions to see what you can do with the event


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Incident Review
Urgency
CRITICAL 2
HIGH 85
MEDIUM 0
LOW 0
INFO 0
Status
All
Name
High Or Critical Priority Host With Malw
Owner
All
Search
Security Domain
All
Time
Date time range
Tag
Submit
87 events (9/17/15 3:00:00.000 AM to 9/18/15 3:16:09.000 AM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
60
30
6:00 AM Thu Sep 17 2015
12:00 PM
6:00 PM
12:00 AM Fri Sep 18
Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM Endpoint High Or Critical Priority Host With Malware Detected Critical In Progress james brodsky
9/18/15 2:29:32.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:29:25.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:30:05.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:55.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:29:13.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/17/15 11:30:00.000 PM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
Click “>” to view more details on the event


Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM
Endpoint
High Or Critical Priority Host With Malware Detected
Critical
In Progress
james brodsky
Description:
A high or critical priority host (10.11.36.20) was detected with malware.
Additional Fields
Value
Action
Destination
10.11.36.20
Destination Business Unit
americas
Destination Category
splunk
pci
Destination City
Pleasanton
Destination Country
USA
Destination IP Address
10.11.36.20
Destination Expected
true
Destination Latitude
37.694452
Destination Longitude
-121.894461
Destination Owner
Bill_williams
Destination PCI Domain
trust
Destination Requires Antivirus
false
Destination Should Time Synchronize
true (should_timesync)
Destination Should Update
true (should_update)
Signature
unknown
Event Details:
event_id
91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777
event_hash
3b330eb1ef89873b2320584a25e1b777
eventtype
suppress_dest
notable
Correlation Search:
Endpoint - High Or Critical Priority Host With Malware - Rule
History:
2015 Sep 17 9:24:06 PM james brodsky
I am working this issue
View all review activity for this Notable Event
Contributing Events:
View infections on 10.11.36.20
Every field “pivot-able”
Last comment and link to review all activity


Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM
Endpoint
High Or Critical Priority Host With Malware Detected
Critical
In Progress
james brodsky
Description:
A high or critical priority host (10.11.36.20) was detected with malware.
Additional Fields
Value
Action
Destination 10.11.36.20
Destination Business Unit americas
Destination Category splunk
pci
Destination City Pleasanton
Destination Country USA
Destination IP Address 10.11.36.20
Destination Expected true
Destination Latitude 37.694452
Destination Longitude -121.894461
Destination Owner Bill_williams
Destination PCI Domain trust
Destination Requires Antivirus false
Destination Should Time Synchronize true (should_timesync)
Destination Should Update true (should_update)
Signature unknown
Event Details:
event_id 91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777
event_hash 3b330eb1ef89873b2320584a25e1b777
eventtype suppress_dest
notable
Correlation Search:
Endpoint - High Or Critical Priority Host With Malware - Rule
History:
2015 Sep 17 9:24:06 PM james brodsky
I am working this issue
View all review activity for this Notable Event
Contributing Events:
View infections on 10.11.36.20
Automatic attribution for asset data

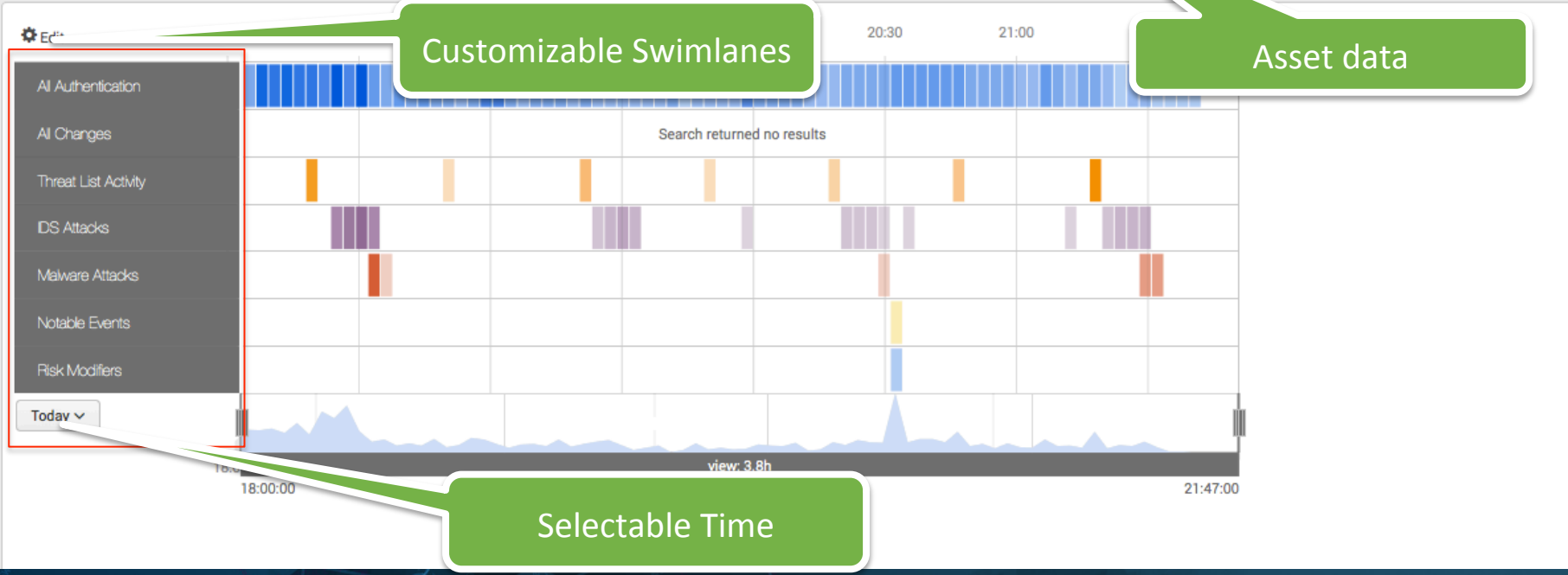

Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM
Endpoint
High Or Critical Priority Host With Malware Detected
Critical
In Progress
james brodsky
Description:
A high or critical priority host (10.11.36.20) was detected with malware.
Additional Fields
Value
Action
Destination
10.11.36.20
Destination Business Unit
Destination Category
Destination City
Destination Country
Destination IP Address
Destination Expected
Destination Latitude
Destination Longitude
Destination Owner
Destination PCI Domain
Destination Requires Antivirus
Destination Should Time Synchronize
Destination Should Update
Signature
unknown
Edit Tags
Access Search (as destination)
Access Search (as source)
Asset Center
Asset Investigator
Domain Dossier
Map 10.11.36.20
Google 10.11.36.20
Intrusion Search (as destination)
Intrusion Search (as source)
Correlation Search:
Endpoint - High Or Critical Priority Host With Malware - Rule
History:
2015 Sep 17 9:24:06 PM james brodsky
I am working this issue
View all review activity for this Notable Event
Contributing Events:
View infections on 10.11.36.20
Event Details:
event_id
91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777
event_hash
3b330eb1ef89873b2320584a25e1b777
eventtype
suppress_dest
notable
Drill to Asset Investigator
Pivot internally within ES, or externally. Customizable.

Asset Investigator

10.11.36.20 search

10.11.36.20

bunit: **americas**
owner: **Bill_williams**
priority: **critical**
is_expected: **true**
long: **-121.894461**
requires_av: **false**
city: **Pleasanton**
lat: **37.694452**
should_timesync: **true**
ip: **10.11.36.20**
category: **splunk, pci**
pci_domain: **trust**
country: **USA**
should_update: **true**



Asset Investigator

10.11.36.20 search

10.11.36.20

bunit: **americas**
owner: **Bill_williams**
priority: **critical**
is_expected: **true**
long: **-121.894461**
requires_av: **false**
city: **Pleasanton**
lat: **37.694452**
should_timesync: **true**
ip: **10.11.36.20**
category: **splunk, pci**
pci_domain: **trust**
country: **USA**
should_update: **true**

Security Posture | Incident Review | Event Investigators | Advanced Threat | Security Domains | Audit | Search | Configure | Enterprise Security

Asset Investigator

10.11.36.20 search

10.11.36.20

bunit: **americas**
owner: **Bill_williams**
priority: **critical**
is_expected: **true**

long: **-121.894461**
requires_av: **false**
city: **Pleasanton**
lat: **37.694452**

should_timesync: **tr**
ip: **10.11.36.20**
category: **splunk, pc**

Drill to search, make a notable event, share a link

Edit

18:00 18:30 19:00 19:30 20:00 20:30 21:00 21:30

All Authentication
All Changes
Threat List Activity
IDS Attacks
Malware Attacks
Notable Events
Risk Modifiers

Search returned no results

Today

18:0 view: 3.8h

18:00:00 21:47:00

(101)

Thu Sep 17
20:31:00 GMT-0600

action
Malware Cloud Lookup
failure

app
login
sshd
+1 more

dest
10.11.36.20
10.11.36.8
+2 more

risk_object
10.11.36.20

risk_score
80

rule_name
High Or Critical Priority Host With Malware Detected

severity
medium

signature
unknown

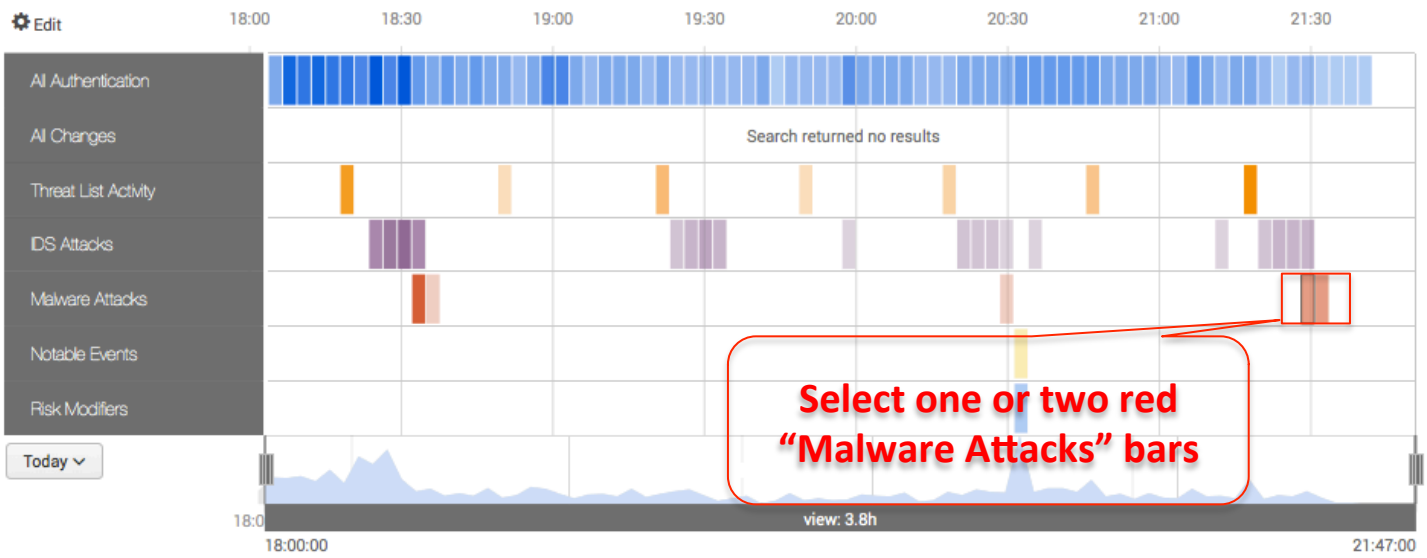
Summarized info from “candlesticks” selected

Asset Investigator

10.11.36.20 search

10.11.36.20

bunit: **americas**
owner: **Bill_williams**
priority: **critical**
is_expected: **true**
long: **-121.894461**
requires_av: **false**
city: **Pleasanton**
lat: **37.694452**
should_timesync: **true**
ip: **10.11.36.20**
category: **splunk, pci**
pci_domain: **trust**
country: **USA**
should_update: **true**



Malware Attacks (3)

Thu Sep 17 21:26:06 - Thu Sep 17 21:28:44 GMT-0600

action
allowed
deferred

dest
10.11.36.20

signature
Adware.Hotbar

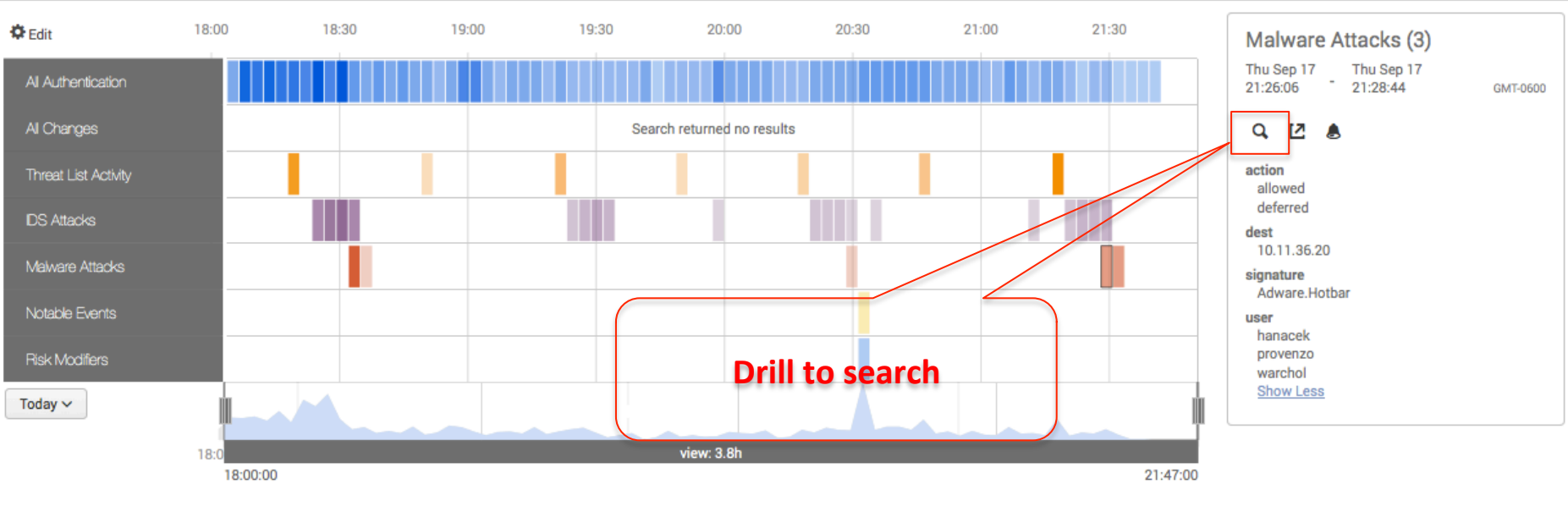
user
hanacek
provenzo
warchol
Show Less

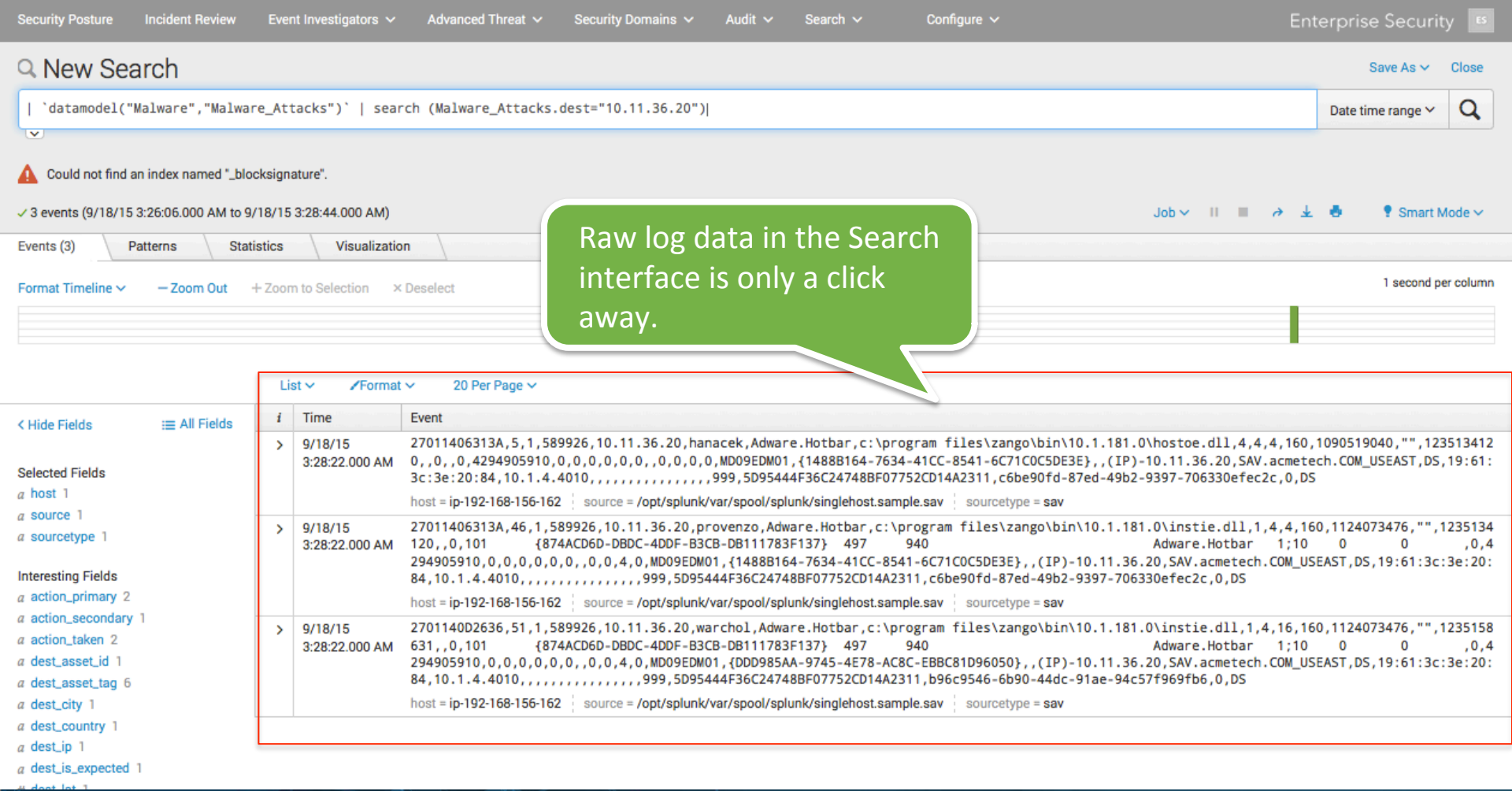
Asset Investigator

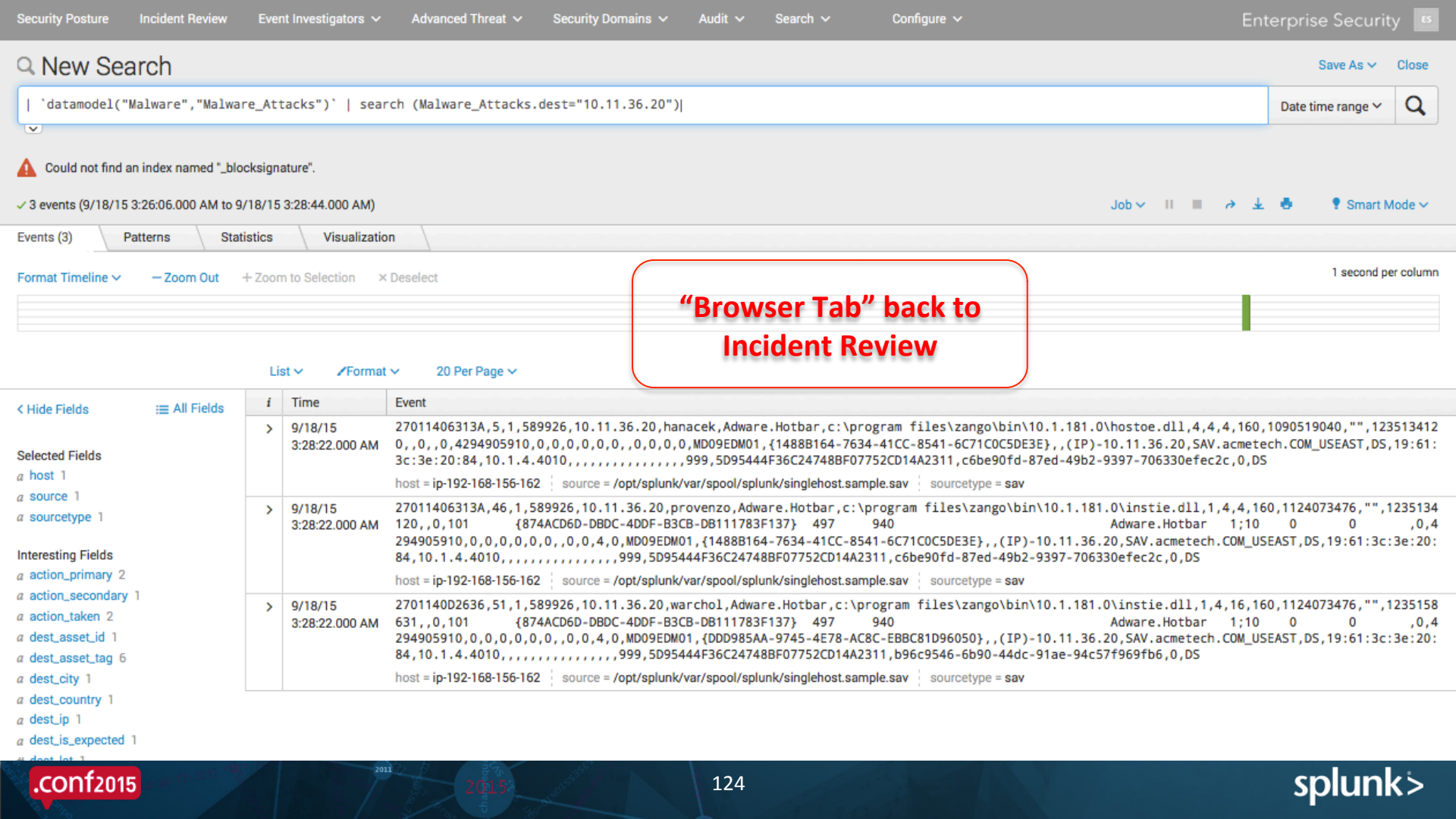
10.11.36.20 search

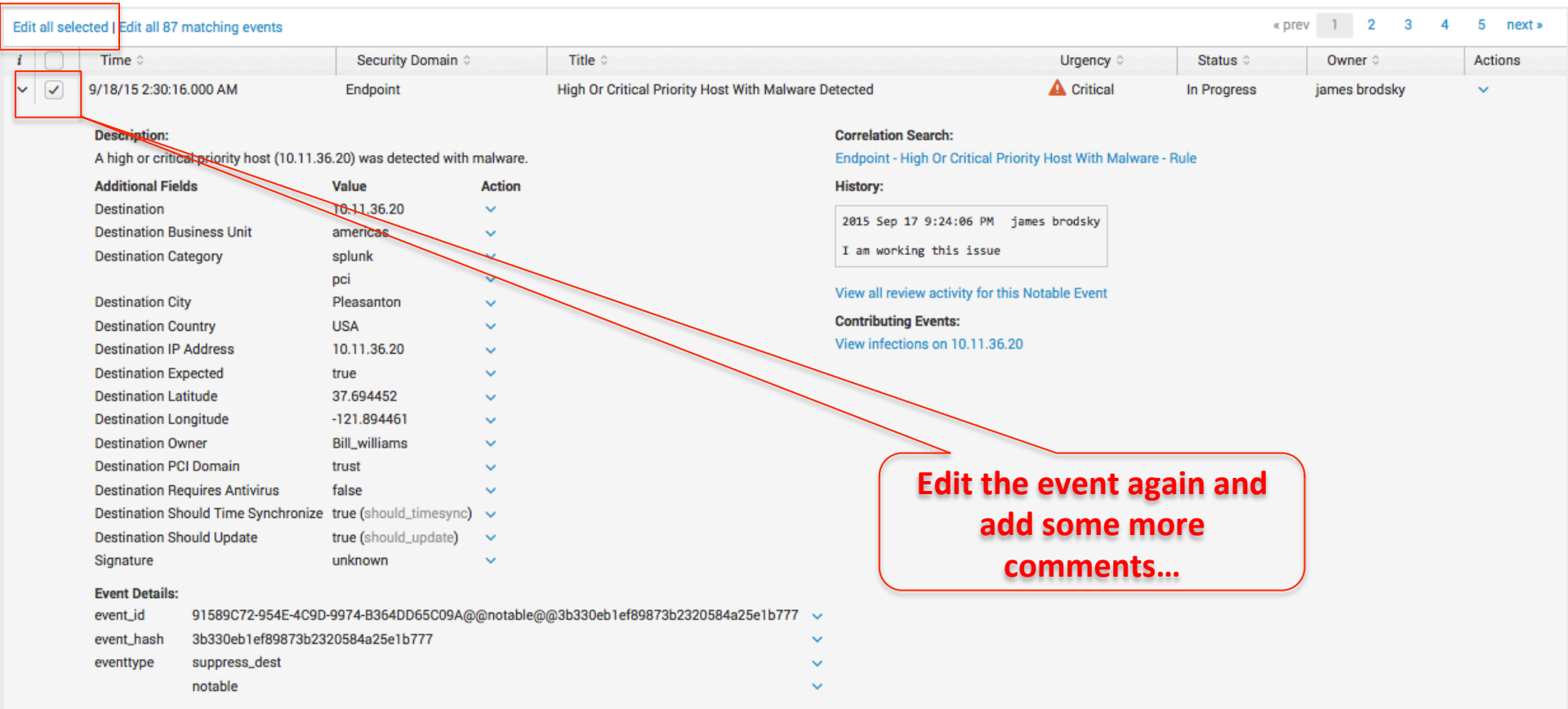
10.11.36.20

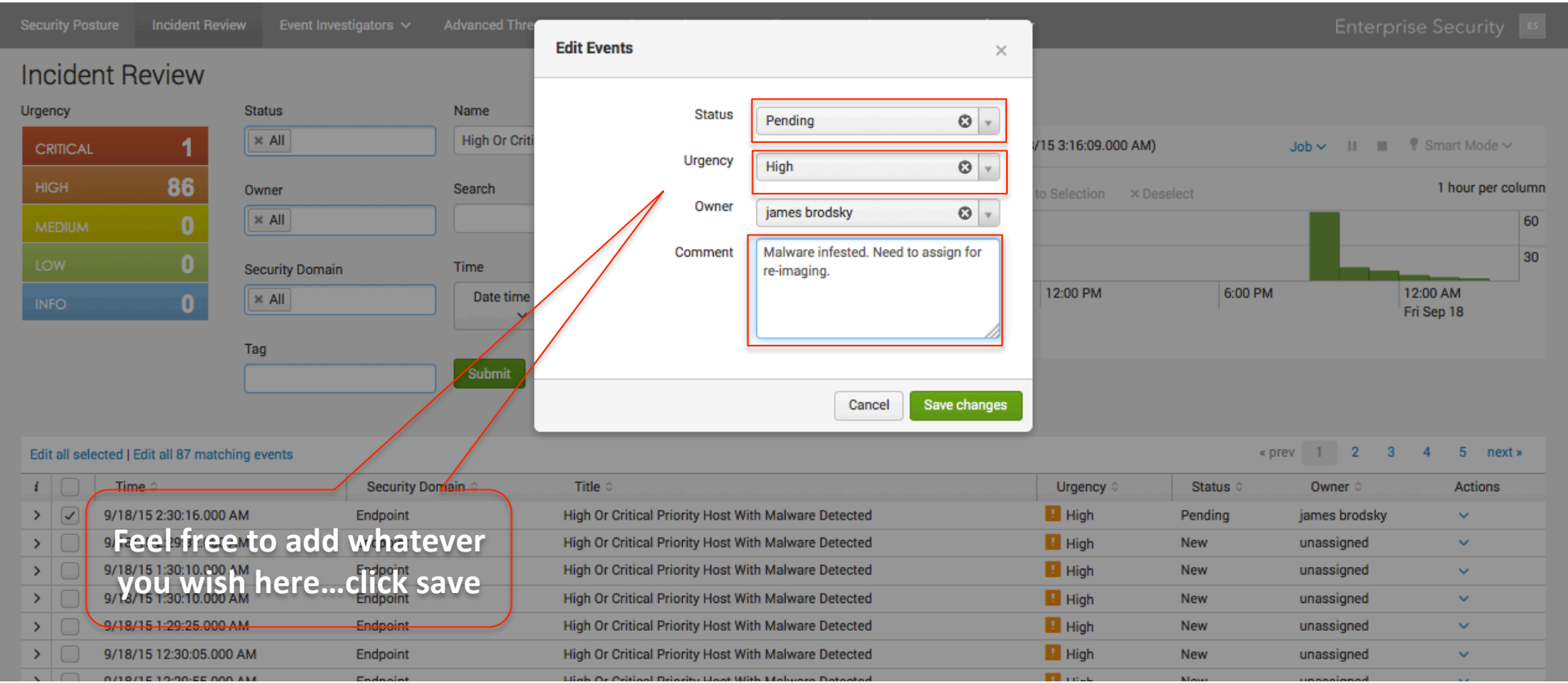
bunit: **americas**
owner: **Bill_williams**
priority: **critical**
is_expected: **true**
long: **-121.894461**
requires_av: **false**
city: **Pleasanton**
lat: **37.694452**
should_timesync: **true**
ip: **10.11.36.20**
category: **splunk, pci**
pci_domain: **trust**
country: **USA**
should_update: **true**




Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
New Search
Save As
Close
| `datamodel("Malware","Malware_Attacks")` | search (Malware_Attacks.dest="10.11.36.20")
Date time range
Could not find an index named "_blocksignature".
3 events (9/18/15 3:26:06.000 AM to 9/18/15 3:28:44.000 AM)
Job
Smart Mode
Events (3)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 second per column
Raw log data in the Search interface is only a click away.
List
Format
20 Per Page
Hide Fields
All Fields
Selected Fields
host 1
source 1
sourcetype 1
Interesting Fields
action_primary 2
action_secondary 1
action_taken 2
dest_asset_id 1
dest_asset_tag 6
dest_city 1
dest_country 1
dest_ip 1
dest_is_expected 1
i
Time
Event
9/18/15 3:28:22.000 AM
27011406313A,5,1,589926,10.11.36.20,hanacek,Adware.Hotbar,c:\program files\zango\bin\10.1.181.0\hostoe.dll,4,4,4,160,1090519040,"",123513412
0,,0,,0,4294905910,0,0,0,0,0,0,,0,0,0,0,MD09EDM01,{1488B164-7634-41CC-8541-6C71C0C5DE3E},,(IP)-10.11.36.20,SAV.acmetech.COM_USEAST,DS,19:61:
3c:3e:20:84,10.1.4.4010,,,,,,,,,,,,,,,999,5D95444F36C24748BF07752CD14A2311,c6be90fd-87ed-49b2-9397-706330efec2c,0,DS
host = ip-192-168-156-162
source = /opt/splunk/var/spool/splunk/singlehost.sample.sav
sourcetype = sav
9/18/15 3:28:22.000 AM
27011406313A,46,1,589926,10.11.36.20,provenzo,Adware.Hotbar,c:\program files\zango\bin\10.1.181.0\instie.dll,1,4,4,160,1124073476,"",1235134
120,,0,101 {874ACD6D-DBDC-4DDF-B3CB-DB111783F137} 497 940 Adware.Hotbar 1;10 0 0 ,0,4
294905910,0,0,0,0,0,0,,0,0,4,0,MD09EDM01,{1488B164-7634-41CC-8541-6C71C0C5DE3E},,(IP)-10.11.36.20,SAV.acmetech.COM_USEAST,DS,19:61:3c:3e:20:
84,10.1.4.4010,,,,,,,,,,,,,,,999,5D95444F36C24748BF07752CD14A2311,c6be90fd-87ed-49b2-9397-706330efec2c,0,DS
host = ip-192-168-156-162
source = /opt/splunk/var/spool/splunk/singlehost.sample.sav
sourcetype = sav
9/18/15 3:28:22.000 AM
2701140D2636,51,1,589926,10.11.36.20,warchol,Adware.Hotbar,c:\program files\zango\bin\10.1.181.0\instie.dll,1,4,16,160,1124073476,"",1235158
631,,0,101 {874ACD6D-DBDC-4DDF-B3CB-DB111783F137} 497 940 Adware.Hotbar 1;10 0 0 ,0,4
294905910,0,0,0,0,0,0,,0,0,4,0,MD09EDM01,{DDD985AA-9745-4E78-AC8C-EBBC81D96050},,(IP)-10.11.36.20,SAV.acmetech.COM_USEAST,DS,19:61:3c:3e:20:
84,10.1.4.4010,,,,,,,,,,,,,,,999,5D95444F36C24748BF07752CD14A2311,b96c9546-6b90-44dc-91ae-94c57f969fb6,0,DS
host = ip-192-168-156-162
source = /opt/splunk/var/spool/splunk/singlehost.sample.sav
sourcetype = sav


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
New Search
Save As
Close
| `datamodel("Malware","Malware_Attacks")` | search (Malware_Attacks.dest="10.11.36.20")|
Date time range
Could not find an index named "_blocksignature".
✓ 3 events (9/18/15 3:26:06.000 AM to 9/18/15 3:28:44.000 AM)
Job
Smart Mode
Events (3)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 second per column
"Browser Tab" back to Incident Review
List
Format
20 Per Page
Hide Fields
All Fields
Selected Fields
host 1
source 1
sourcetype 1
Interesting Fields
action_primary 2
action_secondary 1
action_taken 2
dest_asset_id 1
dest_asset_tag 6
dest_city 1
dest_country 1
dest_ip 1
dest_is_expected 1
i
Time
Event
9/18/15 3:28:22.000 AM
27011406313A,5,1,589926,10.11.36.20,hanacek,Adware.Hotbar,c:\program files\zango\bin\10.1.181.0\hostoe.dll,4,4,4,160,1090519040,"",123513412 0,,0,,0,4294905910,0,0,0,0,0,0,,0,0,0,0,MD09EDM01,{1488B164-7634-41CC-8541-6C71C0C5DE3E},,(IP)-10.11.36.20,SAV.acmetech.COM_USEAST,DS,19:61: 3c:3e:20:84,10.1.4.4010,,,,,,,,,,,,,,,999,5D95444F36C24748BF07752CD14A2311,c6be90fd-87ed-49b2-9397-706330efec2c,0,DS
host = ip-192-168-156-162 source = /opt/splunk/var/spool/splunk/singlehost.sample.sav sourcetype = sav
9/18/15 3:28:22.000 AM
27011406313A,46,1,589926,10.11.36.20,provenzo,Adware.Hotbar,c:\program files\zango\bin\10.1.181.0\instie.dll,1,4,4,160,1124073476,"",1235134 120,,0,101 {874ACD6D-DBDC-4DDF-B3CB-DB111783F137} 497 940 Adware.Hotbar 1;10 0 0 ,0,4 294905910,0,0,0,0,0,0,,0,0,4,0,MD09EDM01,{1488B164-7634-41CC-8541-6C71C0C5DE3E},,(IP)-10.11.36.20,SAV.acmetech.COM_USEAST,DS,19:61:3c:3e:20: 84,10.1.4.4010,,,,,,,,,,,,,,,999,5D95444F36C24748BF07752CD14A2311,c6be90fd-87ed-49b2-9397-706330efec2c,0,DS
host = ip-192-168-156-162 source = /opt/splunk/var/spool/splunk/singlehost.sample.sav sourcetype = sav
9/18/15 3:28:22.000 AM
2701140D2636,51,1,589926,10.11.36.20,warchol,Adware.Hotbar,c:\program files\zango\bin\10.1.181.0\instie.dll,1,4,16,160,1124073476,"",1235158 631,,0,101 {874ACD6D-DBDC-4DDF-B3CB-DB111783F137} 497 940 Adware.Hotbar 1;10 0 0 ,0,4 294905910,0,0,0,0,0,0,,0,0,4,0,MD09EDM01,{DDD985AA-9745-4E78-AC8C-EBBC81D96050},,(IP)-10.11.36.20,SAV.acmetech.COM_USEAST,DS,19:61:3c:3e:20: 84,10.1.4.4010,,,,,,,,,,,,,,,999,5D95444F36C24748BF07752CD14A2311,b96c9546-6b90-44dc-91ae-94c57f969fb6,0,DS
host = ip-192-168-156-162 source = /opt/splunk/var/spool/splunk/singlehost.sample.sav sourcetype = sav


Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM
Endpoint
High Or Critical Priority Host With Malware Detected
Critical
In Progress
james brodsky
Description:
A high or critical priority host (10.11.36.20) was detected with malware.
Additional Fields
Value
Action
Destination
10.11.36.20
Destination Business Unit
americas
Destination Category
splunk
pci
Destination City
Pleasanton
Destination Country
USA
Destination IP Address
10.11.36.20
Destination Expected
true
Destination Latitude
37.694452
Destination Longitude
-121.894461
Destination Owner
Bill_williams
Destination PCI Domain
trust
Destination Requires Antivirus
false
Destination Should Time Synchronize
true (should_timesync)
Destination Should Update
true (should_update)
Signature
unknown
Event Details:
event_id
91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777
event_hash
3b330eb1ef89873b2320584a25e1b777
eventtype
suppress_dest
notable
Correlation Search:
Endpoint - High Or Critical Priority Host With Malware - Rule
History:
2015 Sep 17 9:24:06 PM james brodsky
I am working this issue
View all review activity for this Notable Event
Contributing Events:
View infections on 10.11.36.20
Edit the event again and add some more comments…


Security Posture
Incident Review
Event Investigators
Advanced Thre
Enterprise Security
Incident Review
Urgency
CRITICAL 1
HIGH 86
MEDIUM 0
LOW 0
INFO 0
Status
All
Owner
All
Security Domain
All
Tag
Name
High Or Criti
Search
Time
Date time
Submit
Edit Events
Status
Pending
Urgency
High
Owner
james brodsky
Comment
Malware infested. Need to assign for re-imaging.
Cancel
Save changes
Job
Smart Mode
to Selection
Deselect
1 hour per column
60
30
12:00 PM
6:00 PM
12:00 AM
Fri Sep 18
Edit all selected | Edit all 87 matching events
« prev 1 2 3 4 5 next »
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/18/15 2:30:16.000 AM Endpoint High Or Critical Priority Host With Malware Detected High Pending james brodsky
9/18/15 1:30:10.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 1:29:25.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/18/15 12:30:05.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
Feel free to add whatever you wish here…click save

Edit all selected | Edit all 87 matching events

« prev 1 2 3 4 5 next »

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
✓	9/18/15 2:30:16.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected	High	Pending	james brodsky	

Description:
A high or critical priority host (10.11.36.20) was detected with malware.

Additional Fields	Value	Action
Destination	10.11.36.20	
Destination Business Unit	americas	
Destination Category	splunk	
	pci	
Destination City	Pleasanton	
Destination Country	USA	
Destination IP Address	10.11.36.20	
Destination Expected	true	
Destination Latitude	37.694452	
Destination Longitude	-121.894461	
Destination Owner	Bill_williams	
Destination PCI Domain	trust	
Destination Requires Antivirus	false	
Destination Should Time Synchronize	true (should_timesync)	
Destination Should Update	true (should_update)	
Signature	unknown	

Event Details:

event_id	91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777
event_hash	3b330eb1ef89873b2320584a25e1b777
eventtype	suppress_dest
	notable

Correlation Search:
Endpoint - High Or Critical Priority Host With Malware - Rule

History:

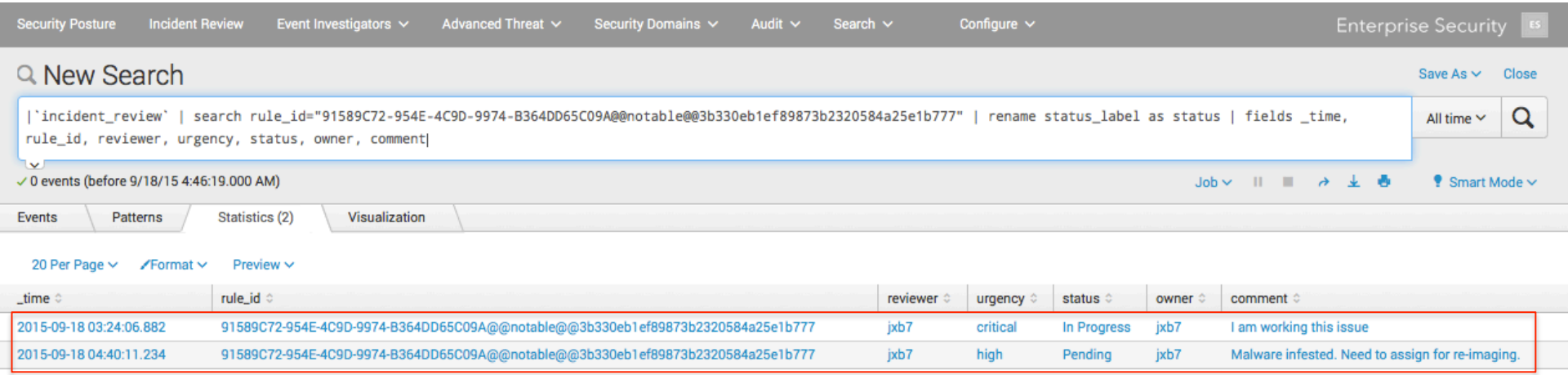
```
2015 Sep 17 10:40:11 PM          james brodsky
Malware infested. Need to assign for re-imaging.
```

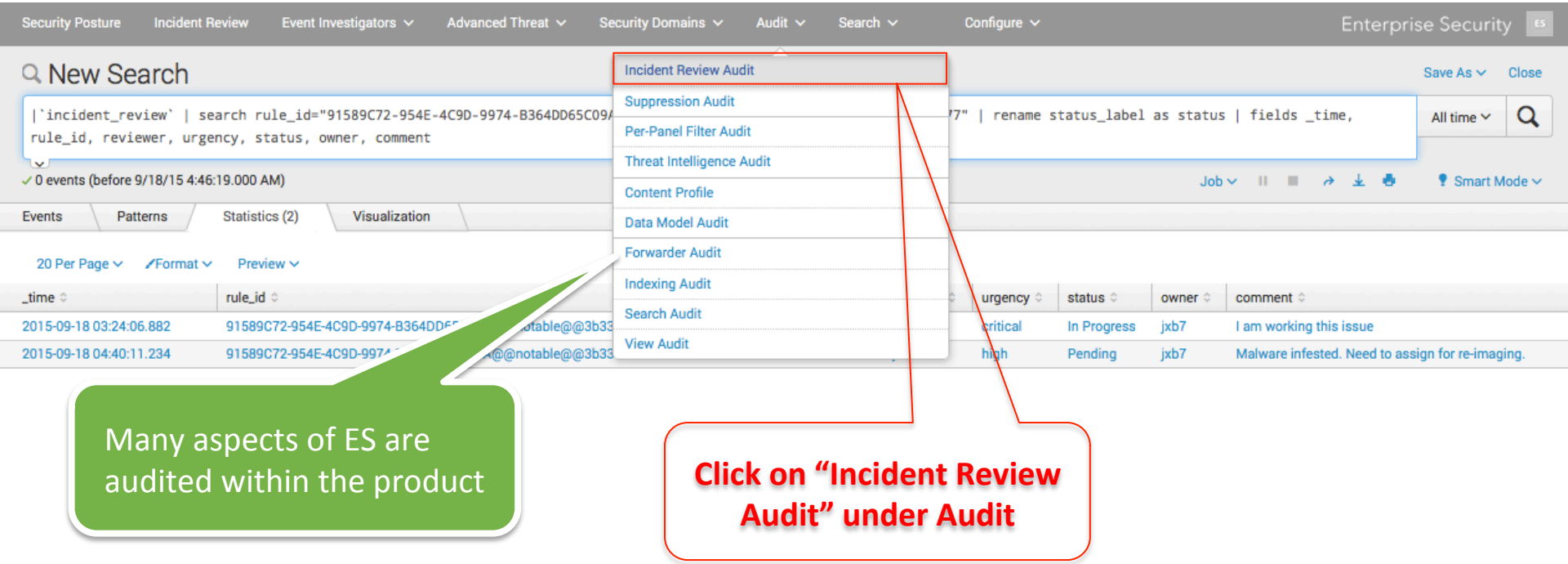
Previous >

View all review activity for this Notable Event

Contributing Events:
View infections on 10.11.36.20

View the review activity for the event

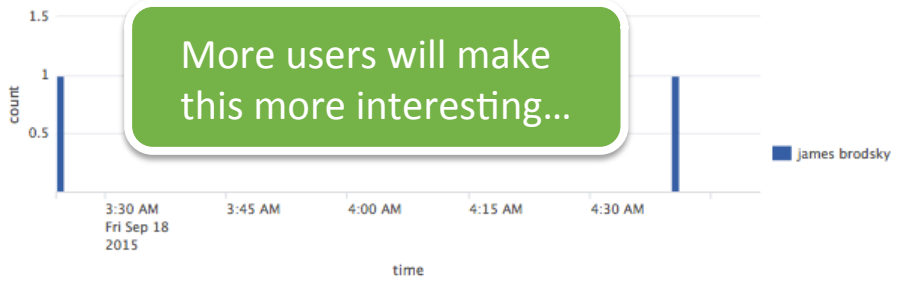

Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
New Search
Save As
Close
|`incident_review` | search rule_id="91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777" | rename status_label as status | fields _time, rule_id, reviewer, urgency, status, owner, comment
All time
0 events (before 9/18/15 4:46:19.000 AM)
Job
Smart Mode
Events
Patterns
Statistics (2)
Visualization
20 Per Page
Format
Preview
_time
rule_id
reviewer
urgency
status
owner
comment
2015-09-18 03:24:06.882
91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777
jxb7
critical
In Progress
jxb7
I am working this issue
2015-09-18 04:40:11.234
91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777
jxb7
high
Pending
jxb7
Malware infested. Need to assign for re-imaging.


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
New Search
Save As
Close
Incident Review Audit
Suppression Audit
Per-Panel Filter Audit
Threat Intelligence Audit
Content Profile
Data Model Audit
Forwarder Audit
Indexing Audit
Search Audit
View Audit
|`incident_review` | search rule_id="91589C72-954E-4C9D-9974-B364DD65C09A
rule_id, reviewer, urgency, status, owner, comment
7" | rename status_label as status | fields _time,
All time
0 events (before 9/18/15 4:46:19.000 AM)
Job
Smart Mode
Events
Patterns
Statistics (2)
Visualization
20 Per Page
Format
Preview
_time
rule_id
urgency
status
owner
comment
2015-09-18 03:24:06.882
91589C72-954E-4C9D-9974-B364DD65
critical
In Progress
jxb7
I am working this issue
2015-09-18 04:40:11.234
91589C72-954E-4C9D-9974
high
Pending
jxb7
Malware infested. Need to assign for re-imaging.
Many aspects of ES are audited within the product
Click on “Incident Review Audit” under Audit

Incident Review Audit

Edit | More Info

Review Activity By Reviewer

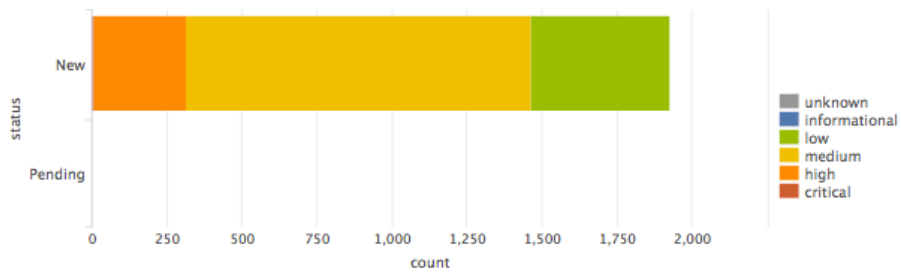


More users will make this more interesting…

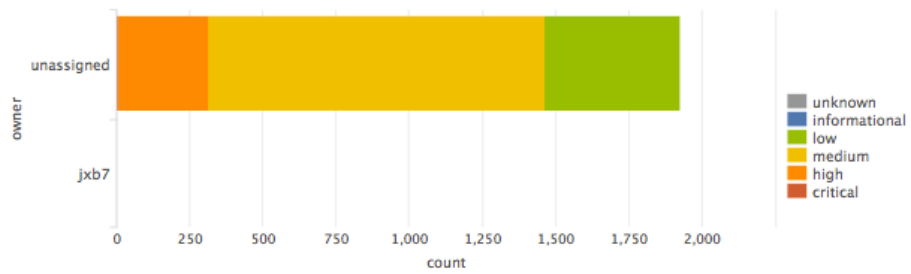
Top Reviewers

reviewer_realname	sparkline	count	firstTime	lastTime
james brodsky		2	09/18/2015 03:24:06	09/18/2015 04:40:11

Notable Events By Status - Last 48 Hours



Notable Events By Owner - Last 48 Hours



Recent Review Activity

_time	rule_id	status	rule_name	owner_realname	comment	reviewer_realname
2015-09-18 04:40:11.234	91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777	Pending	High Or Critical Priority Host With Malware Detected	james brodsky	Malware infested. Need to assign for re-imaging.	james brodsky
2015-09-18 03:24:06.882	91589C72-954E-4C9D-9974-B364DD65C09A@@notable@@3b330eb1ef89873b2320584a25e1b777	In Progress	High Or Critical Priority Host With Malware Detected	james brodsky	I am working this issue	james brodsky

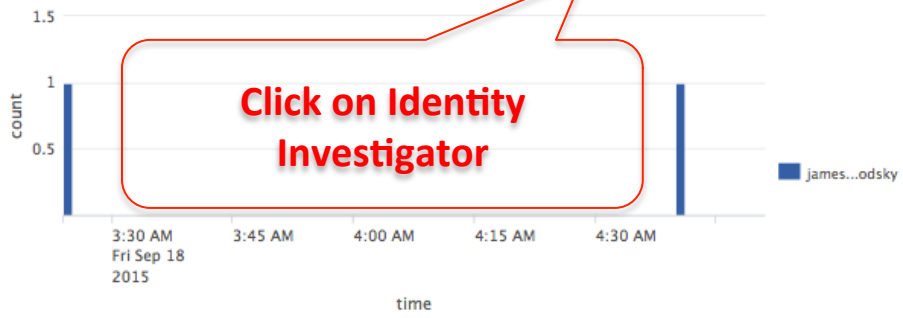
Security Posture | Incident Review | Event Investigators | Advanced Threat | Security Domains | Audit | Search | Configure | Enterprise Security

Asset Investigator
Identity Investigator

Incident Revie

Edit | More Info

Review Activity By Reviewer

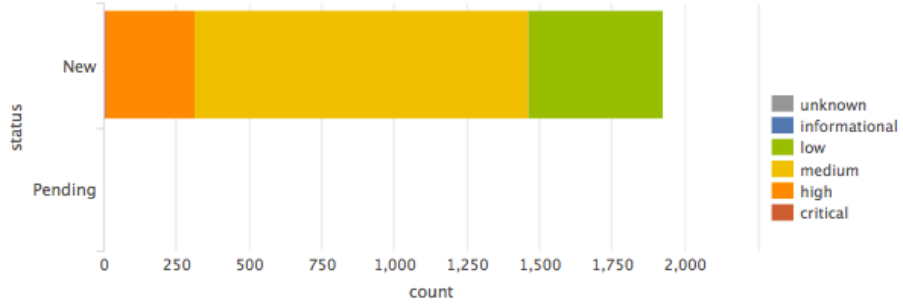


Click on Identity Investigator

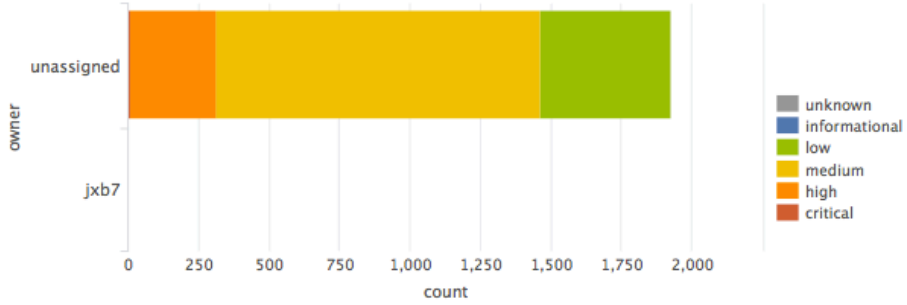
Top Reviewers

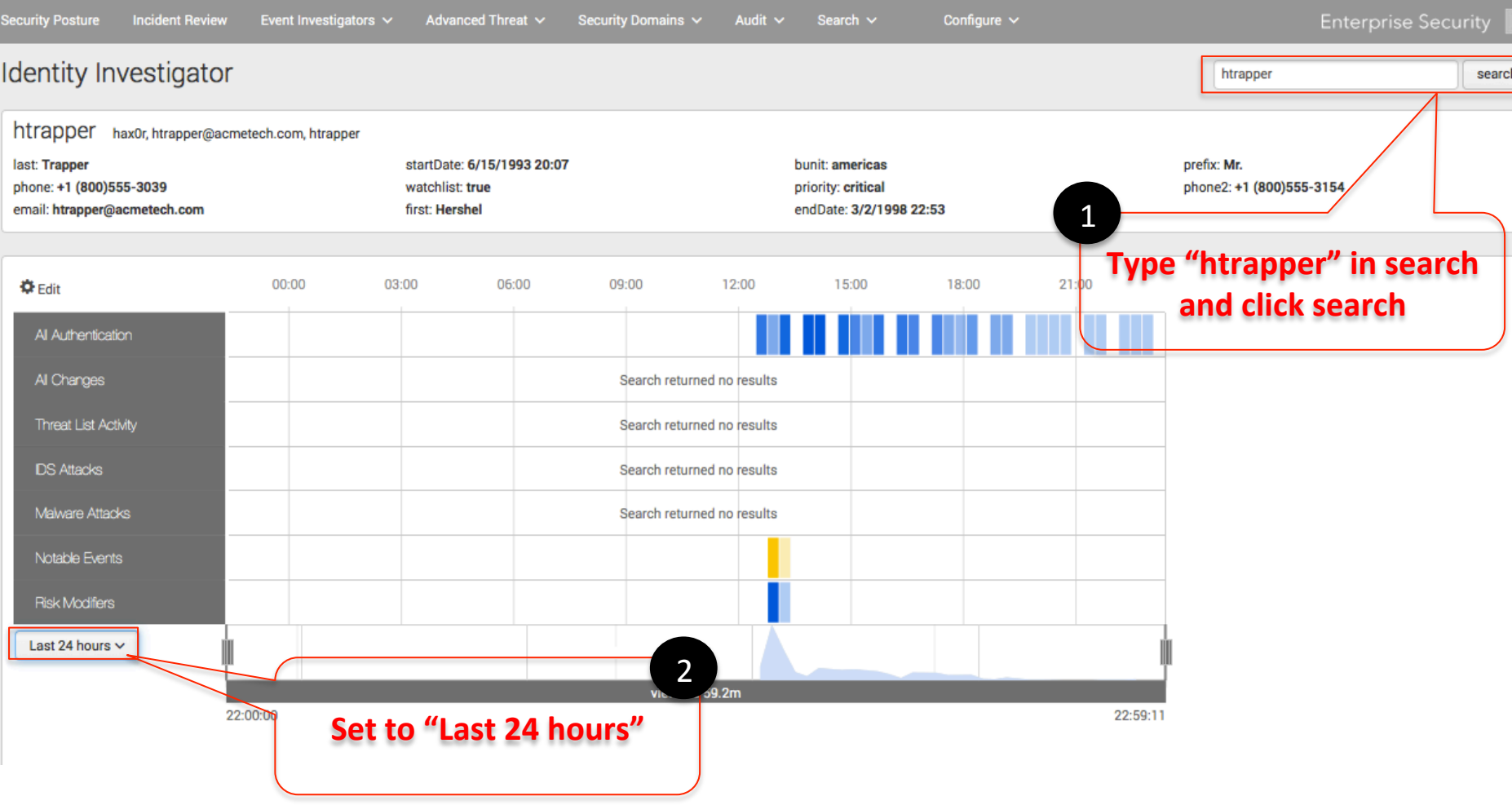
reviewer_realname	sparkline	count	firstTime	lastTime
james brodsky		2	09/18/2015 03:24:06	09/18/2015 04:40:11

Notable Events By Status - Last 48 Hours



Notable Events By Owner - Last 48 Hours




Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Identity Investigator
htrapper
search
htrapper hax0r, htrapper@acmetech.com, htrapper
last: Trapper
phone: +1 (800)555-3039
email: htrapper@acmetech.com
startDate: 6/15/1993 20:07
watchlist: true
first: Hershel
bunit: americas
priority: critical
endDate: 3/2/1998 22:53
prefix: Mr.
phone2: +1 (800)555-3154
1
Type “htrapper” in search and click search
Edit
00:00
03:00
06:00
09:00
12:00
15:00
18:00
21:00
AI Authentication
AI Changes
Search returned no results
Threat List Activity
Search returned no results
IDS Attacks
Search returned no results
Malware Attacks
Search returned no results
Notable Events
Risk Modifiers
Last 24 hours
2
Set to “Last 24 hours”
22:00:00
22:59:11

Identity Investigator

htrapper search

htrapper hax0r, htrapper@acmetech.com, htrapper

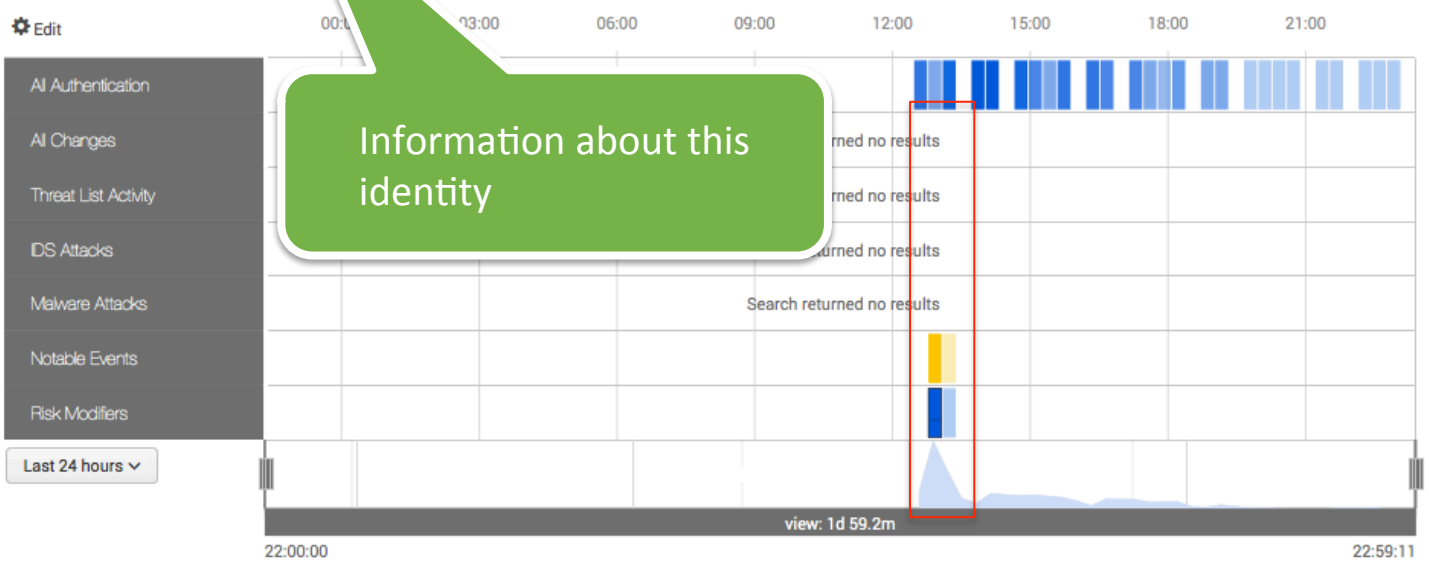
last: **Trapper**
phone: **+1 (800)555-3039**
email: **htrapper@acmetech.com**

startDate: **6/15/1993 20:07**
watchlist: **true**
first: **Hershel**

bunit: **americas**
priority: **critical**
endDate: **3/2/1998 22:53**

prefix: **Mr.**
phone2: **+1 (800)555-3154**

Information about this identity



Risk Modifiers (240)

Thu Sep 17 12:26:15 - Thu Sep 17 12:37:24 GMT-0600

risk_object
Hax0r
htrapper@acmetech.com

risk_score
240

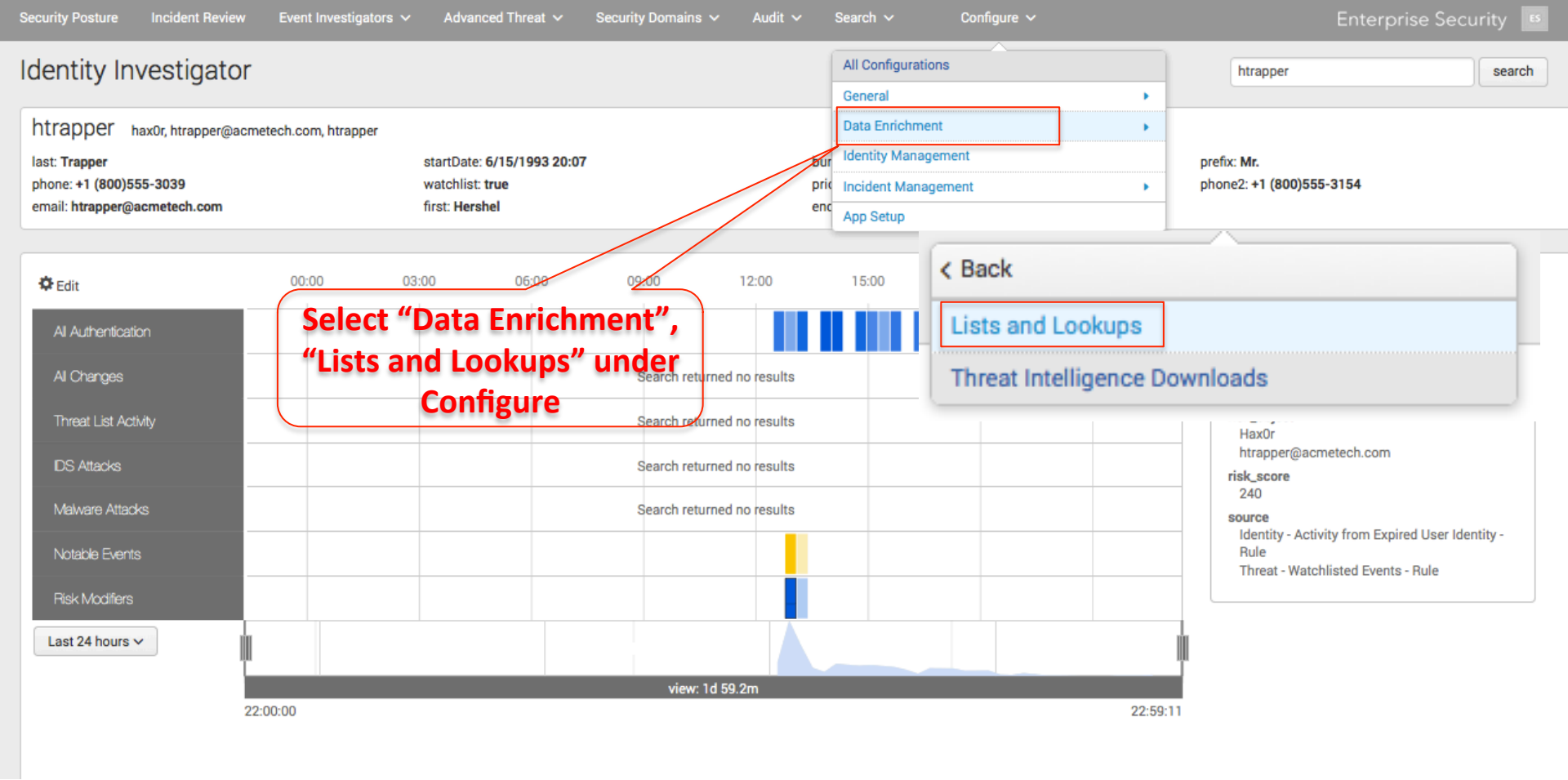
source
Identity - Activity from Expired User Identity - Rule
Threat - Watchlisted Events - Rule

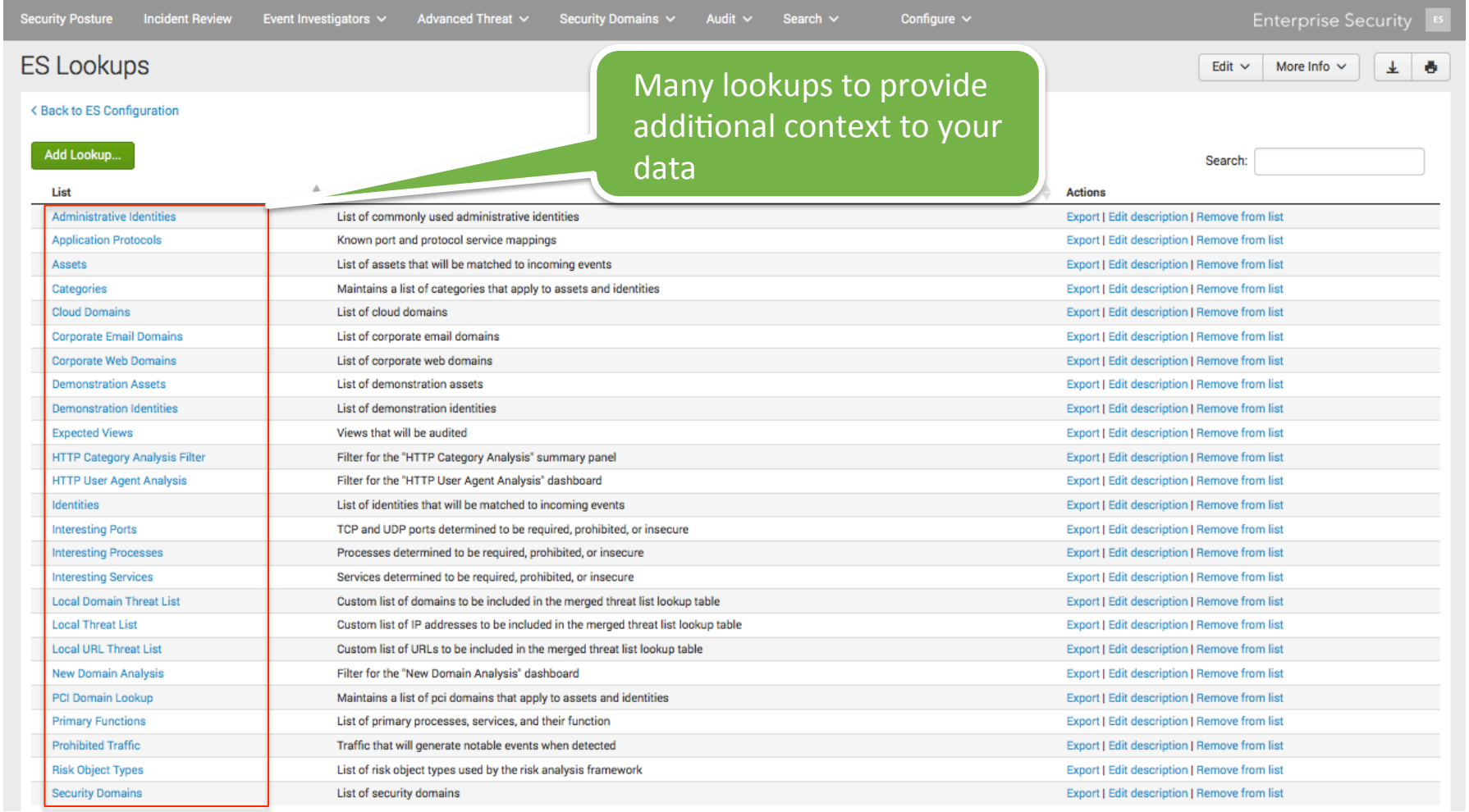
Questions about Incident Response?

splunk>

Lookups and Correlation Searches

splunk>


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Identity Investigator
All Configurations
General
Data Enrichment
Identity Management
Incident Management
App Setup
htrapper
search
htrapper hax0r, htrapper@acmetech.com, htrapper
last: Trapper
phone: +1 (800)555-3039
email: htrapper@acmetech.com
startDate: 6/15/1993 20:07
watchlist: true
first: Hershel
prefix: Mr.
phone2: +1 (800)555-3154
Back
Lists and Lookups
Threat Intelligence Downloads
Select “Data Enrichment”, “Lists and Lookups” under Configure
Edit
00:00
03:00
06:00
09:00
12:00
15:00
AI Authentication
AI Changes
Threat List Activity
IDS Attacks
Malware Attacks
Notable Events
Risk Modifiers
Search returned no results
Search returned no results
Search returned no results
Search returned no results
Last 24 hours
view: 1d 59.2m
22:00:00
22:59:11
Hax0r
htrapper@acmetech.com
risk_score
240
source
Identity - Activity from Expired User Identity - Rule
Threat - Watchlisted Events - Rule


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
ES Lookups
Edit
More Info
Back to ES Configuration
Add Lookup...
Search:
Many lookups to provide additional context to your data
List
Actions
Administrative Identities
List of commonly used administrative identities
Application Protocols
Known port and protocol service mappings
Assets
List of assets that will be matched to incoming events
Categories
Maintains a list of categories that apply to assets and identities
Cloud Domains
List of cloud domains
Corporate Email Domains
List of corporate email domains
Corporate Web Domains
List of corporate web domains
Demonstration Assets
List of demonstration assets
Demonstration Identities
List of demonstration identities
Expected Views
Views that will be audited
HTTP Category Analysis Filter
Filter for the "HTTP Category Analysis" summary panel
HTTP User Agent Analysis
Filter for the "HTTP User Agent Analysis" dashboard
Identities
List of identities that will be matched to incoming events
Interesting Ports
TCP and UDP ports determined to be required, prohibited, or insecure
Interesting Processes
Processes determined to be required, prohibited, or insecure
Interesting Services
Services determined to be required, prohibited, or insecure
Local Domain Threat List
Custom list of domains to be included in the merged threat list lookup table
Local Threat List
Custom list of IP addresses to be included in the merged threat list lookup table
Local URL Threat List
Custom list of URLs to be included in the merged threat list lookup table
New Domain Analysis
Filter for the "New Domain Analysis" dashboard
PCI Domain Lookup
Maintains a list of pci domains that apply to assets and identities
Primary Functions
List of primary processes, services, and their function
Prohibited Traffic
Traffic that will generate notable events when detected
Risk Object Types
List of risk object types used by the risk analysis framework
Security Domains
List of security domains
Export | Edit description | Remove from list

ES Lookups

Edit | More Info

< Back to ES Configuration

Add Lookup...

Search:

List	Description	Actions
Administrative Identities	List of commonly used administrative identities	Export | Edit description | Remove from list
Application Protocols	Known port and protocol service mappings	Export | Edit description | Remove from list
Assets	List of assets that will be matched to incoming events	Export | Edit description | Remove from list
Categories	Maintains a list of categories that apply to assets and identities	Export | Edit description | Remove from list
Cloud Domains	List of cloud domains	Export | Edit description | Remove from list
Corporate Email Domains	List of corporate email domains	Export | Edit description | Remove from list
Corporate Web Domains	List of corporate web domains	Export | Edit description | Remove from list
Demonstration Assets	List of demonstration assets	Export | Edit description | Remove from list
Demonstration Identities	List of demonstration identities	Export | Edit description | Remove from list
Expected Views	Views that will be audited	Export | Edit description | Remove from list
HTTP Category Analysis Filter	Filter for the "HTTP Category Analysis" summary panel	Export | Edit description | Remove from list
HTTP User Agent Analysis	Filter for the "HTTP User Agent Analysis" dashboard	Export | Edit description | Remove from list
Identities	List of identities that will be matched to incoming events	Export | Edit description | Remove from list
Interesting Ports	TCP and UDP ports determined to be required, prohibited, or insecure	Export | Edit description | Remove from list
Interesting Processes	Processes determined to be required, prohibited, or insecure	Export | Edit description | Remove from list
Interesting Services	Services determined to be required, prohibited, or insecure	Export | Edit description | Remove from list
Local Domain Threat List	Custom list of domains to be included in the merged threat list lookup table	Export | Edit description | Remove from list
Local Threat List	Custom list of IP addresses to be included in the merged threat list lookup table	Export | Edit description | Remove from list
Local URL Threat List	Custom list of URLs to be included in the merged threat list lookup table	Export | Edit description | Remove from list
New Domain Analysis	Filter for the "New Domain Analysis" dashboard	Export | Edit description | Remove from list
PCI Domain Lookup	Maintains a list of pci domains that apply to assets and identities	Export | Edit description | Remove from list
Primary Functions	List of primary processes, services, and their function	Export | Edit description | Remove from list
Prohibited Traffic	Traffic that will generate notable events when detected	Export | Edit description | Remove from list
Risk Object Types	List of risk object types used by the risk analysis framework	Export | Edit description | Remove from list
Security Domains	List of security domains	Export | Edit description | Remove from list

Click on "Demonstration Identities"

Edit Lookup

Edit | More Info

< Back to Lookups List

Edit Lookup File

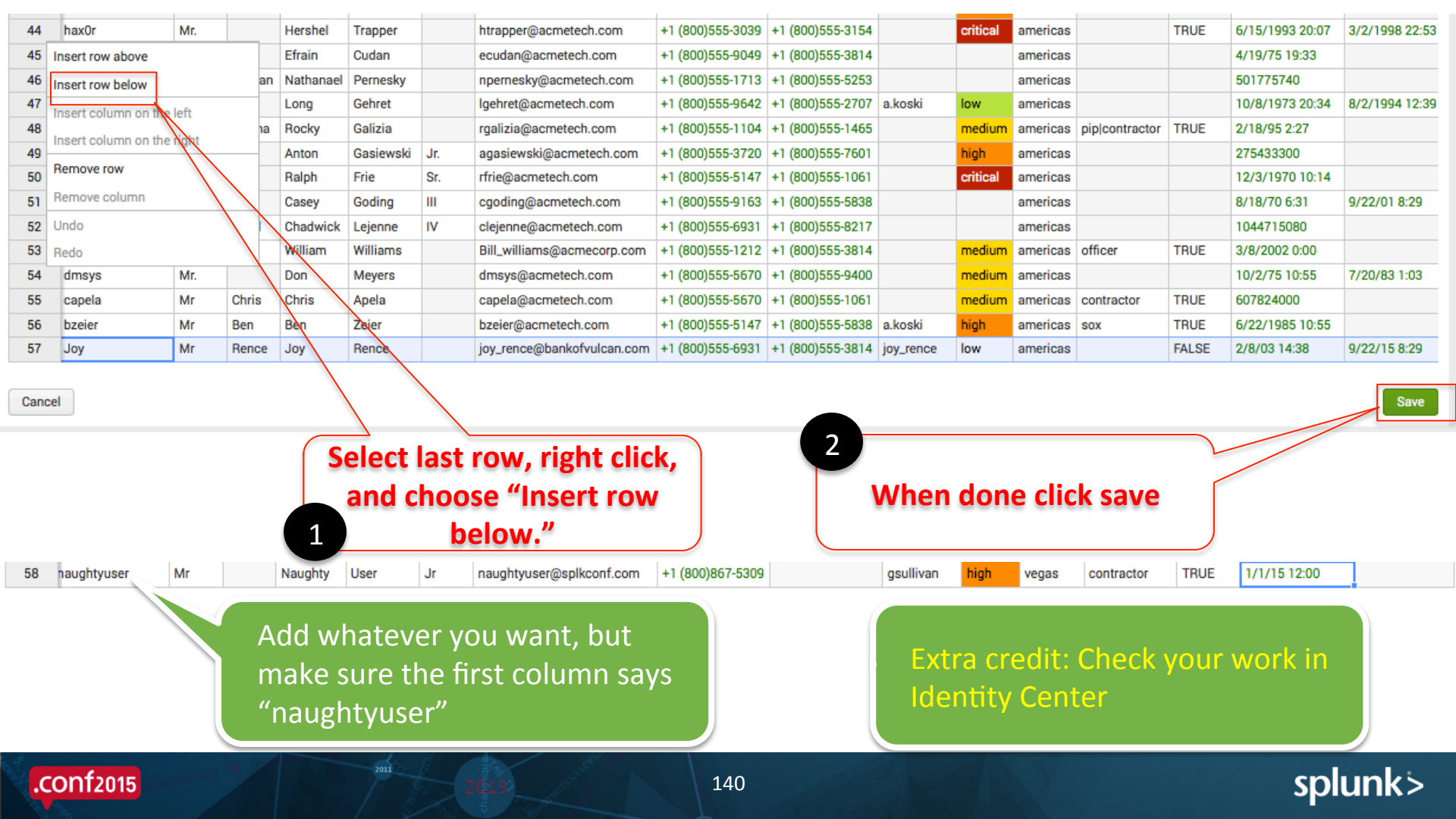
demo_identity_lookup

We want to add "naughtyuser" to this list because it is showing up in our data.

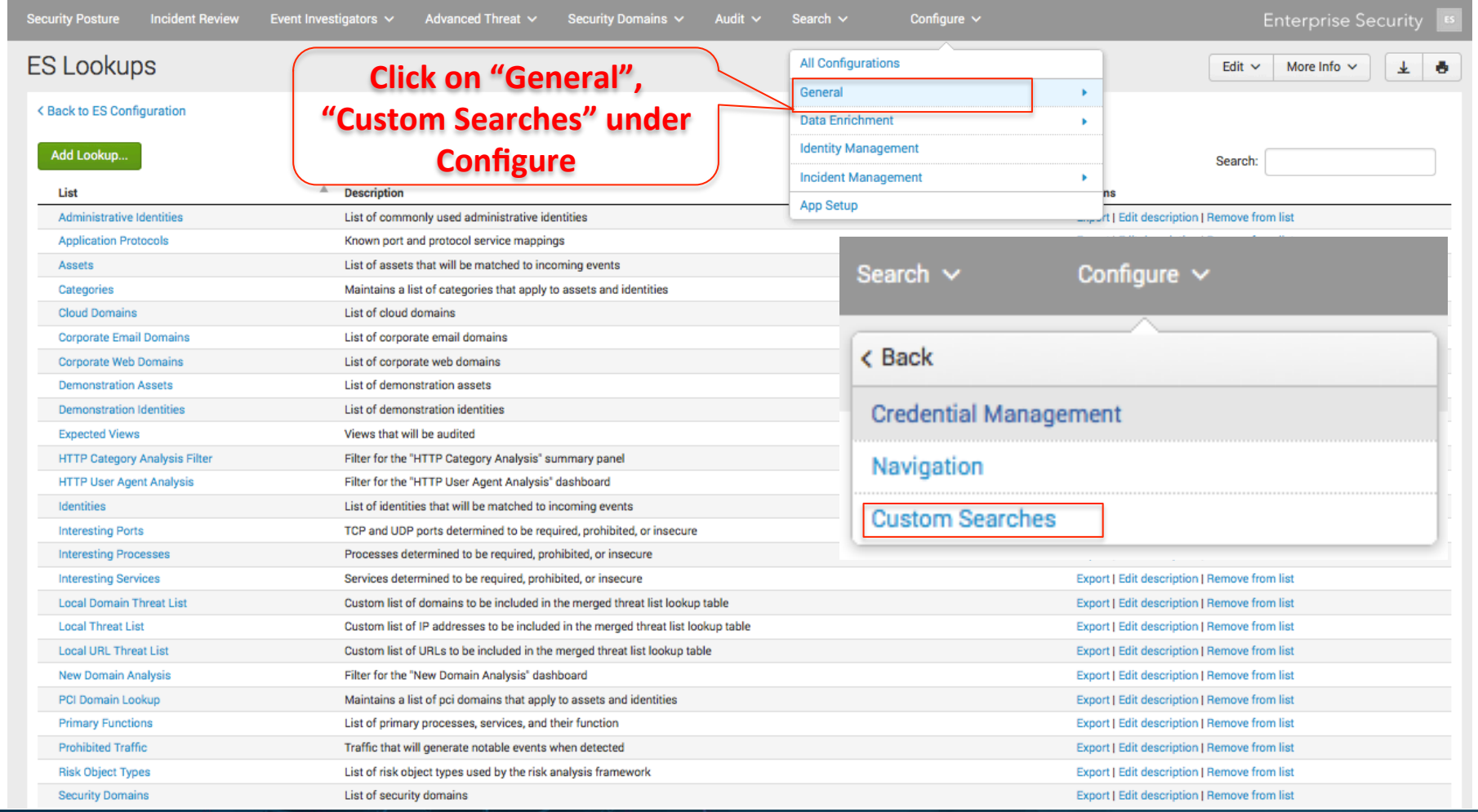
	identity	prefix	nick	first	last						bunit	category	watchlist	startDate	endDate
2		Mr.		Martin		mawe@acmetech.com	+1 (800)555-1562	+1 (800)555-3327		critical	americas			5/1/2003 0:17	
3			Ne		Majcher	rmajcher@acmetech.com	+1 (800)555-8762	+1 (800)555-8549			americas	contractor		9/15/96 1:55	
4				Elouise	Jennifer	ejennifer@acmetech.com	+1 (800)555-7388	+1 (800)555-2669			americas			132388260	
5		Mrs.		Larisa	Kerst	lkerst@acmetech.com	+1 (800)555-4897	+1 (800)555-4311	pepper	low	americas			12/12/2004 17:31	
6		Miss		Miki	Pickle	mpickle@acmetech.com	+1 (800)555-5501	+1 (800)555-7321		medium	americas	pci		8/29/99 2:51	
7	pepper|a.koski	Dr.	Al	Allen	Seykoski	aseykoski@acmetech.com	+1 (800)555-2111	+1 (800)555-9996		high	americas		TRUE	1058023800	1215892140
8				Renda	Mckittrick	rmckittrick@acmetech.com	+1 (800)555-8072	+1 (800)555-2031		critical	americas			10/28/1983 0:27	
9		Ms.		Katharine	Willetts	kwilletts@acmetech.com	+1 (800)555-7596	+1 (800)555-4546			americas	intern		2/13/77 23:14	
10		Mrs.		Germaine	Largin	glargin@acmetech.com	+1 (800)555-3243	+1 (800)555-6764			americas			377537400	
11		Miss		Roma	Aceuedo	raceuedo@acmetech.com	+1 (800)555-1052	+1 (800)555-6529		low	americas		TRUE	5/12/1988 19:55	
12	money|journot	Dr.		Latoyia	Journot	ljournot@acmetech.com	+1 (800)555-3479	+1 (800)555-1554		medium	americas			3/2/88 2:39	3/8/01 6:21
13				Elissa	Whitmoyer	ewhitmoyer@acmetech.com	+1 (800)555-9812	+1 (800)555-7122		high	americas	pci|cardholder		342707520	
14		Ms.		Raylene	Cloward	rcloward@acmetech.com	+1 (800)555-9908	+1 (800)555-5055	money	critical	americas	officer|pip		12/23/1994 16:10	
15		Mrs.		Keena	Horstman	khorstman@acmetech.com	+1 (800)555-4711	+1 (800)555-9586			americas			1/8/88 23:06	
16		Miss	Turtle	Edwina	Berdan	eberdan@acmetech.com	+1 (800)555-2243	+1 (800)555-7697			americas	contractor		1208450280	
17	lurker	Dr.		Karey	Floe	kfloe@acmetech.com	+1 (800)555-1167	+1 (800)555-9058		low	americas			2/7/1972 16:54	2/7/2002 10:43
18				Manie	Infield	minfield@acmetech.com	+1 (800)555-6705	+1 (800)555-1910		medium	americas			4/11/81 12:43	
19		Ms.		Lashunda	Borkoski	lborkoski@acmetech.com	+1 (800)555-6310	+1 (800)555-3184	money	high	americas	pip		585282060	
20		Mrs.	Marty	Martin	Grieves	mgrieves@acmetech.com	+1 (800)555-3560	+1 (800)555-3777		critical	americas			7/7/2003 0:17	
21		Miss		Cathi	Piening	cpiening@acmetech.com	+1 (800)555-4219	+1 (800)555-1444			americas			6/28/71 1:42	

SCROLL

Cancel | Save



44	hax0r	Mr.		Hershel	Trapper		htrapper@acmetech.com	+1 (800)555-3039	+1 (800)555-3154		critical	americas		TRUE	6/15/1993 20:07	3/2/1998 22:53
45				Efrain	Cudan		ecudan@acmetech.com	+1 (800)555-9049	+1 (800)555-3814			americas			4/19/75 19:33	
46				Nathanael	Pernesky		npernesky@acmetech.com	+1 (800)555-1713	+1 (800)555-5253			americas			501775740	
47				Long	Gehret		lgehret@acmetech.com	+1 (800)555-9642	+1 (800)555-2707	a.koski	low	americas			10/8/1973 20:34	8/2/1994 12:39
48				Rocky	Galizia		rgalizia@acmetech.com	+1 (800)555-1104	+1 (800)555-1465		medium	americas	pip|contractor	TRUE	2/18/95 2:27	
49				Anton	Gasiewski	Jr.	agasiewski@acmetech.com	+1 (800)555-3720	+1 (800)555-7601		high	americas			275433300	
50				Ralph	Frie	Sr.	rfrie@acmetech.com	+1 (800)555-5147	+1 (800)555-1061		critical	americas			12/3/1970 10:14	
51				Casey	Goding	III	cgoding@acmetech.com	+1 (800)555-9163	+1 (800)555-5838			americas			8/18/70 6:31	9/22/01 8:29
52				Chadwick	Lejenne	IV	clejenne@acmetech.com	+1 (800)555-6931	+1 (800)555-8217			americas			1044715080	
53				William	Williams		Bill_williams@acmecorp.com	+1 (800)555-1212	+1 (800)555-3814		medium	americas	officer	TRUE	3/8/2002 0:00	
54	dmsys	Mr.		Don	Meyers		dmsys@acmetech.com	+1 (800)555-5670	+1 (800)555-9400		medium	americas			10/2/75 10:55	7/20/83 1:03
55	capela	Mr	Chris	Chris	Apela		capela@acmetech.com	+1 (800)555-5670	+1 (800)555-1061		medium	americas	contractor	TRUE	607824000	
56	bzeier	Mr	Ben	Ben	Zeier		bzeier@acmetech.com	+1 (800)555-5147	+1 (800)555-5838	a.koski	high	americas	sox	TRUE	6/22/1985 10:55	
57	Joy	Mr	Rence	Joy	Rence		joy_rence@bankofvulcan.com	+1 (800)555-6931	+1 (800)555-3814	joy_rence	low	americas		FALSE	2/8/03 14:38	9/22/15 8:29
58	naughtyuser	Mr		Naughty	User	Jr	naughtyuser@splkconf.com	+1 (800)867-5309		gsullivan	high	vegas	contractor	TRUE	1/1/15 12:00	


Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
ES Lookups
Click on “General”, “Custom Searches” under Configure
All Configurations
General
Data Enrichment
Identity Management
Incident Management
App Setup
Edit
More Info
Back to ES Configuration
Add Lookup...
Search:
List
Description
Administrative Identities
List of commonly used administrative identities
Edit description
Remove from list
Application Protocols
Known port and protocol service mappings
Assets
List of assets that will be matched to incoming events
Categories
Maintains a list of categories that apply to assets and identities
Cloud Domains
List of cloud domains
Corporate Email Domains
List of corporate email domains
Corporate Web Domains
List of corporate web domains
Demonstration Assets
List of demonstration assets
Demonstration Identities
List of demonstration identities
Expected Views
Views that will be audited
HTTP Category Analysis Filter
Filter for the "HTTP Category Analysis" summary panel
HTTP User Agent Analysis
Filter for the "HTTP User Agent Analysis" dashboard
Identities
List of identities that will be matched to incoming events
Interesting Ports
TCP and UDP ports determined to be required, prohibited, or insecure
Interesting Processes
Processes determined to be required, prohibited, or insecure
Search
Configure
Back
Credential Management
Navigation
Custom Searches
Interesting Services
Services determined to be required, prohibited, or insecure
Export | Edit description | Remove from list
Local Domain Threat List
Custom list of domains to be included in the merged threat list lookup table
Local Threat List
Custom list of IP addresses to be included in the merged threat list lookup table
Local URL Threat List
Custom list of URLs to be included in the merged threat list lookup table
New Domain Analysis
Filter for the "New Domain Analysis" dashboard
PCI Domain Lookup
Maintains a list of pci domains that apply to assets and identities
Primary Functions
List of primary processes, services, and their function
Prohibited Traffic
Traffic that will generate notable events when detected
Risk Object Types
List of risk object types used by the risk analysis framework
Security Domains
List of security domains

Custom Searches

Edit | More Info

< Back to ES Configuration

New

Click “New”

25 records per page

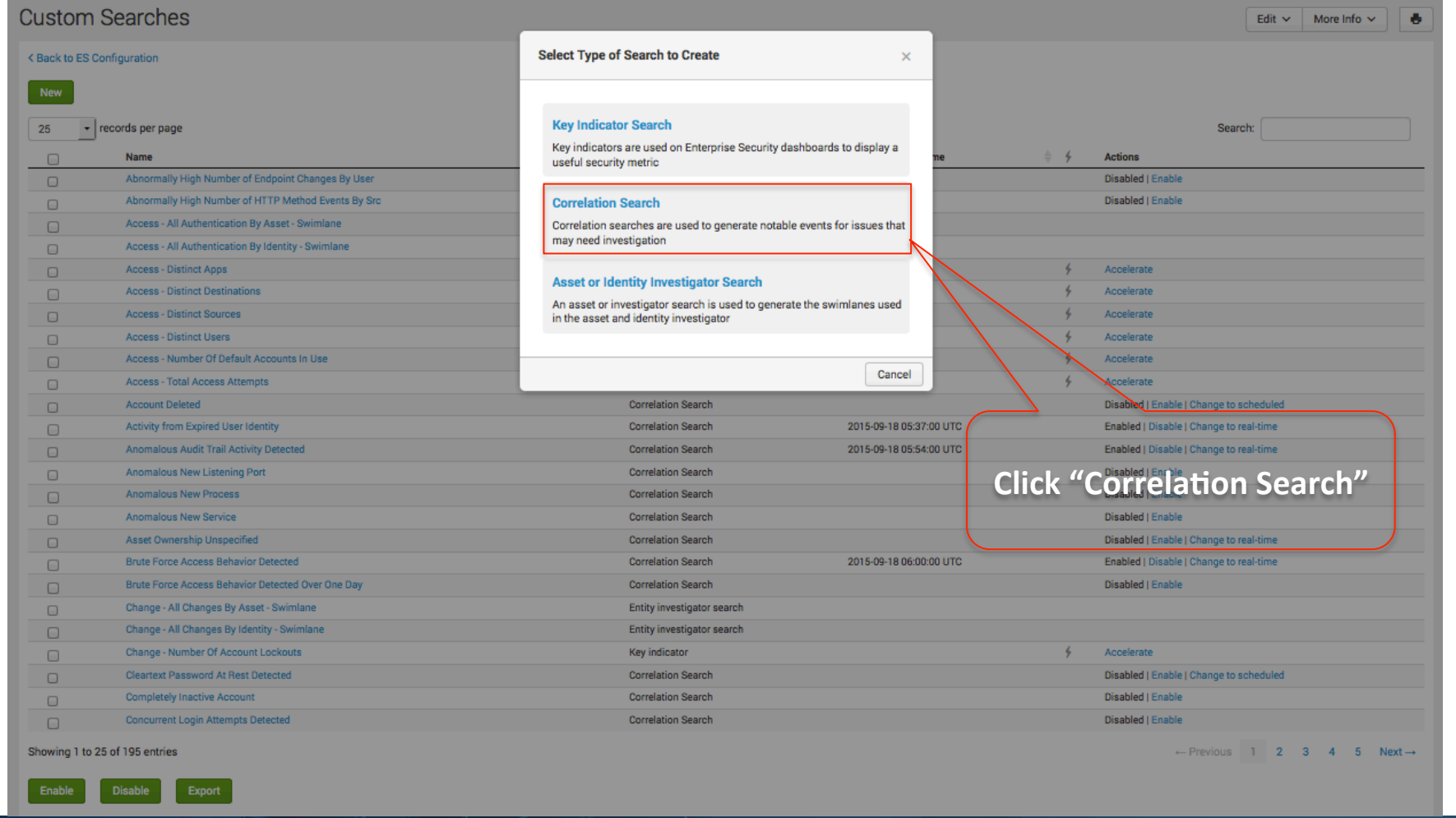
Search:

	Name	Type	Next Scheduled Time	Actions
☐	Abnormally High Number of Endpoint Changes By User	Correlation Search		Disabled | Enable
☐	Abnormally High Number of HTTP Method Events By Src	Correlation Search		Disabled | Enable
☐	Access - All Authentication By Asset - Swimlane	Entity investigator search		
☐	Access - All Authentication By Identity - Swimlane	Entity investigator search		
☐	Access - Distinct Apps	Key indicator		Accelerate
☐	Access - Distinct Destinations	Key indicator		Accelerate
☐	Access - Distinct Sources	Key indicator		Accelerate
☐	Access - Distinct Users	Key indicator		Accelerate
☐	Access - Number Of Default Accounts In Use	Key indicator		Accelerate
☐	Access - Total Access Attempts	Key indicator		Accelerate
☐	Account Deleted	Correlation Search		Disabled | Enable | Change to scheduled
☐	Activity from Expired User Identity	Correlation Search	2015-09-18 05:37:00 UTC	Enabled | Disable | Change to real-time
☐	Anomalous Audit Trail Activity Detected	Correlation Search	2015-09-18 05:54:00 UTC	Enabled | Disable | Change to real-time
☐	Anomalous New Listening Port	Correlation Search		Disabled | Enable
☐	Anomalous New Process	Correlation Search		Disabled | Enable
☐	Anomalous New Service	Correlation Search		Disabled | Enable
☐	Asset Ownership Unspecified	Correlation Search		Disabled | Enable | Change to real-time
☐	Brute Force Access Behavior Detected	Correlation Search	2015-09-18 06:00:00 UTC	Enabled | Disable | Change to real-time
☐	Brute Force Access Behavior Detected Over One Day	Correlation Search		Disabled | Enable
☐	Change - All Changes By Asset - Swimlane	Entity investigator search		
☐	Change - All Changes By Identity - Swimlane	Entity investigator search		
☐	Change - Number Of Account Lockouts	Key indicator		Accelerate
☐	Cleartext Password At Rest Detected	Correlation Search		Disabled | Enable | Change to scheduled
☐	Completely Inactive Account	Correlation Search		Disabled | Enable
☐	Concurrent Login Attempts Detected	Correlation Search		Disabled | Enable

Showing 1 to 25 of 195 entries

← Previous 1 2 3 4 5 Next →

Enable Disable Export


Custom Searches
Edit
More Info
Back to ES Configuration
New
25 records per page
Search:
Name
Actions
Abnormally High Number of Endpoint Changes By User
Disabled | Enable
Abnormally High Number of HTTP Method Events By Src
Disabled | Enable
Access - All Authentication By Asset - Swimlane
Access - All Authentication By Identity - Swimlane
Access - Distinct Apps
Accelerate
Access - Distinct Destinations
Accelerate
Access - Distinct Sources
Accelerate
Access - Distinct Users
Accelerate
Access - Number Of Default Accounts In Use
Accelerate
Access - Total Access Attempts
Accelerate
Account Deleted
Correlation Search
Disabled | Enable | Change to scheduled
Activity from Expired User Identity
Correlation Search
2015-09-18 05:37:00 UTC
Enabled | Disable | Change to real-time
Anomalous Audit Trail Activity Detected
Correlation Search
2015-09-18 05:54:00 UTC
Enabled | Disable | Change to real-time
Anomalous New Listening Port
Correlation Search
Anomalous New Process
Correlation Search
Anomalous New Service
Correlation Search
Disabled | Enable
Asset Ownership Unspecified
Correlation Search
Disabled | Enable | Change to real-time
Brute Force Access Behavior Detected
Correlation Search
2015-09-18 06:00:00 UTC
Enabled | Disable | Change to real-time
Brute Force Access Behavior Detected Over One Day
Correlation Search
Disabled | Enable
Change - All Changes By Asset - Swimlane
Entity investigator search
Change - All Changes By Identity - Swimlane
Entity investigator search
Change - Number Of Account Lockouts
Key indicator
Accelerate
Cleartext Password At Rest Detected
Correlation Search
Disabled | Enable | Change to scheduled
Completely Inactive Account
Correlation Search
Disabled | Enable
Concurrent Login Attempts Detected
Correlation Search
Disabled | Enable
Showing 1 to 25 of 195 entries
← Previous 1 2 3 4 5 Next →
Enable
Disable
Export
Select Type of Search to Create
Key Indicator Search
Key indicators are used on Enterprise Security dashboards to display a useful security metric
Correlation Search
Correlation searches are used to generate notable events for issues that may need investigation
Asset or Identity Investigator Search
An asset or investigator search is used to generate the swimlanes used in the asset and identity investigator
Cancel
Click “Correlation Search”

< Back to Custom Searches

Correlation Search

Search Name*: A .conf Hands On Failed Login Correlation Search

Application Context: search

Description: Finds Failed Logins over 1,000 in an hour

Describes what kind of issues this search is intended to detect

Search*:

Cannot be empty

Edit search in guided mode

Fill in Search Name, App Context, and Description

< Back to Custom Searches

Correlation Search

Search Name*: A .conf Hands On Failed Login Correlation Search

Application Context: search

Description: Finds Failed Logins over 1,000 in an hour

Describes what kind of issues this search is intended to detect

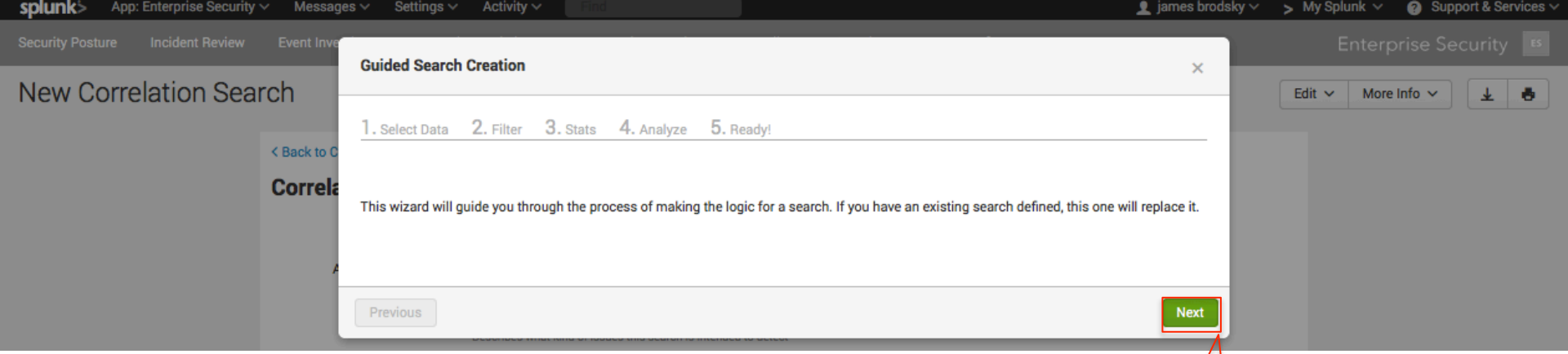
Search*:

Cannot be empty

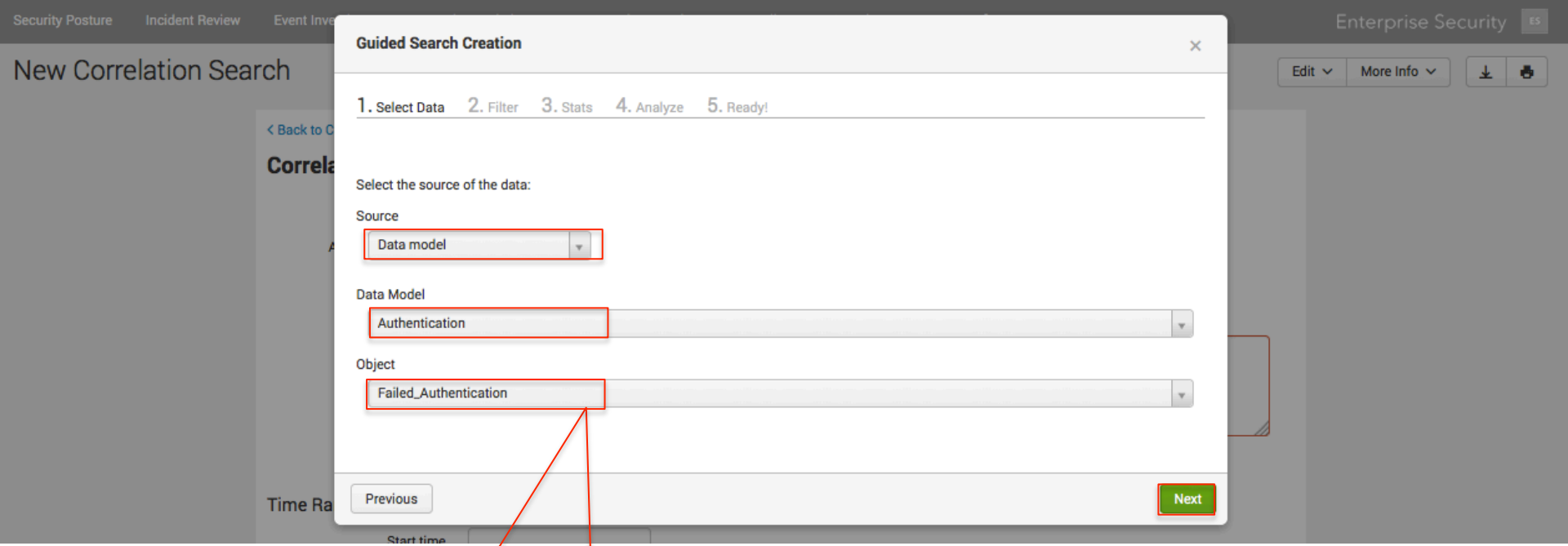
Edit search in guided mode

You could simply type a Splunk search in here if you wanted.

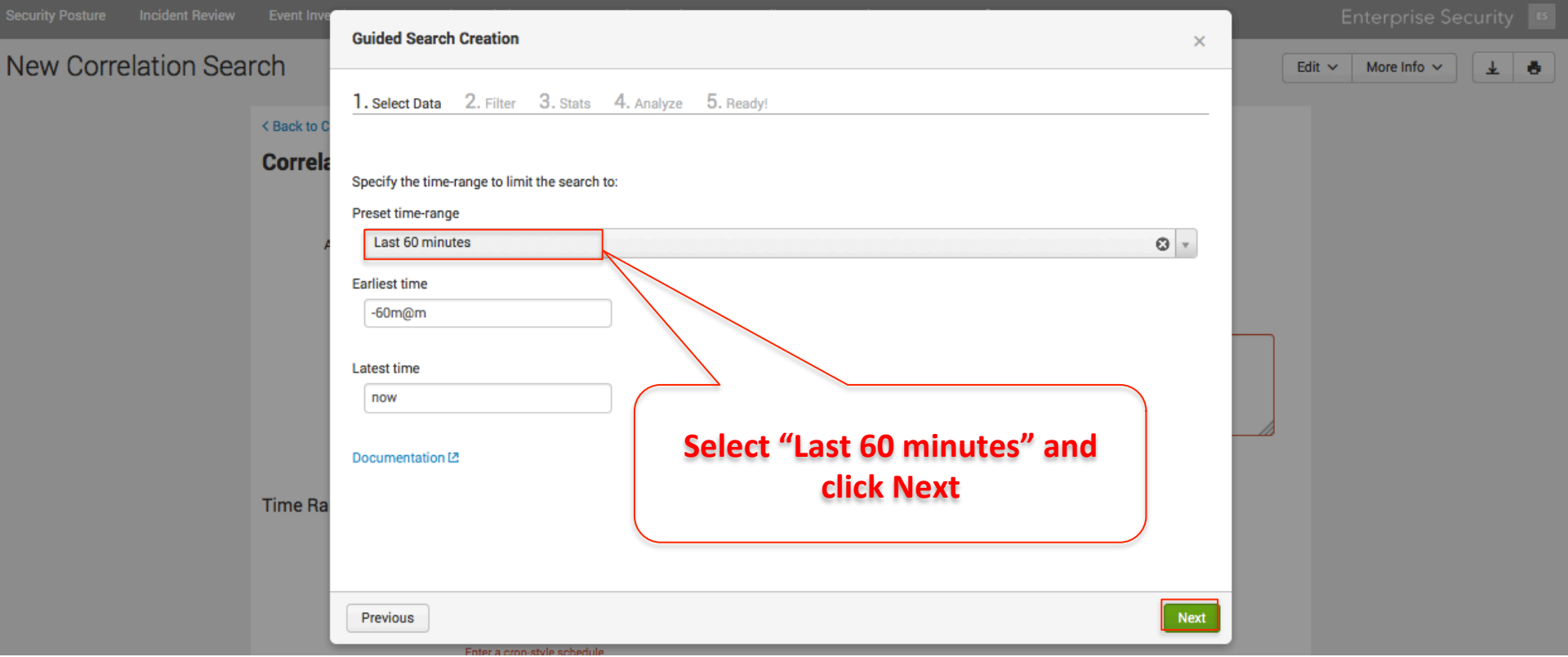
Click "Edit search in guided mode"

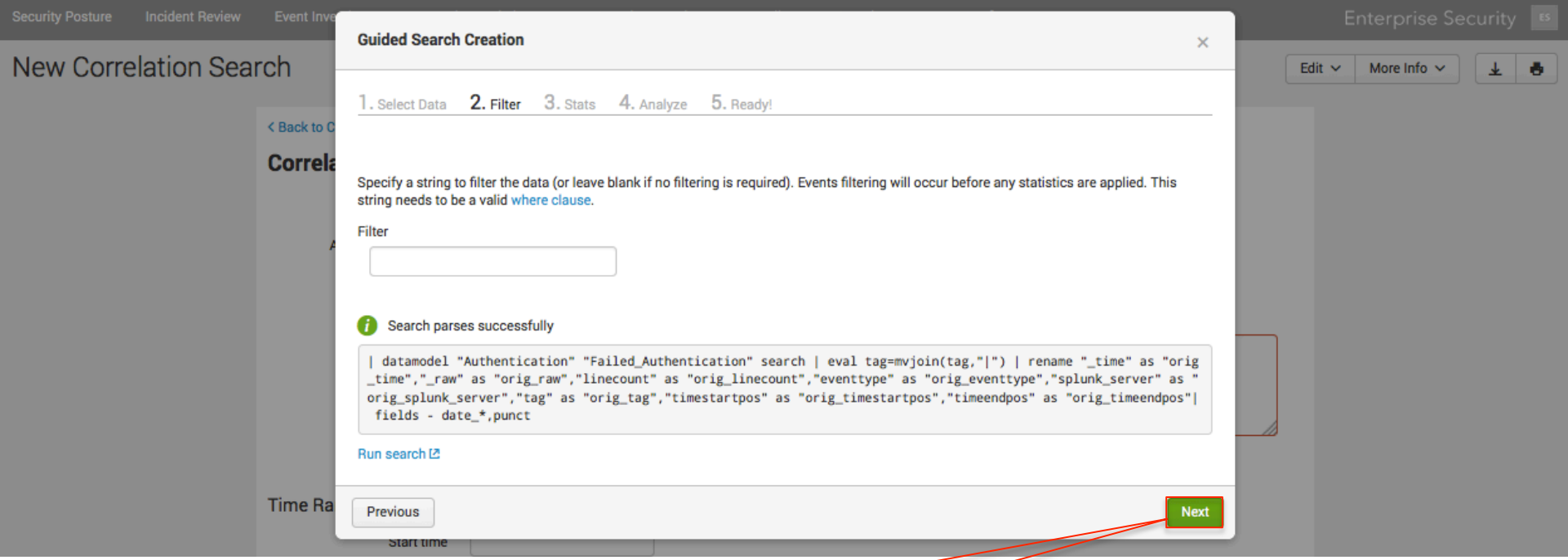

splunk>
App: Enterprise Security
Messages
Settings
Activity
james brodsky
My Splunk
Support & Services
Security Posture
Incident Review
Enterprise Security
New Correlation Search
Edit
More Info
Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
This wizard will guide you through the process of making the logic for a search. If you have an existing search defined, this one will replace it.
Previous
Next

Click “Next”



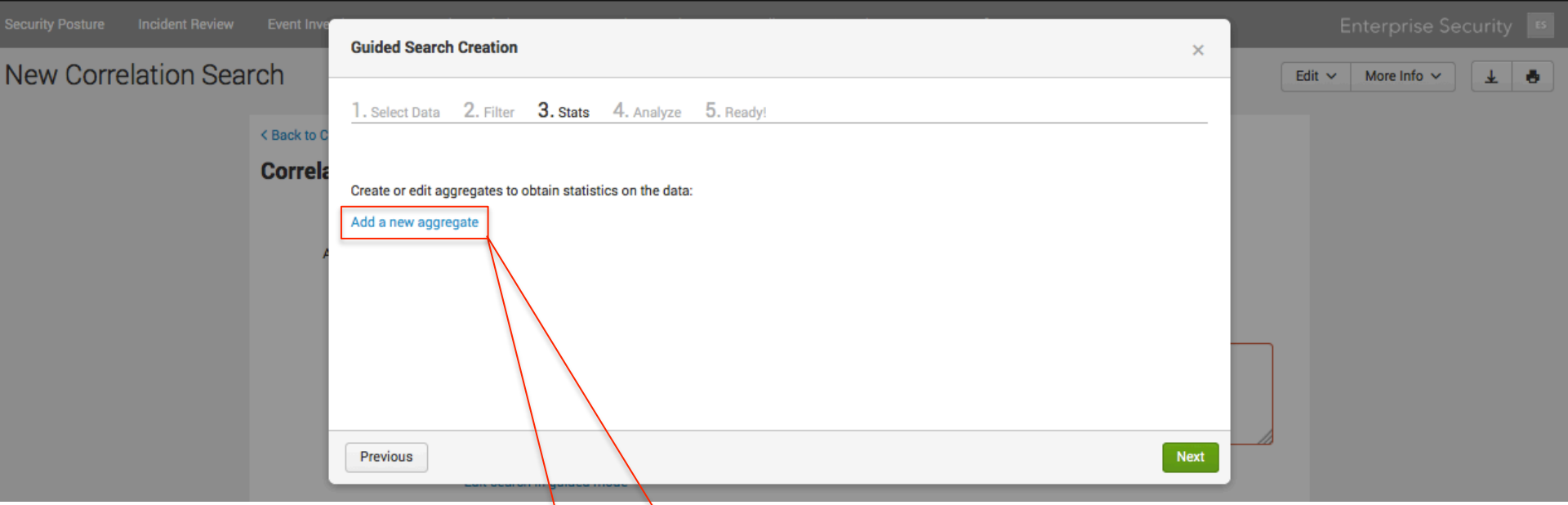
Select "Data Model", "Authentication", "Failed_Authentication" and click Next


Security Posture
Incident Review
Enterprise Security
New Correlation Search
Edit
More Info
Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Specify the time-range to limit the search to:
Preset time-range
Last 60 minutes
Earliest time
-60m@m
Latest time
now
Documentation
Select “Last 60 minutes” and click Next
Previous
Next

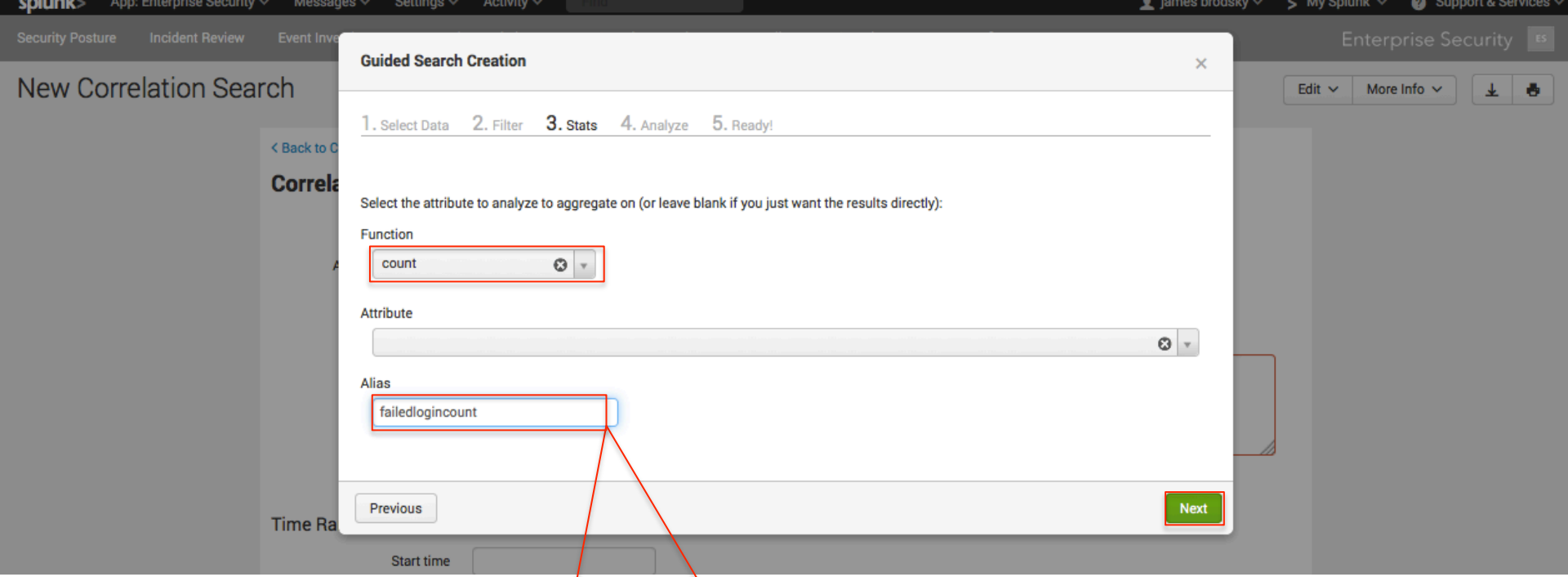


Observe search and click Next

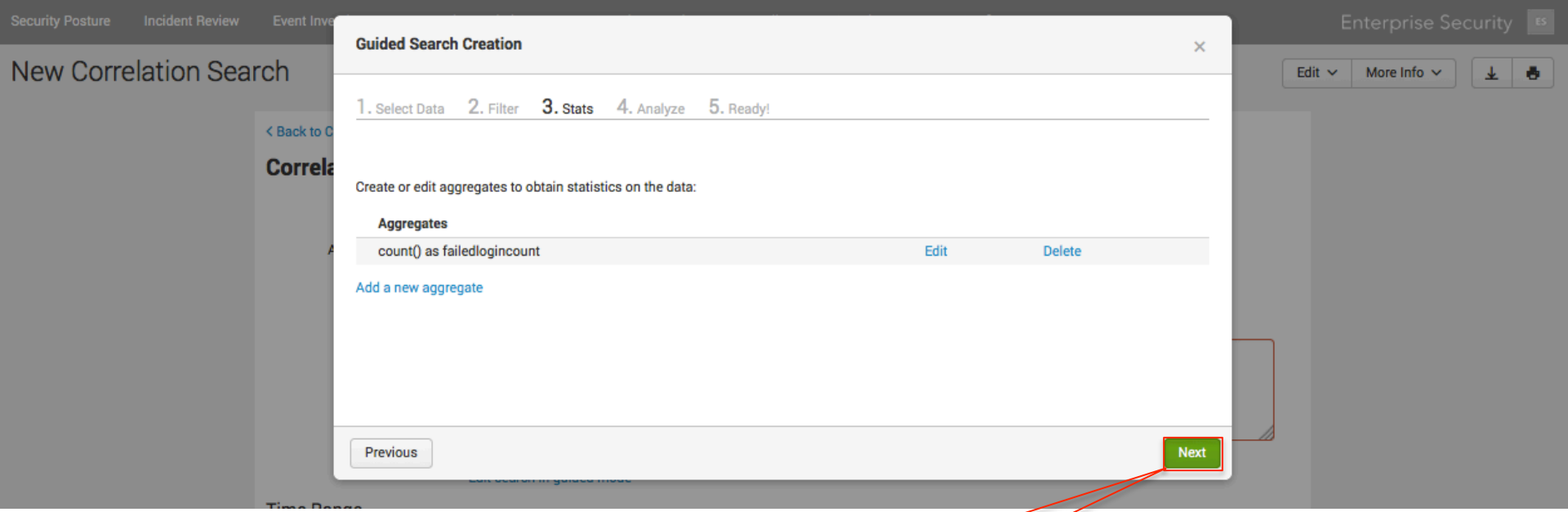
Optional: You can “Run search” at this point and see the events that will return.



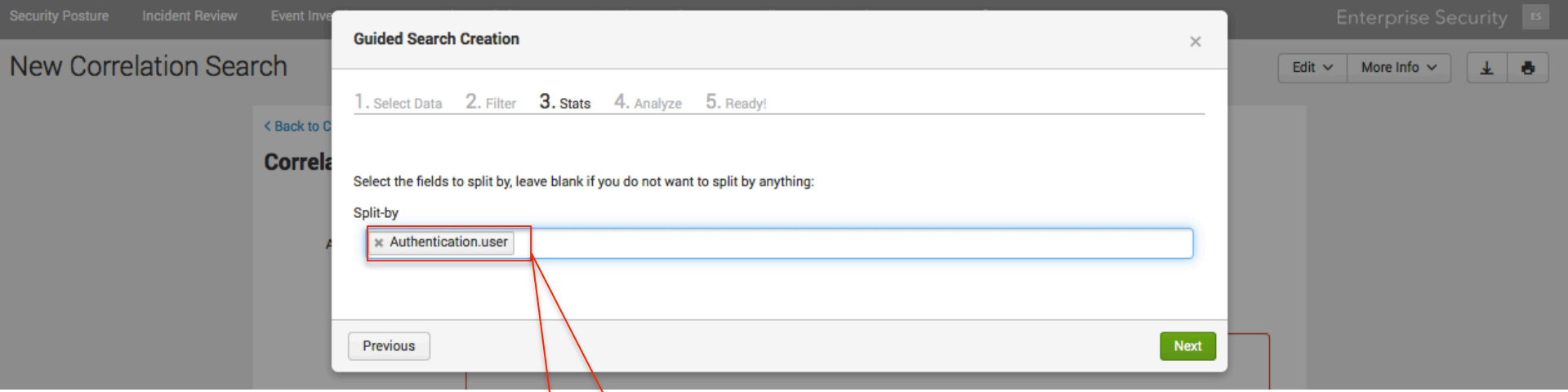
Click “Add a new aggregate”



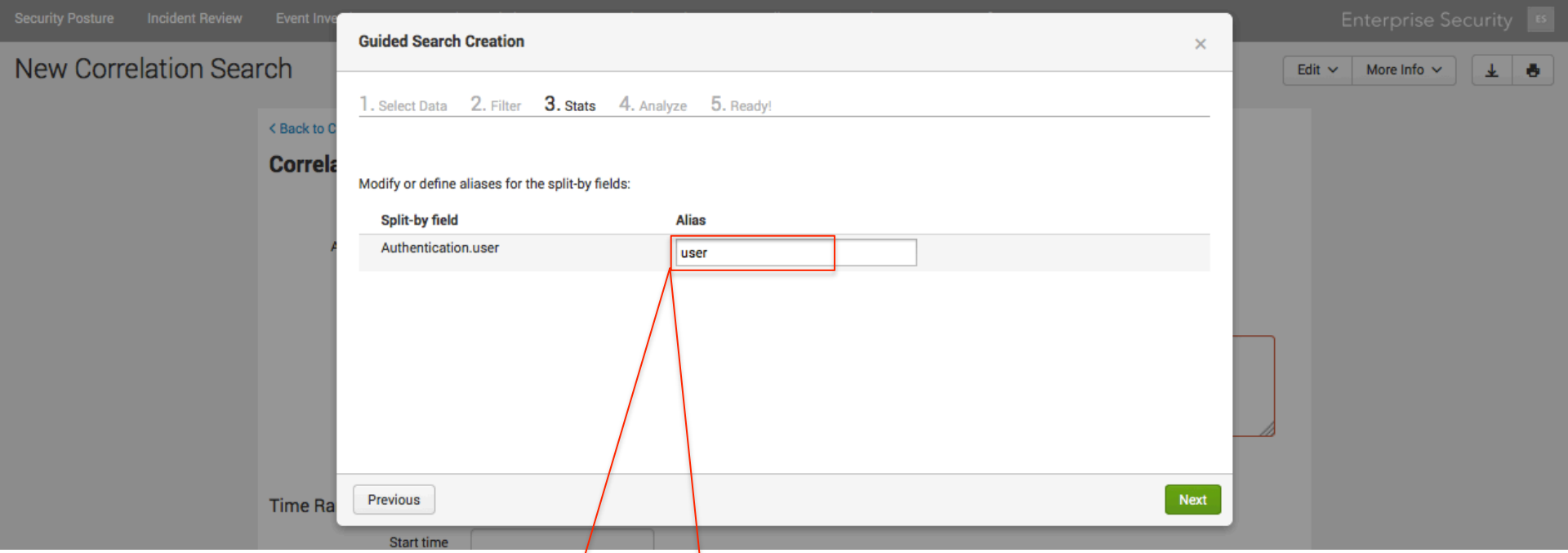
Choose “count” and then alias it as “failedlogincount” and click Next


Security Posture
Incident Review
Enterprise Security
New Correlation Search
Edit
More Info
Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Create or edit aggregates to obtain statistics on the data:
Aggregates
count() as failedlogincount
Edit
Delete
Add a new aggregate
Previous
Next

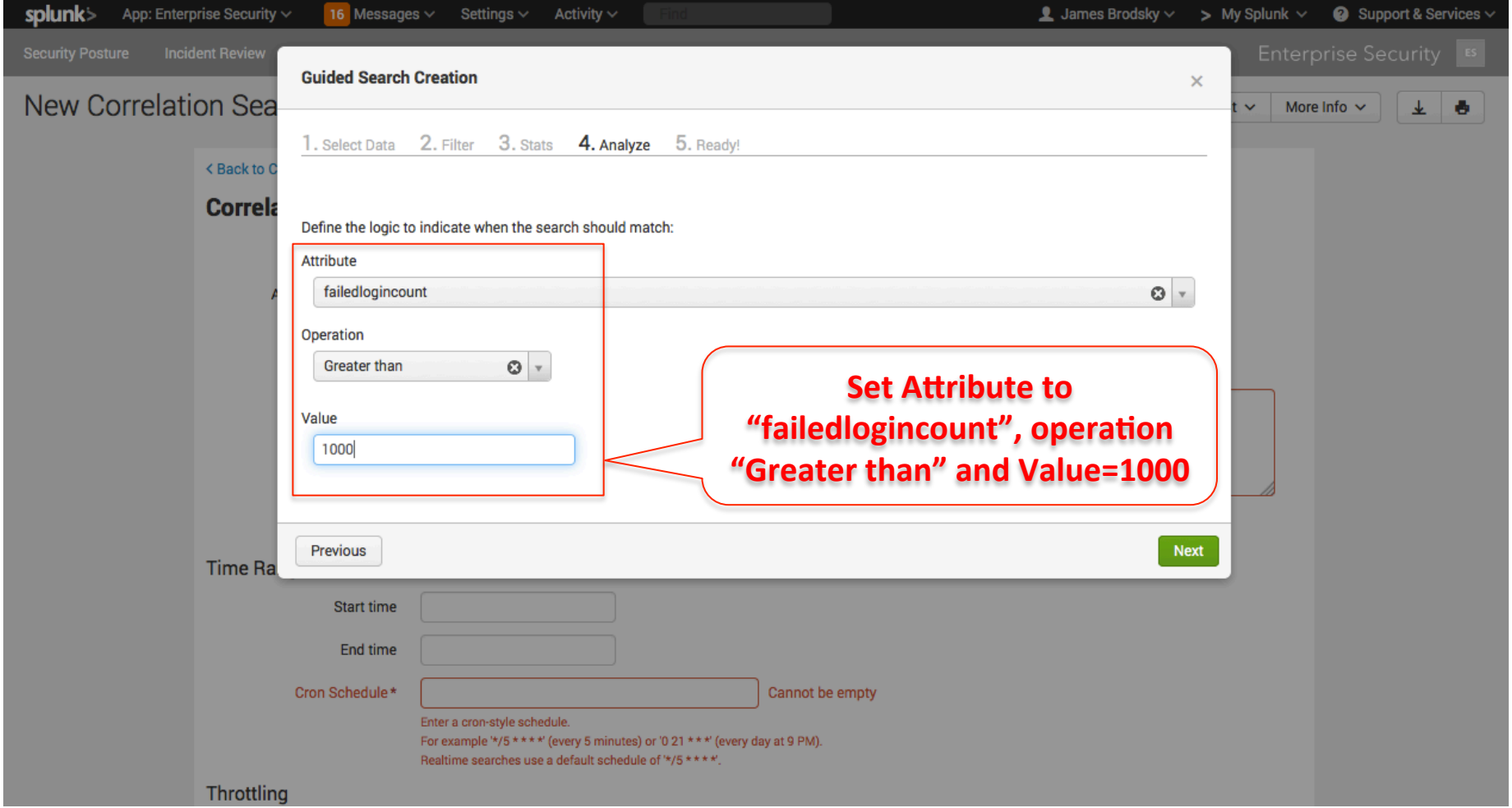
Click Next

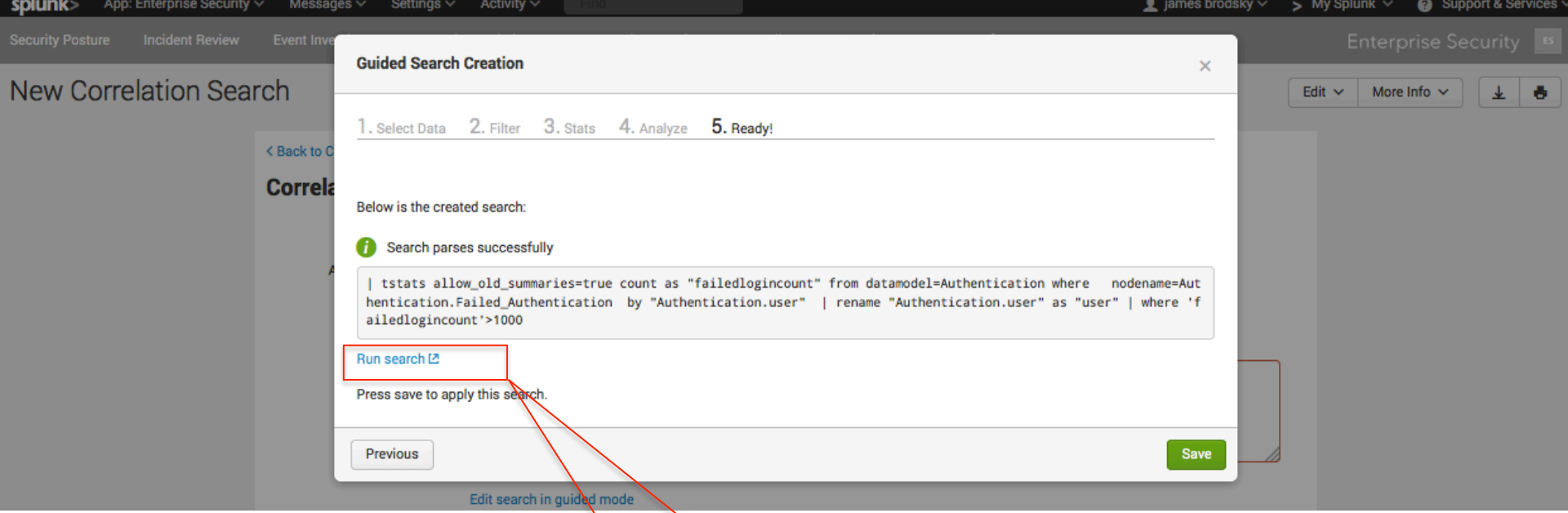


SCROLL to select "Authentication.user" and click Next

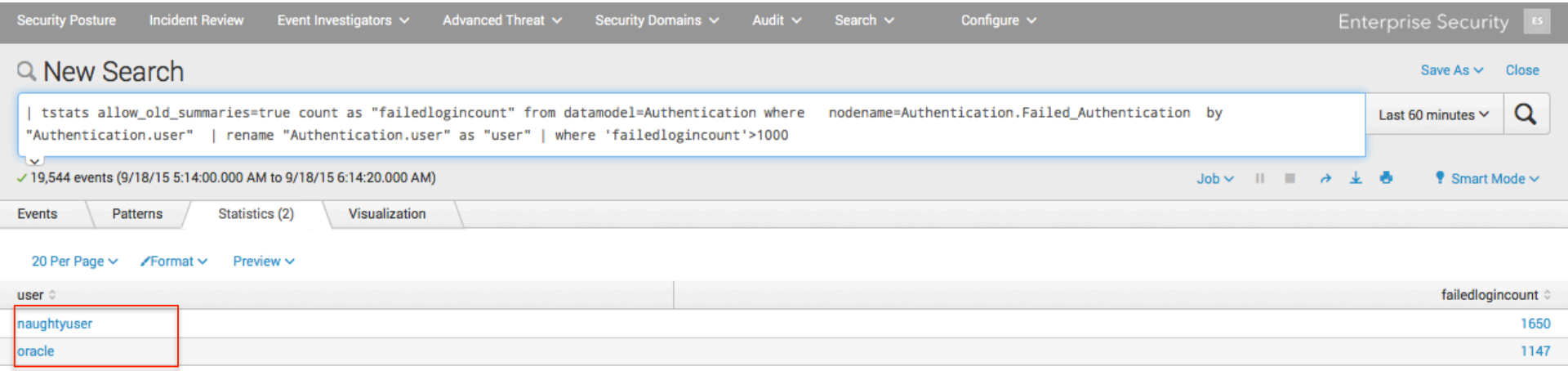


Type “user” in the Alias field and click Next


splunk> App: Enterprise Security 16 Messages Settings Activity James Brodsky My Splunk Support & Services
Security Posture Incident Review Enterprise Security
New Correlation Sea
More Info
Guided Search Creation
1. Select Data 2. Filter 3. Stats 4. Analyze 5. Ready!
Define the logic to indicate when the search should match:
Attribute
failedlogincount
Operation
Greater than
Value
1000
Set Attribute to "failedlogincount", operation "Greater than" and Value=1000
Previous
Next
Time Ra
Start time
End time
Cron Schedule *
Cannot be empty
Enter a cron-style schedule.
For example '*/5 * * * *' (every 5 minutes) or '0 21 * * *' (every day at 9 PM).
Realtime searches use a default schedule of '*/5 * * * *'.
Throttling



Click “run search” to test the search.



This should create two notable events…so let's make sure that happens.

Time Range

Start time: -60m@m

End time: now

Cron Schedule*: */5 * * * *

Enter a cron-style schedule.
For example '*/5 * * * *' (every 5 minutes) or '0 21 * * *' (every day at 9 PM).
Realtime searches use a default schedule of '*/5 * * * *'.

Throttling

Window duration:

Indicates how many seconds to ignore other events that match (i.e. have the same field values)

Fields to group by: Type a field and press enter

Indicates what fields to consider when determining if another event matches this one

Fill in "cron" style schedule – every 5 minutes

Time Range

Start time: -60m@m

End time: now

Cron Schedule*: */5 * * * *

Enter a cron-style schedule.
For example '*/5 * * * *' (every 5 minutes) or '0 21 * * *' (every day at 9 PM).
Realtime searches use a default schedule of '*/5 * * * *'.

Throttling

Window duration: 86400

Indicates how many seconds to ignore other events that match (i.e. have the same field values)

Fields to group by: user x | Type a field and press enter

Indicates what fields to consider when determining if another event matches this one

Put "86400" as the window duration. Put "user" as the field to throttle by.

Notable Event

Create notable event ☑

Title: User $user$ has had more than 1K failed logins.

Notable events created by this search will have this title (supports variable substitution)

Description: User $user$ had $failedlogincount$ logins.

Notable events created by this search will have this description (supports variable substitution)

Security Domain:

Severity: medium

Default Owner: (leave as system default)

Default Status: New

Drill-down name:

Supports variable substitution with fields from the matching event

Drill-down search:

Supports variable substitution with fields from the matching event

Drill-down earliest offset:

Defines how far back from the time of the event to start looking for related events

Drill-down latest offset:

Defines how far back from the time of the event to stop looking for related events

Check the "notable event" box and fill in the fields as shown. Note the "$" signs around the variables!

Risk Scoring

Create risk modifier ☑

Score* 100

Indicates how much to adjust the score for the given risk object

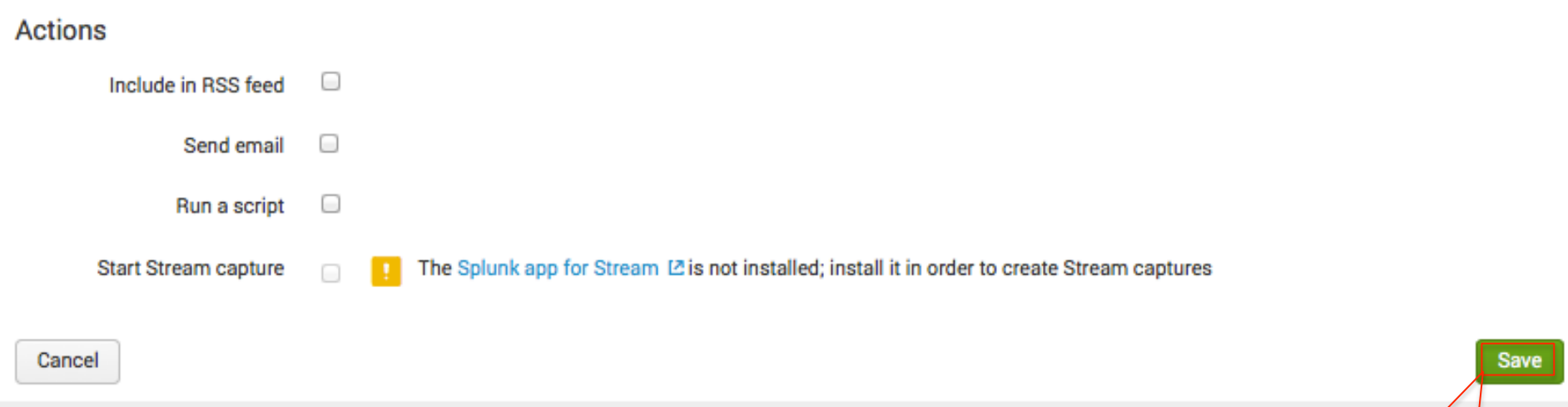
Risk object field* user

Indicates what field in the results indicates the risk object (such as the system or the user) that the score applies to

Risk object type* user

Indicates the type of risk object this applies to (usually 'system' or 'user')

Let's assign risk to the user. Check the box and fill in the three fields as shown.



Save the search and go back to Incident Review.

Incident Review

Urgency

CRITICAL	9
HIGH	318
MEDIUM	1252
LOW	485
INFO	0

Status: × All

Name:

Owner: × All

Search:

Security Domain: × All

Time: Last 24 hours

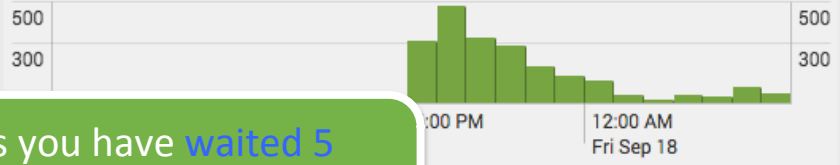
Tag:

Submit

Job | Smart Mode

✓ 2,064 events (9/17/15 6:00:00.000 AM to 9/18/15 6:30:57.000 AM)

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



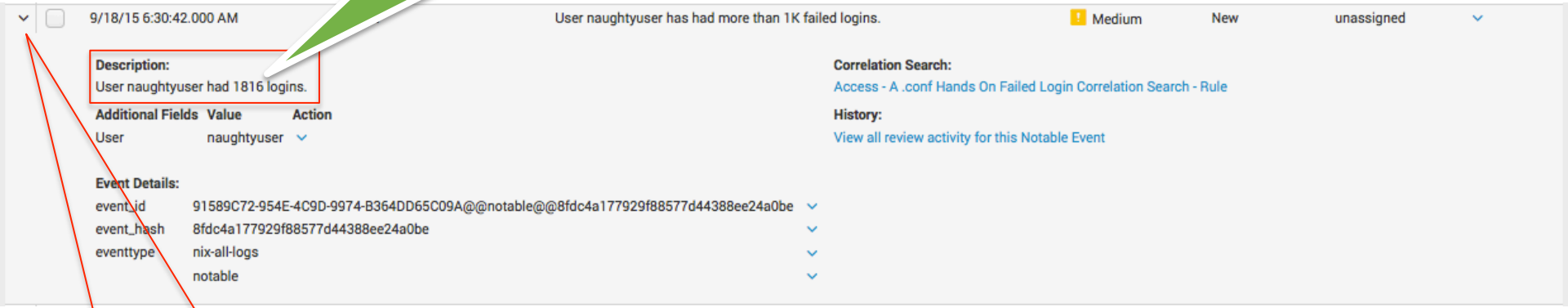
As long as you have waited 5 minutes you should have new notable events!

Edit all selected | Edit all 2064 matching events

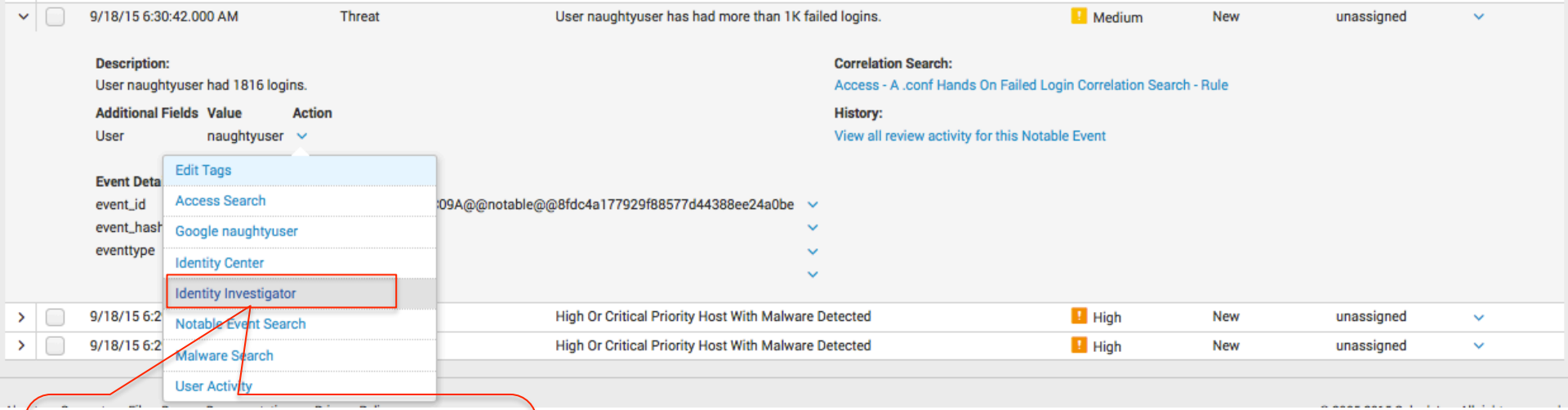
« prev 1 2 3 4 5 6 7 8 9 10 next »

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	9/18/15 6:30:42.000 AM	Threat	User oracle has had more than 1K failed logins.	Low	New	unassigned	
>	9/18/15 6:30:42.000 AM	Threat	User naughtyuser has had more than 1K failed logins.	Medium	New	unassigned	
>	9/18/15 6:29:40.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected	High	New	unassigned	
>	9/18/15 6:29:36.000 AM	Endpoint	High Or Critical Priority Host With Malware Detected	High	New	unassigned	
>	9/18/15 6:26:16.000 AM	Access	Excessive Failed Logins	Low	New	unassigned	
>	9/18/15 6:19:10.000 AM	Threat	Watchlisted Event Observed	Medium	New	unassigned	
>	9/18/15 6:19:10.000 AM	Threat	Watchlisted Event Observed	Medium	New	unassigned	

Variable substitution working



Expand your new event



Launch Identity Investigator against "naughtyuser"

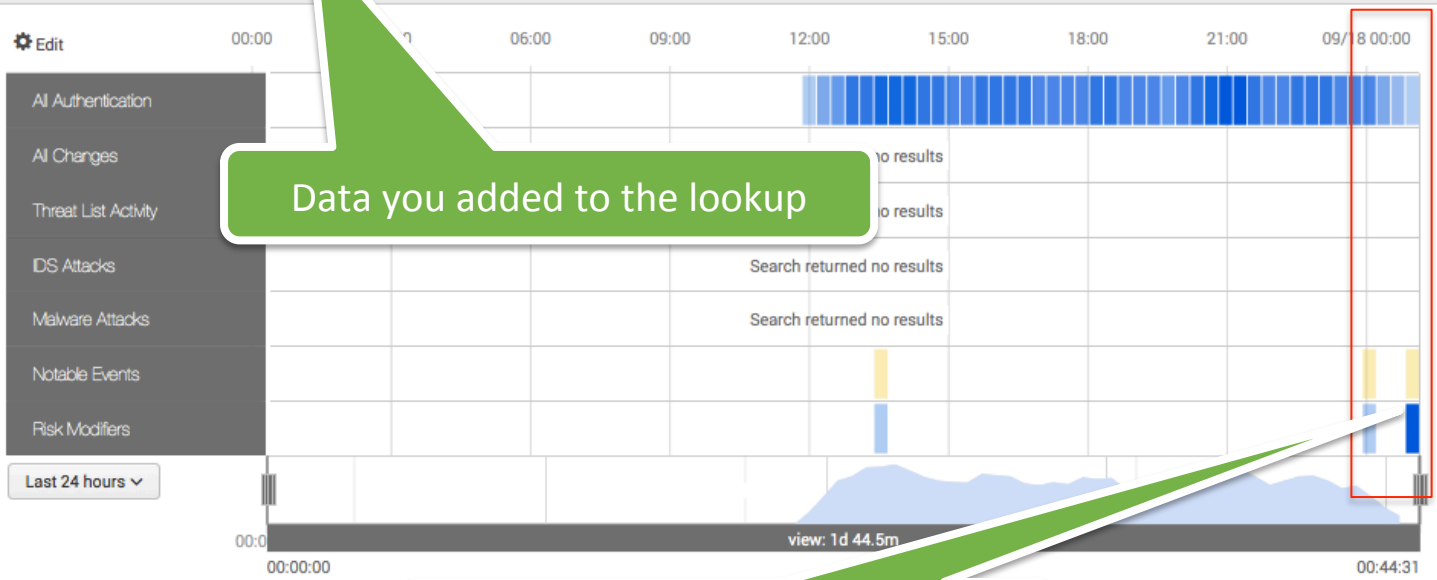
Identity Investigator

naughtyuser search

naughtyuser

naughtyuser, naughtyuser@splkconf.com

last: **User**	email: **naughtyuser@splkconf.com**	prefix: **Mr**	managedBy: **gsullivan**
watchlist: **true**	phone: **+1 (800)867-5309**	bunit: **vegas**	priority: **high**
category: **contractor**	suffix: **Jr**	startDate: **1/1/15 12:00**	first: **Naughty**



Data you added to the lookup

Bonus: Go find “naughtyuser” in Risk Analysis dashboard…

Notable Events and Risk

Final Questions?

splunk>

Next Steps…

- Play in your ES Sandbox for 15 days
- Explore some of the areas we didn't get to cover today
- Ask questions of your sales team
- Once ES 4.0 releases, help yourself to another sandbox to see the new features
- TELL YOUR FRIENDS!

FAQ Link

- During .conf2015 there were several questions asked by audience members – some of which were captured, and the answers are provided here:

https://

THANK YOU

splunk>