.conf2014

YOUR DATA ADVENTURE

Best Kept Secrets of the Splunk App for Enterprise Security

Dimitri McKay
Security Specialist | Splunk

splunk>

Disclaimer

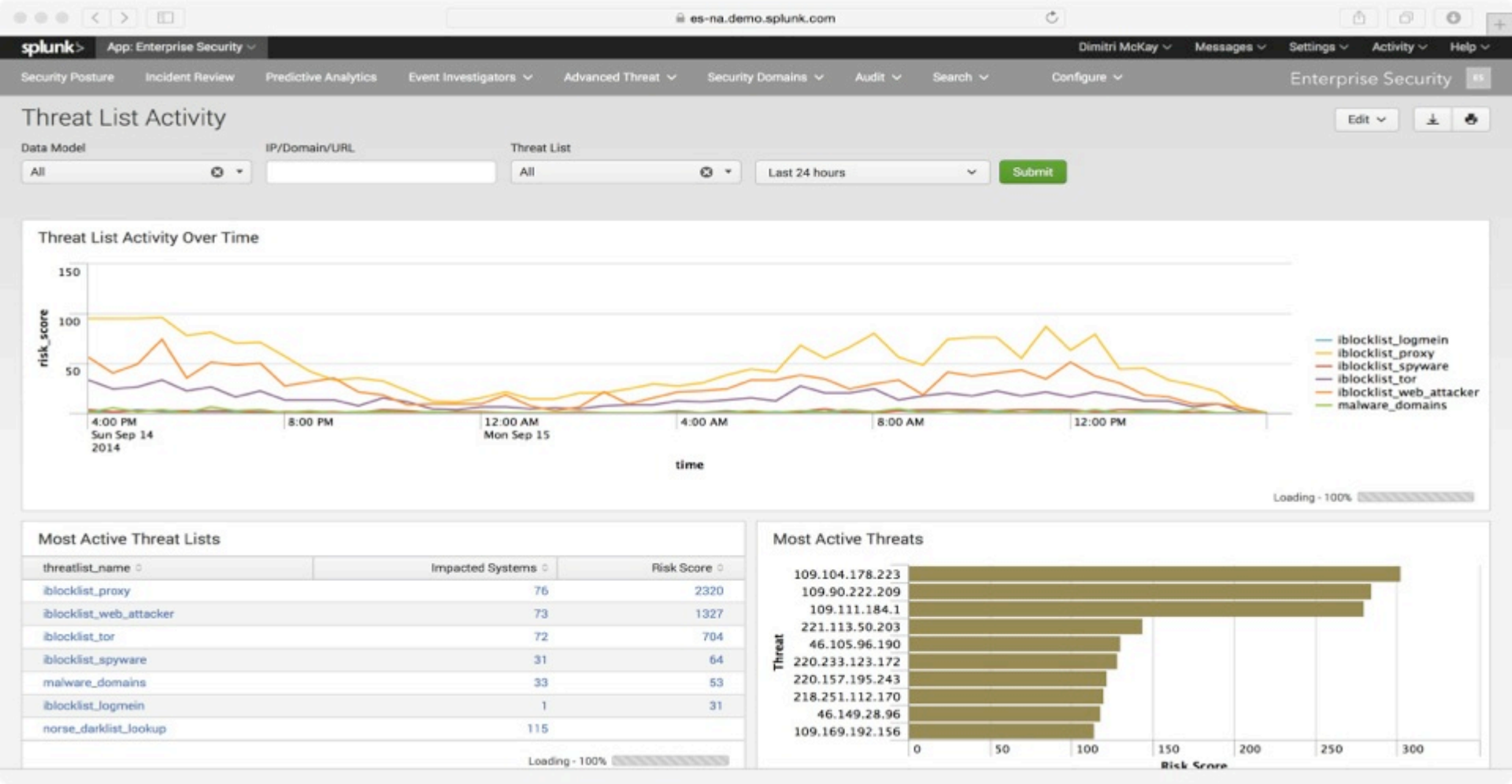
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results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

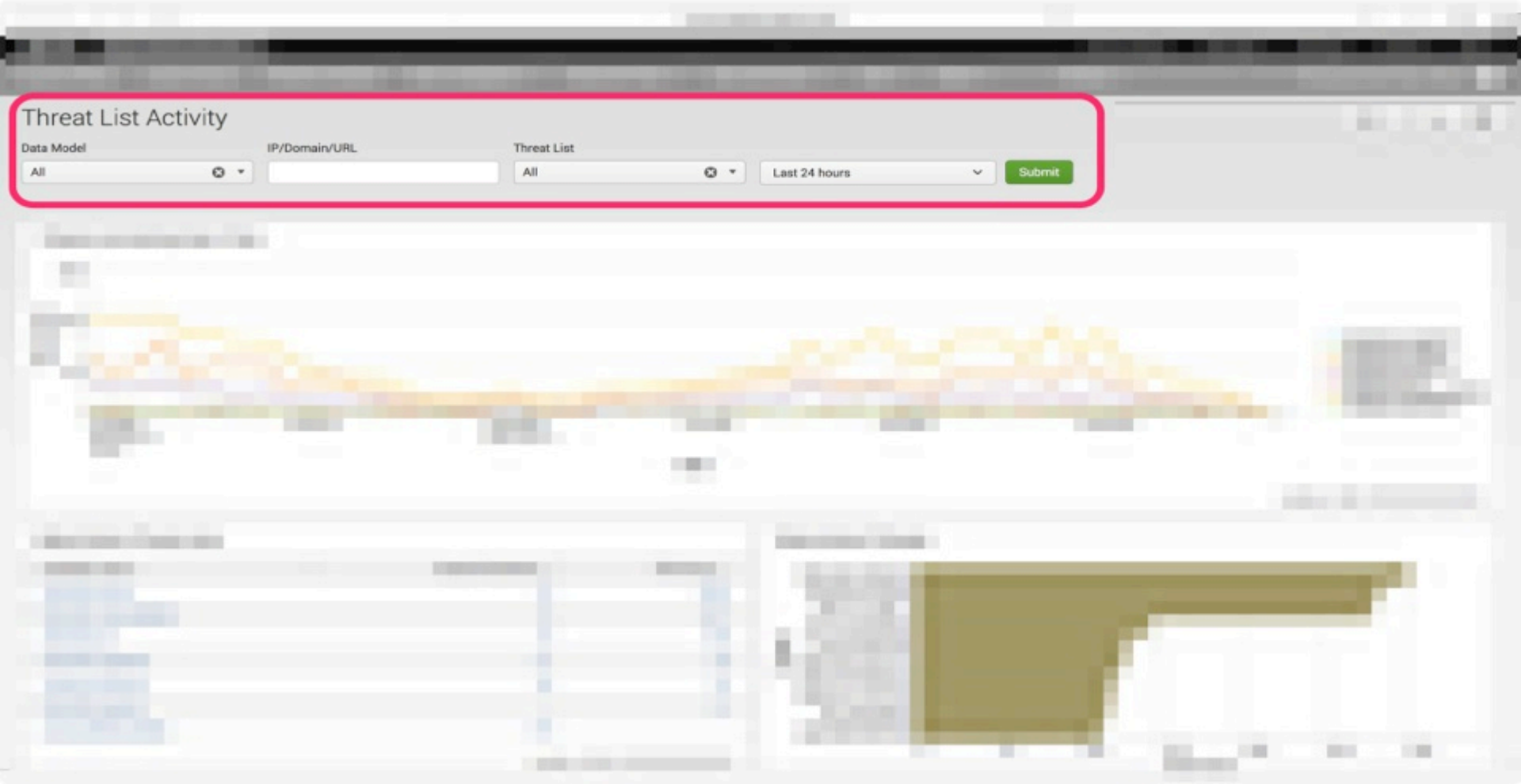
Agenda

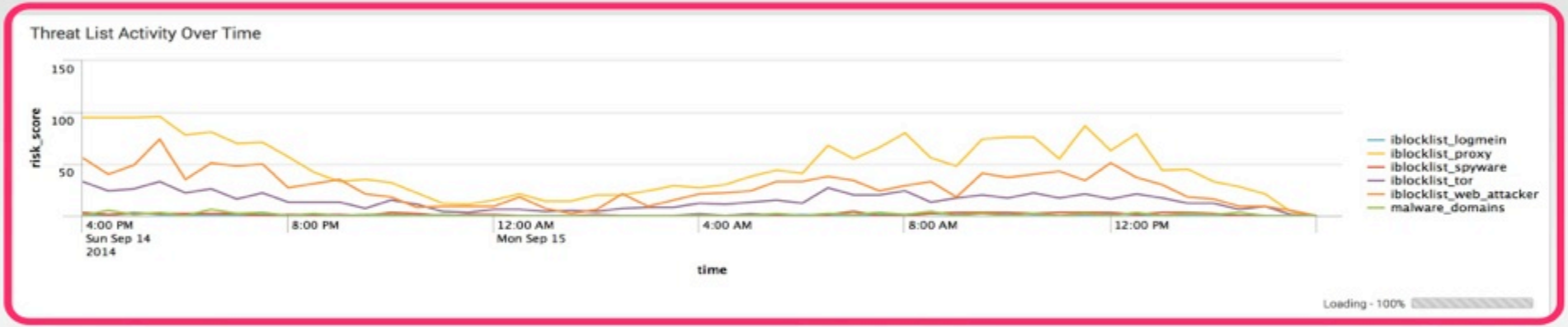
- Agenda (Hi. That's this page.)
- Risk Intelligence Framework
- Asset Investigator
- Risk Scoring Framework
- Guided Search
- Dashboard Creation via GUI
- Summary

Threat Intelligence Framework

splunk>


es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Threat List Activity
Edit
Data Model
All
IP/Domain/URL
Threat List
All
Last 24 hours
Submit
Threat List Activity Over Time
150
100
50
risk_score
4:00 PM Sun Sep 14 2014
8:00 PM
12:00 AM Mon Sep 15
4:00 AM
8:00 AM
12:00 PM
time
iblocklist_logmein
iblocklist_proxy
iblocklist_spyware
iblocklist_tor
iblocklist_web_attacker
malware_domains
Loading - 100%
Most Active Threat Lists
threatlist_name
Impacted Systems
Risk Score
iblocklist_proxy 76 2320
iblocklist_web_attacker 73 1327
iblocklist_tor 72 704
iblocklist_spyware 31 64
malware_domains 33 53
iblocklist_logmein 1 31
norse_darklist_lookup 115
Loading - 100%
Most Active Threats
109.104.178.223
109.90.222.209
109.111.184.1
221.113.50.203
46.105.96.190
220.233.123.172
220.157.195.243
218.251.112.170
46.149.28.96
109.169.192.156
Threat
0
50
100
150
200
250
300
Risk Score

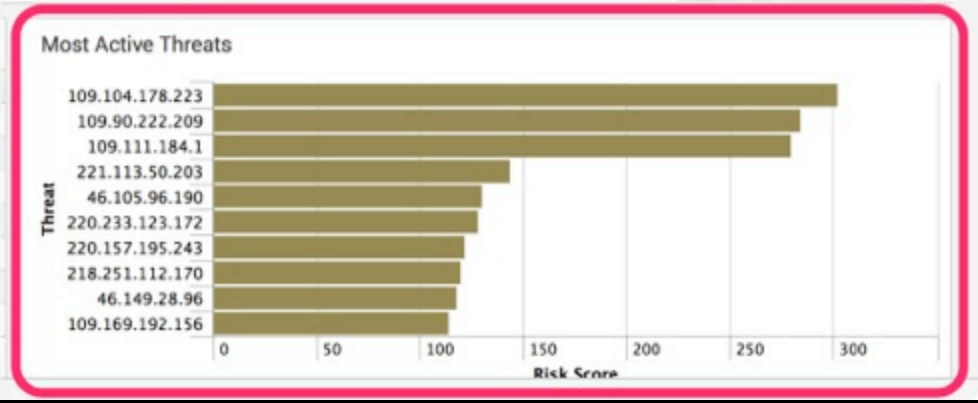

Threat List Activity
Data Model
All
IP/Domain/URL
Threat List
All
Last 24 hours
Submit


Threat List Activity Over Time
150
100
50
risk_score
4:00 PM
Sun Sep 14
2014
8:00 PM
12:00 AM
Mon Sep 15
4:00 AM
8:00 AM
12:00 PM
time
iblocklist_logmein
iblocklist_proxy
iblocklist_spyware
iblocklist_tor
iblocklist_web_attacker
malware_domains
Loading - 100%

Most Active Threat Lists

threatlist_name	Impacted Systems	Risk Score
iblocklist_proxy	76	2320
iblocklist_web_attacker	73	1327
iblocklist_tor	72	704
iblocklist_spyware	31	64
malware_domains	33	53
iblocklist_logmein	1	31
norse_darklist_lookup	115	

Loading - 100%


Most Active Threats
109.104.178.223
109.90.222.209
109.111.184.1
221.113.50.203
46.105.96.190
220.233.123.172
220.157.195.243
218.251.112.170
46.149.28.96
109.169.192.156
Threat
0
50
100
150
200
250
300
Risk Score

es-na.demo.splunk.com

splunk> App: Enterprise Security | Dimitri McKay | Messages | Settings | Activity | Help

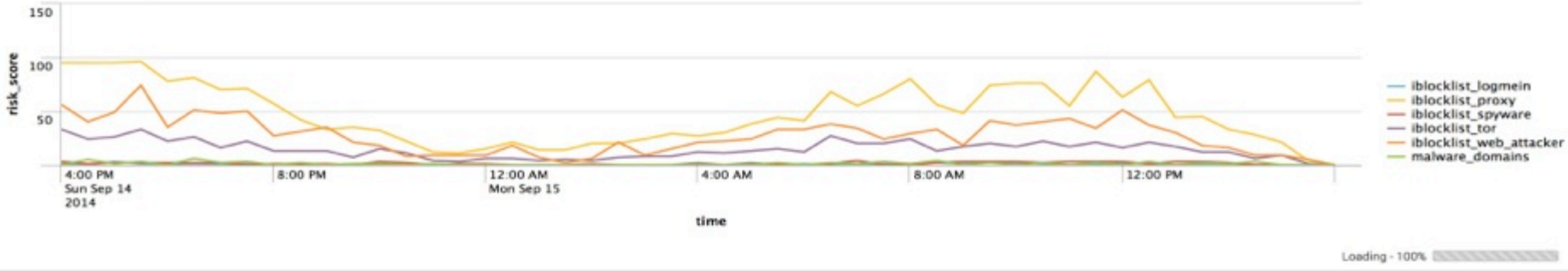
Security Posture | Incident Review | Predictive Analytics | Event Investigators | Advanced Threat | Security Domains | Audit | Search | Configure | Enterprise Security

Threat List Activity

Edit

Data Model: All | IP/Domain/URL: | Threat List: All | Last 24 hours | Submit

Threat List Activity Over Time



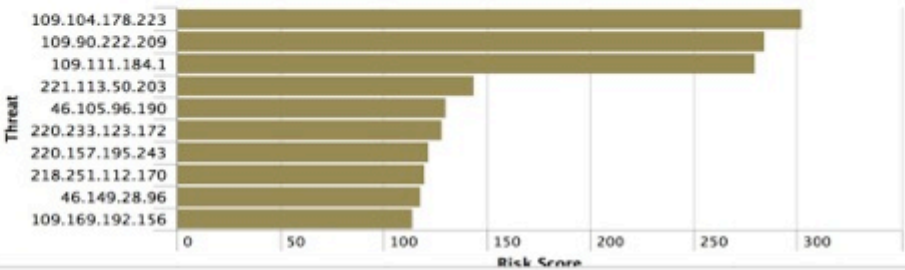
Loading - 100%

Most Active Threat Lists

threatlist_name	Impacted Systems	Risk Score
ibloclist_proxy	76	2320
ibloclist_web_attacker	73	1327
ibloclist_tor	72	704
ibloclist_spyware	31	64
malware_domains	33	53
ibloclist_logmein	1	31
norse_darklist_lookup	115	

Loading - 100%

Most Active Threats



Asset Investigator

splunk>

Edit all selected | Edit all 5 matching events

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
⌄	9/19/14 8:59:03.000 PM	Network	Vulnerability Scanner Detected (10.11.36.20)	⚠ Critical	New	unassigned	⌄

Description:

A potential vulnerability scanner was detected. 10.11.36.20 has generated events against 29 targets in the last hour. This may be indicative of a vulnerability scanner since vulnerability scanners generally trigger events against a high number of unique targets.

Correlation Search:

Network - Vulnerability Scanner Detection (by targets) - Rule

History:

View all review activity for this Notable Event

Contributing Events:

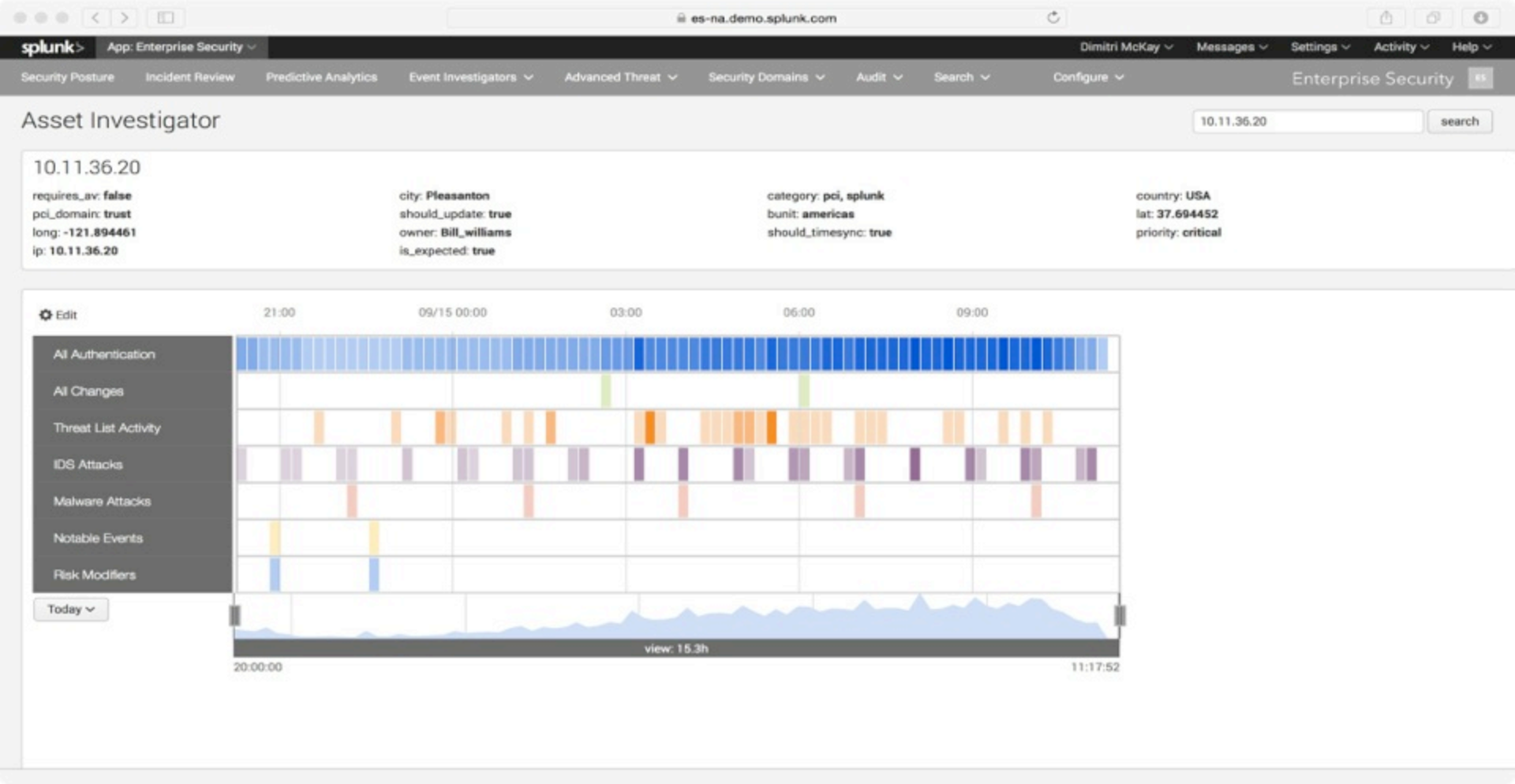
View all attack events from device 10.11.36.20

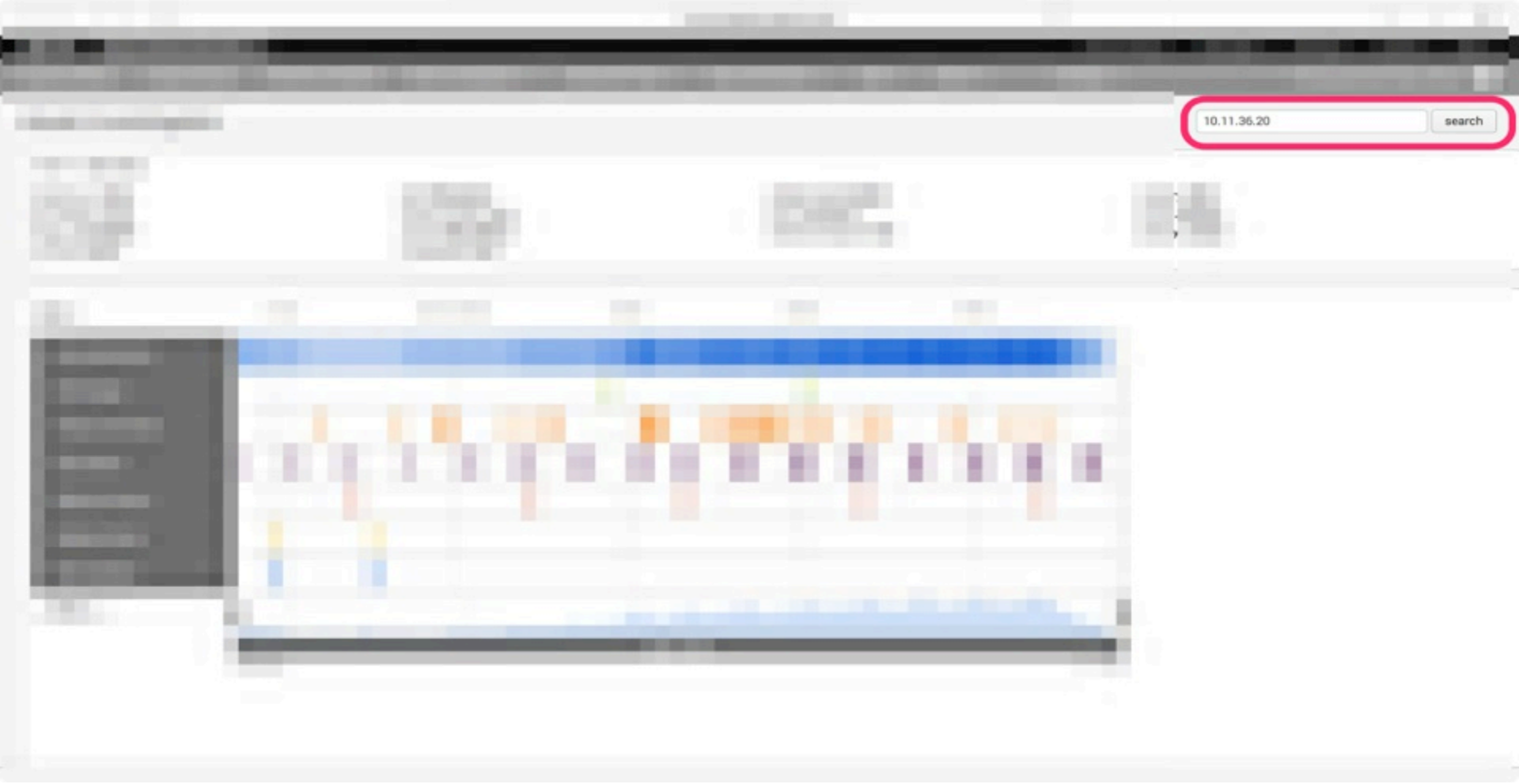
Additional Fields	Value	Action
Source	10.11.36.20	⌄
Source Business Unit		
Source Category		
Source City		
Source Country		
Source IP Address		
Source Expected		
Source Latitude		
Source Longitude		
Source Owner		
Source PCI Domain		
Source Requires Antivirus		
Source Should Time Synchr		
Source Should Update		

- Edit Tags
- Access Search (as destination)
- Access Search (as source)
- Asset Center
- Asset Investigator
- Domain Dossier
- DShield Activity Report
- Map 10.11.36.20
- Google 10.11.36.20
- Intrusion Search (as destination)

Event Details:

event_id	es-lb2-na.demo.splunk.com@@notable@@7a9a6523233cd0de2f9d872f1a9a7c52 ⌄
event_hash	7a9a6523233cd0de2f9d872f1a9a7c52 ⌄
eventtype	suppress_src ⌄
	notable ⌄


es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Asset Investigator
10.11.36.20
search
10.11.36.20
requires_av: false
pci_domain: trust
long: -121.894461
ip: 10.11.36.20
city: Pleasanton
should_update: true
owner: Bill_williams
is_expected: true
category: pci, splunk
bunit: americas
should_timesync: true
country: USA
lat: 37.694452
priority: critical
Edit
21:00
09/15 00:00
03:00
06:00
09:00
All Authentication
All Changes
Threat List Activity
IDS Attacks
Malware Attacks
Notable Events
Risk Modifiers
Today
view: 15.3h
20:00:00
11:17:52


10.11.36.20
search

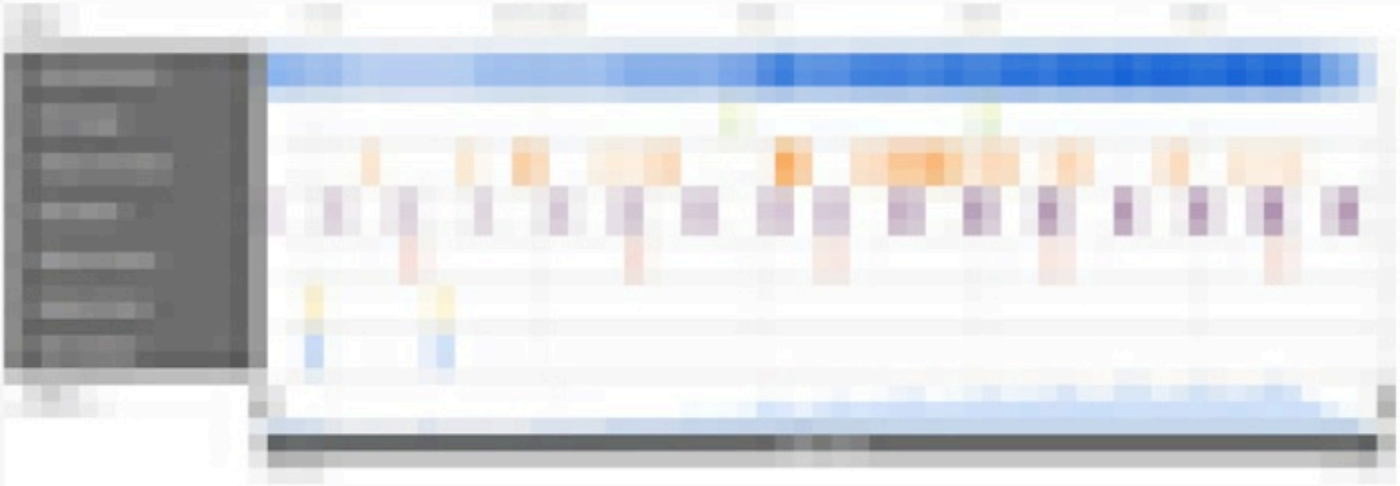
10.11.36.20

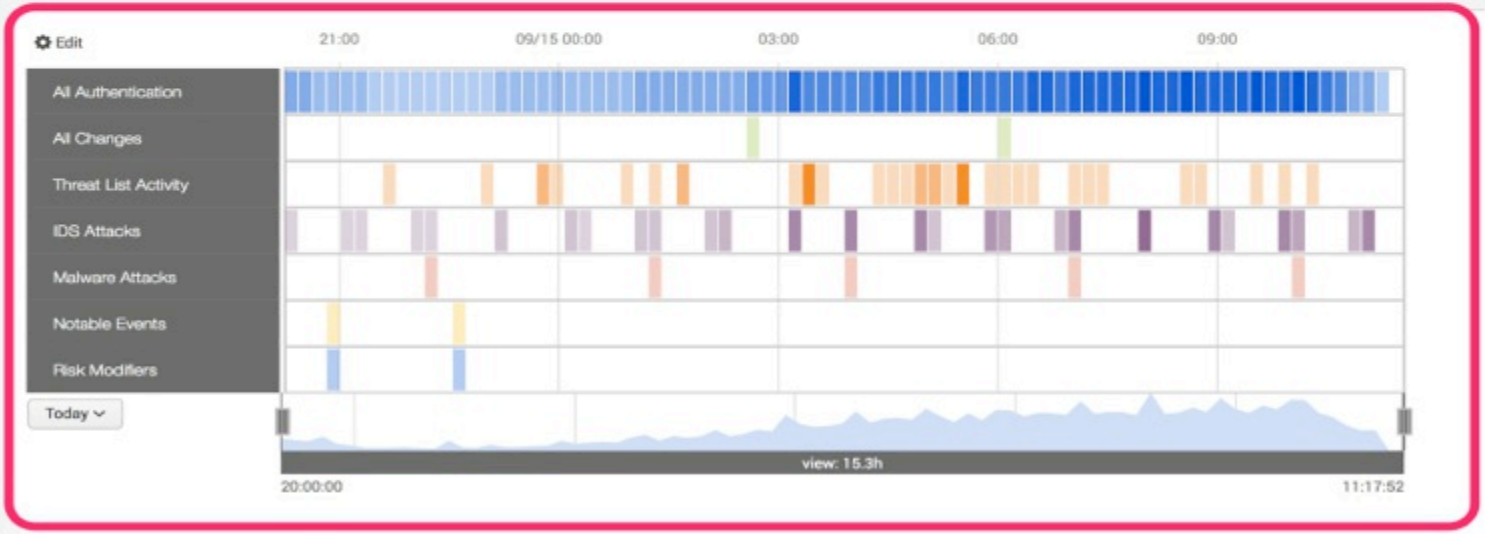
requires_av: **false**
pci_domain: **trust**
long: **-121.894461**
ip: **10.11.36.20**

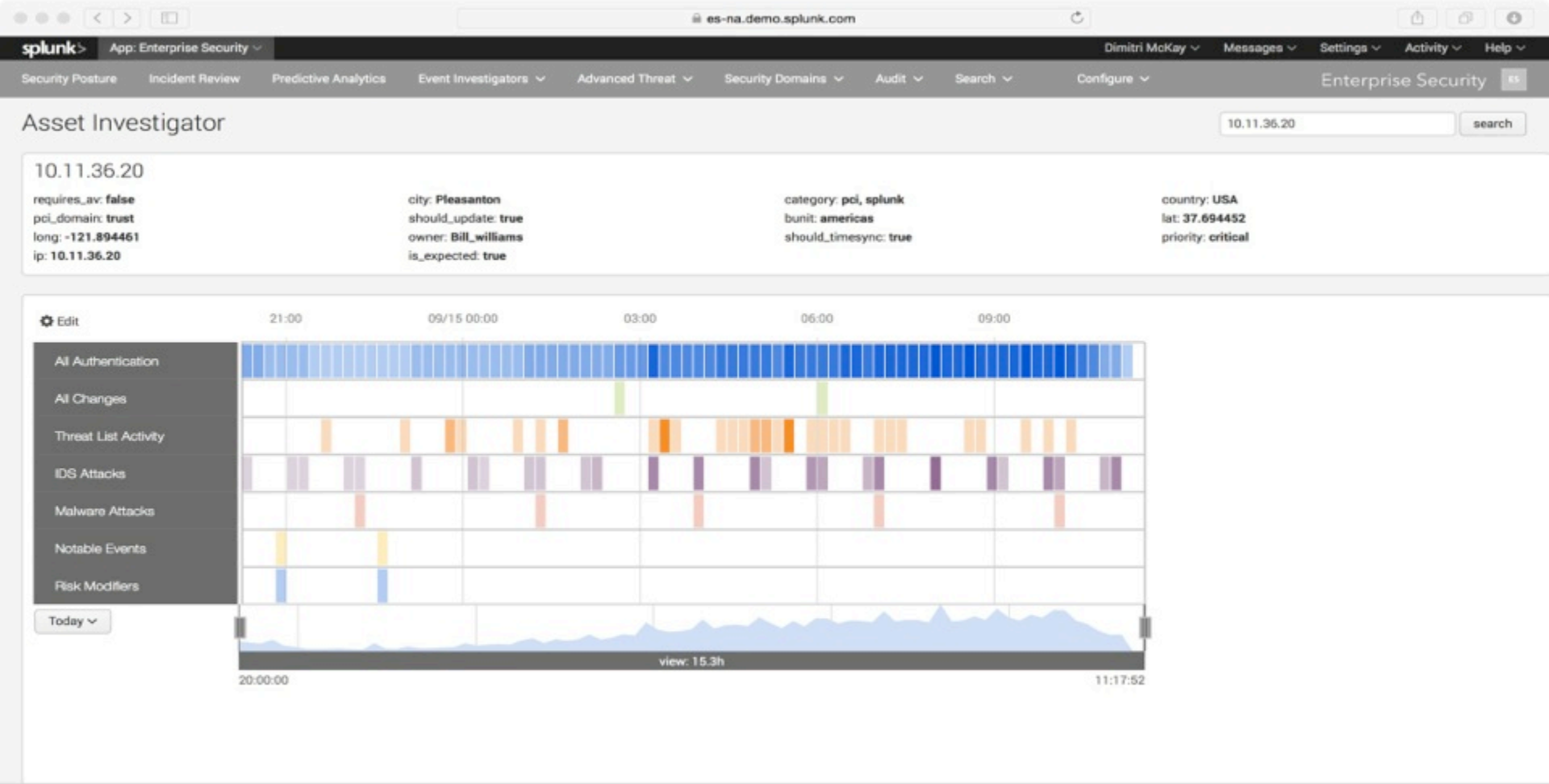
city: **Pleasanton**
should_update: **true**
owner: **Bill_williams**
is_expected: **true**

category: **pci, splunk**
bunit: **americas**
should_timesync: **true**

country: **USA**
lat: **37.694452**
priority: **critical**

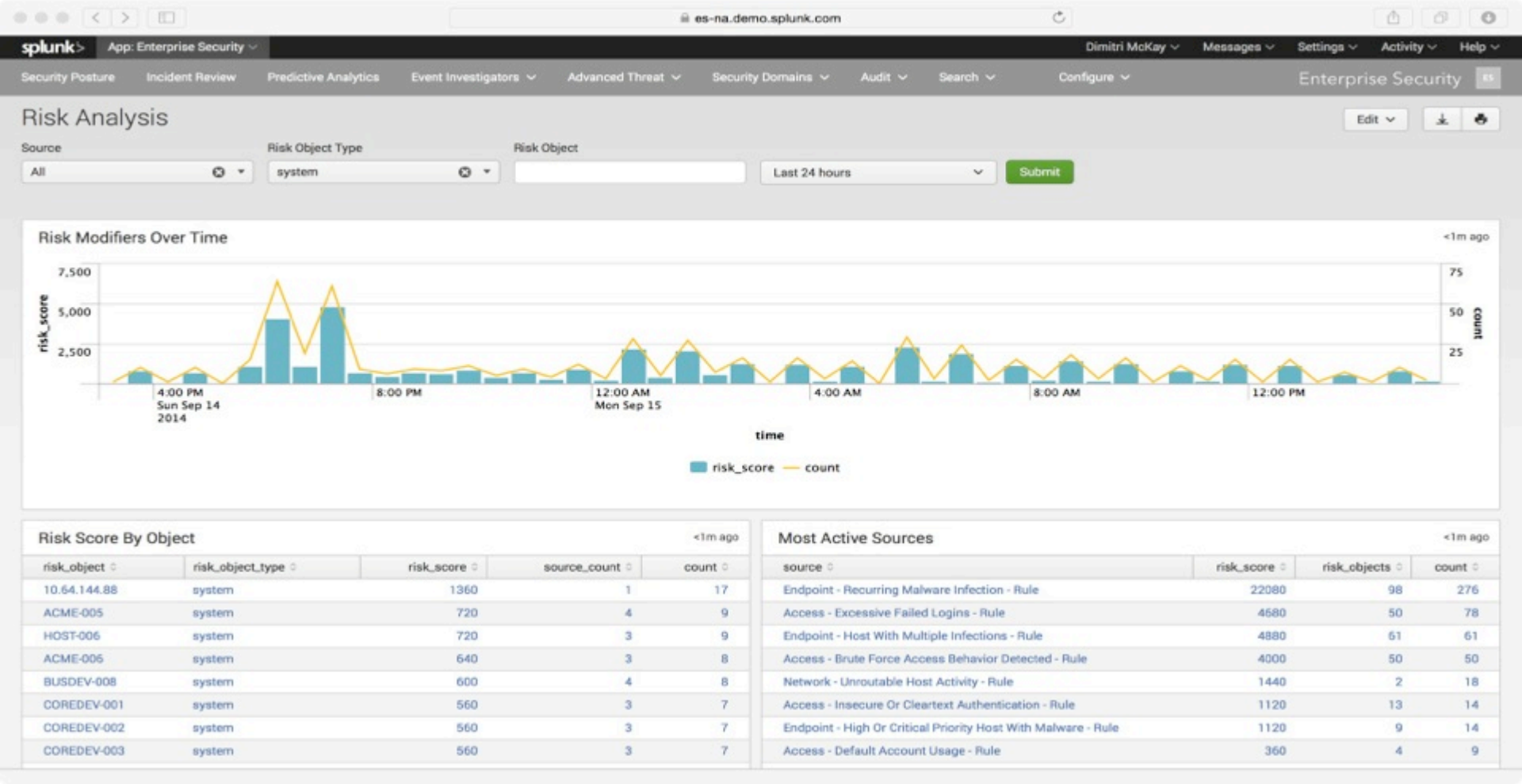


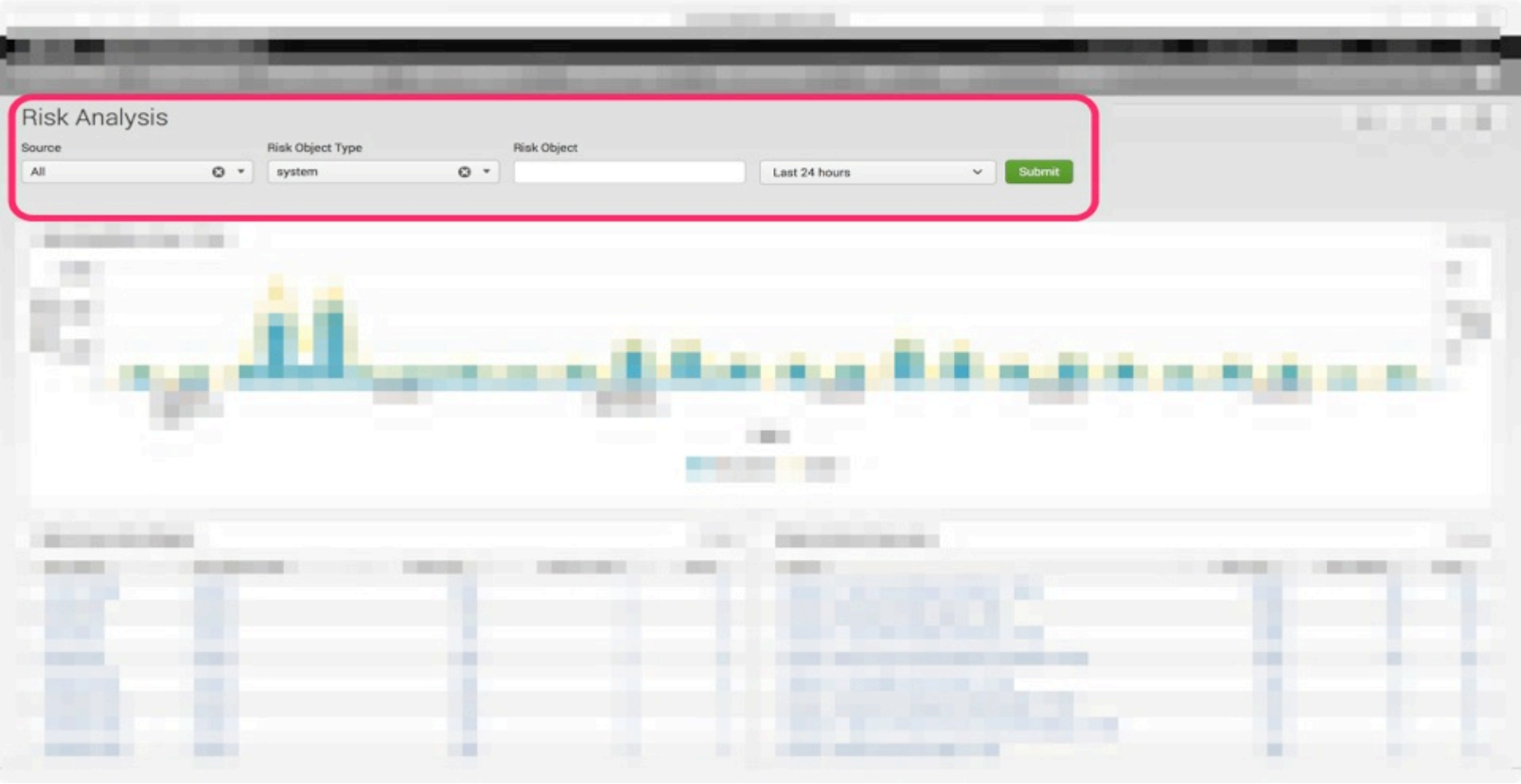

Edit
21:00
09/15 00:00
03:00
06:00
09:00
All Authentication
All Changes
Threat List Activity
IDS Attacks
Malware Attacks
Notable Events
Risk Modifiers
Today
view: 15.3h
20:00:00
11:17:52


es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay
Messages
Settings
Activity
Help
Security Posture
Incident Review
Predictive Analytics
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Asset Investigator
10.11.36.20
search
10.11.36.20
requires_av: false
pci_domain: trust
long: -121.894461
ip: 10.11.36.20
city: Pleasanton
should_update: true
owner: Bill_williams
is_expected: true
category: pci, splunk
bunit: americas
should_timesync: true
country: USA
lat: 37.694452
priority: critical
Edit
21:00
09/15 00:00
03:00
06:00
09:00
All Authentication
All Changes
Threat List Activity
IDS Attacks
Malware Attacks
Notable Events
Risk Modifiers
Today
view: 15.3h
20:00:00
11:17:52

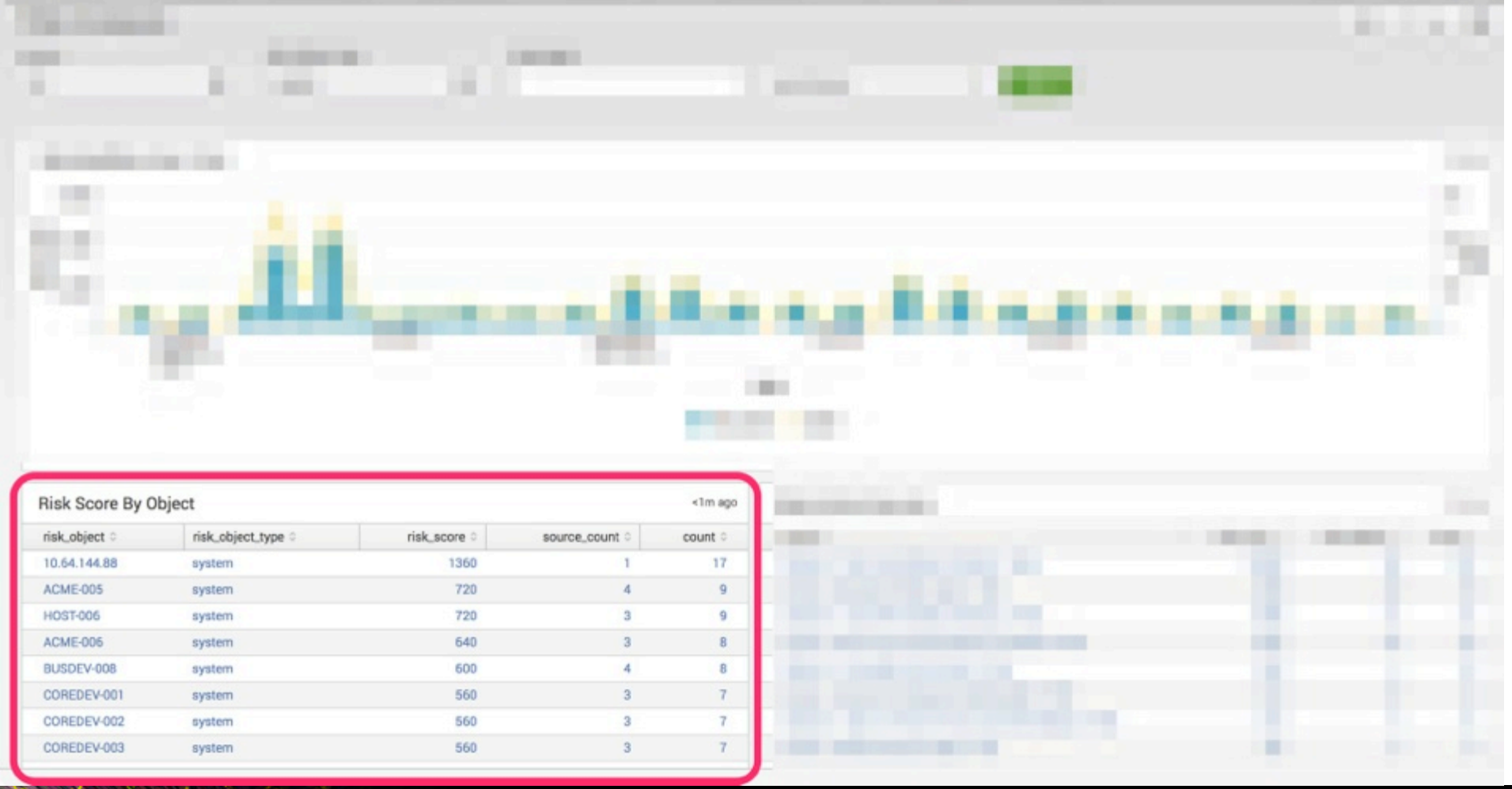
Risk Scoring Framework

splunk>


es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Risk Analysis
Edit
Source
All
Risk Object Type
system
Risk Object
Last 24 hours
Submit
Risk Modifiers Over Time
<1m ago
7,500
5,000
2,500
risk_score
75
50
25
count
4:00 PM Sun Sep 14 2014
8:00 PM
12:00 AM Mon Sep 15
4:00 AM
8:00 AM
12:00 PM
time
risk_score
count
Risk Score By Object
<1m ago
risk_object
risk_object_type
risk_score
source_count
count
10.64.144.88 system 1360 1 17
ACME-005 system 720 4 9
HOST-006 system 720 3 9
ACME-006 system 640 3 8
BUSDEV-008 system 600 4 8
COREDEV-001 system 560 3 7
COREDEV-002 system 560 3 7
COREDEV-003 system 560 3 7
Most Active Sources
<1m ago
source
risk_score
risk_objects
count
Endpoint - Recurring Malware Infection - Rule 22080 98 276
Access - Excessive Failed Logins - Rule 4680 50 78
Endpoint - Host With Multiple Infections - Rule 4880 61 61
Access - Brute Force Access Behavior Detected - Rule 4000 50 50
Network - Unroutable Host Activity - Rule 1440 2 18
Access - Insecure Or Cleartext Authentication - Rule 1120 13 14
Endpoint - High Or Critical Priority Host With Malware - Rule 1120 9 14
Access - Default Account Usage - Rule 360 4 9


Risk Analysis
Source
All
Risk Object Type
system
Risk Object
Last 24 hours
Submit


Risk Modifiers Over Time
<1m ago
7,500
5,000
2,500
risk_score
75
50
25
count
4:00 PM
Sun Sep 14
2014
8:00 PM
12:00 AM
Mon Sep 15
4:00 AM
8:00 AM
12:00 PM
time
risk_score
count



Risk Score By Object

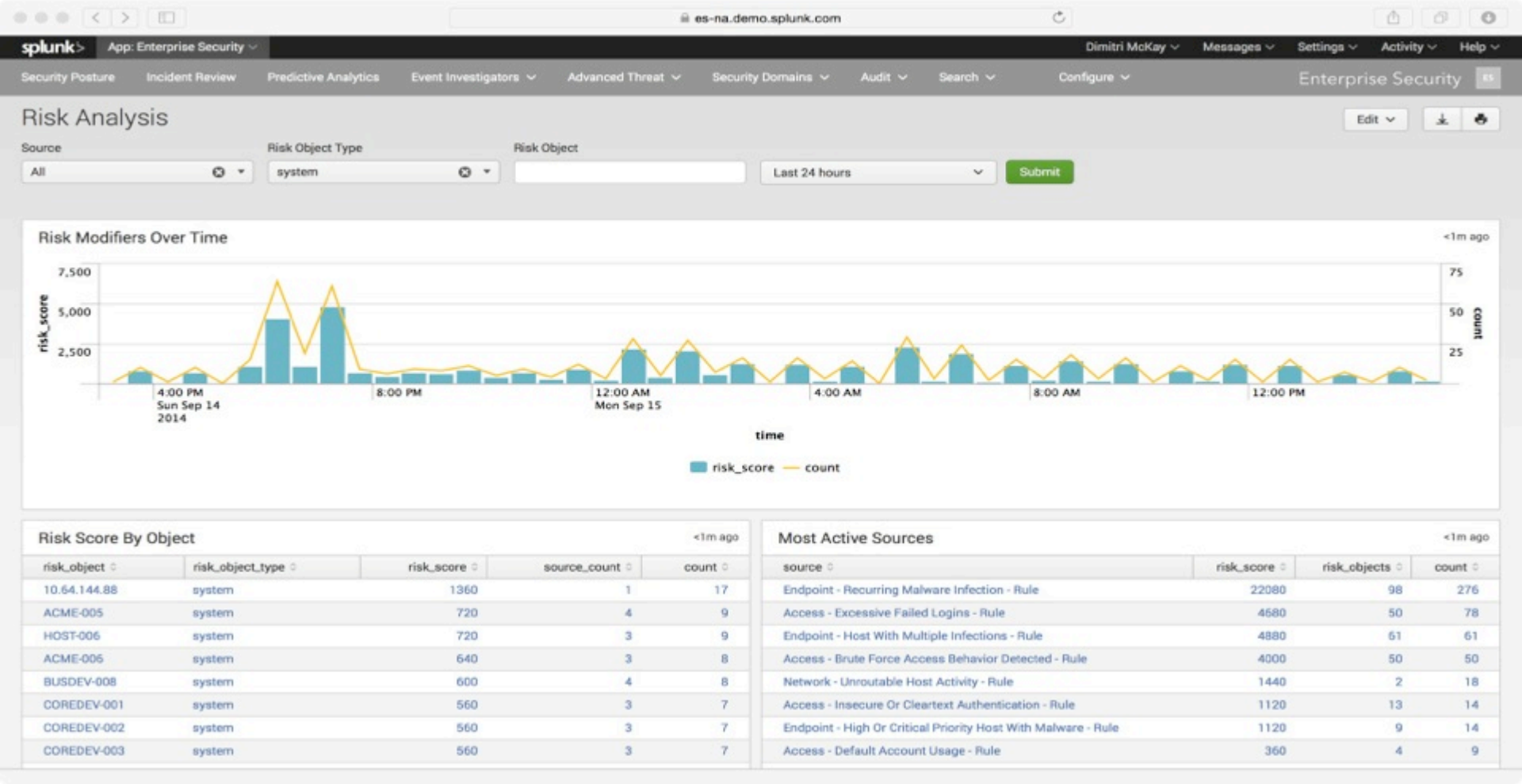
<1m ago

risk_object	risk_object_type	risk_score	source_count	count
10.64.144.88	system	1360	1	17
ACME-005	system	720	4	9
HOST-006	system	720	3	9
ACME-006	system	640	3	8
BUSDEV-008	system	600	4	8
COREDEV-001	system	560	3	7
COREDEV-002	system	560	3	7
COREDEV-003	system	560	3	7

Most Active Sources

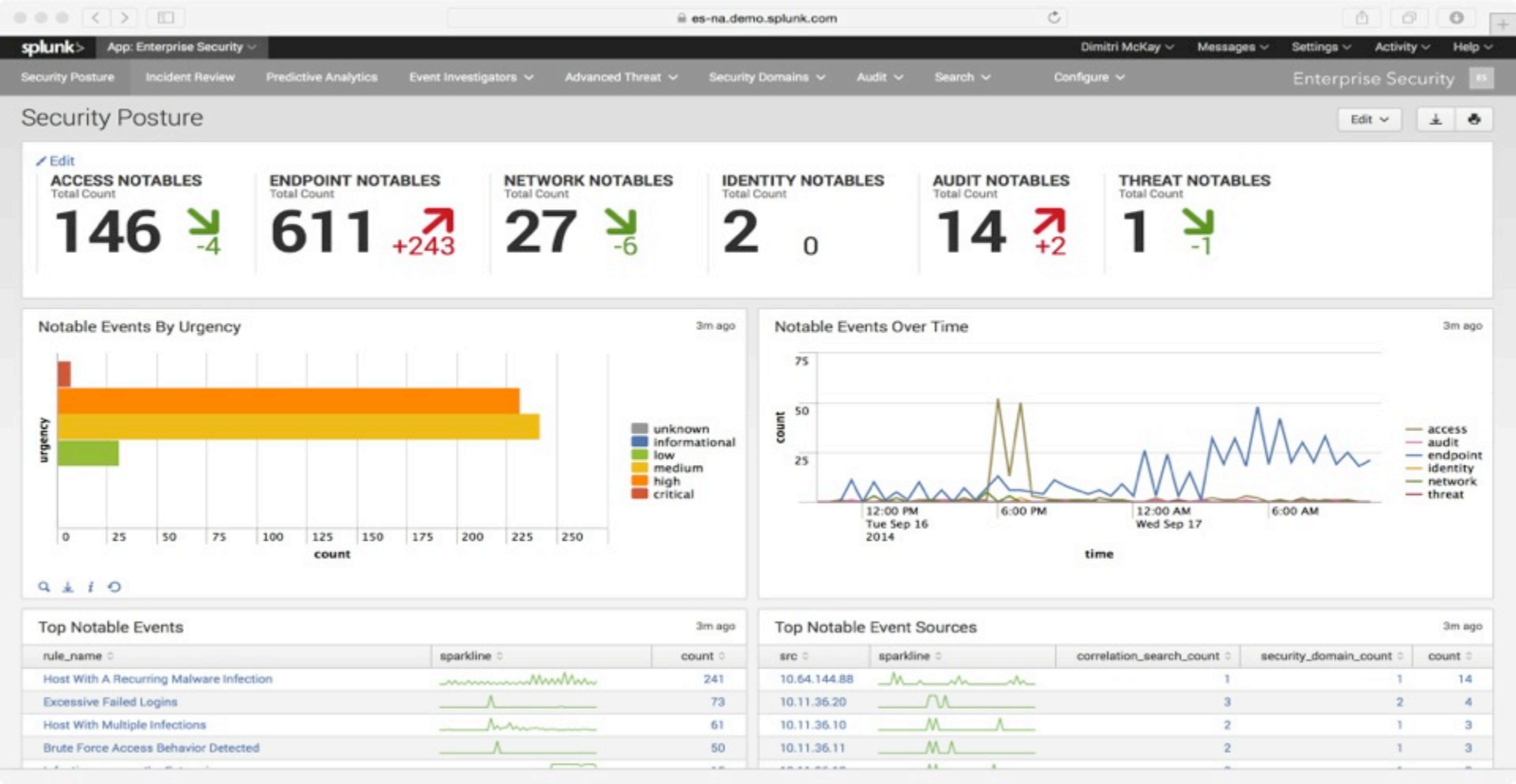
<1m ago

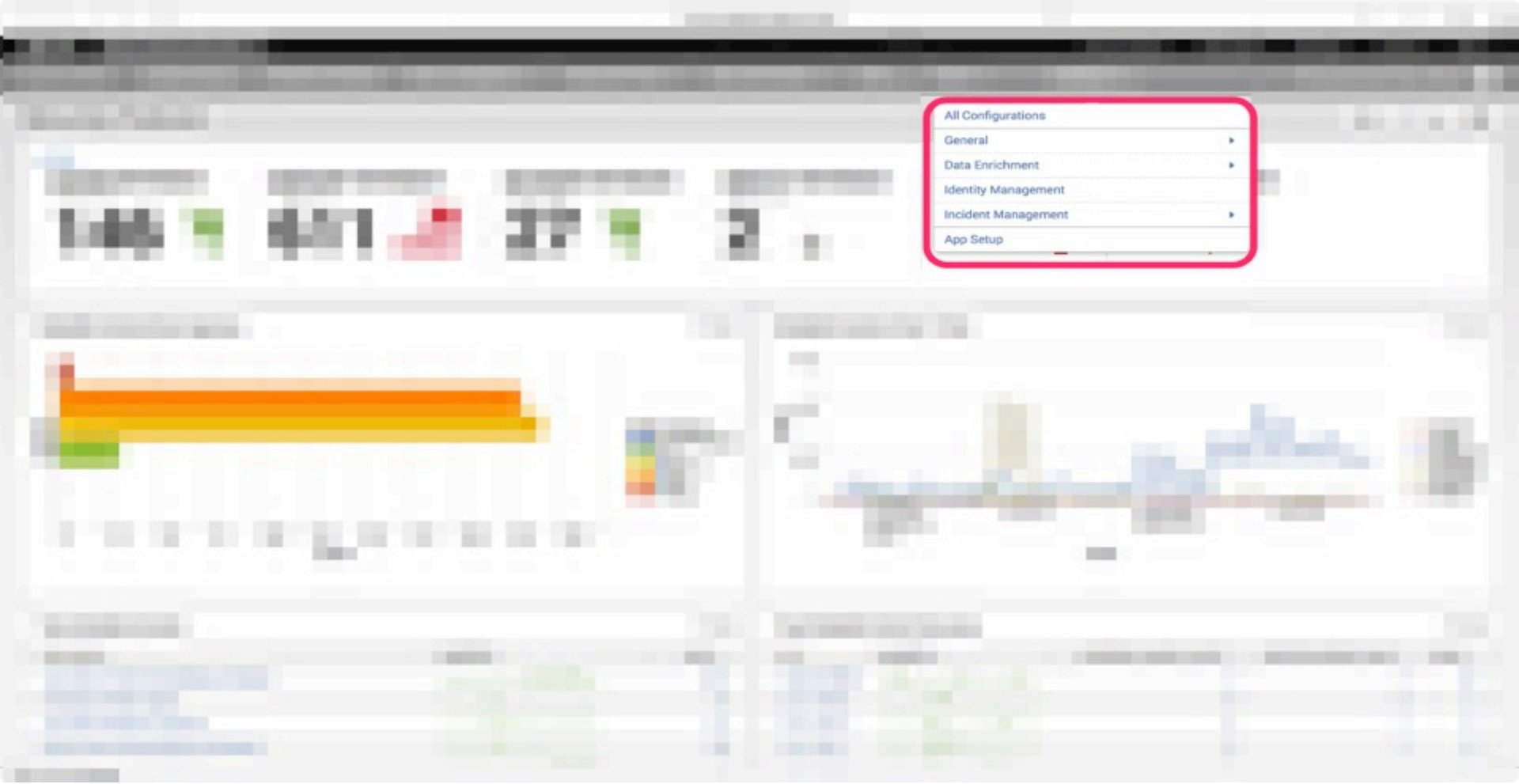
source	risk_score	risk_objects	count
Endpoint - Recurring Malware Infection - Rule	22080	98	276
Access - Excessive Failed Logins - Rule	4680	50	78
Endpoint - Host With Multiple Infections - Rule	4880	61	61
Access - Brute Force Access Behavior Detected - Rule	4000	50	50
Network - Unroutable Host Activity - Rule	1440	2	18
Access - Insecure Or Cleartext Authentication - Rule	1120	13	14
Endpoint - High Or Critical Priority Host With Malware - Rule	1120	9	14
Access - Default Account Usage - Rule	360	4	9

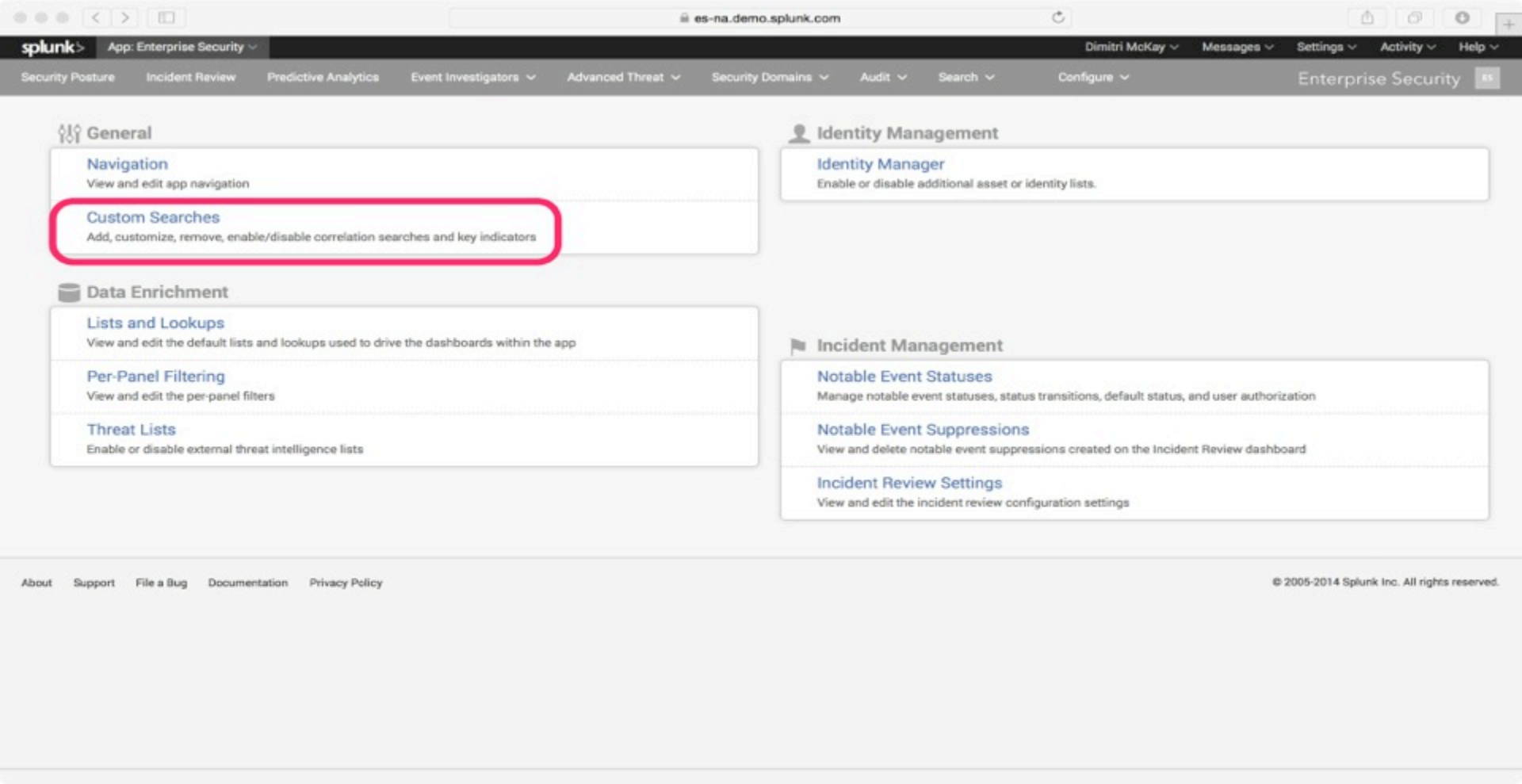

es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Risk Analysis
Edit
Source
All
Risk Object Type
system
Risk Object
Last 24 hours
Submit
Risk Modifiers Over Time
<1m ago
7,500
5,000
2,500
risk_score
75
50
25
count
4:00 PM Sun Sep 14 2014
8:00 PM
12:00 AM Mon Sep 15
4:00 AM
8:00 AM
12:00 PM
time
risk_score
count
Risk Score By Object
<1m ago
risk_object
risk_object_type
risk_score
source_count
count
10.64.144.88 system 1360 1 17
ACME-005 system 720 4 9
HOST-006 system 720 3 9
ACME-006 system 640 3 8
BUSDEV-008 system 600 4 8
COREDEV-001 system 560 3 7
COREDEV-002 system 560 3 7
COREDEV-003 system 560 3 7
Most Active Sources
<1m ago
source
risk_score
risk_objects
count
Endpoint - Recurring Malware Infection - Rule 22080 98 276
Access - Excessive Failed Logins - Rule 4680 50 78
Endpoint - Host With Multiple Infections - Rule 4880 61 61
Access - Brute Force Access Behavior Detected - Rule 4000 50 50
Network - Unroutable Host Activity - Rule 1440 2 18
Access - Insecure Or Cleartext Authentication - Rule 1120 13 14
Endpoint - High Or Critical Priority Host With Malware - Rule 1120 9 14
Access - Default Account Usage - Rule 360 4 9

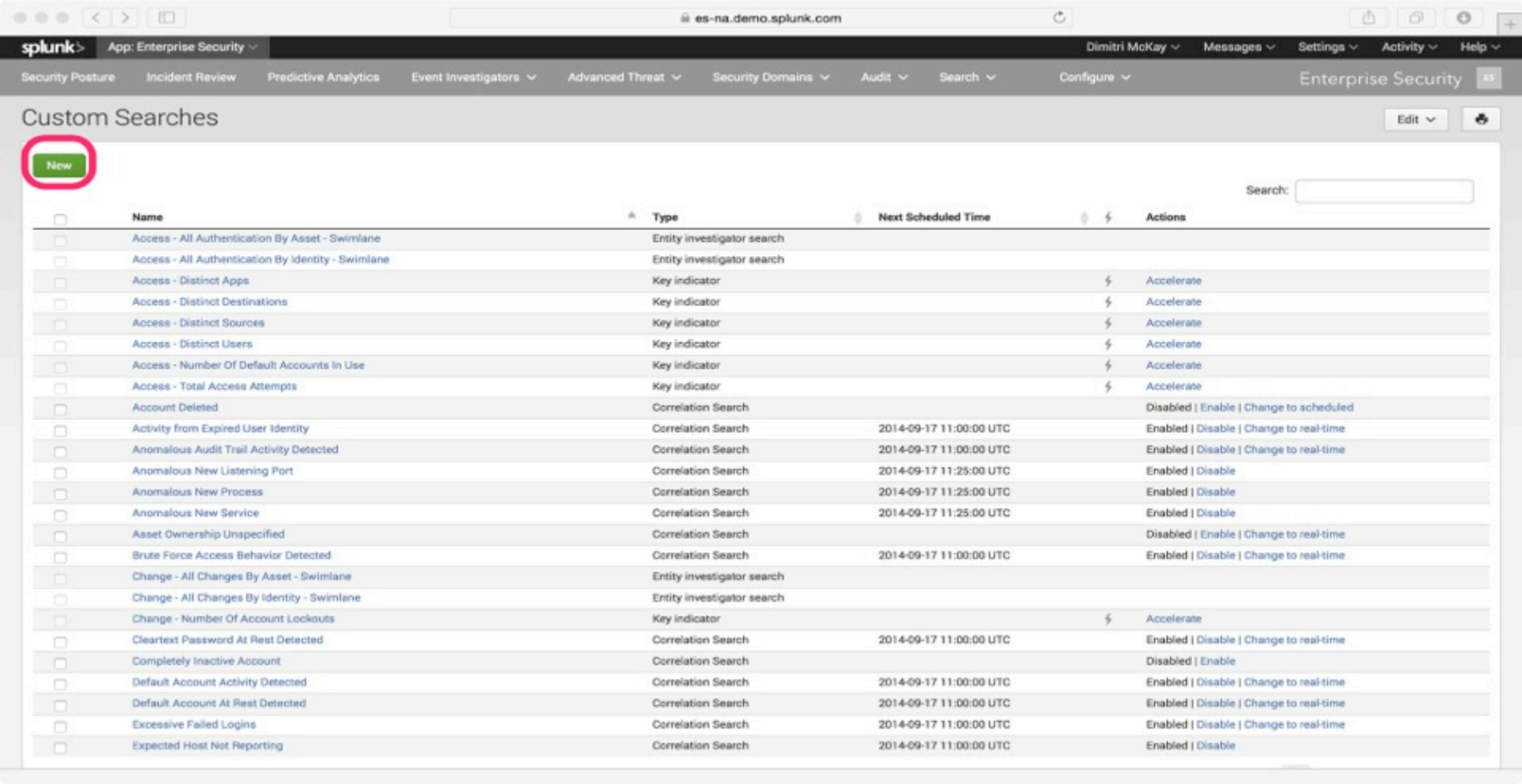
Guided Search

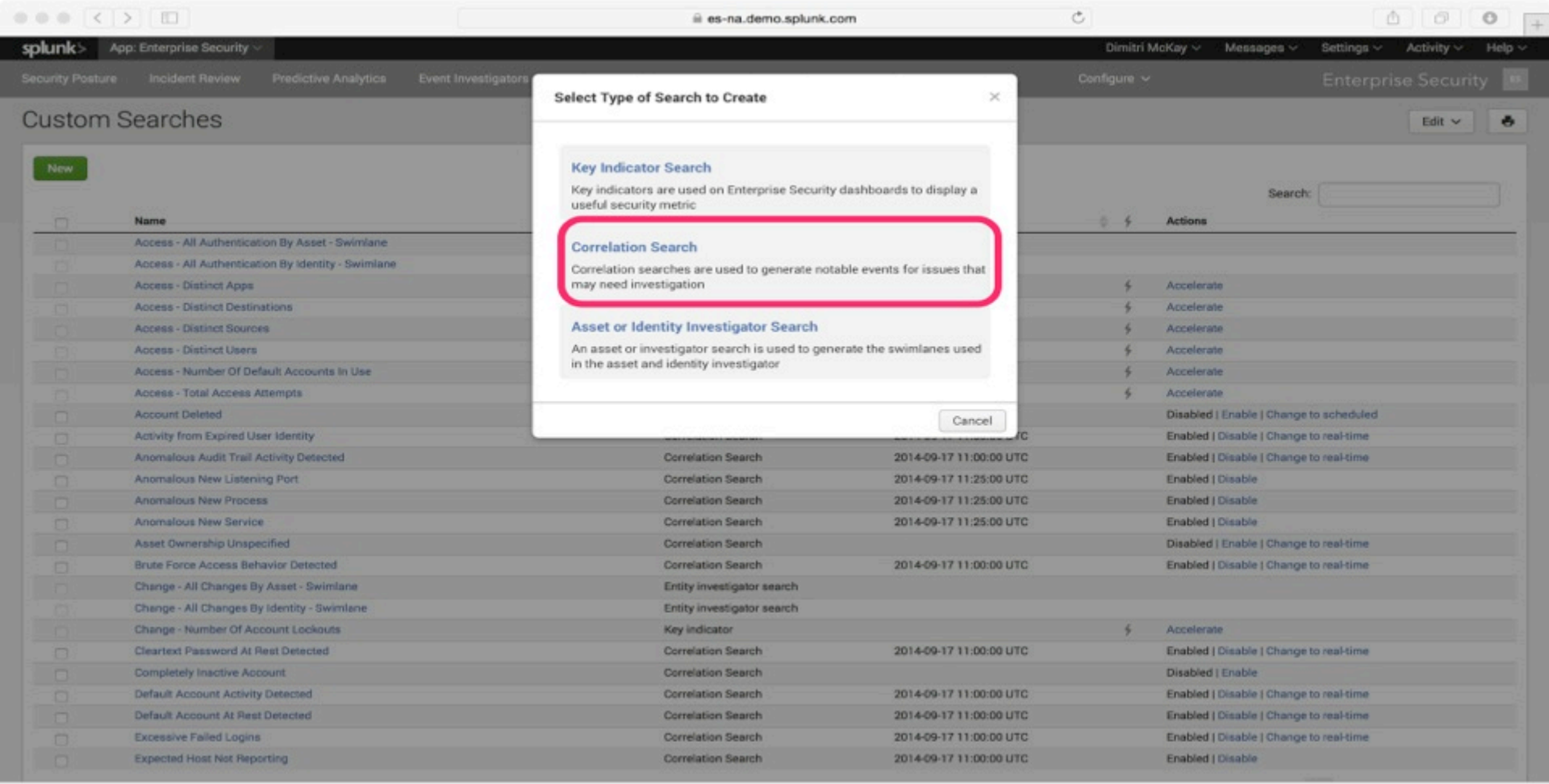
splunk>

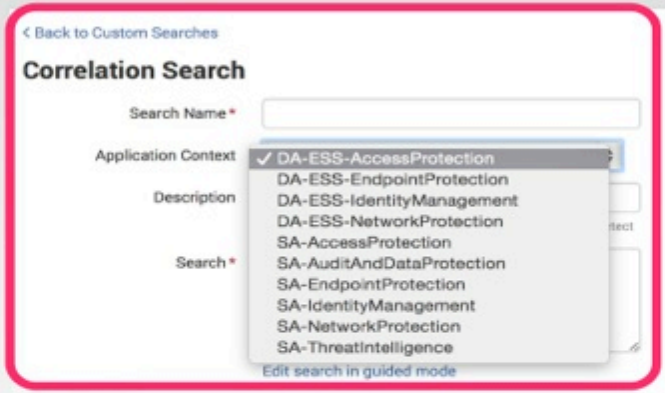

es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Security Posture
Edit
Edit
ACCESS NOTABLES
Total Count
146 -4
ENDPOINT NOTABLES
Total Count
611 +243
NETWORK NOTABLES
Total Count
27 -6
IDENTITY NOTABLES
Total Count
2 0
AUDIT NOTABLES
Total Count
14 +2
THREAT NOTABLES
Total Count
1 -1
Notable Events By Urgency
3m ago
urgency
unknown
informational
low
medium
high
critical
0 25 50 75 100 125 150 175 200 225 250
count
Notable Events Over Time
3m ago
75
50
25
count
12:00 PM Tue Sep 16 2014
6:00 PM
12:00 AM Wed Sep 17
6:00 AM
time
access
audit
endpoint
identity
network
threat
Top Notable Events
3m ago
rule_name sparkline count
Host With A Recurring Malware Infection 241
Excessive Failed Logins 73
Host With Multiple Infections 61
Brute Force Access Behavior Detected 50
Top Notable Event Sources
3m ago
src sparkline correlation_search_count security_domain_count count
10.64.144.88 1 1 14
10.11.36.20 3 2 4
10.11.36.10 2 1 3
10.11.36.11 2 1 3

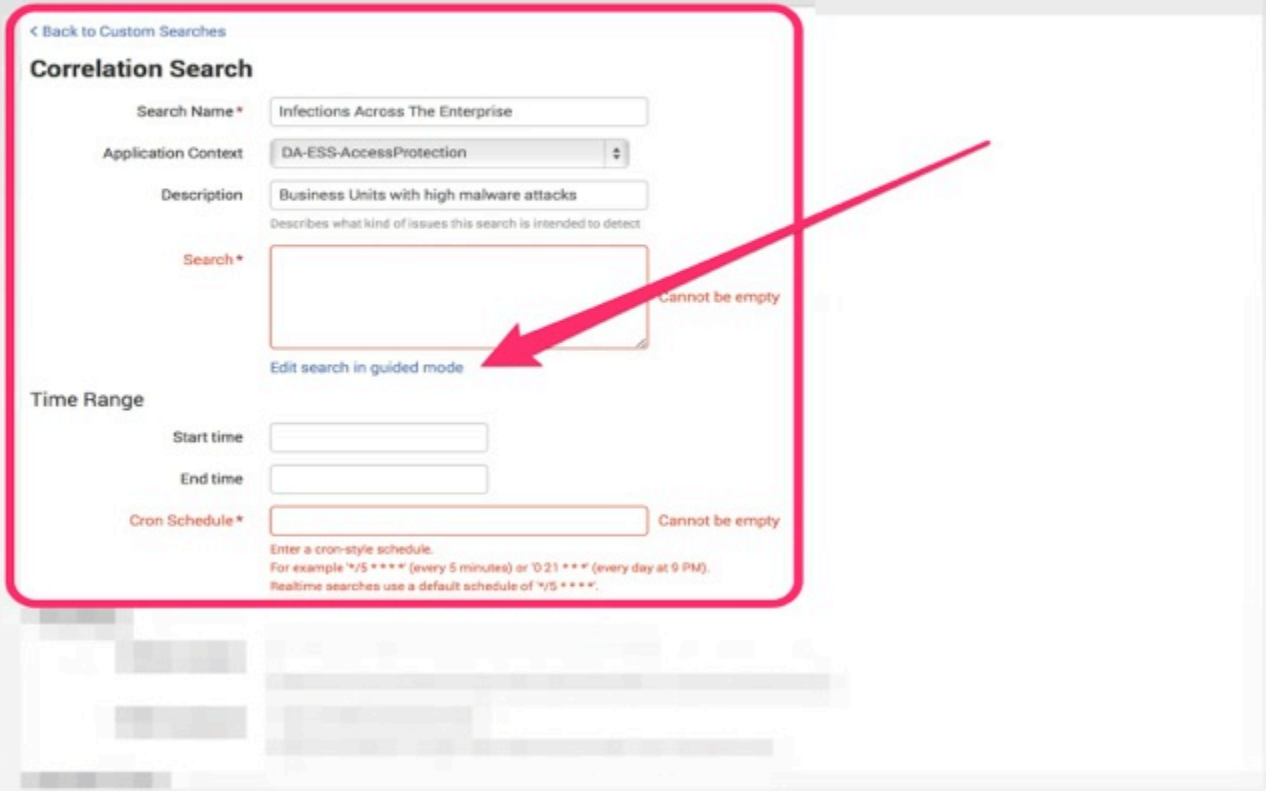

All Configurations
General
Data Enrichment
Identity Management
Incident Management
App Setup

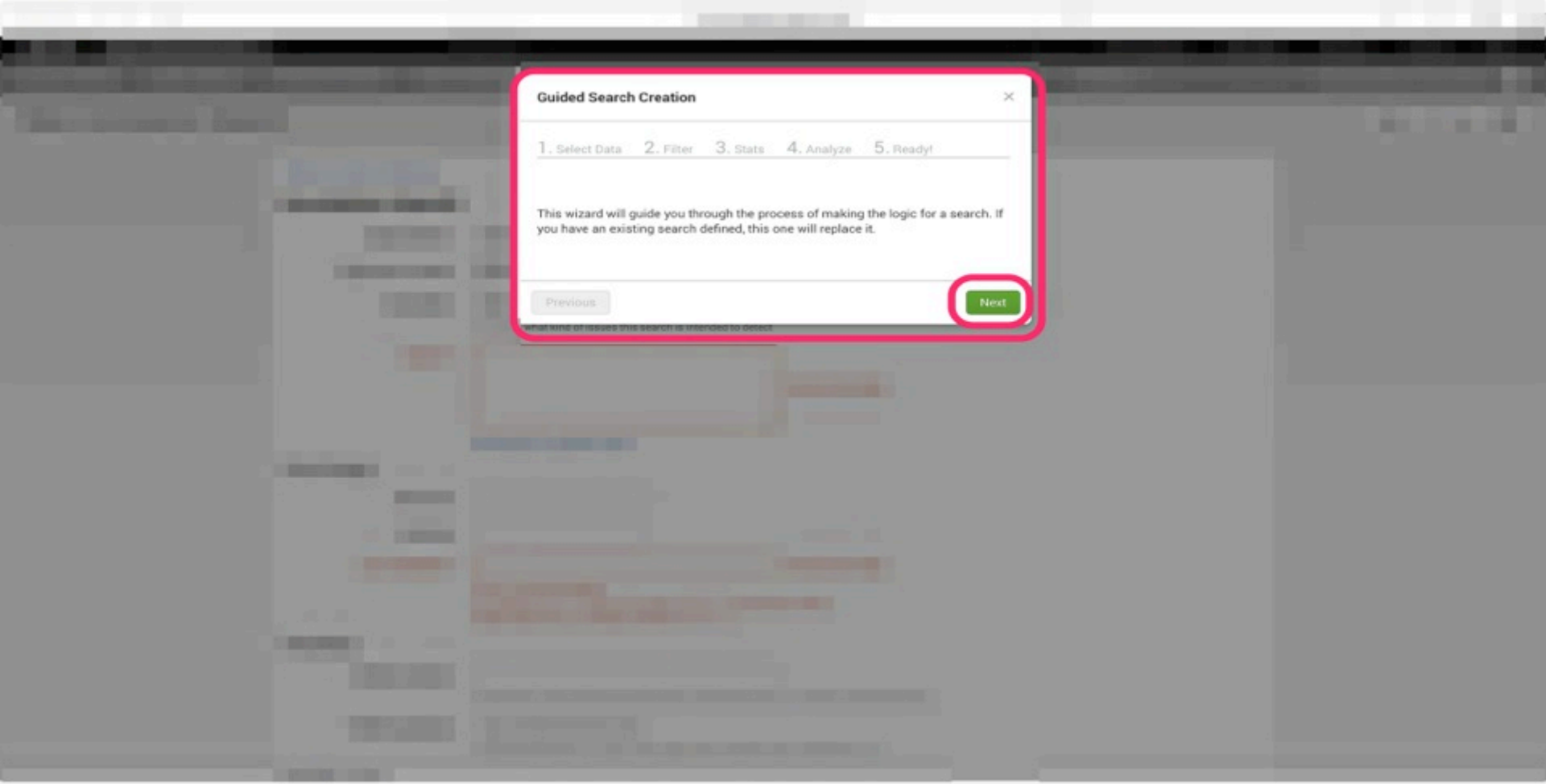

es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay
Messages
Settings
Activity
Help
Security Posture
Incident Review
Predictive Analytics
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
General
Navigation
View and edit app navigation
Custom Searches
Add, customize, remove, enable/disable correlation searches and key indicators
Data Enrichment
Lists and Lookups
View and edit the default lists and lookups used to drive the dashboards within the app
Per-Panel Filtering
View and edit the per-panel filters
Threat Lists
Enable or disable external threat intelligence lists
Identity Management
Identity Manager
Enable or disable additional asset or identity lists.
Incident Management
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
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2014 Splunk Inc. All rights reserved.

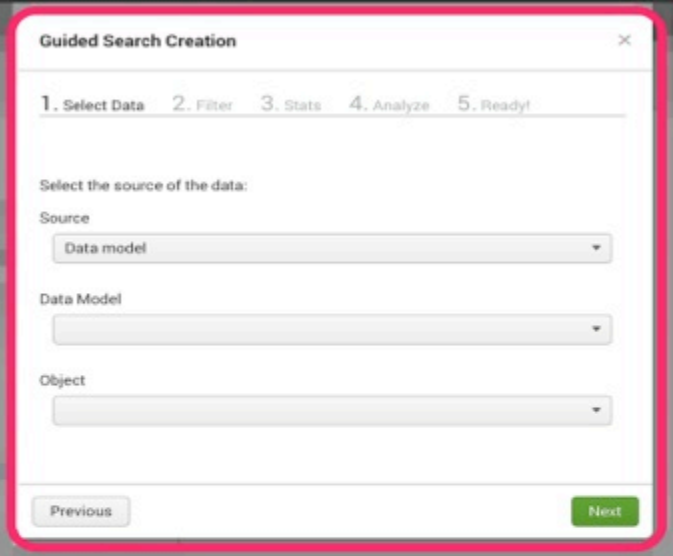

es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Custom Searches
Edit
New
Search:
Name Type Next Scheduled Time Actions
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 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Anomalous Audit Trail Activity Detected Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Anomalous New Listening Port Correlation Search 2014-09-17 11:25:00 UTC Enabled | Disable
Anomalous New Process Correlation Search 2014-09-17 11:25:00 UTC Enabled | Disable
Anomalous New Service Correlation Search 2014-09-17 11:25:00 UTC Enabled | Disable
Asset Ownership Unspecified Correlation Search Disabled | Enable | Change to real-time
Brute Force Access Behavior Detected Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
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 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Completely Inactive Account Correlation Search Disabled | Enable
Default Account Activity Detected Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Default Account At Rest Detected Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Excessive Failed Logins Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Expected Host Not Reporting Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable

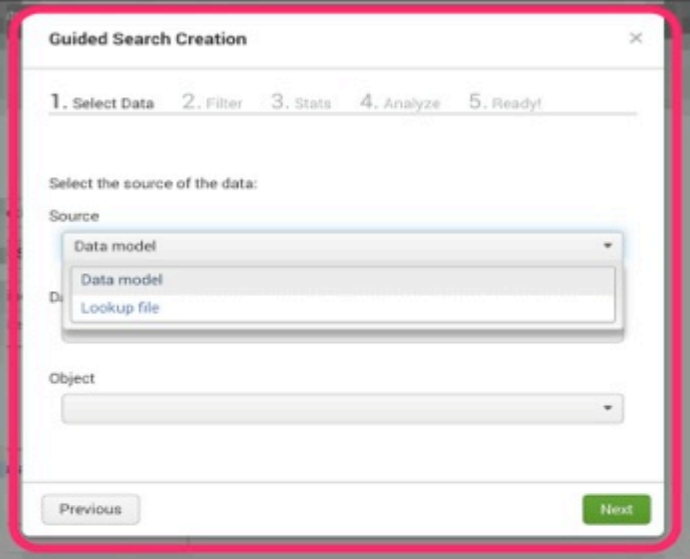

es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Configure Enterprise Security
Custom Searches
Edit
New
Search:
Select Type of Search to Create
Key Indicator Search
Key indicators 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
Name
Actions
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 Disabled | Enable | Change to scheduled
Activity from Expired User Identity Enabled | Disable | Change to real-time
Anomalous Audit Trail Activity Detected Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Anomalous New Listening Port Correlation Search 2014-09-17 11:25:00 UTC Enabled | Disable
Anomalous New Process Correlation Search 2014-09-17 11:25:00 UTC Enabled | Disable
Anomalous New Service Correlation Search 2014-09-17 11:25:00 UTC Enabled | Disable
Asset Ownership Unspecified Correlation Search Disabled | Enable | Change to real-time
Brute Force Access Behavior Detected Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
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 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Completely Inactive Account Correlation Search Disabled | Enable
Default Account Activity Detected Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Default Account At Rest Detected Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Excessive Failed Logins Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable | Change to real-time
Expected Host Not Reporting Correlation Search 2014-09-17 11:00:00 UTC Enabled | Disable

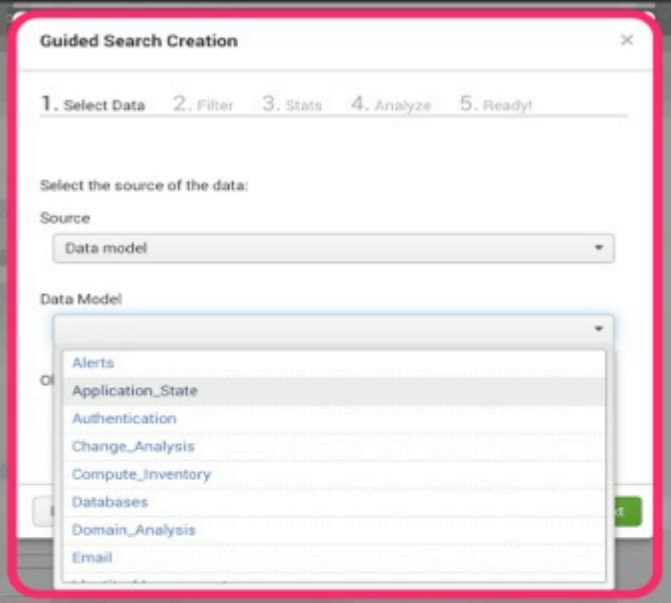

Back to Custom Searches
Correlation Search
Search Name *
Application Context
Description
Search *
DA-ESS-AccessProtection
DA-ESS-EndpointProtection
DA-ESS-IdentityManagement
DA-ESS-NetworkProtection
SA-AccessProtection
SA-AuditAndDataProtection
SA-EndpointProtection
SA-IdentityManagement
SA-NetworkProtection
SA-ThreatIntelligence
Edit search in guided mode

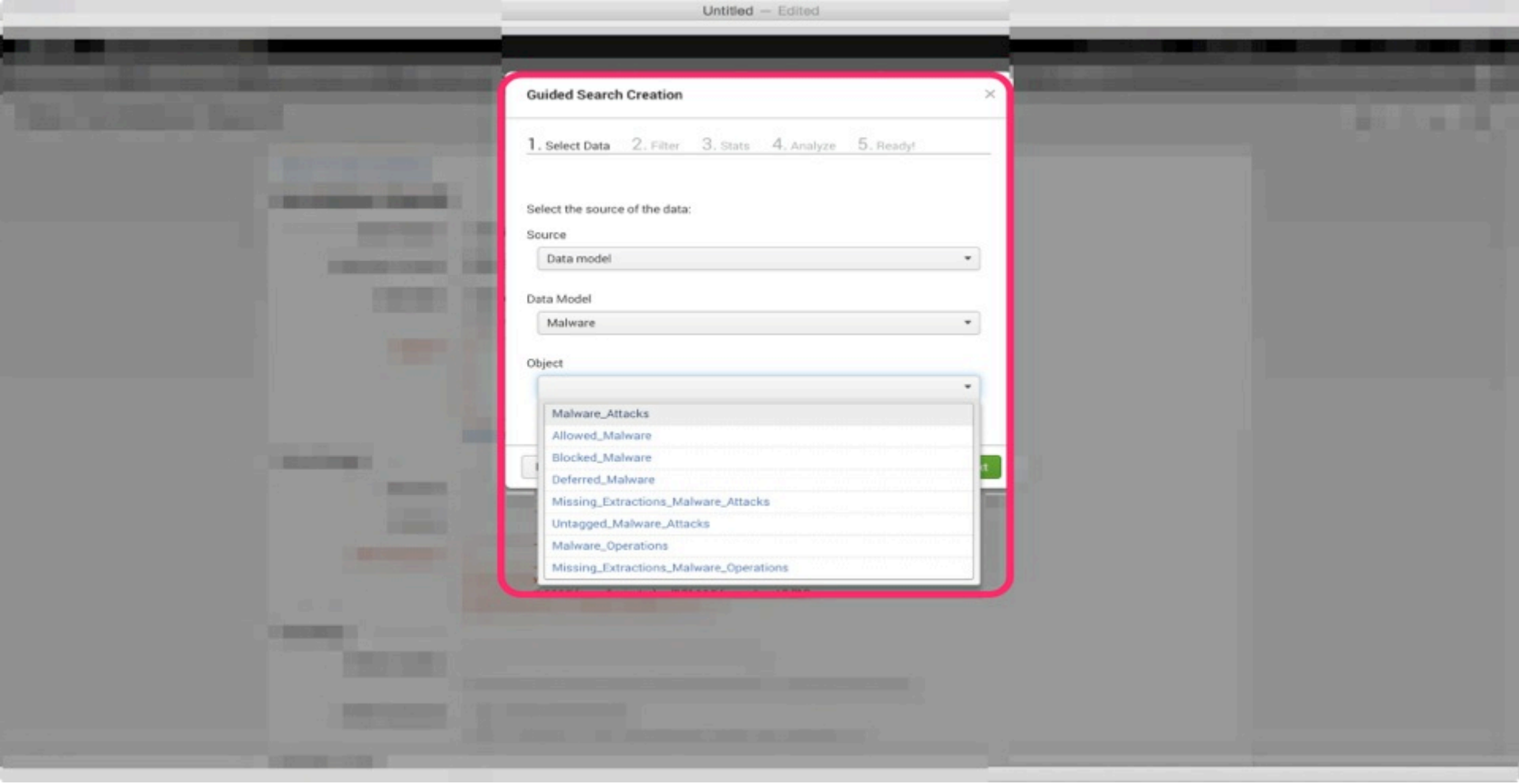

Back to Custom Searches
Correlation Search
Search Name *
Infections Across The Enterprise
Application Context
DA-ESS-AccessProtection
Description
Business Units with high malware attacks
Describes what kind of issues this search is intended to detect
Search *
Cannot be empty
Edit search in guided mode
Time Range
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 * * * *'.

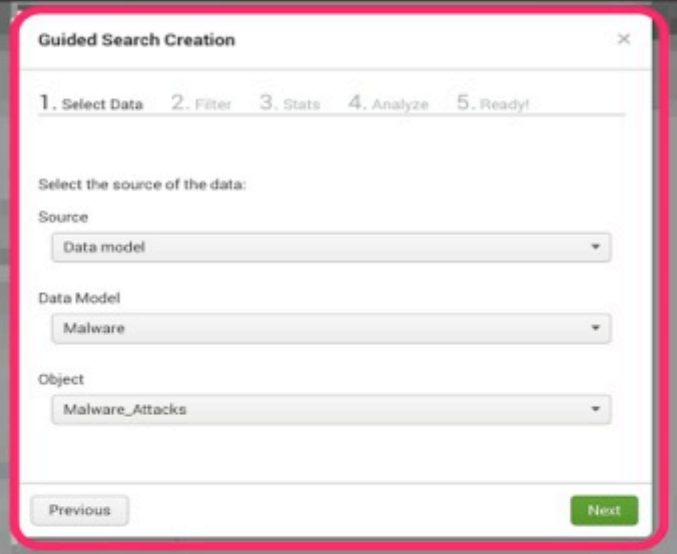

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
This wizard will guide you through the process of making the logic for a search. If you have an existing search defined, this one will replace it.
Previous
Next

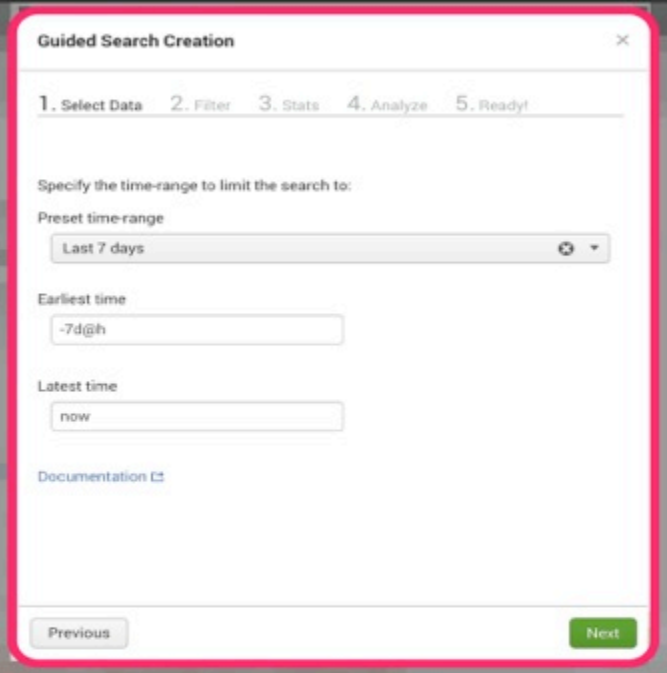

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Select the source of the data:
Source
Data model
Data Model
Object
Previous
Next

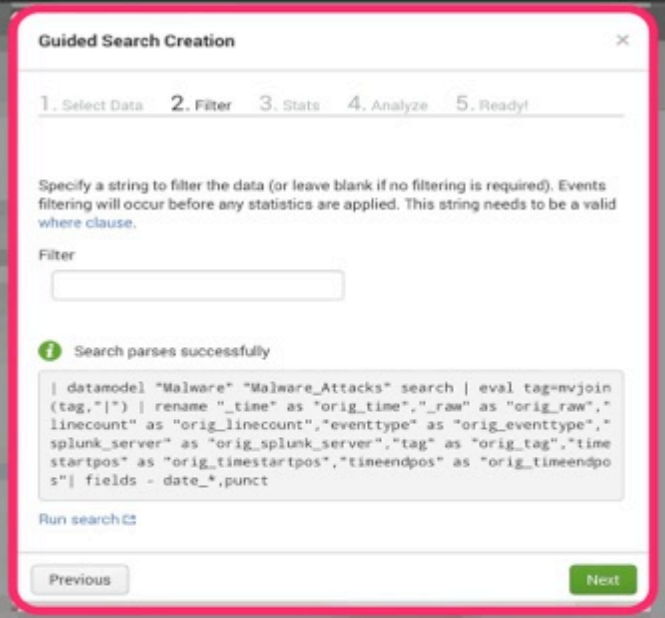

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Select the source of the data:
Source
Data model
Data model
Lookup file
Object
Previous
Next

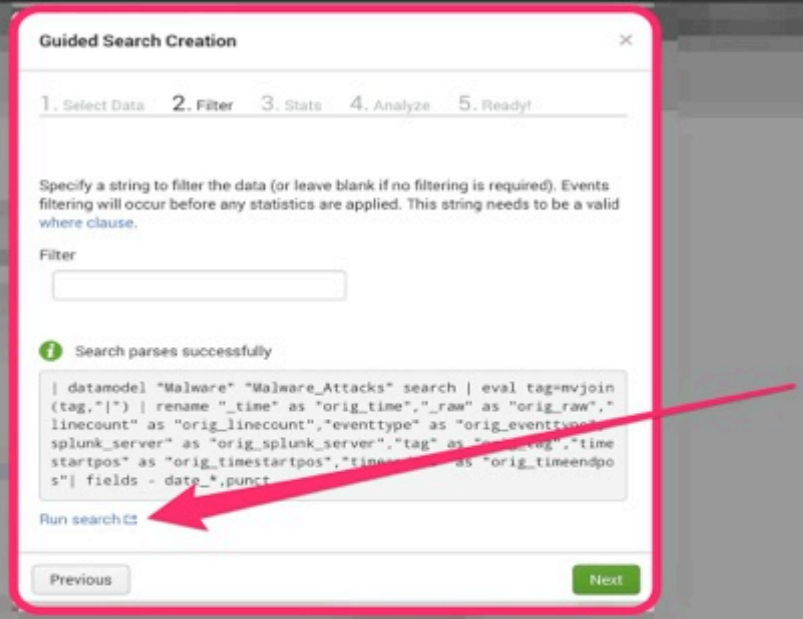

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Select the source of the data:
Source
Data model
Data Model
Alerts
Application_State
Authentication
Change_Analysis
Compute_Inventory
Databases
Domain_Analysis
Email

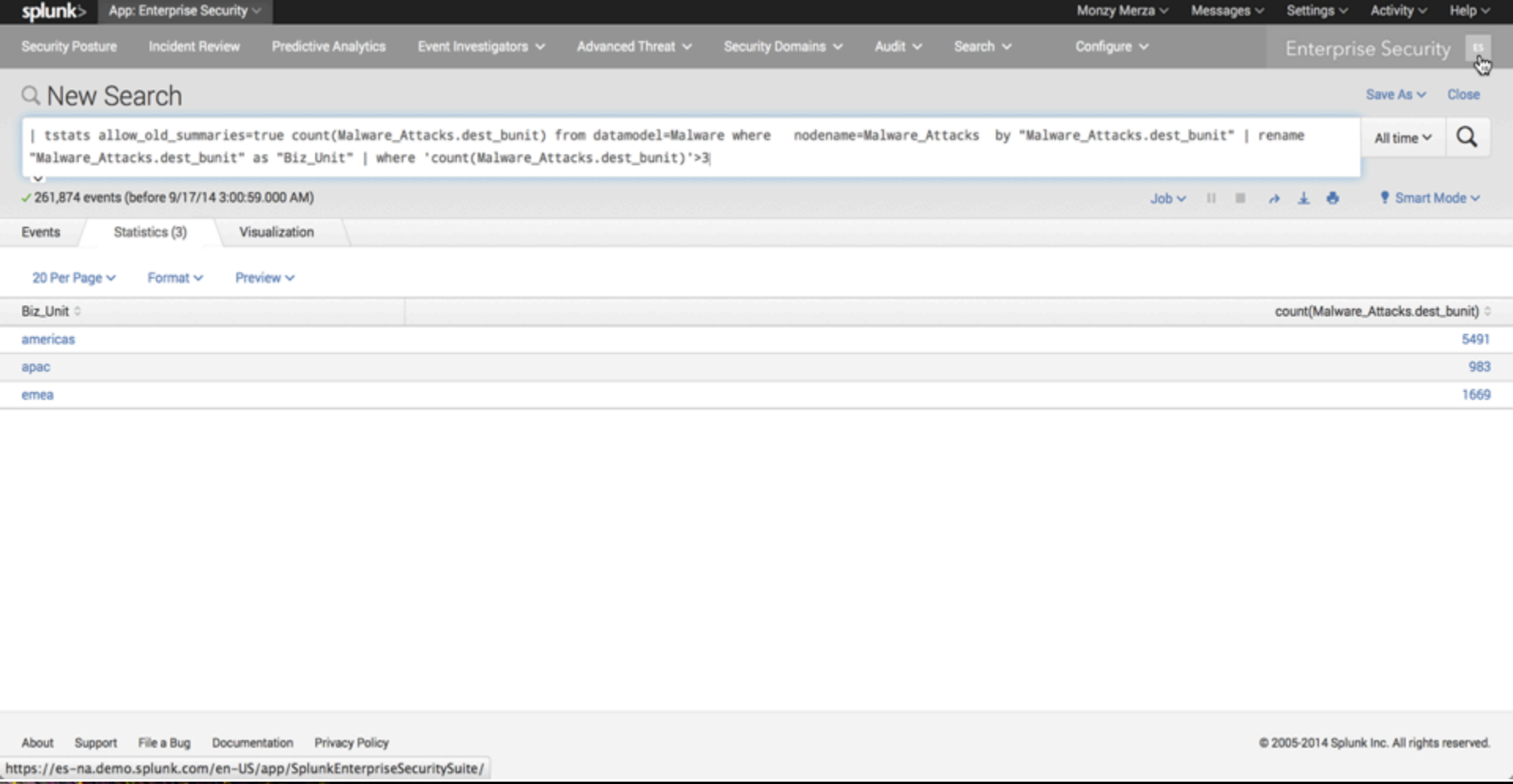

Untitled — Edited
Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Select the source of the data:
Source
Data model
Data Model
Malware
Object
Malware_Attacks
Allowed_Malware
Blocked_Malware
Deferred_Malware
Missing_Extractions_Malware_Attacks
Untagged_Malware_Attacks
Malware_Operations
Missing_Extractions_Malware_Operations

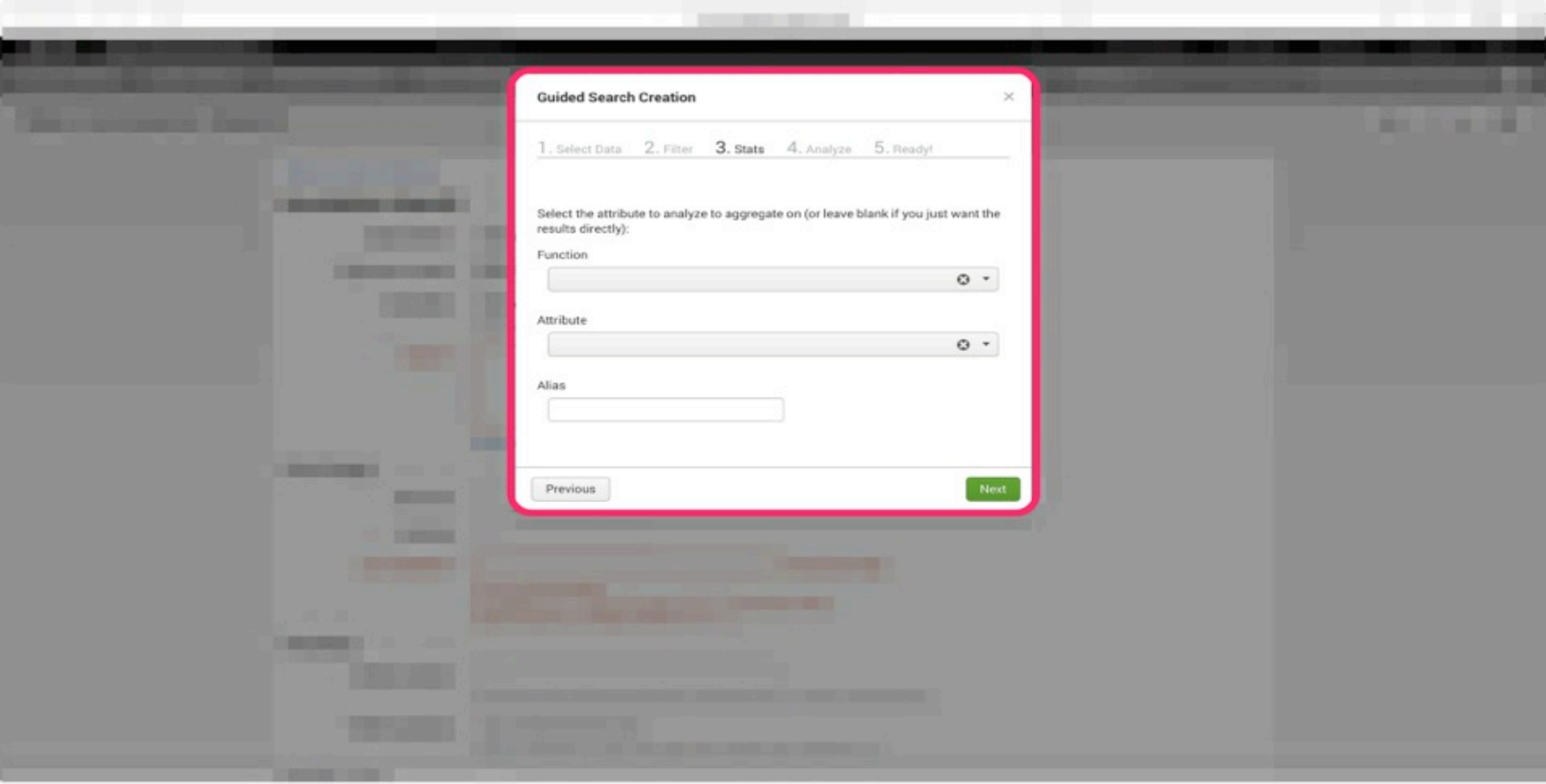

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Select the source of the data:
Source
Data model
Data Model
Malware
Object
Malware_Attacks
Previous
Next

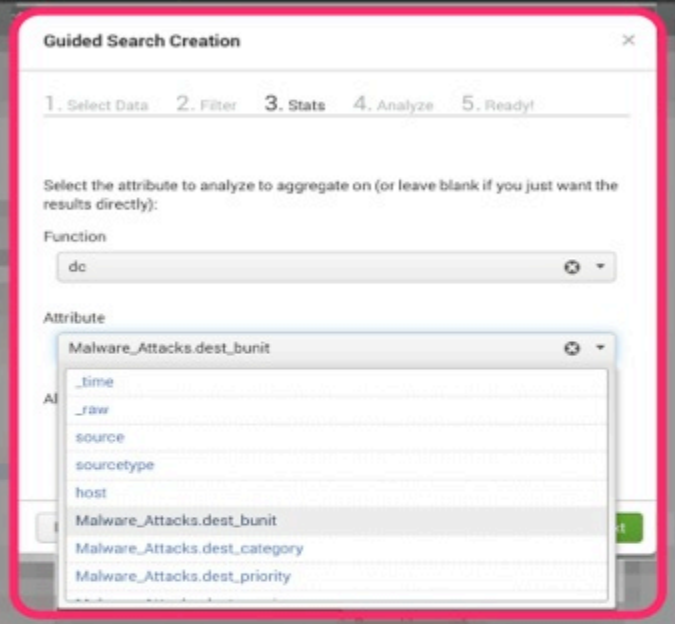

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Specify the time-range to limit the search to:
Preset time-range
Last 7 days
Earliest time
-7d@h
Latest time
now
Documentation
Previous
Next

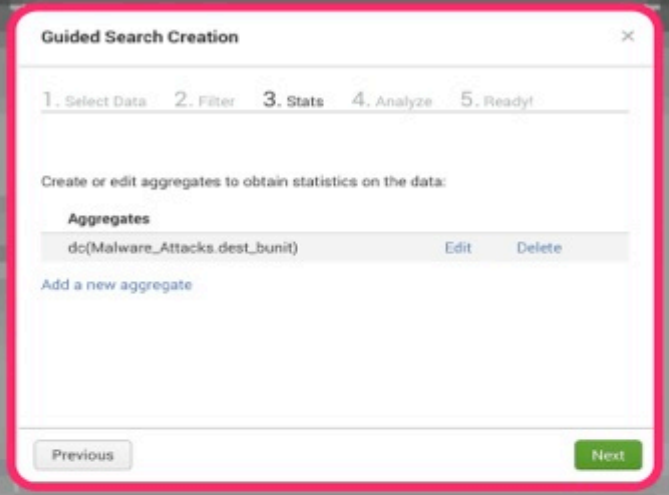

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Specify a string to filter the data (or leave blank if no filtering is required). Events filtering will occur before any statistics are applied. This string needs to be a valid where clause.
Filter
Search parses successfully
| datamodel "Malware" "Malware_Attacks" search | eval tag=mvjoin (tag,"|") | rename "_time" as "orig_time","_raw" as "orig_raw","linecount" as "orig_linecount","eventtype" as "orig_eventtype","splunk_server" as "orig_splunk_server","tag" as "orig_tag","timestartpos" as "orig_timestartpos","timeendpos" as "orig_timeendpos"| fields - date_*,punct
Run search
Previous
Next

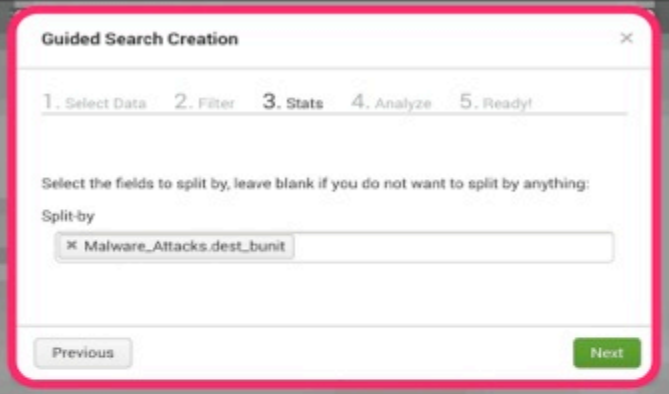

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Specify a string to filter the data (or leave blank if no filtering is required). Events filtering will occur before any statistics are applied. This string needs to be a valid where clause.
Filter
Search parses successfully
| datamodel "Malware" "Malware_Attacks" search | eval tag=mvjoin (tag,"|") | rename "_time" as "orig_time","_raw" as "orig_raw","
linecount" as "orig_linecount","eventtype" as "orig_eventtype","
splunk_server" as "orig_splunk_server","tag" as "orig_tag","time
startpos" as "orig_timestartpos","time as "orig_timeendpo
s"| fields - data_*,punct
Run search
Previous
Next

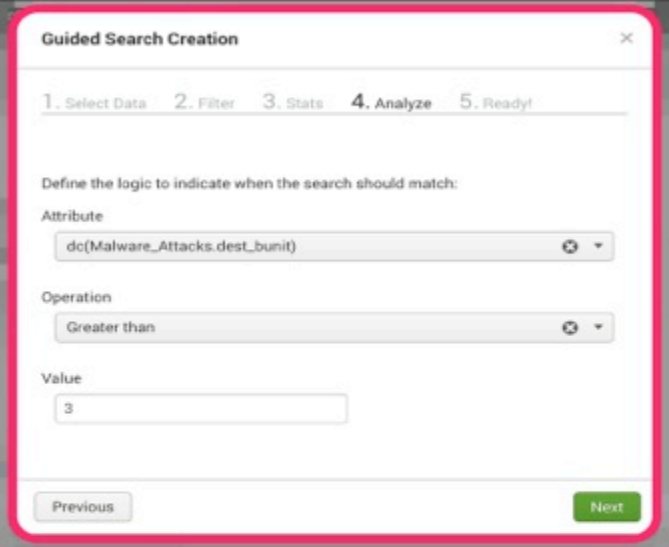

splunk> App: Enterprise Security
Monzy Merza Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
New Search
Save As Close
| tstats allow_old_summaries=true count(Malware_Attacks.dest_bunit) from datamodel=Malware where nodename=Malware_Attacks by "Malware_Attacks.dest_bunit" | rename "Malware_Attacks.dest_bunit" as "Biz_Unit" | where 'count(Malware_Attacks.dest_bunit)'>3
All time
✓ 261,874 events (before 9/17/14 3:00:59.000 AM)
Job
Smart Mode
Events Statistics (3) Visualization
20 Per Page Format Preview
Biz_Unit count(Malware_Attacks.dest_bunit)
americas 5491
apac 983
emea 1669
About Support File a Bug Documentation Privacy Policy
© 2005-2014 Splunk Inc. All rights reserved.
https://es-na.demo.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/

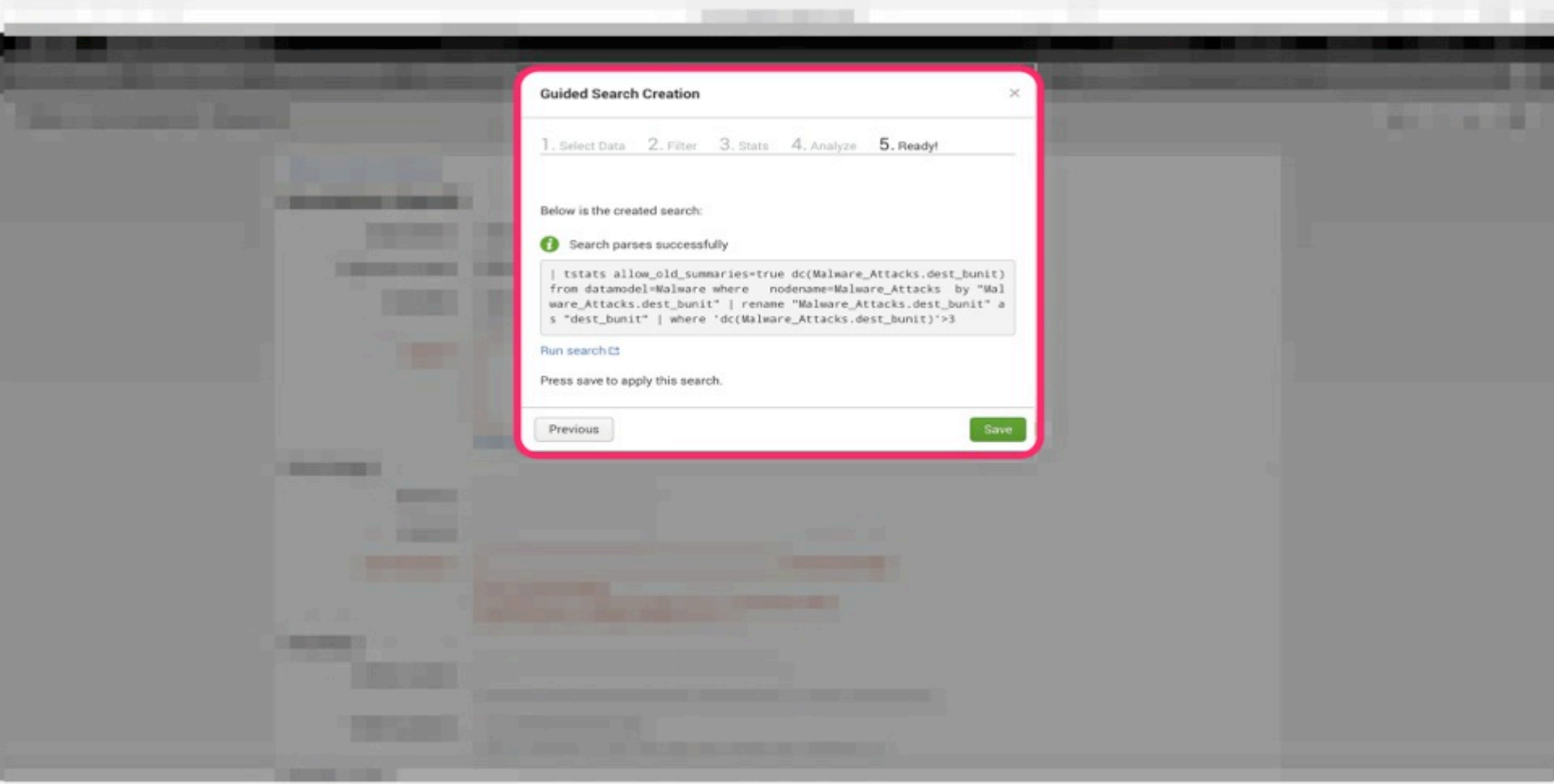

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Select the attribute to analyze to aggregate on (or leave blank if you just want the results directly):
Function
Attribute
Alias
Previous
Next

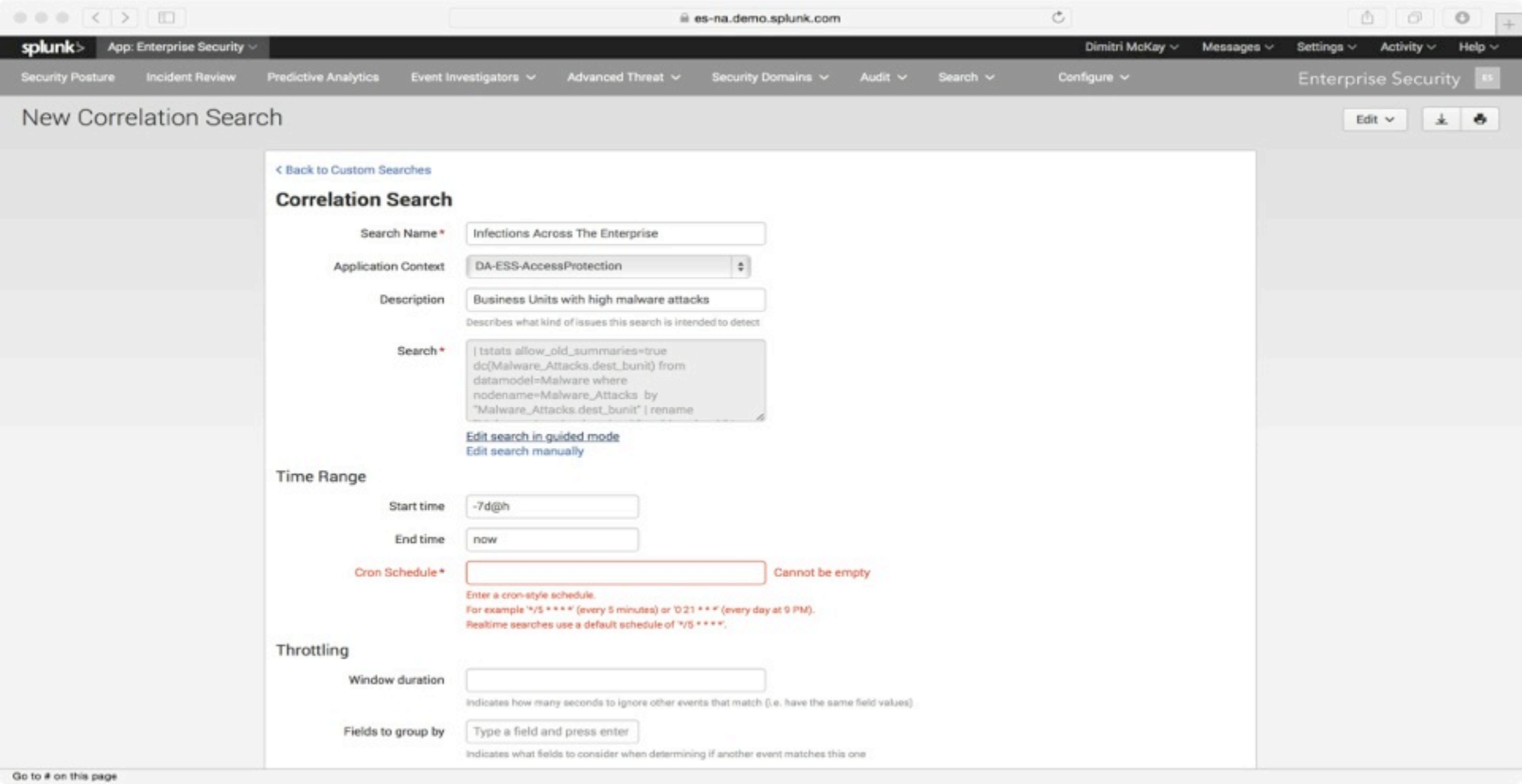

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Select the attribute to analyze to aggregate on (or leave blank if you just want the results directly):
Function
dc
Attribute
Malware_Attacks.dest_bunit
_time
_raw
source
sourcetype
host
Malware_Attacks.dest_bunit
Malware_Attacks.dest_category
Malware_Attacks.dest_priority


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
dc(Malware_Attacks.dest_bunit)
Edit
Delete
Add a new aggregate
Previous
Next

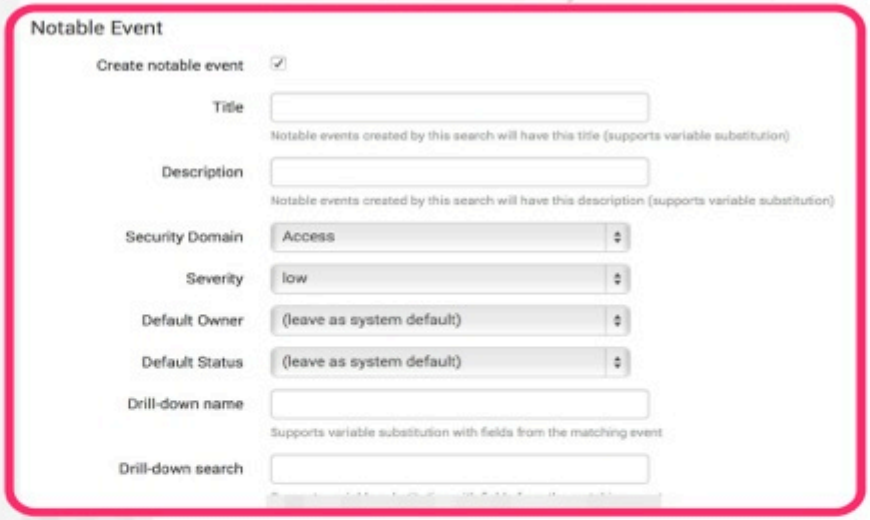

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Select the fields to split by, leave blank if you do not want to split by anything:
Split-by
Malware_Attacks.dest_bunit
Previous
Next

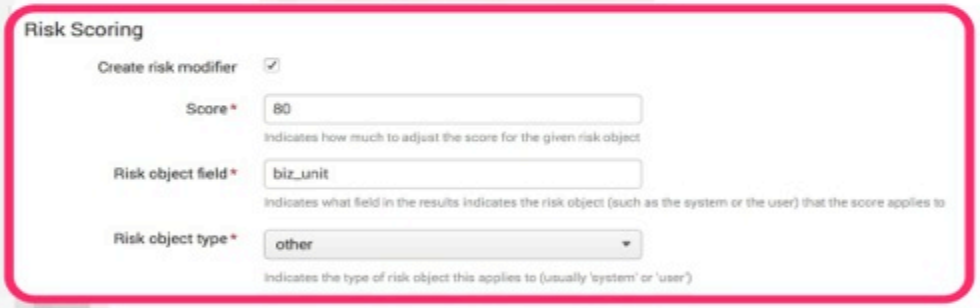

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Define the logic to indicate when the search should match:
Attribute
dc(Malware_Attacks.dest_bunit)
Operation
Greater than
Value
3
Previous
Next

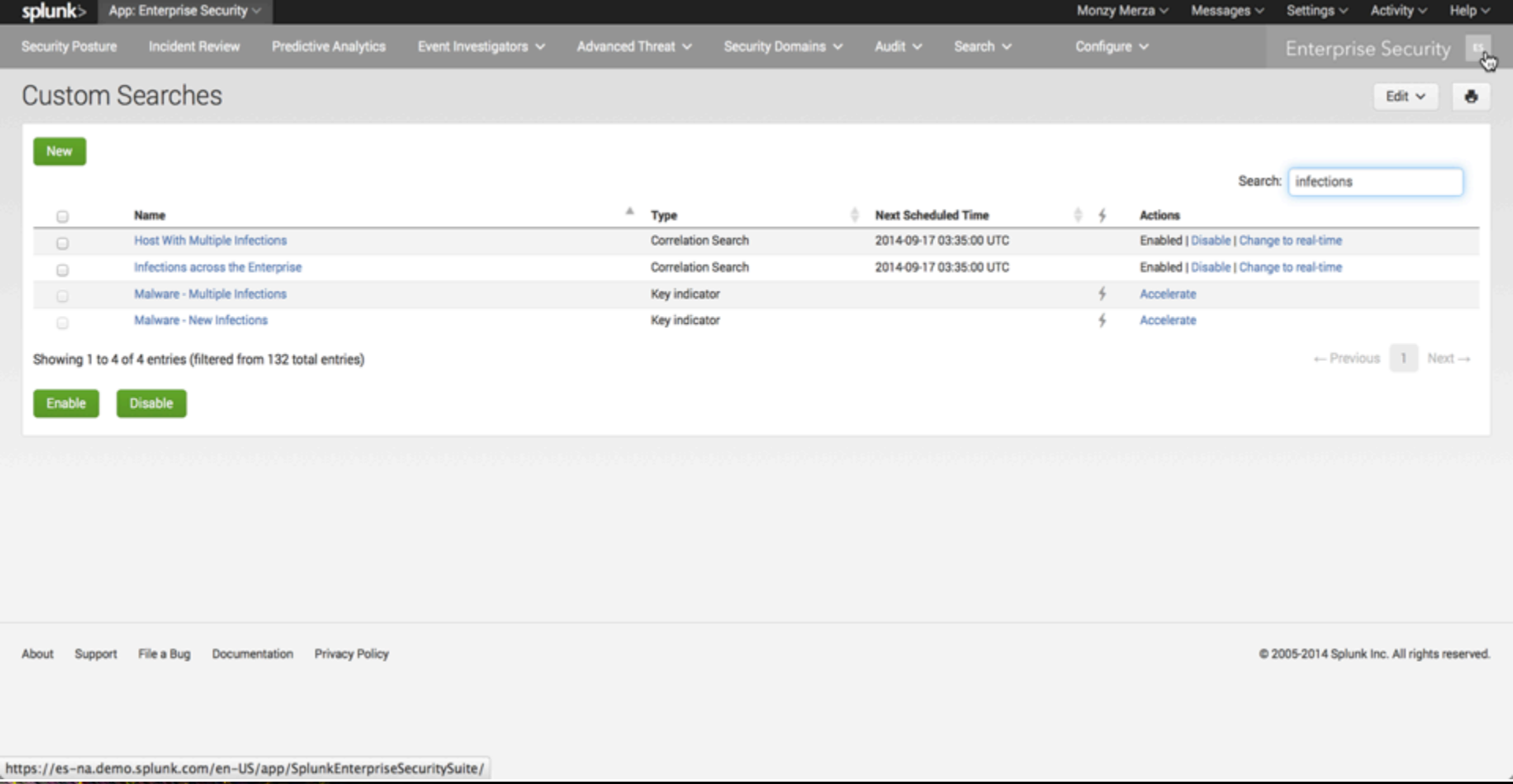

Guided Search Creation
1. Select Data
2. Filter
3. Stats
4. Analyze
5. Ready!
Below is the created search:
Search parses successfully
| tstats allow_old_summaries=true dc(Malware_Attacks.dest_bunit) from datamodel=Malware where nodename=Malware_Attacks by "Malware_Attacks.dest_bunit" | rename "Malware_Attacks.dest_bunit" as "dest_bunit" | where 'dc(Malware_Attacks.dest_bunit)'>3
Run search
Press save to apply this search.
Previous
Save


es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay
Messages
Settings
Activity
Help
Security Posture
Incident Review
Predictive Analytics
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
New Correlation Search
Edit
< Back to Custom Searches
Correlation Search
Search Name *
Infections Across The Enterprise
Application Context
DA-ESS-AccessProtection
Description
Business Units with high malware attacks
Describes what kind of issues this search is intended to detect
Search *
| tstats allow_old_summaries=true dc(Malware_Attacks.dest_bunit) from datamodel=Malware where nodename=Malware_Attacks by "Malware_Attacks.dest_bunit" | rename
Edit search in guided mode
Edit search manually
Time Range
Start time
-7d@h
End time
now
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
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
Go to # on this page


Time Range
Start time
-7d@h
End time
now
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 * * * *'.

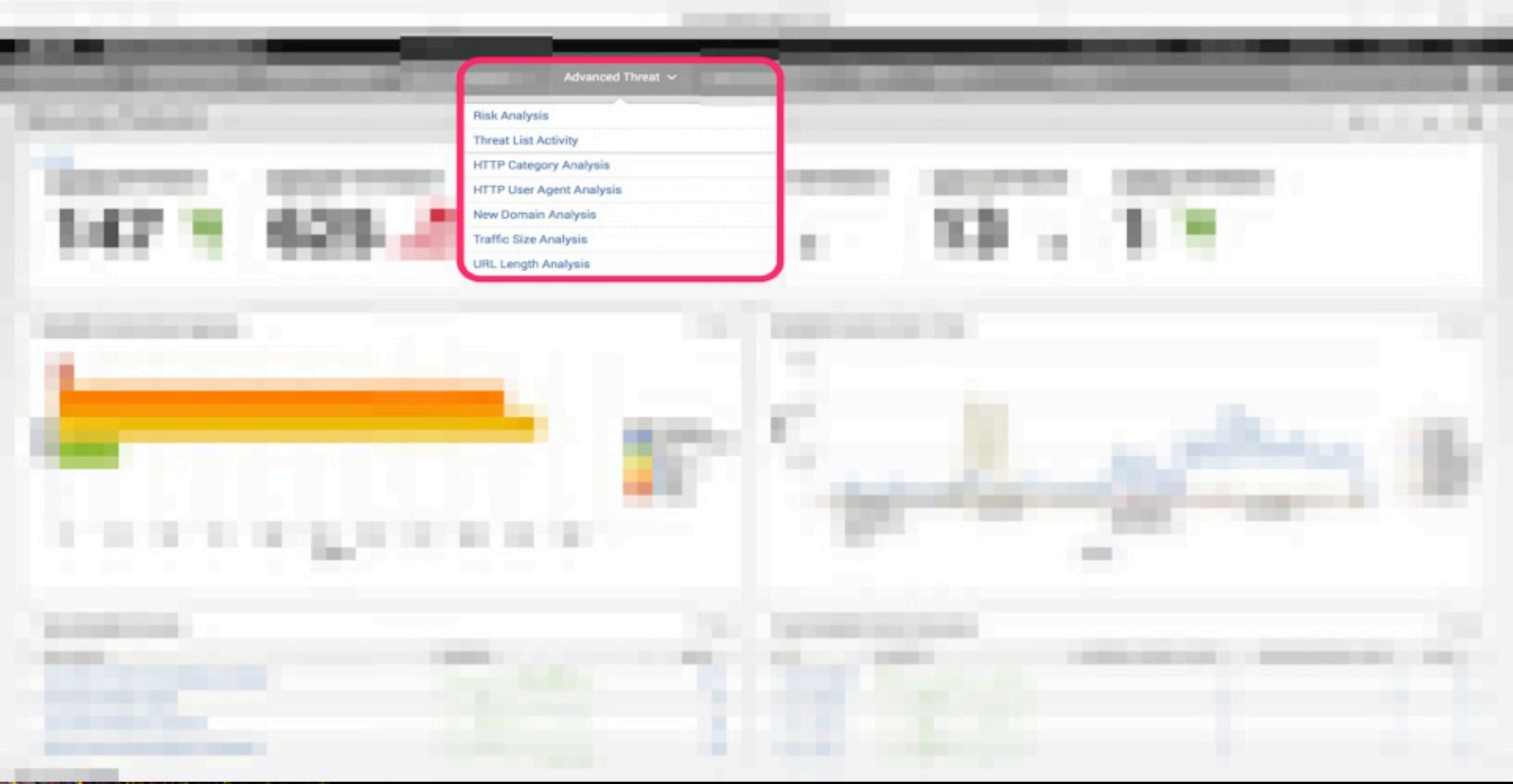

Notable Event
Create notable event
Title
Notable events created by this search will have this title (supports variable substitution)
Description
Notable events created by this search will have this description (supports variable substitution)
Security Domain
Access
Severity
low
Default Owner
(leave as system default)
Default Status
(leave as system default)
Drill-down name
Supports variable substitution with fields from the matching event
Drill-down search

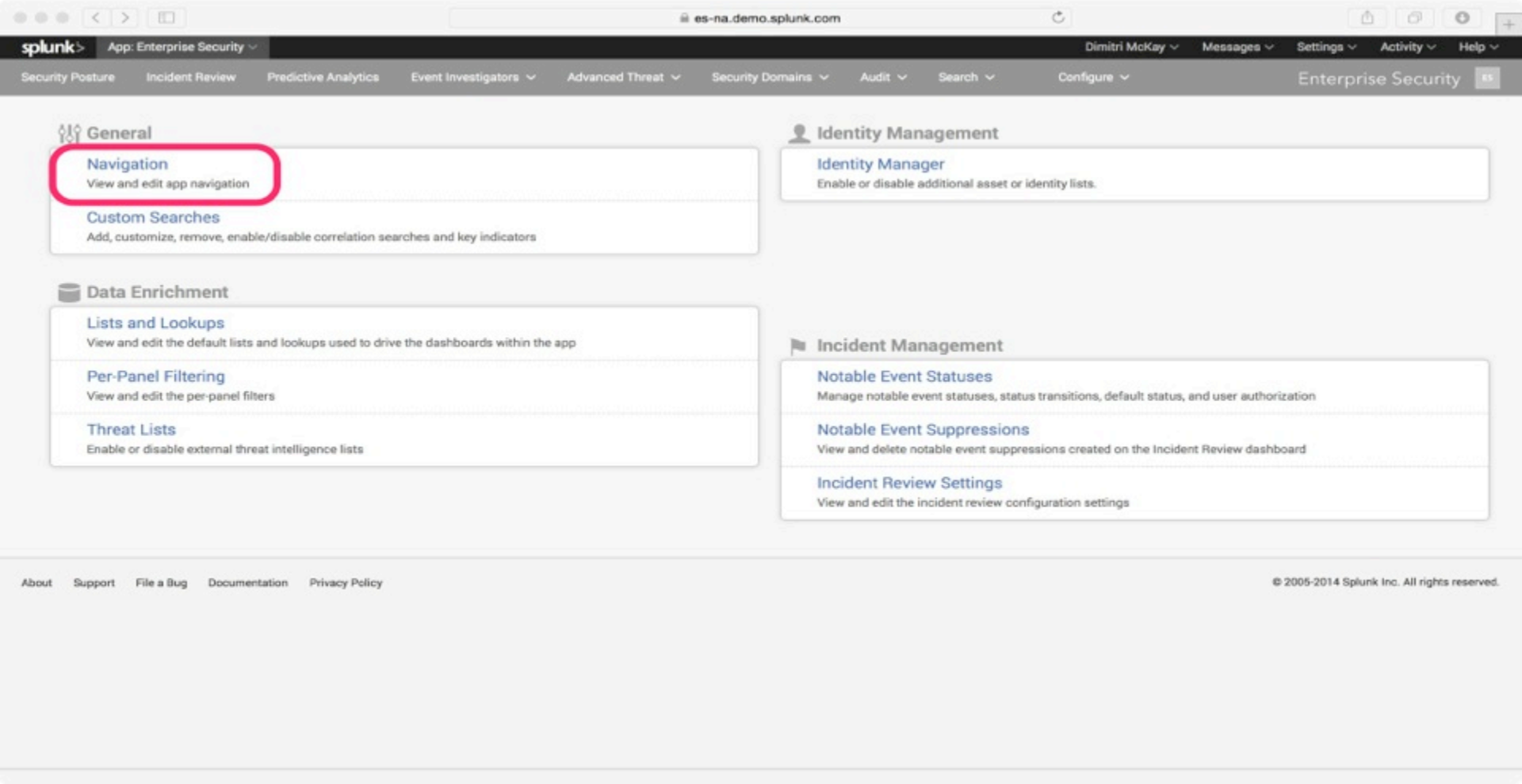

Risk Scoring
Create risk modifier
Score *
80
Indicates how much to adjust the score for the given risk object
Risk object field *
biz_unit
Indicates what field in the results indicates the risk object (such as the system or the user) that the score applies to
Risk object type *
other
Indicates the type of risk object this applies to (usually 'system' or 'user')

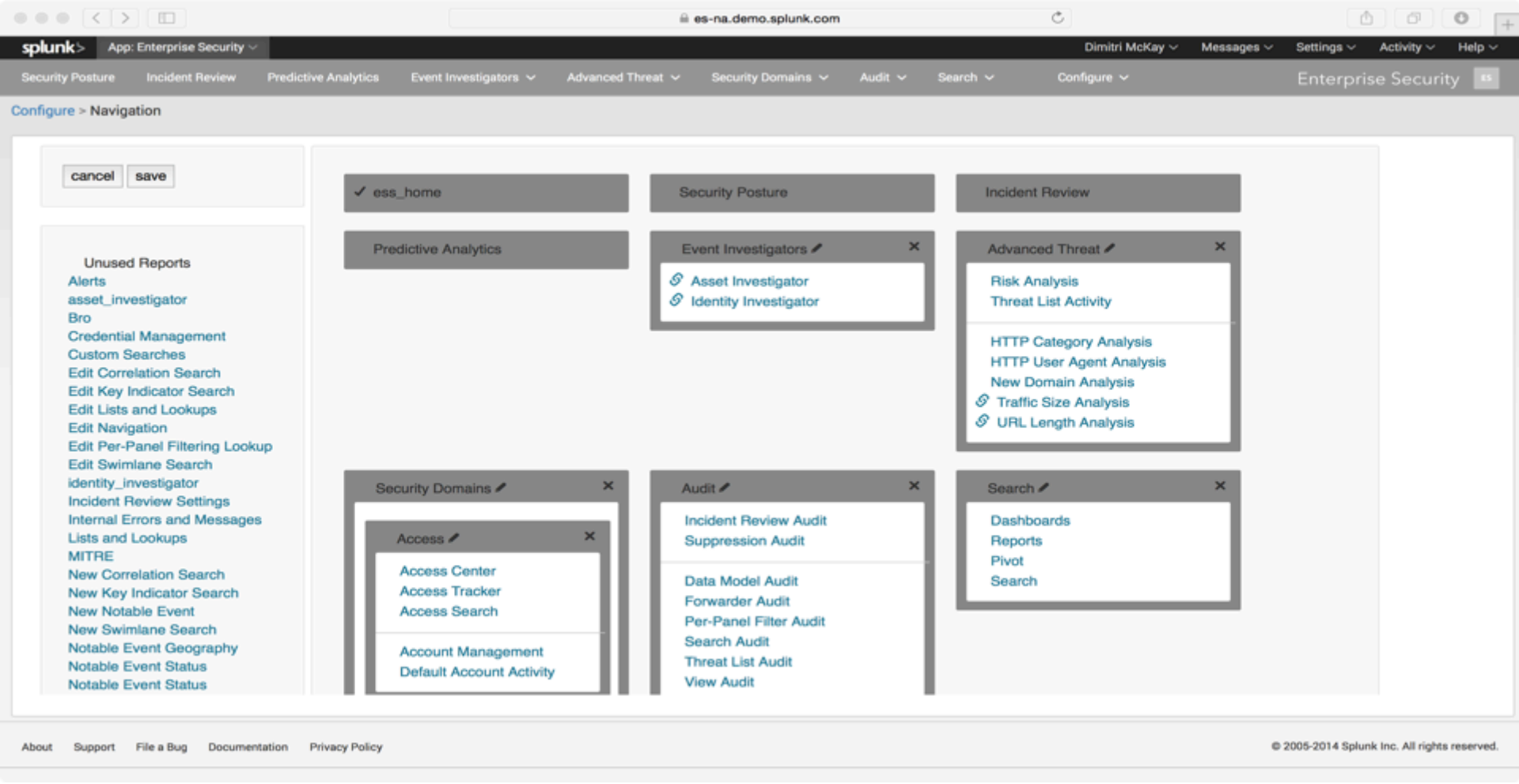

splunk> App: Enterprise Security
Monzy Merza Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure Enterprise Security
Custom Searches
Edit
New
Search: infections
Name Type Next Scheduled Time Actions
Host With Multiple Infections Correlation Search 2014-09-17 03:35:00 UTC Enabled | Disable | Change to real-time
Infections across the Enterprise Correlation Search 2014-09-17 03:35:00 UTC Enabled | Disable | Change to real-time
Malware - Multiple Infections Key indicator Accelerate
Malware - New Infections Key indicator Accelerate
Showing 1 to 4 of 4 entries (filtered from 132 total entries)
← Previous 1 Next →
Enable Disable
About Support File a Bug Documentation Privacy Policy
© 2005-2014 Splunk Inc. All rights reserved.
https://es-na.demo.splunk.com/en-US/app/SplunkEnterpriseSecuritySuite/

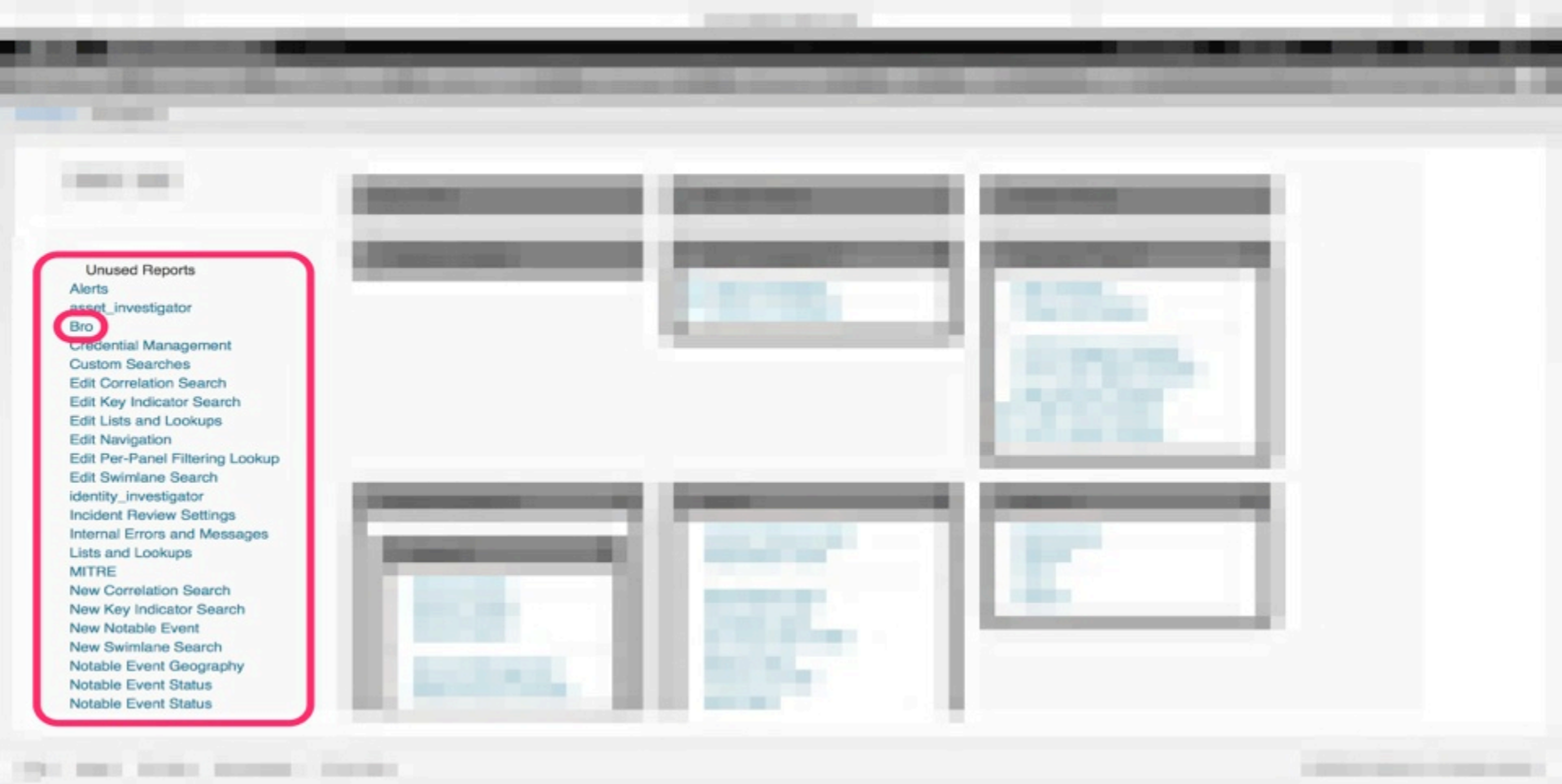
Dashboard Creation Via GUI

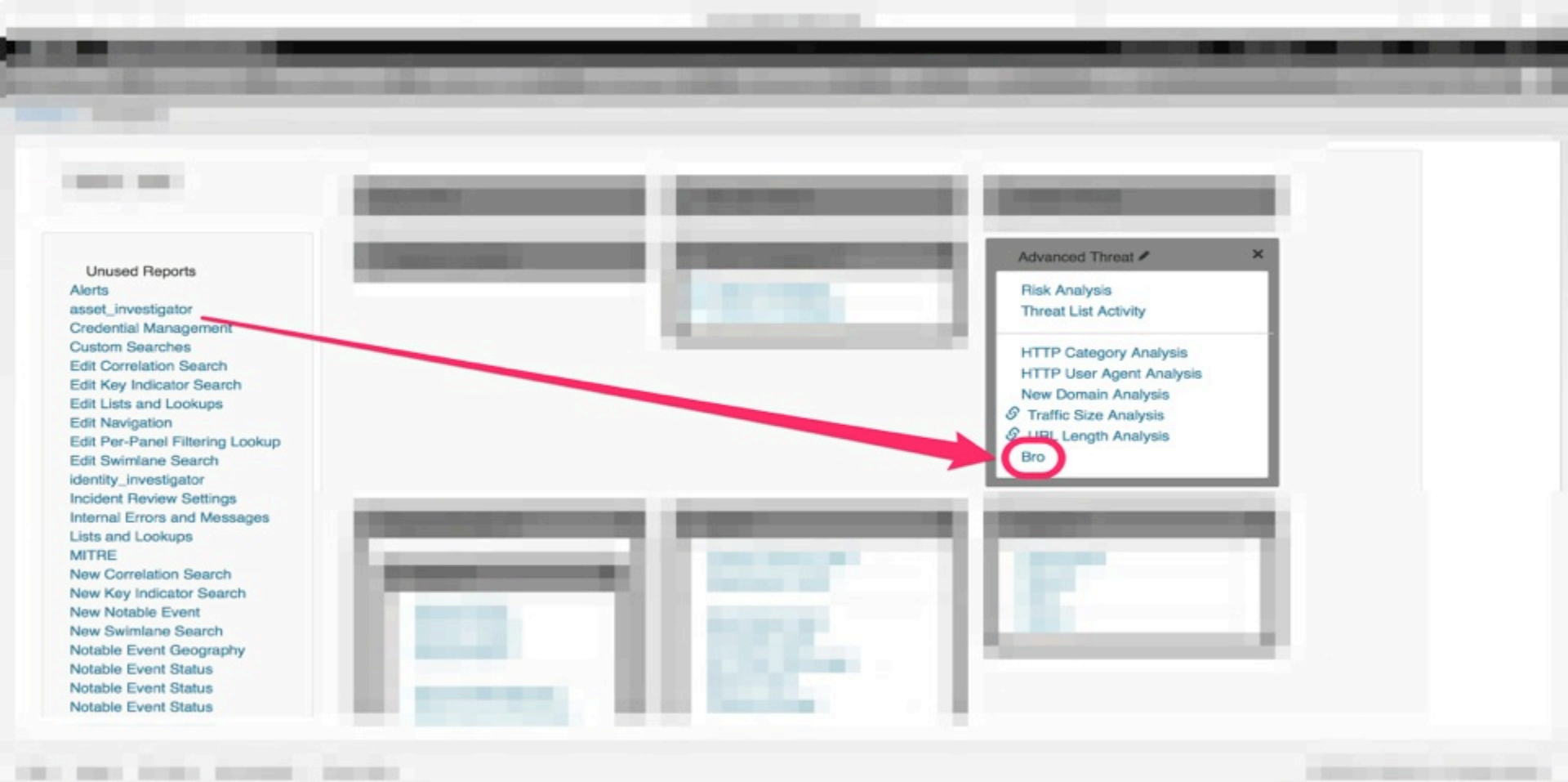
splunk>

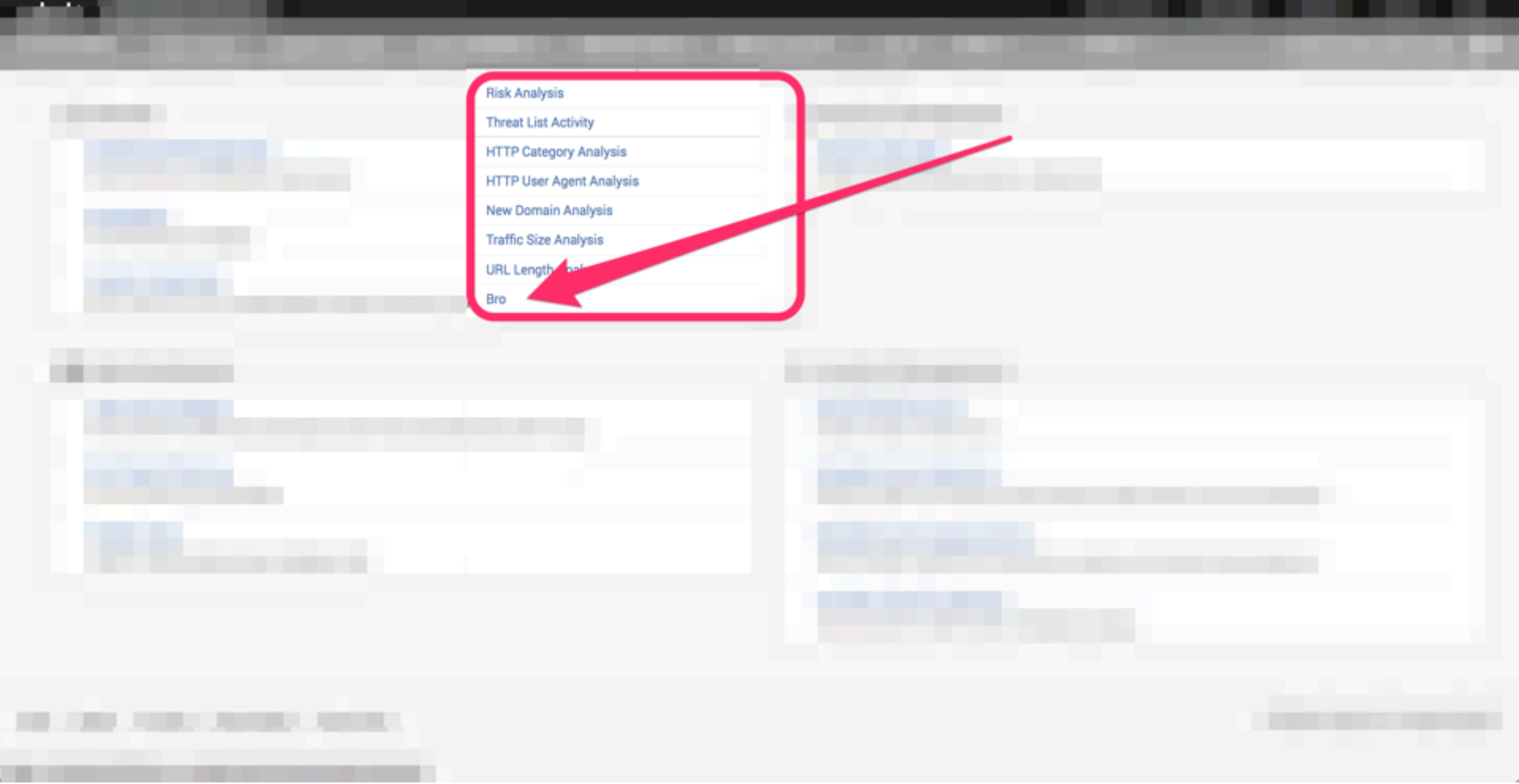

Advanced Threat
Risk Analysis
Threat List Activity
HTTP Category Analysis
HTTP User Agent Analysis
New Domain Analysis
Traffic Size Analysis
URL Length Analysis

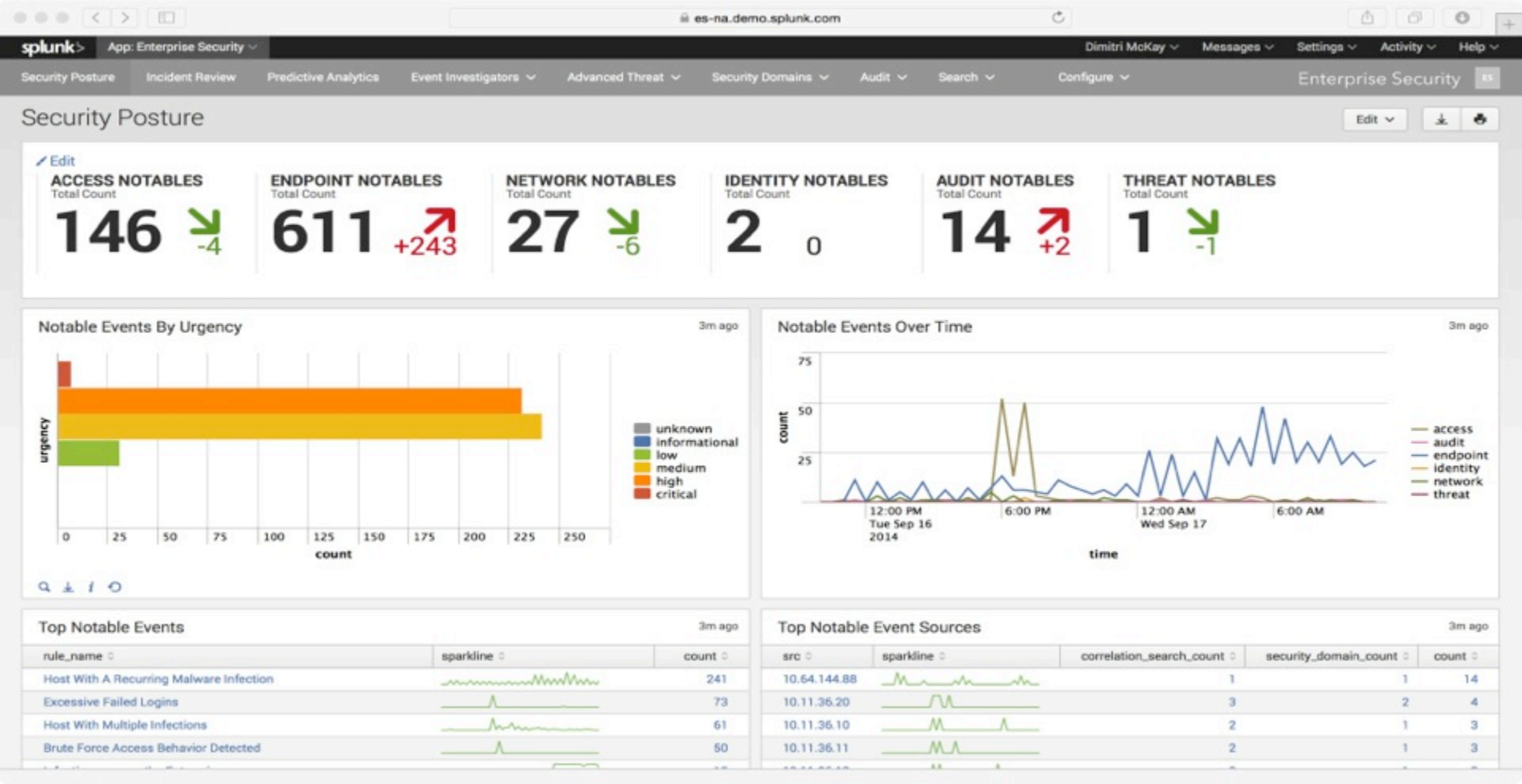

es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay
Messages
Settings
Activity
Help
Security Posture
Incident Review
Predictive Analytics
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
General
Navigation
View and edit app navigation
Custom Searches
Add, customize, remove, enable/disable correlation searches and key indicators
Data Enrichment
Lists and Lookups
View and edit the default lists and lookups used to drive the dashboards within the app
Per-Panel Filtering
View and edit the per-panel filters
Threat Lists
Enable or disable external threat intelligence lists
Identity Management
Identity Manager
Enable or disable additional asset or identity lists.
Incident Management
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
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2014 Splunk Inc. All rights reserved.


es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Configure > Navigation
cancel save
ess_home
Security Posture
Incident Review
Predictive Analytics
Event Investigators
Asset Investigator
Identity Investigator
Advanced Threat
Risk Analysis
Threat List Activity
HTTP Category Analysis
HTTP User Agent Analysis
New Domain Analysis
Traffic Size Analysis
URL Length Analysis
Unused Reports
Alerts
asset_investigator
Bro
Credential Management
Custom Searches
Edit Correlation Search
Edit Key Indicator Search
Edit Lists and Lookups
Edit Navigation
Edit Per-Panel Filtering Lookup
Edit Swimlane Search
identity_investigator
Incident Review Settings
Internal Errors and Messages
Lists and Lookups
MITRE
New Correlation Search
New Key Indicator Search
New Notable Event
New Swimlane Search
Notable Event Geography
Notable Event Status
Notable Event Status
Security Domains
Access
Access Center
Access Tracker
Access Search
Account Management
Default Account Activity
Audit
Incident Review Audit
Suppression Audit
Data Model Audit
Forwarder Audit
Per-Panel Filter Audit
Search Audit
Threat List Audit
View Audit
Search
Dashboards
Reports
Pivot
Search
About Support File a Bug Documentation Privacy Policy
© 2005-2014 Splunk Inc. All rights reserved.


Unused Reports
Alerts
assgt_investigator
Bro
Credential Management
Custom Searches
Edit Correlation Search
Edit Key Indicator Search
Edit Lists and Lookups
Edit Navigation
Edit Per-Panel Filtering Lookup
Edit Swimlane Search
identity_investigator
Incident Review Settings
Internal Errors and Messages
Lists and Lookups
MITRE
New Correlation Search
New Key Indicator Search
New Notable Event
New Swimlane Search
Notable Event Geography
Notable Event Status
Notable Event Status


Unused Reports
Alerts
asset_investigator
Credential Management
Custom Searches
Edit Correlation Search
Edit Key Indicator Search
Edit Lists and Lookups
Edit Navigation
Edit Per-Panel Filtering Lookup
Edit Swimlane Search
identity_investigator
Incident Review Settings
Internal Errors and Messages
Lists and Lookups
MITRE
New Correlation Search
New Key Indicator Search
New Notable Event
New Swimlane Search
Notable Event Geography
Notable Event Status
Notable Event Status
Notable Event Status
Advanced Threat
Risk Analysis
Threat List Activity
HTTP Category Analysis
HTTP User Agent Analysis
New Domain Analysis
Traffic Size Analysis
URL Length Analysis
Bro


Risk Analysis
Threat List Activity
HTTP Category Analysis
HTTP User Agent Analysis
New Domain Analysis
Traffic Size Analysis
Bro


es-na.demo.splunk.com
splunk> App: Enterprise Security
Dimitri McKay Messages Settings Activity Help
Security Posture Incident Review Predictive Analytics Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Security Posture
Edit
Edit
ACCESS NOTABLES
Total Count
146 -4
ENDPOINT NOTABLES
Total Count
611 +243
NETWORK NOTABLES
Total Count
27 -6
IDENTITY NOTABLES
Total Count
2 0
AUDIT NOTABLES
Total Count
14 +2
THREAT NOTABLES
Total Count
1 -1
Notable Events By Urgency
3m ago
urgency
unknown
informational
low
medium
high
critical
0 25 50 75 100 125 150 175 200 225 250
count
Notable Events Over Time
3m ago
75
50
25
count
12:00 PM Tue Sep 16 2014
6:00 PM
12:00 AM Wed Sep 17
6:00 AM
time
access
audit
endpoint
identity
network
threat
Top Notable Events
3m ago
rule_name sparkline count
Host With A Recurring Malware Infection 241
Excessive Failed Logins 73
Host With Multiple Infections 61
Brute Force Access Behavior Detected 50
Top Notable Event Sources
3m ago
src sparkline correlation_search_count security_domain_count count
10.64.144.88 1 1 14
10.11.36.20 3 2 4
10.11.36.10 2 1 3
10.11.36.11 2 1 3

Q&A

splunk>

Learn, share and hack

Security office hours: 11:00 AM – 2:00 PM @Room 103 Everyday

Geek out, share ideas with Enterprise Security developers

Red Team / Blue Team - Challenge your skills and learn new tricks

Mon-Wed: 3:00 PM – 6:00 PM @Splunk Community Lounge

Thurs: 11:00 AM – 2:00 PM

Birds of a feather- Collaborate and brainstorm with security ninjas

Thurs: 12:00 PM – 1:00 PM @Meal Room

THANK YOU

@dimitrimckay

splunk>