Managed Threat Intelligence in Enterprise Security!

Brian Luger

Software Engineer, Splunk

splunk>

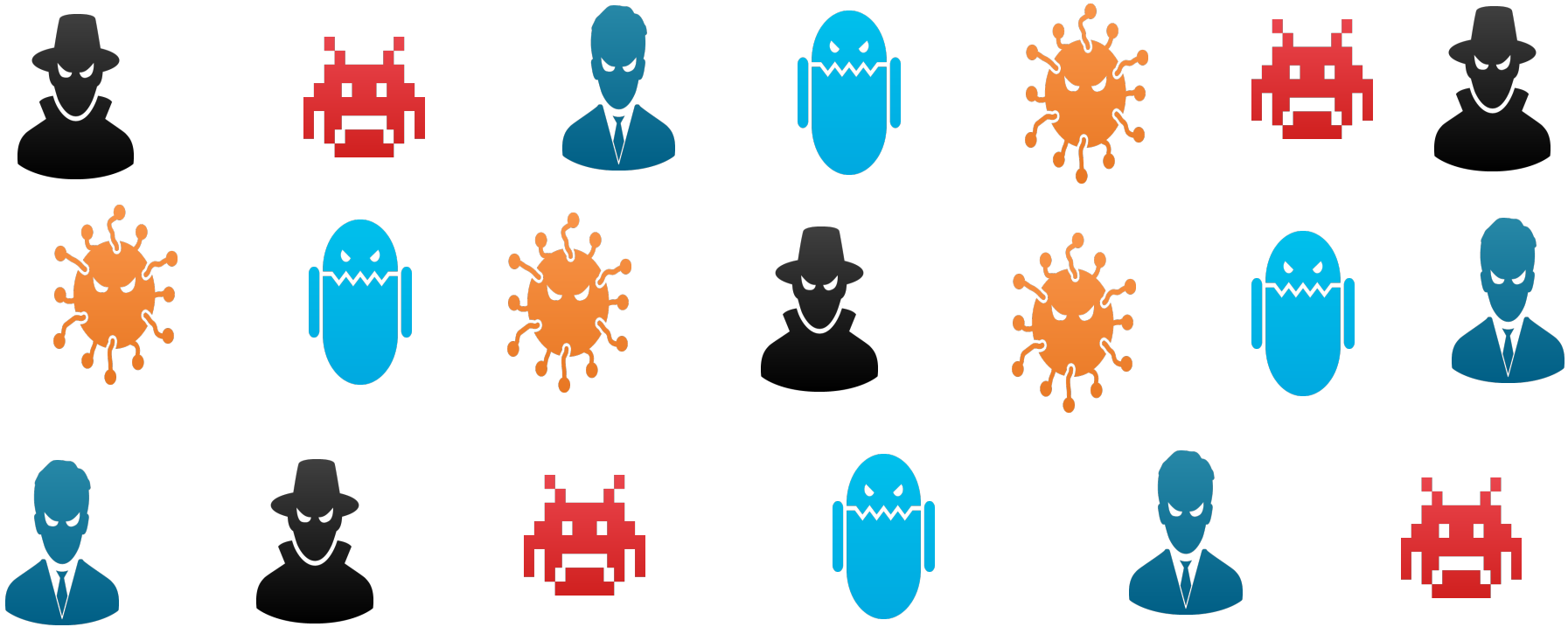
Disclaimer

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.

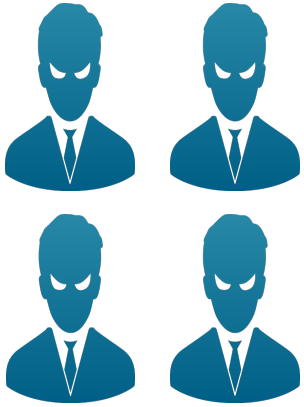
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

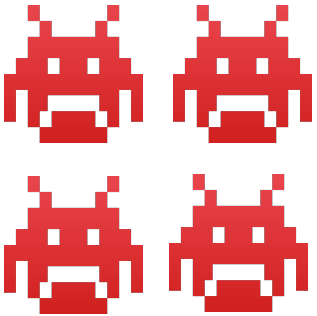
Current State of Threat Intelligence

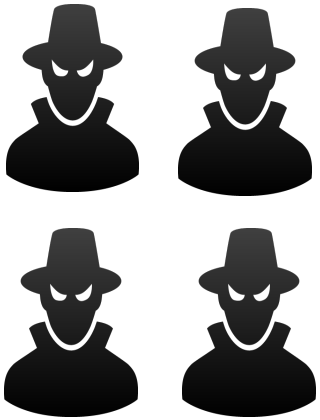
Not all Threat Intelligence is Created equal!

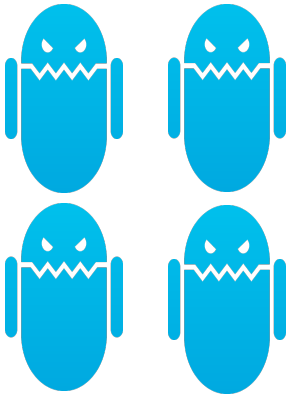


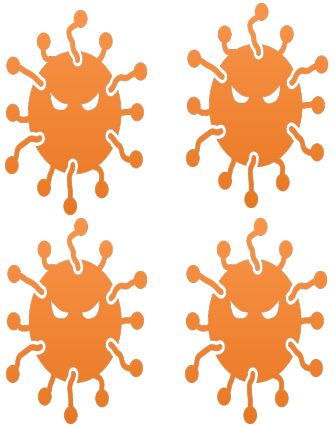
Threat Categorization





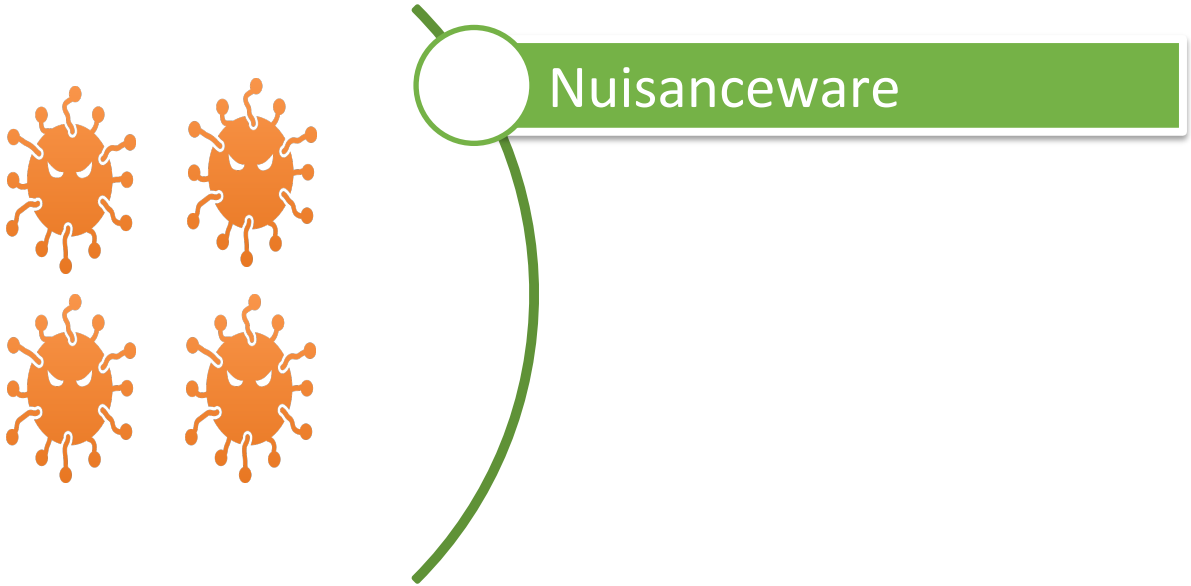




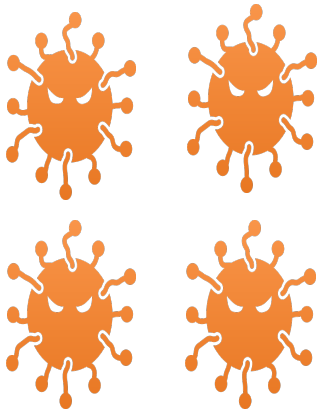


Commodity

Commodity

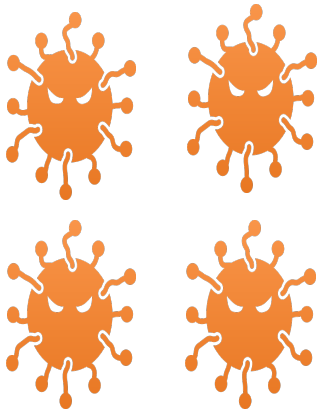


Commodity



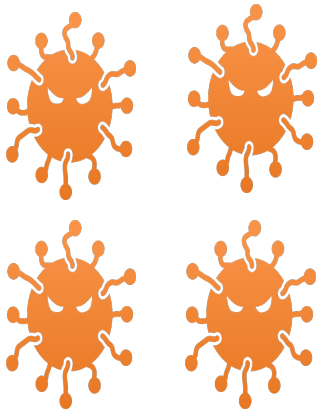
- Nuisanceware
- Adware

Commodity



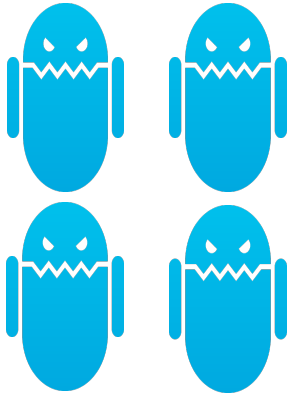
- Nuisanceware
- Adware
- FakeAV

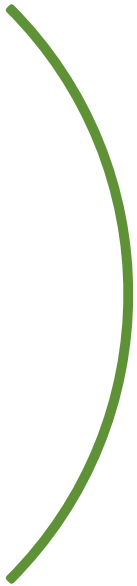
Commodity



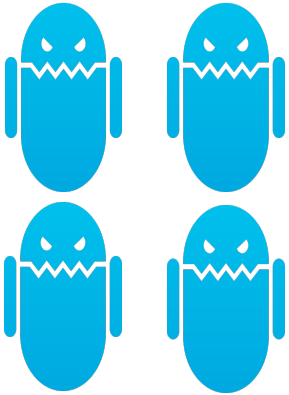
- Nuisanceware
- Adware
- FakeAV
- "Viruses”

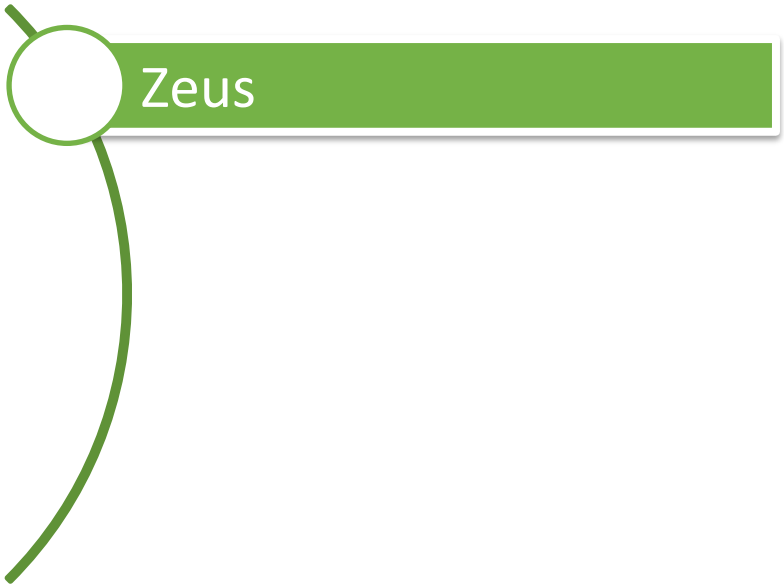
Financial



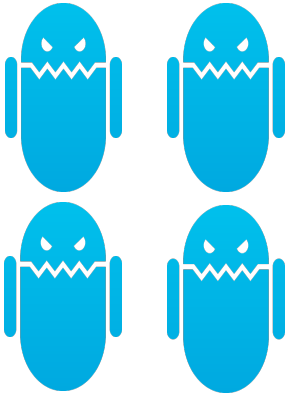


Financial



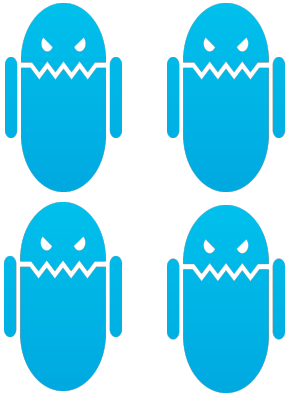


Financial



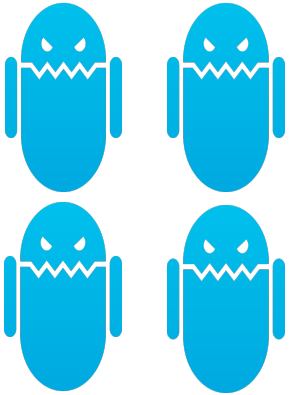
- Zeus
- Spyware

Financial



- Zeus
- Spyware
- Ransomware

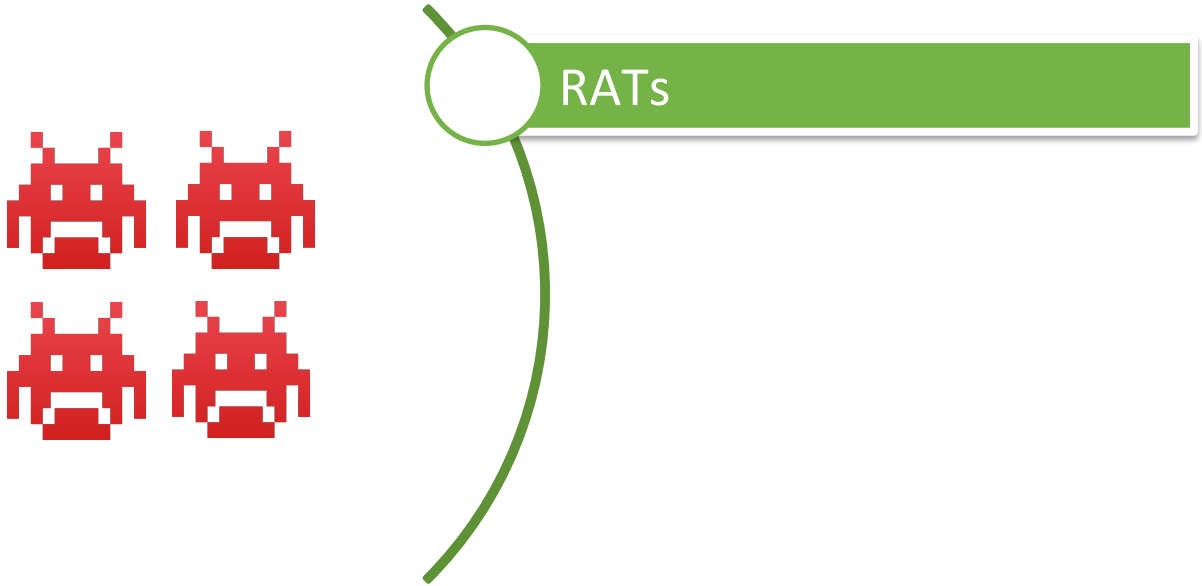
Financial



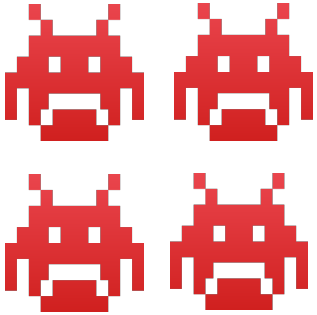
- Zeus
- Spyware
- Ransomware
- Phishing Sites

Advanced Threats

Advanced Threats

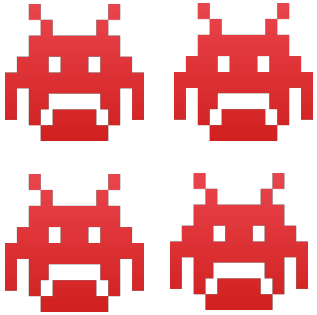


Advanced Threats



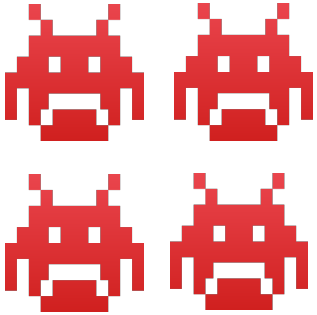
- RATs
- Web Shells

Advanced Threats



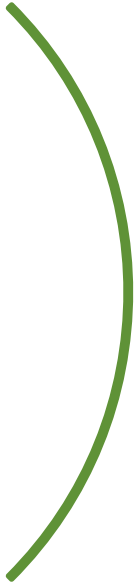
- RATs
- Web Shells
- Proxies

Advanced Threats



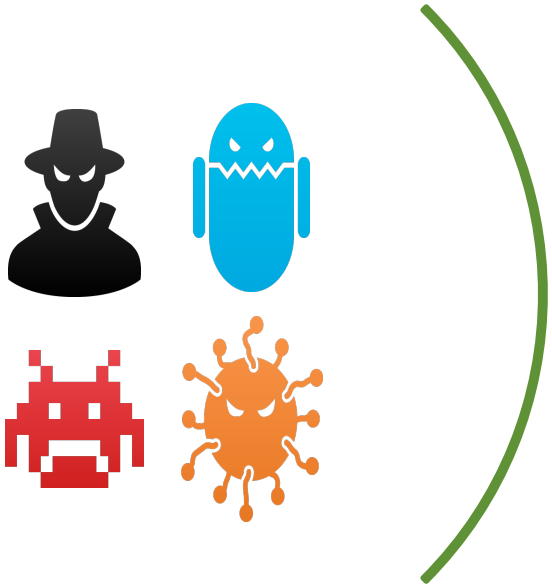
- RATs
- Web Shells
- Proxies
- Phishing Emails/Sites

Unknown Threats

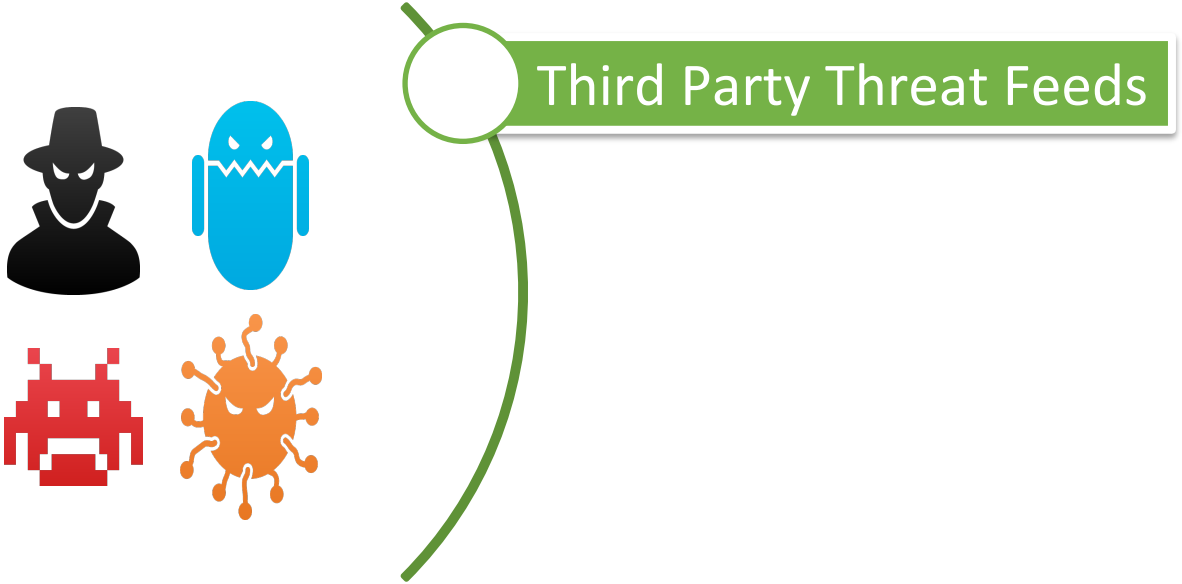



A Place For
Everything &
Everything
In Its Place

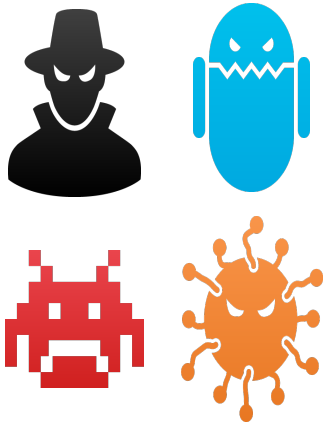
Open Source Intelligence (OS-INT)



Open Source Intelligence (OS-INT)

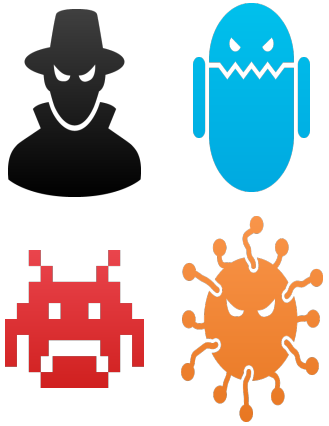


Open Source Intelligence (OS-INT)



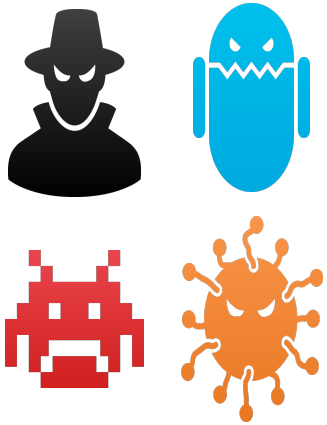
- Third Party Threat Feeds
- Public TAXII Feeds

Open Source Intelligence (OS-INT)

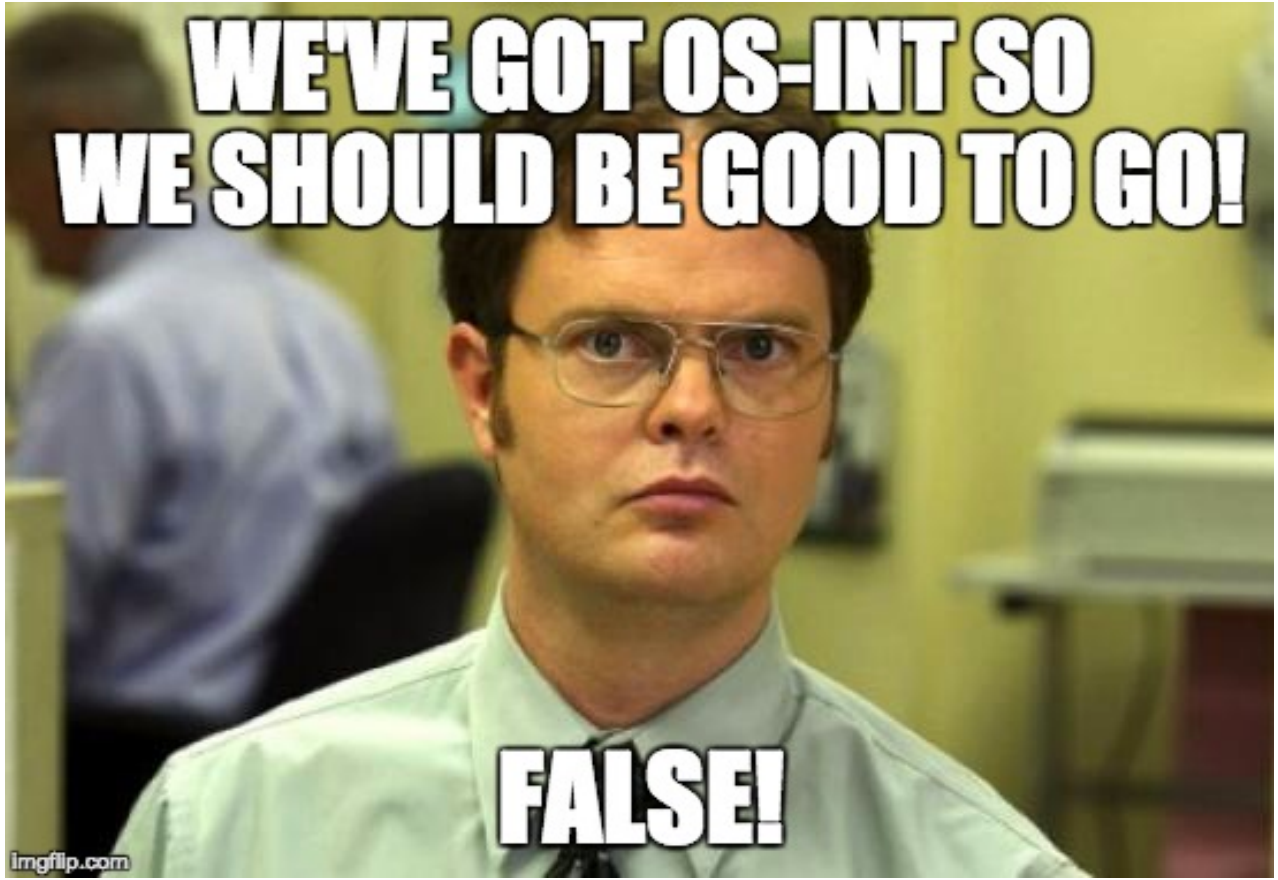


- Third Party Threat Feeds
- Public TAXII Feeds
- Public Intel Reports

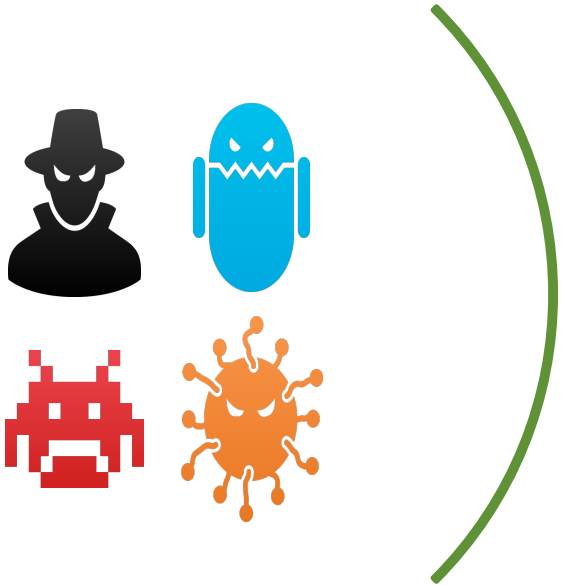
Open Source Intelligence (OS-INT)



- Third Party Threat Feeds
- Public TAXII Feeds
- Public Intel Reports
- Google

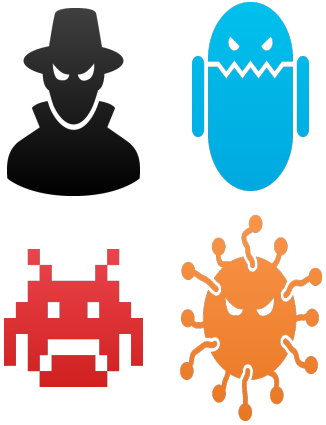

WE'VE GOT OS-INT SO
WE SHOULD BE GOOD TO GO!
FALSE!
imgflip.com

Issues with OS-INT



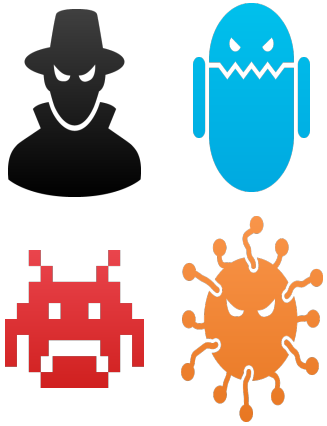
Issues with OS-INT

Issues with OS-INT



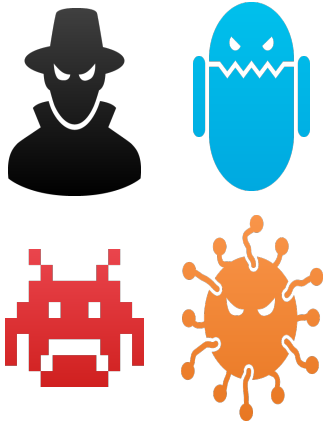
- Quantity over Quality
- Little to no context

Issues with OS-INT



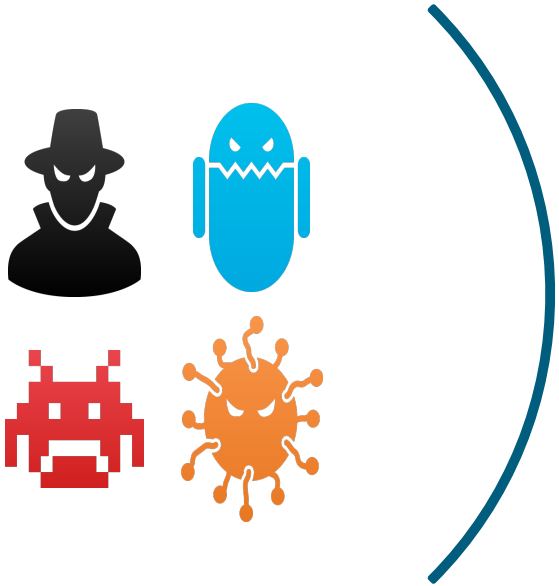
- Quantity over Quality
- Little to no context
- It's Burned Intel

Issues with OS-INT

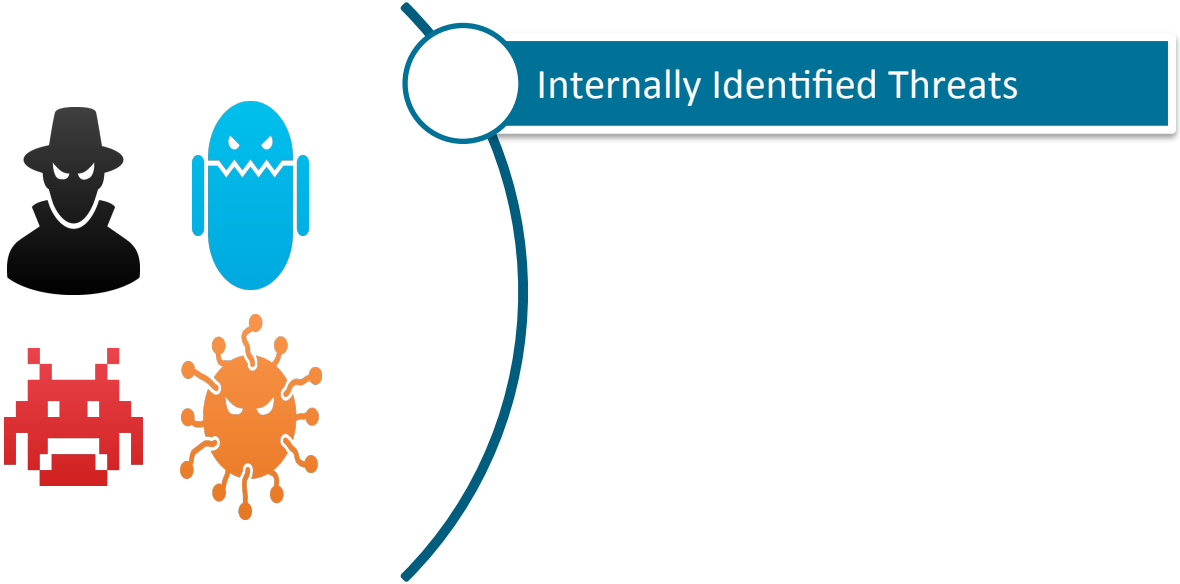


- Quantity over Quality
- Little to no context
- It's Burned Intel
- Not Specific to Your Organization

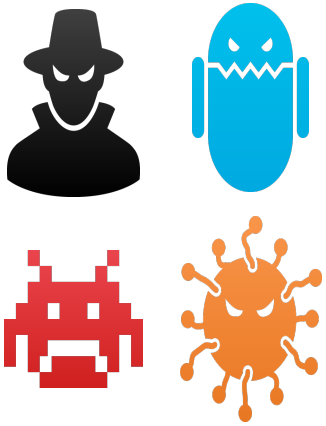
Targeted Intelligence



Targeted Intelligence

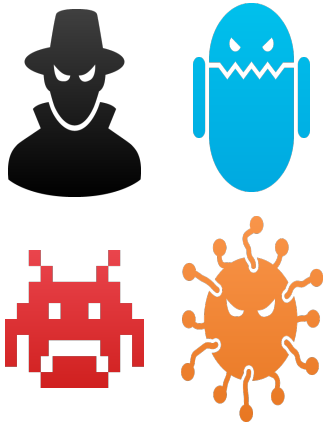


Targeted Intelligence



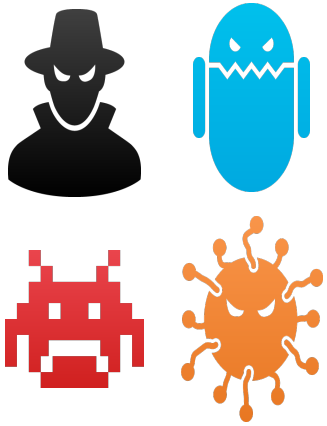
- Internally Identified Threats
- Relevant to Business Sector

Targeted Intelligence



- Internally Identified Threats
- Relevant to Business Sector
- Spear Phishing Emails

Targeted Intelligence

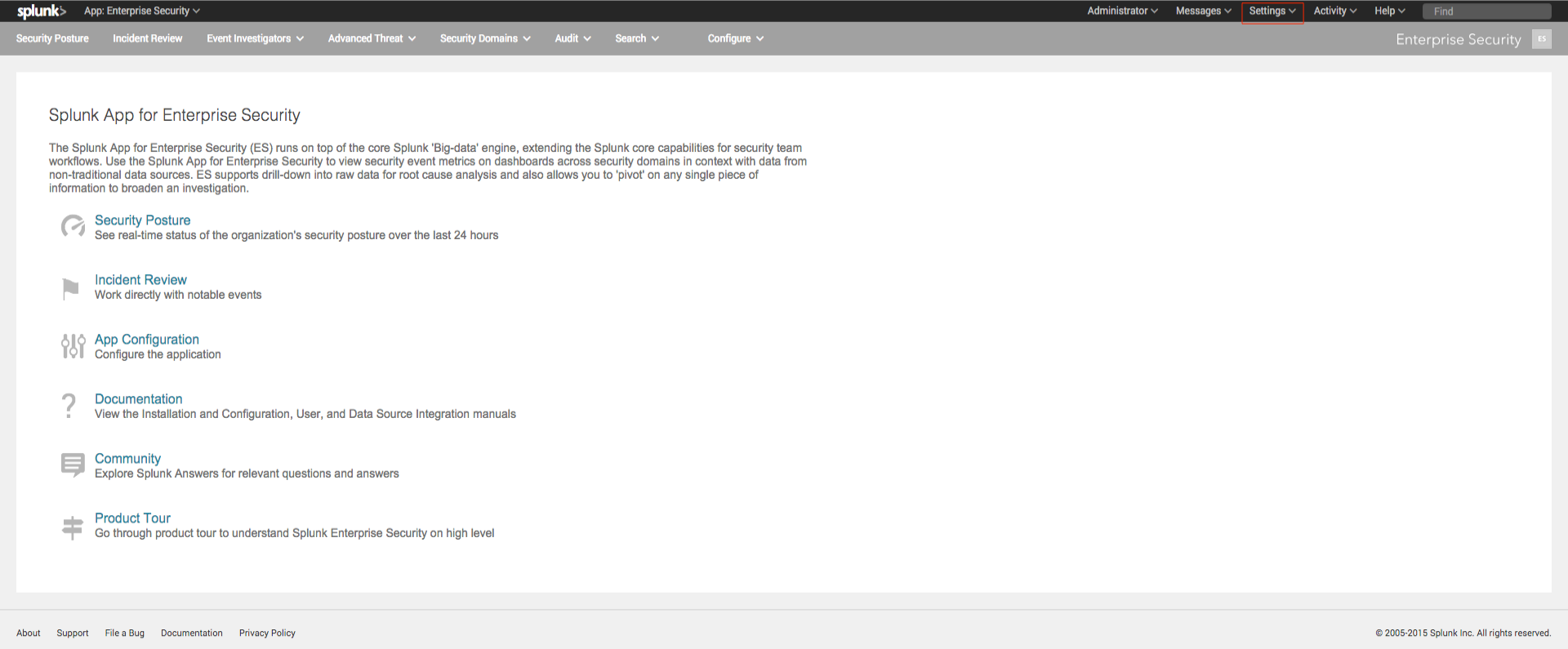


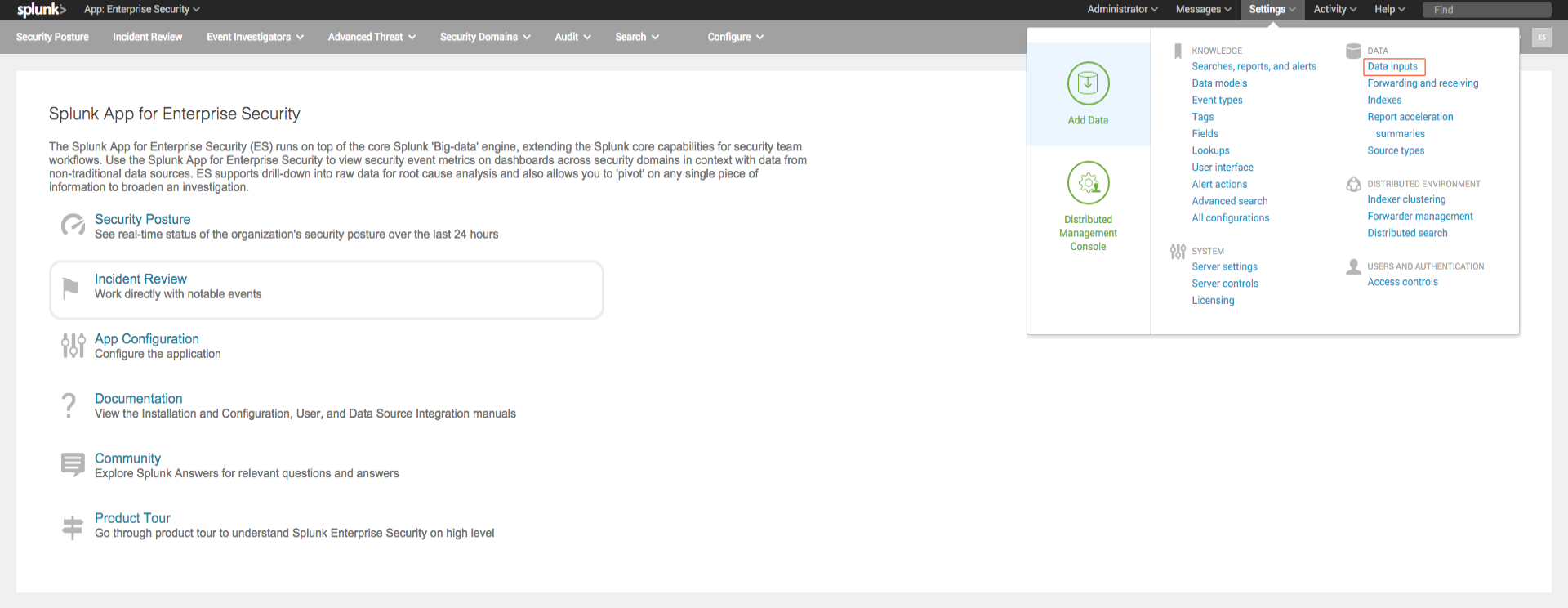
- Internally Identified Threats
- Relevant to Business Sector
- Spear Phishing Emails
- Breach Related Artifacts

How Can I Manage My Threat Intel?

ES Threat Intelligence Manager

ES Threat Intelligence Manager


splunk> App: Enterprise Security
Administrator Messages Settings Activity Help Find
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
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
About Support File a Bug Documentation Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.


splunk> App: Enterprise Security
Administrator Messages Settings Activity Help Find
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure
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
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Distributed search
SYSTEM
Server settings
Server controls
Licensing
USERS AND AUTHENTICATION
Access controls
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
About Support File a Bug Documentation Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.
https://127.0.0.1:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review

Data inputs

Local inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to Forwarding and receiving.

Type	Inputs	Actions
Files & directories Index a local file or monitor an entire directory.	22	Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	1	Add new
Scripts Run custom scripts to collect or generate more data.	35	Add new
App Imports Update Updates the app imports with all apps matching a given regular expression.	1	Add new
Configuration Checker Runs configuration checks.	8	Add new
Data Migrator Perform one-time data migrations.	5	Add new
Data Model Acceleration Enforcement Enforces data model acceleration settings.	19	Add new
Identity Management Merges asset and identity information into Splunk lookup tables.	5	Add new
PCAP Watch directories for packet capture files (*.pcap) and process them using Bro.	0	Add new
Threat Intelligence Manager Merges threat information into Threat Intelligence KV Store collections.	8	Add new
Threat Intelligence Downloads Downloads threat lists or other threat intelligence feeds from remote hosts.	25	Add new
Threat List Manager Merges threatlist information into Splunk lookup tables.	1	Add new
Network Queries Perform network queries.	1	Add new

Forwarded inputs

Type	Inputs	Actions
Windows Event Logs Collect event logs from forwarders.	0	Add new

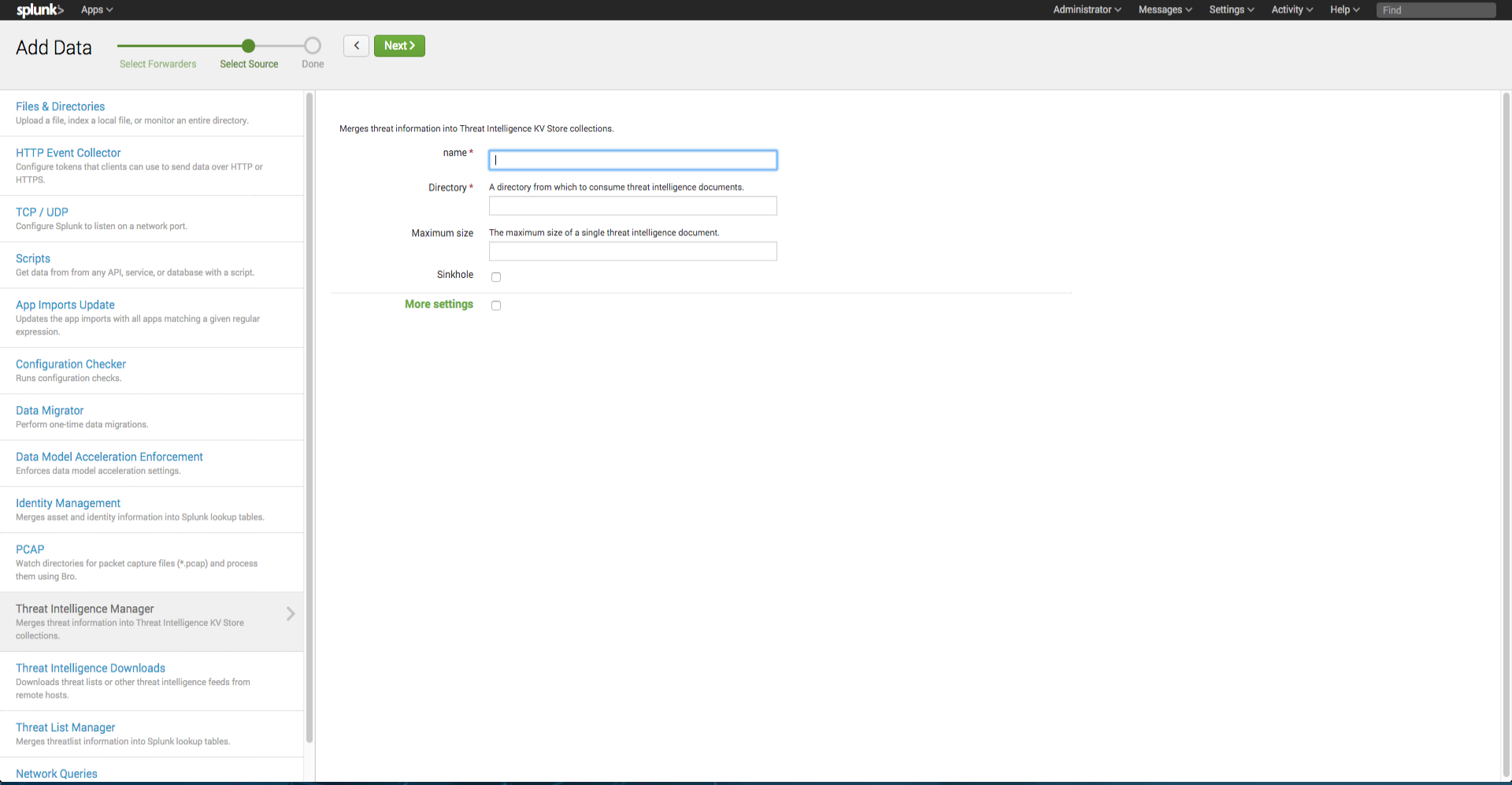
Threat Intelligence Manager

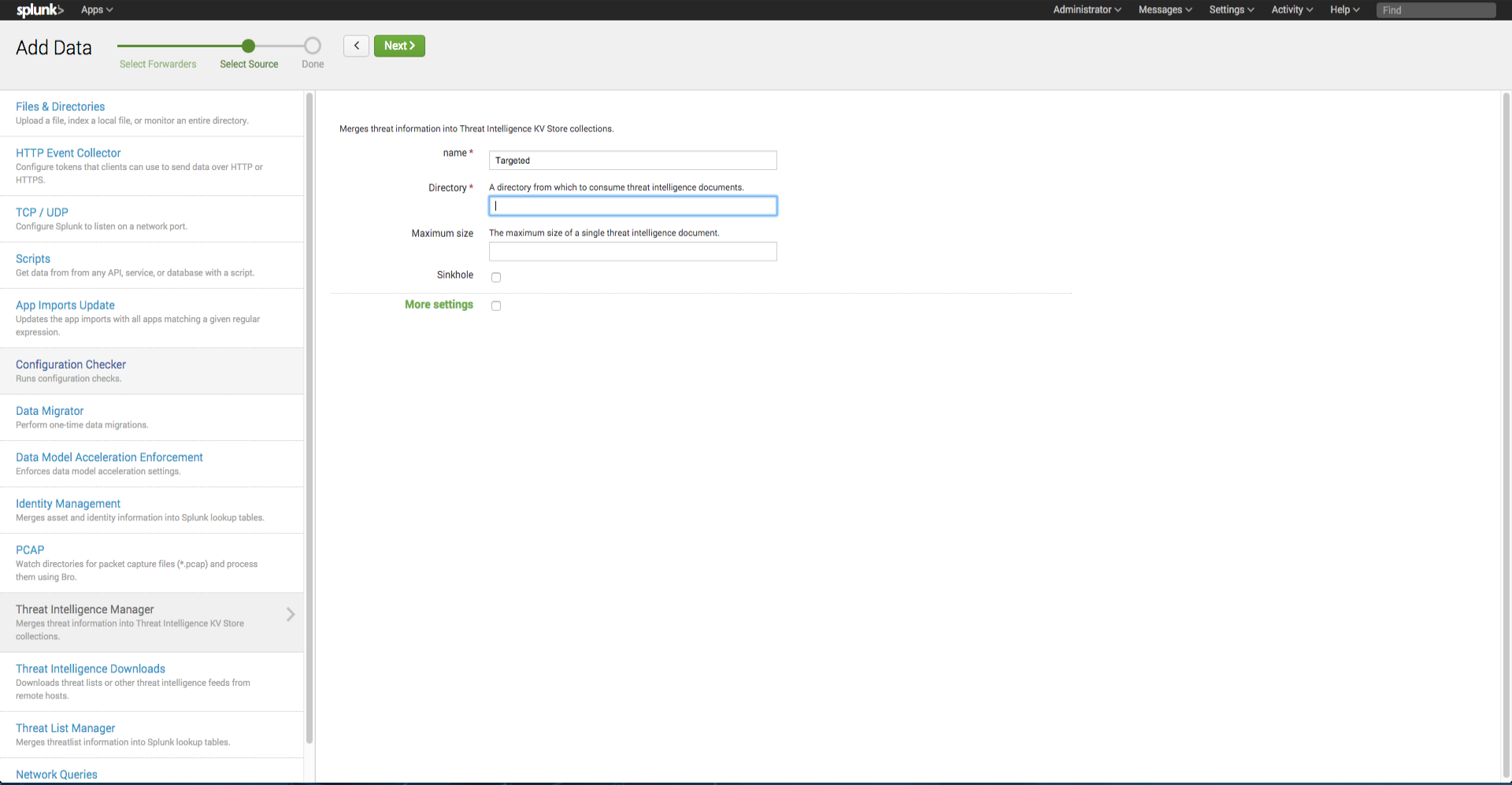
New

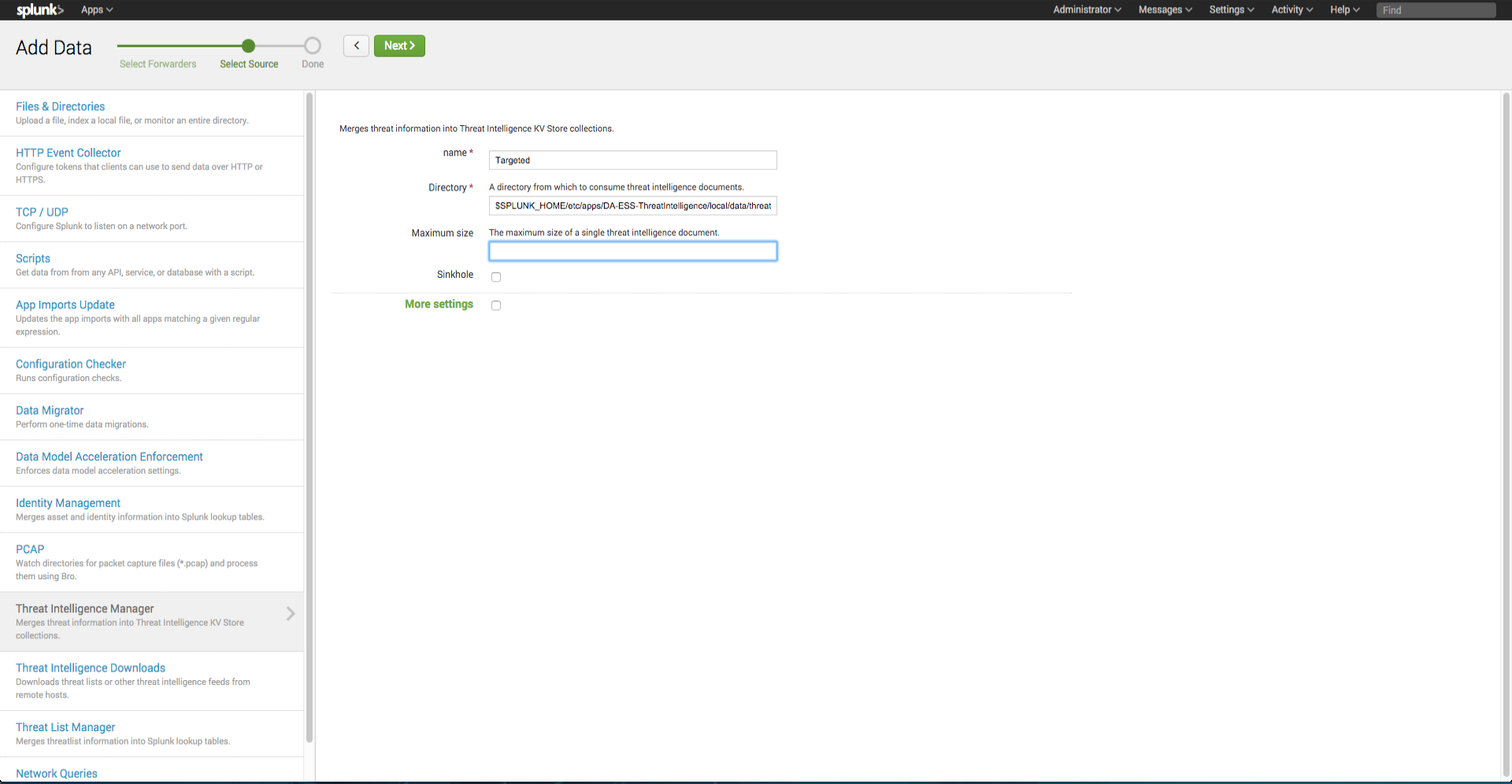
Showing 1-8 of 8 items

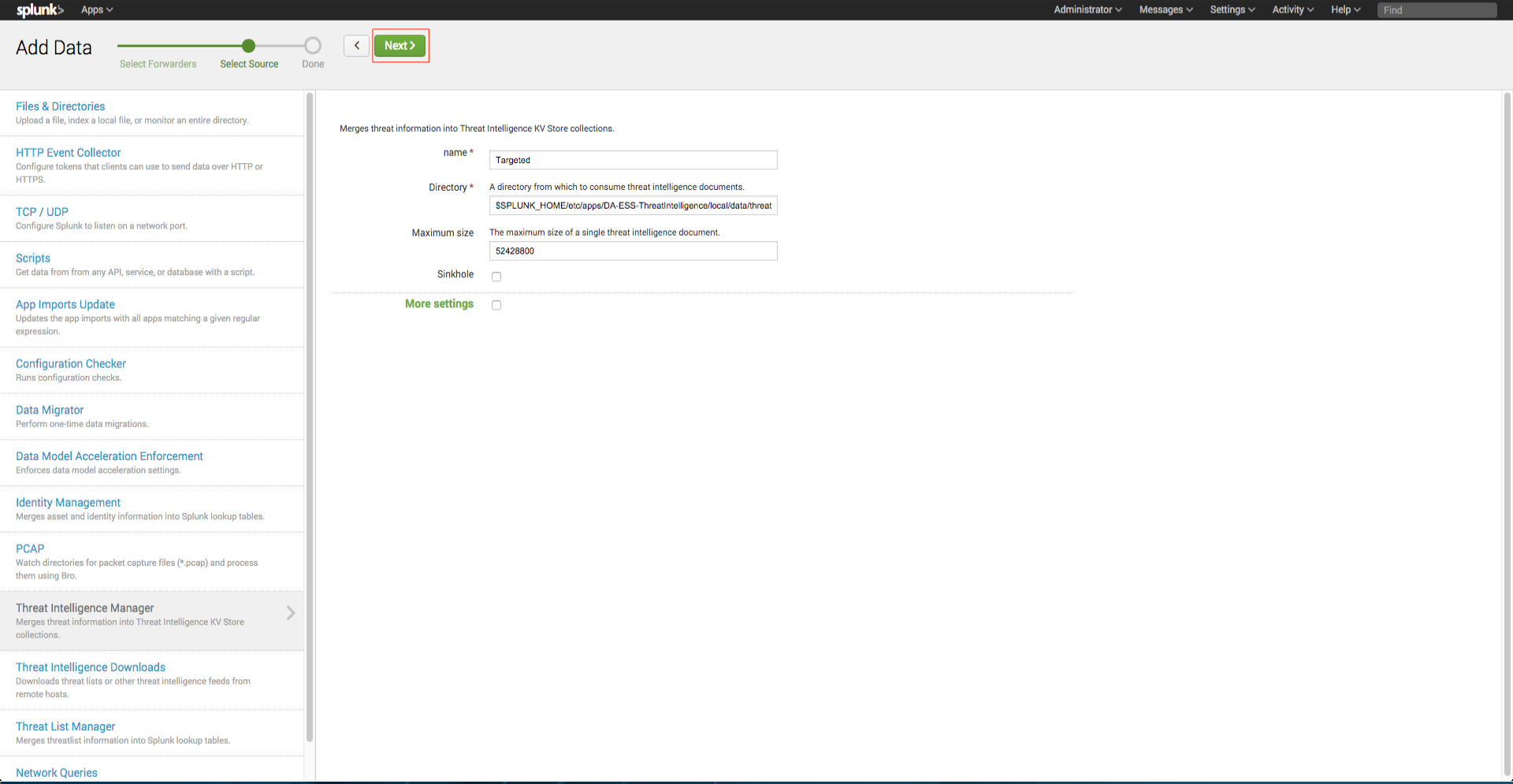
Results per page 25

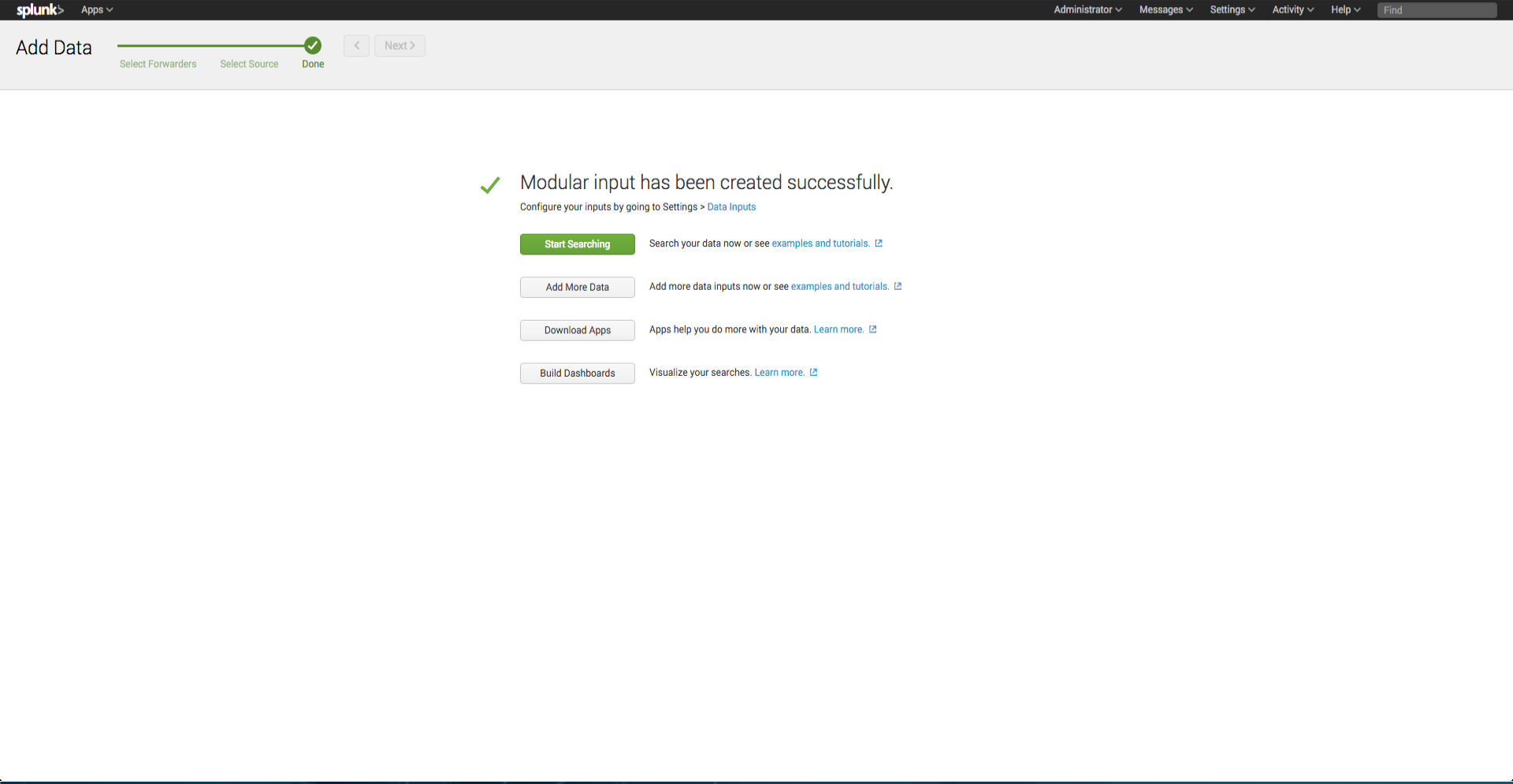
name	Directory	Maximum size	Sinkhole	Source type	Index	Status	Actions
Advanced Threat	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/advanced_threat	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
Commodity	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/commodity	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
Financial	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/financial	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
Unknown	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/unknown	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
da_ess_threat_default	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone
da_ess_threat_local	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone
local_lookups	ignored	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone
sa_threat_local	$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/local/data/threat_intel	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone


splunk> Apps
Administrator Messages Settings Activity Help Find
Add Data
Select Forwarders
Select Source
Done
Next >
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure Splunk to listen on a network port.
Scripts
Get data from from any API, service, or database with a script.
App Imports Update
Updates the app imports with all apps matching a given regular expression.
Configuration Checker
Runs configuration checks.
Data Migrator
Perform one-time data migrations.
Data Model Acceleration Enforcement
Enforces data model acceleration settings.
Identity Management
Merges asset and identity information into Splunk lookup tables.
PCAP
Watch directories for packet capture files (*.pcap) and process them using Bro.
Threat Intelligence Manager
Merges threat information into Threat Intelligence KV Store collections.
Threat Intelligence Downloads
Downloads threat lists or other threat intelligence feeds from remote hosts.
Threat List Manager
Merges threatlist information into Splunk lookup tables.
Network Queries
Merges threat information into Threat Intelligence KV Store collections.
name *
Directory *
A directory from which to consume threat intelligence documents.
Maximum size
The maximum size of a single threat intelligence document.
Sinkhole
More settings


splunk> Apps
Administrator Messages Settings Activity Help Find
Add Data
Select Forwarders
Select Source
Done
Next >
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure Splunk to listen on a network port.
Scripts
Get data from from any API, service, or database with a script.
App Imports Update
Updates the app imports with all apps matching a given regular expression.
Configuration Checker
Runs configuration checks.
Data Migrator
Perform one-time data migrations.
Data Model Acceleration Enforcement
Enforces data model acceleration settings.
Identity Management
Merges asset and identity information into Splunk lookup tables.
PCAP
Watch directories for packet capture files (*.pcap) and process them using Bro.
Threat Intelligence Manager
Merges threat information into Threat Intelligence KV Store collections.
Threat Intelligence Downloads
Downloads threat lists or other threat intelligence feeds from remote hosts.
Threat List Manager
Merges threatlist information into Splunk lookup tables.
Network Queries
Merges threat information into Threat Intelligence KV Store collections.
name *
Targeted
Directory *
A directory from which to consume threat intelligence documents.
Maximum size
The maximum size of a single threat intelligence document.
Sinkhole
More settings


splunk> Apps
Administrator Messages Settings Activity Help Find
Add Data
Select Forwarders
Select Source
Done
Next >
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure Splunk to listen on a network port.
Scripts
Get data from from any API, service, or database with a script.
App Imports Update
Updates the app imports with all apps matching a given regular expression.
Configuration Checker
Runs configuration checks.
Data Migrator
Perform one-time data migrations.
Data Model Acceleration Enforcement
Enforces data model acceleration settings.
Identity Management
Merges asset and identity information into Splunk lookup tables.
PCAP
Watch directories for packet capture files (*.pcap) and process them using Bro.
Threat Intelligence Manager
Merges threat information into Threat Intelligence KV Store collections.
Threat Intelligence Downloads
Downloads threat lists or other threat intelligence feeds from remote hosts.
Threat List Manager
Merges threatlist information into Splunk lookup tables.
Network Queries
Merges threat information into Threat Intelligence KV Store collections.
name *
Targeted
Directory *
A directory from which to consume threat intelligence documents.
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat
Maximum size
The maximum size of a single threat intelligence document.
Sinkhole
More settings


splunk> Apps
Administrator Messages Settings Activity Help Find
Add Data
Select Forwarders
Select Source
Done
Next >
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure Splunk to listen on a network port.
Scripts
Get data from from any API, service, or database with a script.
App Imports Update
Updates the app imports with all apps matching a given regular expression.
Configuration Checker
Runs configuration checks.
Data Migrator
Perform one-time data migrations.
Data Model Acceleration Enforcement
Enforces data model acceleration settings.
Identity Management
Merges asset and identity information into Splunk lookup tables.
PCAP
Watch directories for packet capture files (*.pcap) and process them using Bro.
Threat Intelligence Manager
Merges threat information into Threat Intelligence KV Store collections.
Threat Intelligence Downloads
Downloads threat lists or other threat intelligence feeds from remote hosts.
Threat List Manager
Merges threatlist information into Splunk lookup tables.
Network Queries
Merges threat information into Threat Intelligence KV Store collections.
name *
Targeted
Directory *
A directory from which to consume threat intelligence documents.
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat
Maximum size
The maximum size of a single threat intelligence document.
52428800
Sinkhole
More settings


splunk> Apps
Administrator Messages Settings Activity Help Find
Add Data
Select Forwarders Select Source Done
Next >
Modular input has been created successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples and tutorials.
Add More Data
Add more data inputs now or see examples and tutorials.
Download Apps
Apps help you do more with your data. Learn more.
Build Dashboards
Visualize your searches. Learn more.

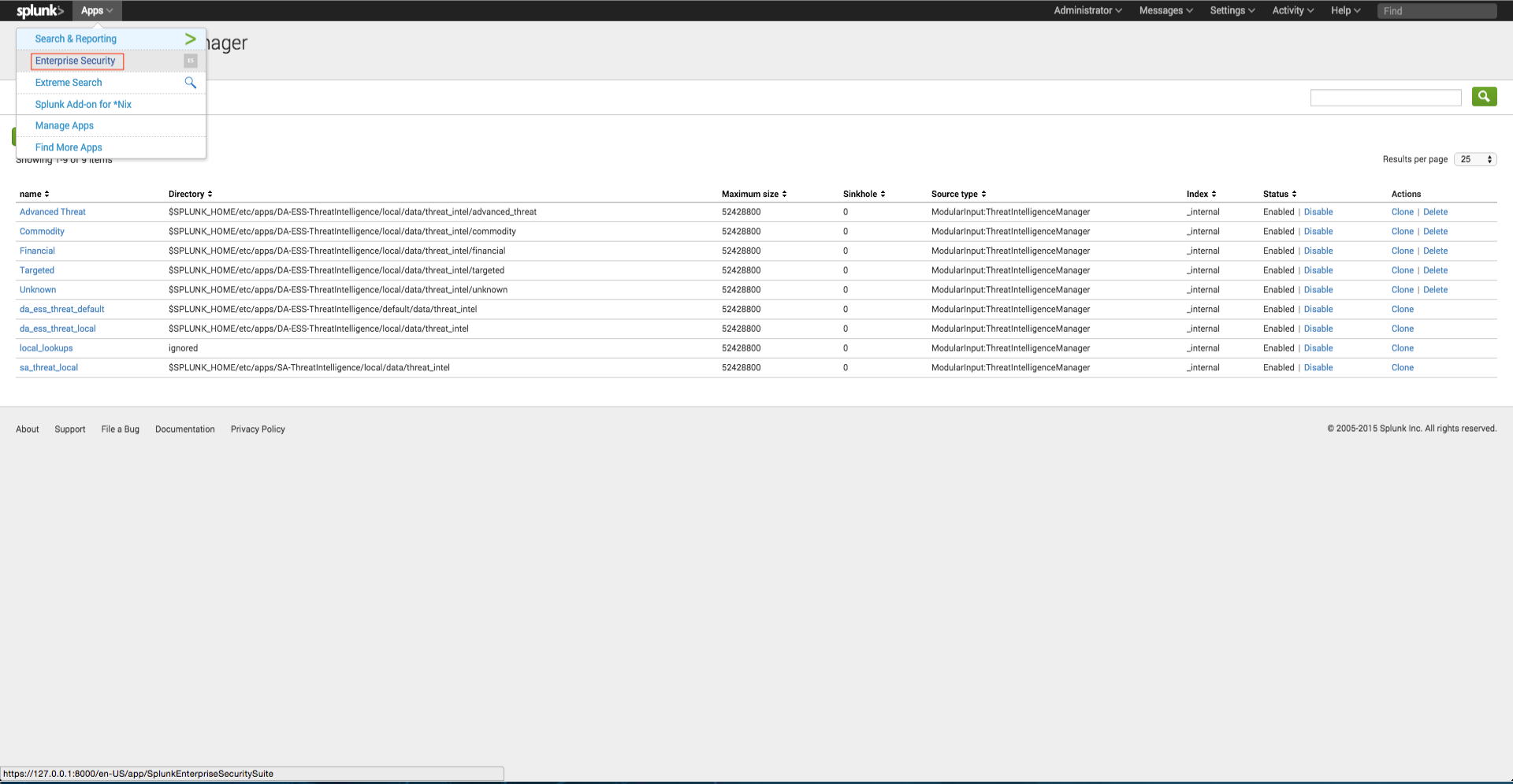
Threat Intelligence Manager

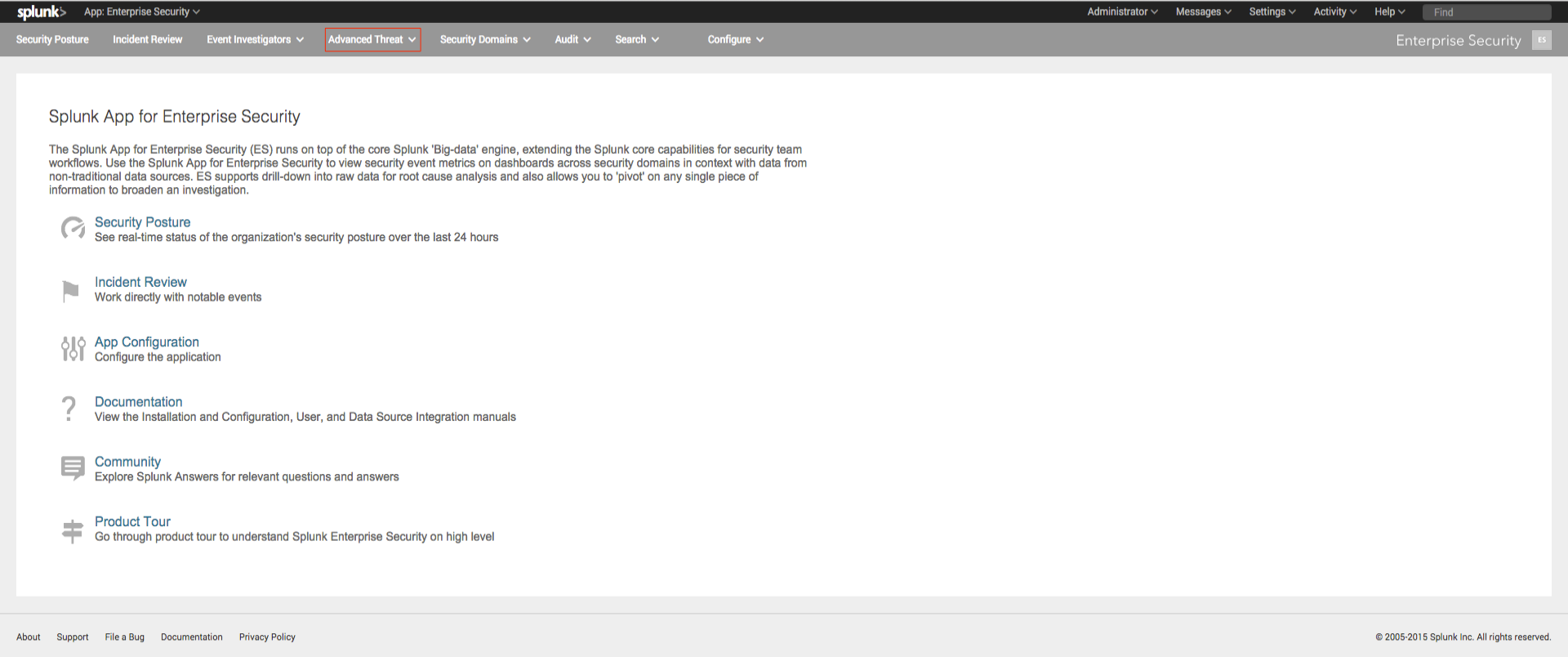
New

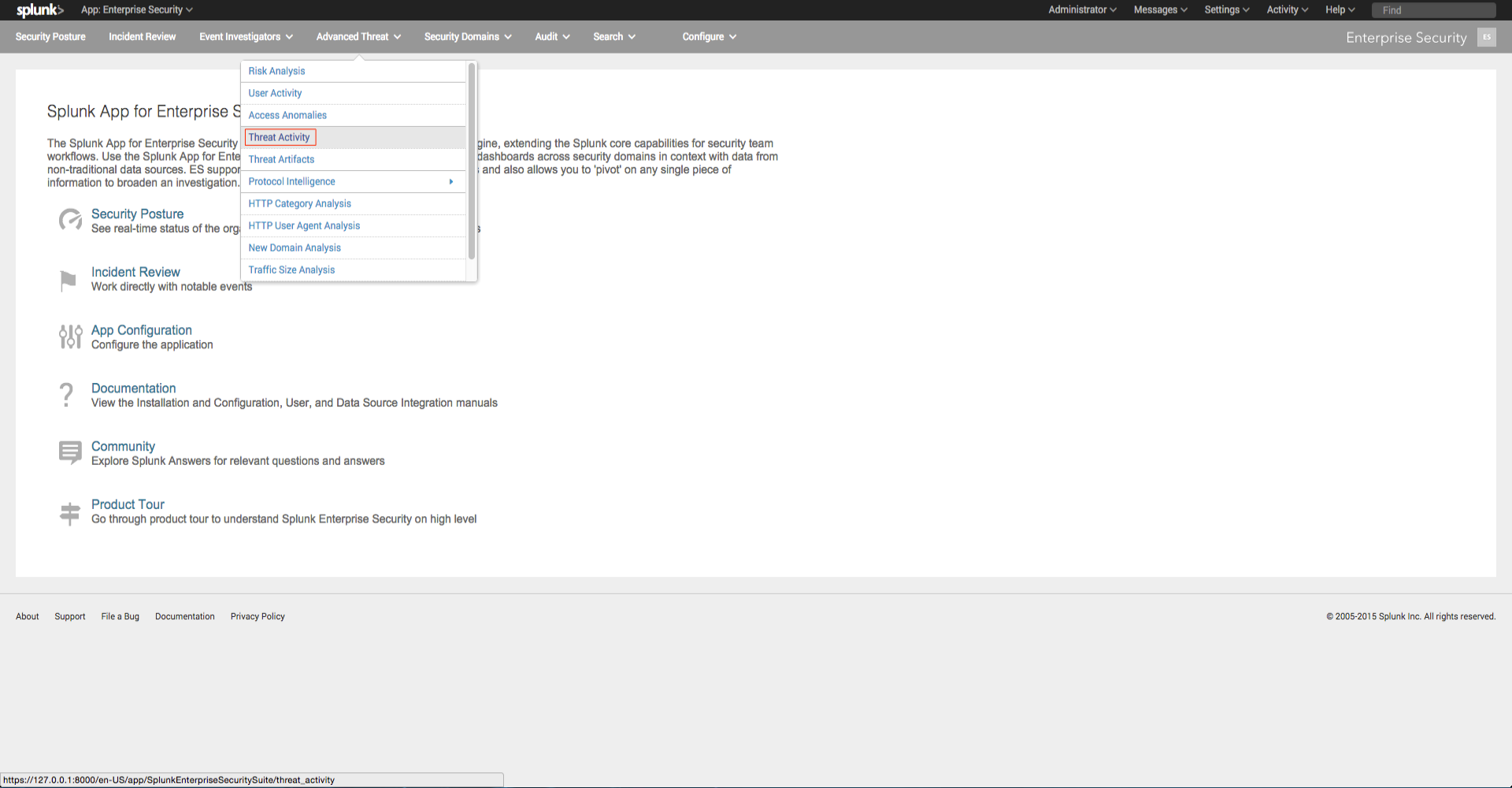
Showing 1-9 of 9 items

Results per page 25

name	Directory	Maximum size	Sinkhole	Source type	Index	Status	Actions
Advanced Threat	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/advanced_threat	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
Commodity	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/commodity	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
Financial	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/financial	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
Targeted	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/targeted	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
Unknown	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/unknown	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone | Delete
da_ess_threat_default	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone
da_ess_threat_local	$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone
local_lookups	ignored	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone
sa_threat_local	$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/local/data/threat_intel	52428800	0	ModularInput:ThreatIntelligenceManager	_internal	Enabled | Disable	Clone


splunk>
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search & Reporting
Enterprise Security
Extreme Search
Splunk Add-on for *Nix
Manage Apps
Find More Apps
Results per page
25
name
Directory
Maximum size
Sinkhole
Source type
Index
Status
Actions
Advanced Threat
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/advanced_threat
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone | Delete
Commodity
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/commodity
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone | Delete
Financial
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/financial
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone | Delete
Targeted
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/targeted
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone | Delete
Unknown
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/unknown
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone | Delete
da_ess_threat_default
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone
da_ess_threat_local
$SPLUNK_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone
local_lookups
ignored
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone
sa_threat_local
$SPLUNK_HOME/etc/apps/SA-ThreatIntelligence/local/data/threat_intel
52428800
0
ModularInput:ThreatIntelligenceManager
_internal
Enabled | Disable
Clone
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.


splunk> App: Enterprise Security
Administrator
Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
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
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.


splunk> App: Enterprise Security
Administrator
Messages
Settings
Activity
Help
Find
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
Splunk App for Enterprise S
The Splunk App for Enterprise Security
gine, extending the Splunk core capabilities for security team
workflows. Use the Splunk App for Ente
dashboards across security domains in context with data from
non-traditional data sources. ES suppor
and also allows you to 'pivot' on any single piece of
information to broaden an investigation.
Security Posture
See real-time status of the org
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
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.
https://127.0.0.1:8000/en-US/app/SplunkEnterpriseSecuritySuite/threat_activity

Threat Activity

Edit | More Info

Threat Group: All

Threat Category: All

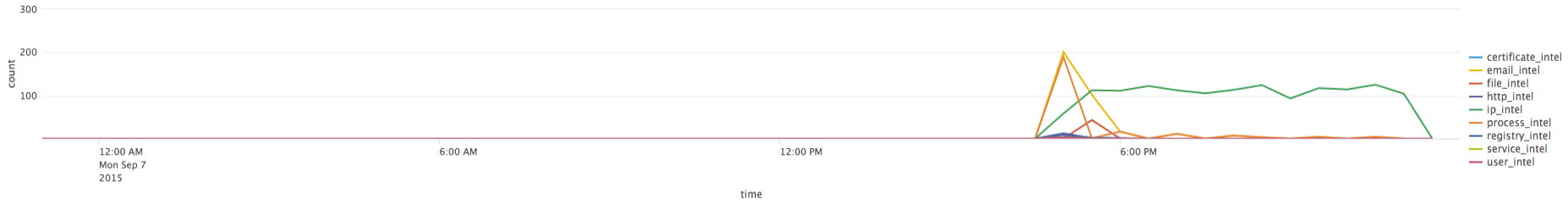
Search: Threat Match Value | Last 24 hours | Submit

Advanced Filter...

Edit

THREAT MATCHES	THREAT COLLECTIONS	THREAT CATEGORIES	THREAT SOURCES	THREAT ACTIVITY
Unique Count	Unique Count	Unique Count	Unique Count	Total Count
924 +924	9 +9	13 +13	20 +20	2k +2k

Threat Activity Over Time



Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		558	1410
email_intel	Email Address Matches Email Subject Matches File Name Matches Network Resolution Matches Source And Destination Matches		1	348
process_intel	Network Resolution Matches Process Matches Source And Destination Matches		2	235
file_intel	File Hash Matches		24	43

Most Active Threat Sources

source_id	source_path	source_type	count
iblocklist_proxy	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.csv	csv	530
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	348
iblocklist_web_attacker	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_web_attacker.csv	csv	330
iblocklist_spyware	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.csv	csv	289
6bd24113-2922-4d25-b490-f727f47ba948	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	234
iblocklist_tor	/usr/local/bamboo/splunk-install/current/etc/apps/SA-	csv	161

Threat Activity

Edit | More Info

Threat Group: All

Threat Category: All

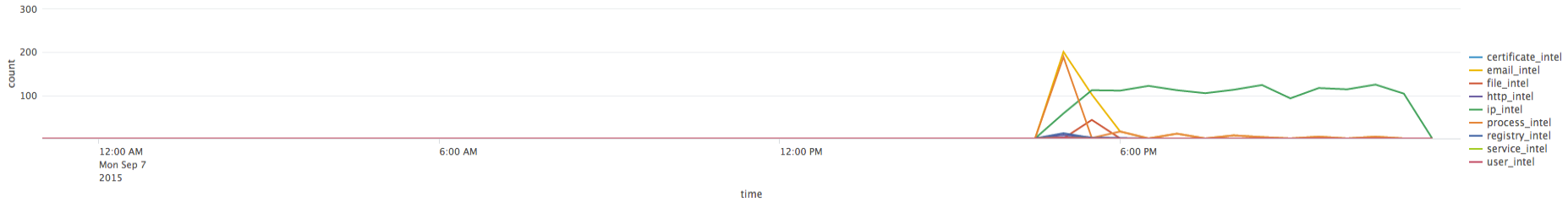
- All
- Financial
- Unknown
- Commodity
- Targeted
- APT
- Email Utility
- HTTP Utility

Search: Threat Match Value | Last 24 hours | Submit | Advanced Filter...

Edit

THREAT MATCHES	THREAT CATEGORIES	THREAT SOURCES	THREAT ACTIVITY
Unique Count	Unique Count	Unique Count	Total Count
924 +924	13 +13	20 +20	2k +2k

Threat Activity Over Time



Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		558	1410
email_intel	Email Address Matches Email Subject Matches File Name Matches Network Resolution Matches Source And Destination Matches		1	348
process_intel	Network Resolution Matches Process Matches Source And Destination Matches		2	235
file_intel	File Hash Matches		24	43

Most Active Threat Sources

source_id	source_path	source_type	count
iblocklist_proxy	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.csv	csv	530
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	348
iblocklist_web_attacker	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_web_attacker.csv	csv	330
iblocklist_spyware	/usr/local/bamboo/splunk-install/current/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.csv	csv	289
6bd24113-2922-4d25-b490-f727f47ba948	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	234
iblocklist_tor	/usr/local/bamboo/splunk-install/current/etc/apps/SA-	csv	161

Threat Activity

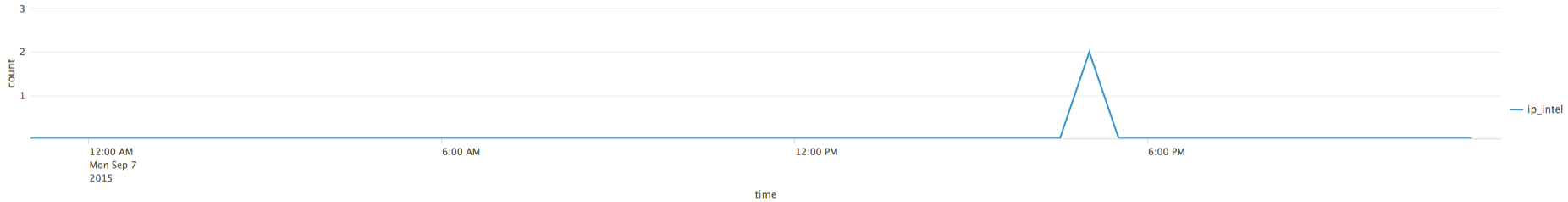
Edit | More Info

Threat Group: All | Threat Category: APT | 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
924 +924	9 +9	13 +13	20 +20	2k +2k

Threat Activity Over Time



Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Source And Destination Matches		1	2

Most Active Threat Sources

source_id	source_path	source_type	count
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	2

Threat Activity Details

_time	threat_match_field	threat_match_value	filter	sourcetype	src	dest	threat_collection	threat_group	threat_category
2015-9-7 17:15:00	dest	204.13.162.123		FireEye_CEF	129.17.73.122 158.138.219.125	204.13.162.123	ip_intel	F admin338 japanorus nitro th3bug wl	APT APT APT

Threat Activity

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 | More Info

Threat Group: All | Threat Ca: APT | Last 24 hours | Submit | Advanced Filter...

Edit

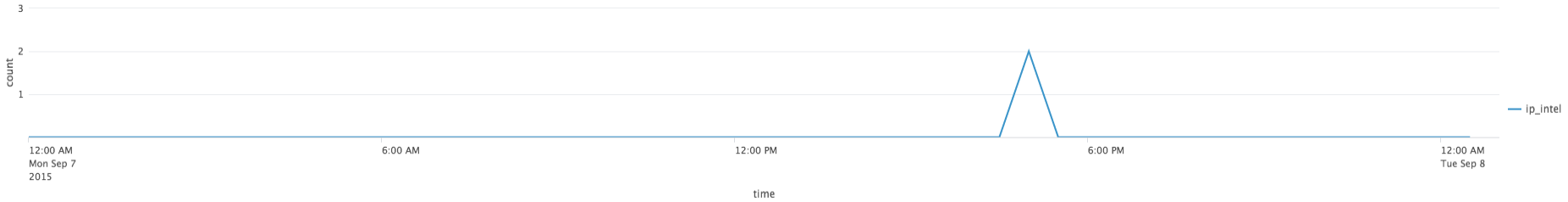
THREAT MATCHES Unique Count: 954 +954

THRE Unique: 9 ...ORIES

THREAT SOURCES Unique Count: 20 +20

THREAT ACTIVITY Total Count: 2k +2k

Threat Activity Over Time



Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Source And Destination Matches		1	2

Most Active Threat Sources

source_id	source_path	source_type	count
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	2

Threat Activity Details

_time	threat_match_field	threat_match_value	filter	sourcetype	src	dest	threat_collection	threat_group	threat_category
2015-9-7 17:15:00	dest	204.13.162.123		FireEye_CEF	129.17.73.122 158.138.219.125	204.13.162.123	ip_intel	F admin338 japanorus nitro th3bug wl	APT APT APT

soln-esnightly.sv.splunk.com:8000/splunk-es/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

Threat Overview | Network | Endpoint | Certificate | Email

Threat Overview

source_id	source_path	source_type	threat_group	threat_category	malware_alias	count
0c7c902c-67f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel.ioc	ioc	APT	Utility		5
0c7c902c-61f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.1.ioc	ioc	APT1.1	Utility1.1		5
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	Email APT	Email Utility		7
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F (and 6 more)	APT (and 2 more)		503
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc	ioc	HTTP APT	HTTP Utility		10
fc2d3e44-80a6-4add-ad94-de9f289e62ff	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc	ioc	IP APT	IP Utility		9
6bd24113-2922-4d25-b490-f727f47ba948	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	Process APT	Process Backdoor		12
4a2c5f60-f4c0-4844-ba1f-a14dac9fa36c	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/registry_intel.ioc	ioc	Registry APT	Registry Backdoor		9
7f9a6986-f00a-4071-99d3-484c9158beba	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/service_intel.ioc	ioc	Service APT	Service Backdoor		6
e651c4e4-6cce-4cfc-8bd4-ebc203907ef4	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/user_intel.ioc	ioc	User APT	User Utility		2

« prev 1 2 3 next »

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
file_intel	stix	japanorus	APT		194
file_intel	stix	menupass	APT		194
file_intel	stix	nitro	APT		194
file_intel	stix	th3bug	APT		194
file_intel	stix	wl	APT		194
process_intel	stix	undefined	undefined		15
registry_intel	ioc	Registry APT	Registry Backdoor		9

« prev 1 2 next »

Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category	malware_alias
ip_intel	csv	0	9992	0	0	9992	malware_domains	threatlist_domain	
ip_intel	csv	6163	0	0	0	6163	iblocklist_tor	threatlist	
ip_intel	csv	5817	0	0	0	5817	iblocklist_proxy	threatlist	
ip_intel	csv	3662	0	0	0	3662	iblocklist_spyware	threatlist	
ip_intel	stix	0	2046	0	0	2046	undefined	undefined	
ip_intel	csv	1499	0	0	0	1499	iblocklist_web_attacker	threatlist	
ip_intel	stix	164	145	0	0	309	F	APT	
ip_intel	stix	164	145	0	0	309	admin338	APT	
ip_intel	stix	164	145	0	0	309	japanorus	APT	
ip_intel	stix	164	145	0	0	309	menupass	APT	

« prev 1 2 3 next »

Email Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
email_intel	ioc	Email APT	Email Utility		6

Certificate Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
certificate_intel	stix	undefined	undefined		13

Threat Artifacts

Edit | More Info

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

Threat Category dropdown: All, Financial, Unknown, Commodity, Targeted, APT, Email Utility, HTTP Utility

Threat Overview | Network | Email

Threat Overview

source_id	source_path	source_type	threat_group	threat_category	malware_alias	count
0c7c902c-67f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel.ioc	ioc	APT	Utility		5
0c7c902c-61f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.1.ioc	ioc	APT1.1	Utility1.1		5
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	Email APT	Email Utility		7
fireeye:stix-b7b16e67-4292-46a3-ba64-60	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F (and 6 more)	APT (and 2 more)		503
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc	ioc	HTTP APT	HTTP Utility		10
fc2d3e44-80a6-4add-ad94-de9f289e62ff	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc	ioc	IP APT	IP Utility		9
6bd24113-2922-4d25-b490-f727f47ba948	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	Process APT	Process Backdoor		12
4a2c5f60-f4c0-4844-ba1f-a14dac9fa36c	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/registry_intel.ioc	ioc	Registry APT	Registry Backdoor		9
7f9a6986-f00a-4071-99d3-484c9158beba	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/service_intel.ioc	ioc	Service APT	Service Backdoor		6
e651c4e4-6cce-4cfc-8bd4-ebc203907ef4	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/user_intel.ioc	ioc	User APT	User Utility		2

« prev 1 2 3 next »

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
file_intel	stix	japanorus	APT		194
file_intel	stix	menupass	APT		194
file_intel	stix	nitro	APT		194
file_intel	stix	th3bug	APT		194
file_intel	stix	wl	APT		194
process_intel	stix	undefined	undefined		15
registry_intel	ioc	Registry APT	Registry Backdoor		9

« prev 1 2 next »

Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category	malware_alias
ip_intel	csv	0	9992	0	0	9992	malware_domains	threatlist_domain	
ip_intel	csv	6163	0	0	0	6163	iblocklist_tor	threatlist	
ip_intel	csv	5817	0	0	0	5817	iblocklist_proxy	threatlist	
ip_intel	csv	3662	0	0	0	3662	iblocklist_spyware	threatlist	
ip_intel	stix	0	2046	0	0	2046	undefined	undefined	
ip_intel	csv	1499	0	0	0	1499	iblocklist_web_attacker	threatlist	
ip_intel	stix	164	145	0	0	309	F	APT	
ip_intel	stix	164	145	0	0	309	admin338	APT	
ip_intel	stix	164	145	0	0	309	japanorus	APT	
ip_intel	stix	164	145	0	0	309	menupass	APT	

« prev 1 2 3 next »

Email Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
email_intel	ioc	Email APT	Email Utility		6

Certificate Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
certificate_intel	stix	undefined	undefined		13

Threat Artifacts

Edit | More Info

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

Threat Overview | Network | Endpoint | Certificate | Email

Threat Overview

source_id	source_path	source_type	threat_group	threat_category	malware_alias	count
0c7c902c-67f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel.ioc	ioc	APT	Utility		5
0c7c902c-61f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.1.ioc	ioc	APT1.1	Utility1.1		5
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	Email APT	Email Utility		7
fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F (and 6 more)	APT (and 2 more)		503
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc	ioc	HTTP APT	HTTP Utility		10
fc2d3e44-80a6-4add-ad94-de9f289e62ff	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc	ioc	IP APT	IP Utility		9
6bd24113-2922-4d25-b490-f727f47ba948	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	Process APT	Process Backdoor		12
4a2c5f60-f4c0-4844-ba1f-a14dac9fa36c	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/registry_intel.ioc	ioc	Registry APT	Registry Backdoor		9
7f9a6986-f00a-4071-99d3-484c9158beba	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/service_intel.ioc	ioc	Service APT	Service Backdoor		6
e651c4e4-6cce-4cfc-8bd4-ebc203907ef4	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/user_intel.ioc	ioc	User APT	User Utility		2

« prev 1 2 3 next »

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
file_intel	stix	japanorus	APT		194
file_intel	stix	menupass	APT		194
file_intel	stix	nitro	APT		194
file_intel	stix	th3bug	APT		194
file_intel	stix	wl	APT		194
process_intel	stix	undefined	undefined		15
registry_intel	ioc	Registry APT	Registry Backdoor		9

« prev 1 2 next »

Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category	malware_alias
ip_intel	csv	0	9992	0	0	9992	malware_domains	threatlist_domain	
ip_intel	csv	6163	0	0	0	6163	iblocklist_tor	threatlist	
ip_intel	csv	5817	0	0	0	5817	iblocklist_proxy	threatlist	
ip_intel	csv	3662	0	0	0	3662	iblocklist_spyware	threatlist	
ip_intel	stix	0	2046	0	0	2046	undefined	undefined	
ip_intel	csv	1499	0	0	0	1499	iblocklist_web_attacker	threatlist	
ip_intel	stix	164	145	0	0	309	F	APT	
ip_intel	stix	164	145	0	0	309	admin338	APT	
ip_intel	stix	164	145	0	0	309	japanorus	APT	
ip_intel	stix	164	145	0	0	309	menupass	APT	

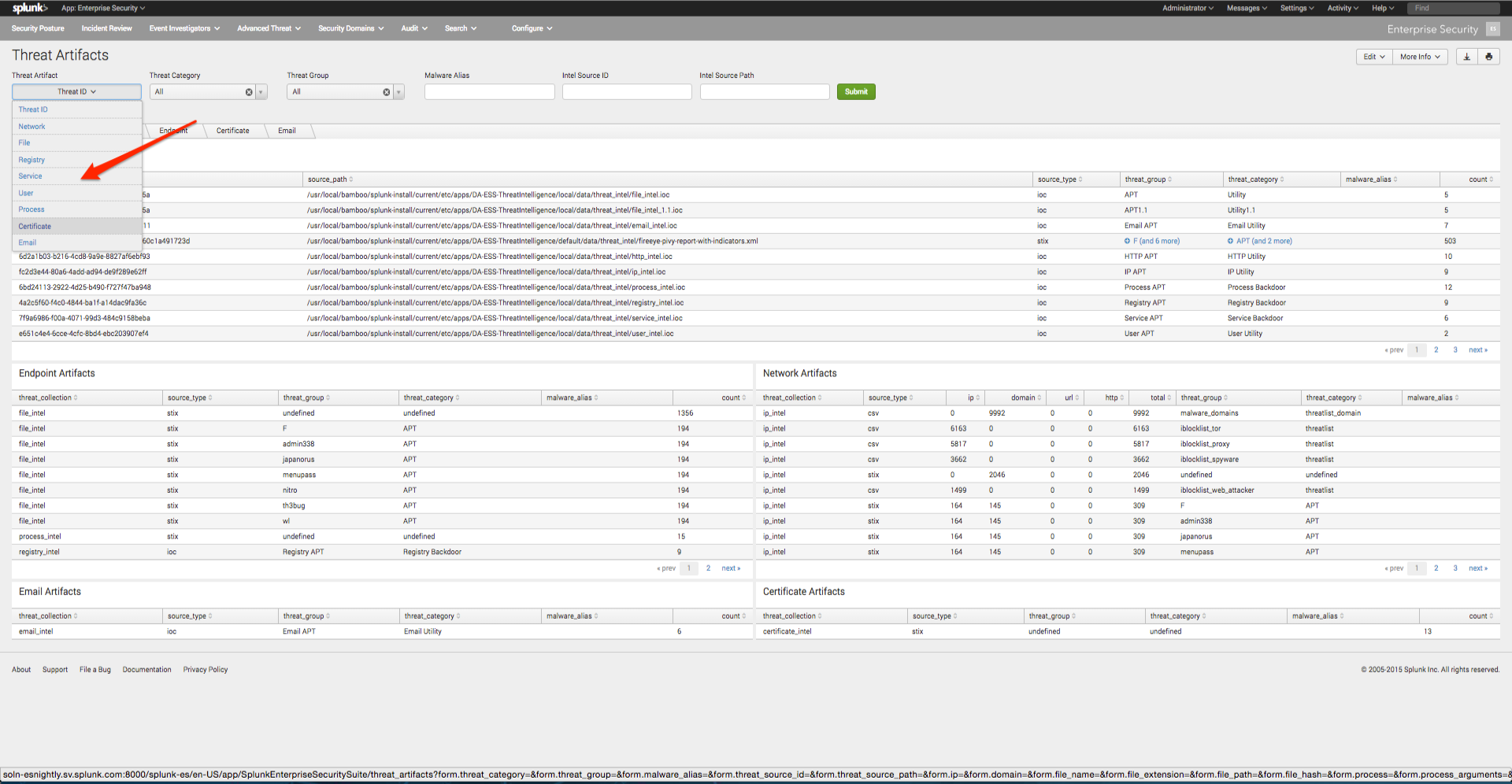
« prev 1 2 3 next »

Email Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
email_intel	ioc	Email APT	Email Utility		6

Certificate Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
certificate_intel	stix	undefined	undefined		13



soln-esnightly.sv.splunk.com:8000/splunk-es/en-US/app/SplunkEnterpriseSecuritySuite/threat_artifacts?form.threat_category=&form.threat_group=&form.malware_alias=&form.threat_source_id=&form.threat_source_path=&form.ip=&form.domain=&form.file_name=&form.file_extension=&form.file_path=&form.file_hash=&form.process=&form.process_arguments=&

Threat Artifacts

Threat Artifact: Certificate

Serial Number	Subject	Issuer	Validity Not After	Validity Not Before	
					Submit

Edit | More Info

Threat Overview | Network | Endpoint | Certificate | Email

Threat Overview

source_id	source_path	source_type	threat_group	threat_category	malware_alias	count
0c7c902c-67f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel.ioc	ioc	APT	Utility		5
0c7c902c-61f8-479c-9f44-4d985106365a	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/file_intel_1.1.ioc	ioc	APT1.1	Utility1.1		5
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/email_intel.ioc	ioc	Email APT	Email Utility		7
fireeye:stix-b7b116e67-4292-46a3-ba64-60c1a491723d	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F (and 6 more)	APT (and 2 more)		503
6d2a1b03-b216-4cd8-9a9e-8827af6ebf93	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/http_intel.ioc	ioc	HTTP APT	HTTP Utility		10
fc2d3e44-80a6-4add-ad94-de9f289e62ff	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/ip_intel.ioc	ioc	IP APT	IP Utility		9
6bd24113-2922-4d25-b490-f727f47ba948	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/process_intel.ioc	ioc	Process APT	Process Backdoor		12
4a2c5f60-f4c0-4844-ba1f-a14dac9fa36c	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/registry_intel.ioc	ioc	Registry APT	Registry Backdoor		9
7f9a6986-f00a-4071-99d3-484c9158beba	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/service_intel.ioc	ioc	Service APT	Service Backdoor		6
e651c4e4-6cce-4cfc-8bd4-ebc203907ef4	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat_intel/user_intel.ioc	ioc	User APT	User Utility		2

« prev 1 2 3 next »

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
file_intel	stix	japanorus	APT		194
file_intel	stix	menupass	APT		194
file_intel	stix	nitro	APT		194
file_intel	stix	th3bug	APT		194
file_intel	stix	wl	APT		194
process_intel	stix	undefined	undefined		15
registry_intel	ioc	Registry APT	Registry Backdoor		9

« prev 1 2 next »

Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group	threat_category	malware_alias
ip_intel	csv	0	9992	0	0	9992	malware_domains	threatlist_domain	
ip_intel	csv	6163	0	0	0	6163	iblocklist_tor	threatlist	
ip_intel	csv	5817	0	0	0	5817	iblocklist_proxy	threatlist	
ip_intel	csv	3662	0	0	0	3662	iblocklist_spyware	threatlist	
ip_intel	stix	0	2046	0	0	2046	undefined	undefined	
ip_intel	csv	1499	0	0	0	1499	iblocklist_web_attacker	threatlist	
ip_intel	stix	164	145	0	0	309	F	APT	
ip_intel	stix	164	145	0	0	309	admin338	APT	
ip_intel	stix	164	145	0	0	309	japanorus	APT	
ip_intel	stix	164	145	0	0	309	menupass	APT	

« prev 1 2 3 next »

Email Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
email_intel	ioc	Email APT	Email Utility		6

Certificate Artifacts

threat_collection	source_type	threat_group	threat_category	malware_alias	count
certificate_intel	stix	undefined	undefined		13

Threat Artifacts

Edit | More Info

Threat Artifact: Certificate | Serial Number | Subject | Issuer | Validity Not After | Validity Not Before | Submit

Threat Overview | Network | Endpoint | Certificate | Email

HTTP Intelligence

i	http_method	url	uri_path	uri_query	http_version	header	data	http_content_type	http_referrer	http_user_agent	http_user_agent_length	status	cookie	threat_group	threat_category	source_id
>		*/SugarCE520e/index.php* (and 1 more)					newdata		*/admin/common/script.js.php* (and 1 more)	*Microsoft BITS/6.6* (and 1 more)				HTTP APT	HTTP Utility	6d2a1b03-b216-4cd8-9a9e-8827af6ebf93

IP Intelligence

i	ip	domain	threat_collection	organization_id	organization_name	address	city	state_prov	postal_code	country	threat_group
>	*0.0.0.0*	47.255.160.10.in-addr.arpa (and 4 more)	ip_intel								IP APT
>	*99.12.45.6*	47.255.160.10.in-addr.arpa (and 4 more)	ip_intel								IP APT
>	*unknown*	47.255.160.10.in-addr.arpa (and 4 more)	ip_intel								IP APT
>	0.0.0.0	47.255.160.10.in-addr.arpa (and 4 more)	ip_intel								IP APT (and
>	1.33.225.20		ip_intel				Tokyo			Japan	iblocklist_tor
>	1.34.163.57		ip_intel							Taiwan	iblocklist_tor
>	1.169.182.227		ip_intel							Taiwan	iblocklist_proxy
>	1.169.206.132		ip_intel							Taiwan	iblocklist_tor
>	1.172.188.203		ip_intel							Taiwan	iblocklist_proxy
>	1.227.92.185		ip_intel				Seoul			Republic of Korea	iblocklist_proxy

« prev 1 2 3 4 5 6 7 8 9 10 next »

Domain Intelligence

domain	ip	threat_collection	threat_group	threat_category	source_id
0000mps.webpreview.dsl.net		ip_intel	malware_domains	threatlist_domain	malware_domains
000webseucadastro.vai.la		ip_intel	malware_domains	threatlist_domain	malware_domains
00cf.com		ip_intel	malware_domains	threatlist_domain	malware_domains
00game.net		ip_intel	malware_domains	threatlist_domain	malware_domains
0fees.net		ip_intel	malware_domains	threatlist_domain	malware_domains
0g8e.webcam		ip_intel	malware_domains	threatlist_domain	malware_domains
0kgg.com		ip_intel	malware_domains	threatlist_domain	malware_domains
0x.x.gg		ip_intel	malware_domains	threatlist_domain	malware_domains
0zpd.com		ip_intel	malware_domains	threatlist_domain	malware_domains
001.vwoool.com		ip_intel	malware_domains	threatlist_domain	malware_domains

« prev 1 2 3 4 5 6 7 8 9 10 next »

Threat Artifacts

Edit | More Info

Threat Artifact: Certificate | Serial Number | Subject | Issuer | Validity Not After | Validity Not Before | Submit

Threat Overview | Network | Endpoint | Certificate | Email

File Intelligence

i	file_hash	file_name	file_extension	file_path	file_size	threat_collection	threat_group	threat_category	source_id
>	ffcc7271e951055f12b61f520ce1e4c7					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	ff9aa093a37819af65a06046ea0c830c					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	ff9aa093a37819af65a06046ea0c830c					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	ff2d1edbcaf04e8a02dc61fc225e2b91					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	ff2d1edbcaf04e8a02dc61fc225e2b91					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	ff085d421518772ce2df75282363279f					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	ff085d421518772ce2df75282363279f					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	fefa3638e4d6f2e00b5194ae3fa0c931					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	fefa3638e4d6f2e00b5194ae3fa0c931					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	feb406ff01d9fd5abc5ea079e0543e31					file_intel	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240

« prev 1 2 3 4 5 6 7 8 9 10 next »

Registry Intelligence

i	registry_hive	registry_path	registry_key_name	registry_value_name	registry_value_type	registry_value_text	registry_value_da
>	threat.log	*CurrentVersion\SvcHost\SaSaut\threat* (and 2 more)		ServiceDLL (and 1 more)	REG_BINARY	Comhtml.mshtml.1 (and 1 more)	0x00000003(3)
>	system						
>							*{B02DAAF7-C67
>							*acrod32.exe*
>				ServiceDLL			
>							*java.exe*
>	HKEY_LOCAL_MACHINE						
>							*lssap32.exe*
>							iprinp32.dll
>	SOFTWARE						

« prev 1 2 3 4 5 6 7 8 next »

Process Intelligence

i	process	process_arguments	process_handle_name	process_handle_type	threat_group	threat_category	source_id
>	*updatasched.exe*				undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>	/bin/cmd1	arg1	*AFX_Ideas_H*	Mutant	Process APT	Process Backdoor	6bd24113-2922-4d25-b490-f727f47ba948
>			*rio16drv*		undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>			*HAHAHAHAHAHAH*		undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>			AdobeReaderX		undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>			ADR64		undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>			ADR32		undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>				Mutant	undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>			*rio32drv*		undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240
>			*LETUSHAVEAGOODTIME*		undefined	undefined	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240

« prev 1 2 3 next »

Service Intelligence

i	service	descriptive_name	service_description	status	service_type	start_mode	threat_group	threat_category	source_id
>	*OSEASV* (and 1 more)	Device File System	Saves installation reports	new	newtype	*mode1*	Service APT	Service Backdoor	7f9a6986-f00a-4071-99d3-484c9158beba

User Intelligence

user	full_name	group_name	user_description	threat_group	threat_category	source_id
ACMEDC01$ (and 1 more)	test user	all	define user	User APT	User Utility	e651c4e4-6cce-4cfc-8bd4-ebc203907ef4

Threat Artifacts

Edit More Info

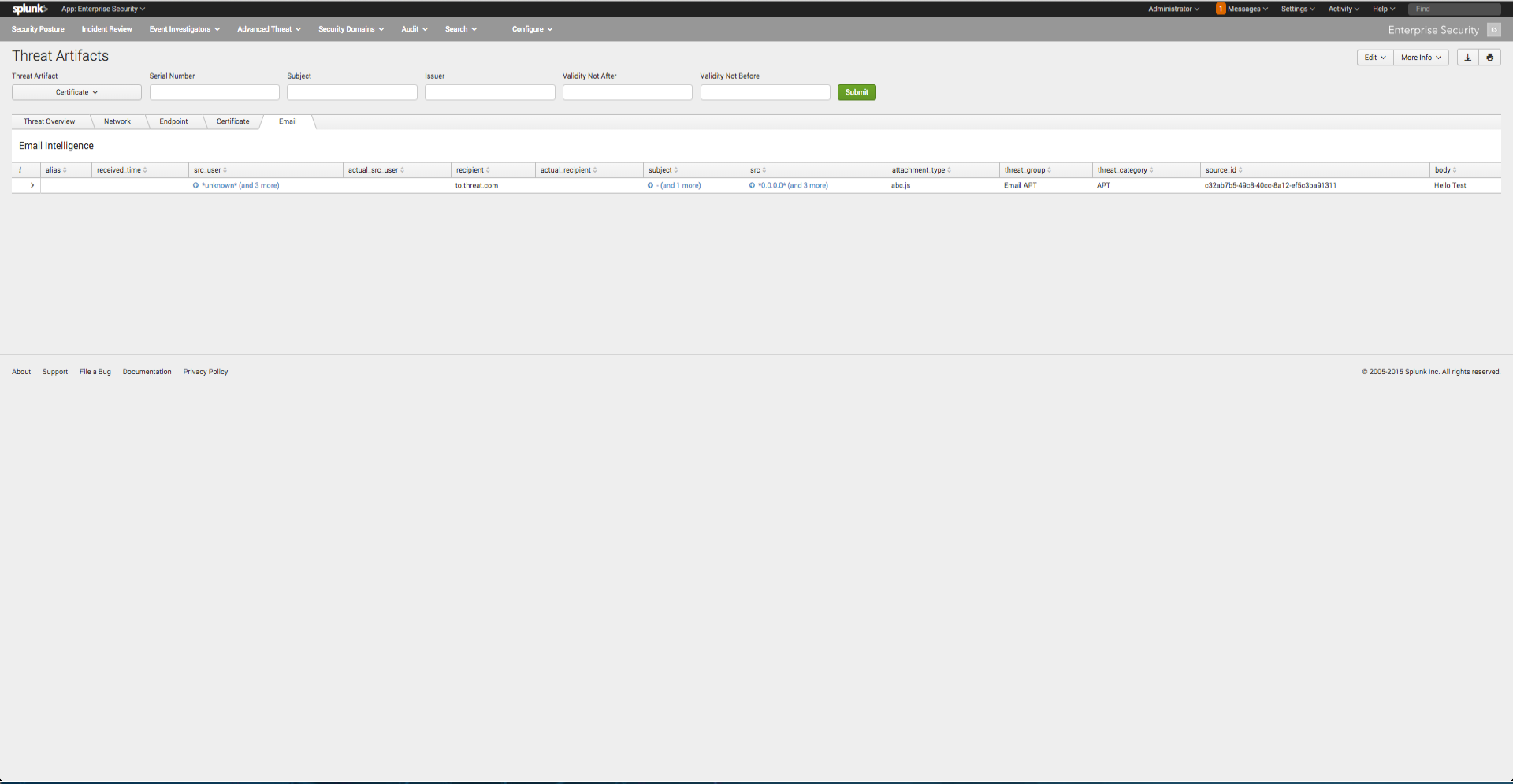
Threat Artifact: Certificate | Serial Number | Subject | Issuer | Validity Not After | Validity Not Before | Submit

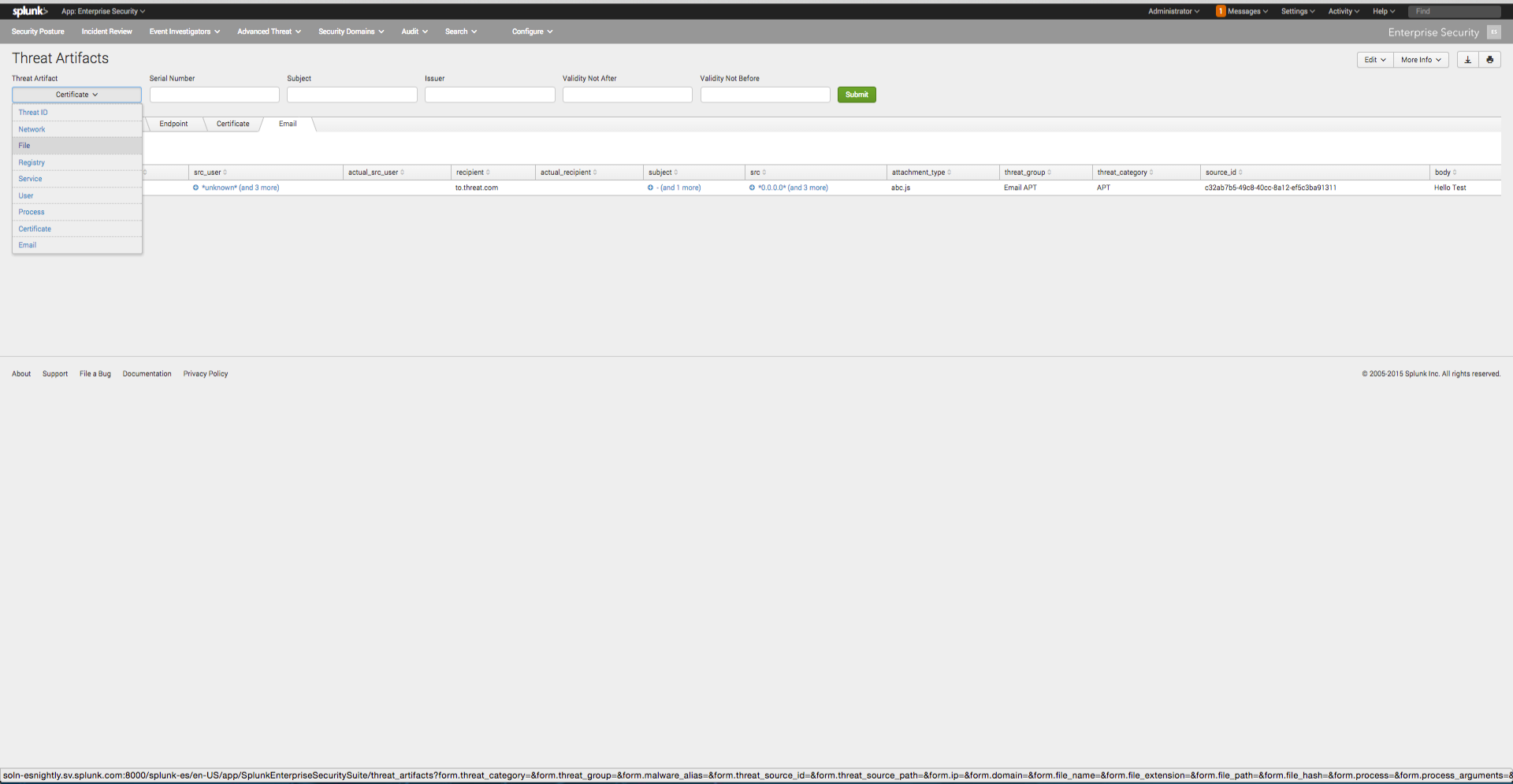
Threat Overview | Network | Endpoint | Certificate | Email

Certificate Intelligence

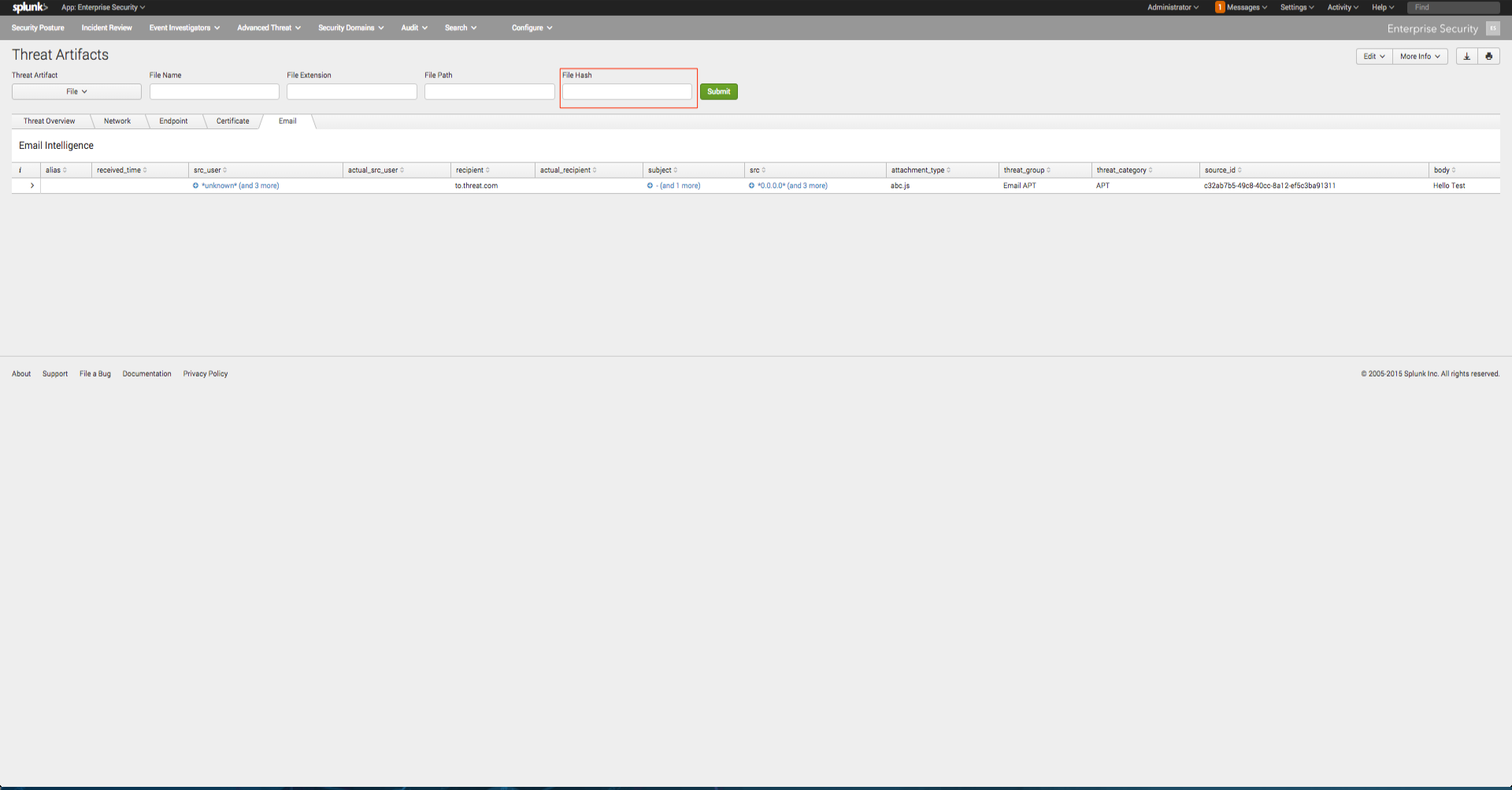
i	alias	certificate_serial	certificate_issuer	certificate_subject	certificate_start_time	certificate_end_time	certificate_version	certificate_handshake_type	certificate_publickey_algorithm	certificate_signature_algorithm	certificate_supported_next_protocol	certificate_serial_clean
>		0x7c:a2:74:d0:fb:c3:d1:54:b3:d1:a3:00:62:e3:7e:f6	CN=mail.aol.com	CN=mail.aol.com			3		rsaEncryption	md5WithRSAEncryption		0x7ca274d0fbc3d154b3d1a
>		0x72:a2:5c:8a:b4:18:71:4e:bf:c6:6f:3f:98:d6:f7:74	CN=NS	CN=NS			3		rsaEncryption	sha1WithRSA		0x72a25c8ab418714ebfc66
>		0x4c:0b:1d:19:74:86:a7:66:b4:1a:bf:40:27:21:76:28	CN=WEBMAIL	CN=WEBMAIL			3		rsaEncryption	sha1WithRSA		0x4c0b1d197486a766b41at
>		0x46:37:ea:15:b6:54:96:4c:b6:44:2b:7b:06:1a:a5:30	CN=ALPHA	CN=ALPHA			3		rsaEncryption	sha1WithRSA		0x4637ea15b654964cb644
>		0x2f:09:dd:e0:ff:81:b7:6c:bf:2f:17:92:0c:d8:bd:57	CN=EMAIL	CN=EMAIL			3		rsaEncryption	sha1WithRSA		0x2f09dde0ff81b76cbf2f17
>		0x20:82:92:3f:43:2c:8f:75:b7:ef:0f:6a:d9:3c:8e:5d	CN=SUR	CN=SUR			3		rsaEncryption	sha1WithRSA		0x2082923f432c8f75b7ef0f
>		0x0a:38:c9:27:08:6f:96:4b:be:75:dc:9f:c0:1a:c6:28	CN=mail.yahoo.com	CN=mail.yahoo.com			3		rsaEncryption	md5WithRSAEncryption		0x0a38c927086f964bbe75d
>		0x1	C=US, ST=Some-State, O=www.virtuallythere.com, OU=new, CN=new	C=US, ST=Some-State, O=www.virtuallythere.com, OU=new, CN=new			3		rsaEncryption	sha1WithRSAEncryption		0x1
>		0x0e:97:88:1c:6c:a1:37:96:42:03:bc:45:42:24:75:6c	CN=LM-68AB71FBD8F5	CN=LM-68AB71FBD8F5			3		rsaEncryption	sha1WithRSA		0x0e97881c6ca137964203b
>		0x52:55:38:16:fb:0d:1a:8a:4b:45:04:cb:06:bc:c4:af	CN=SERVER	CN=SERVER			3		rsaEncryption	sha1WithRSA		0x5255381 6fb0d1a8a4b450

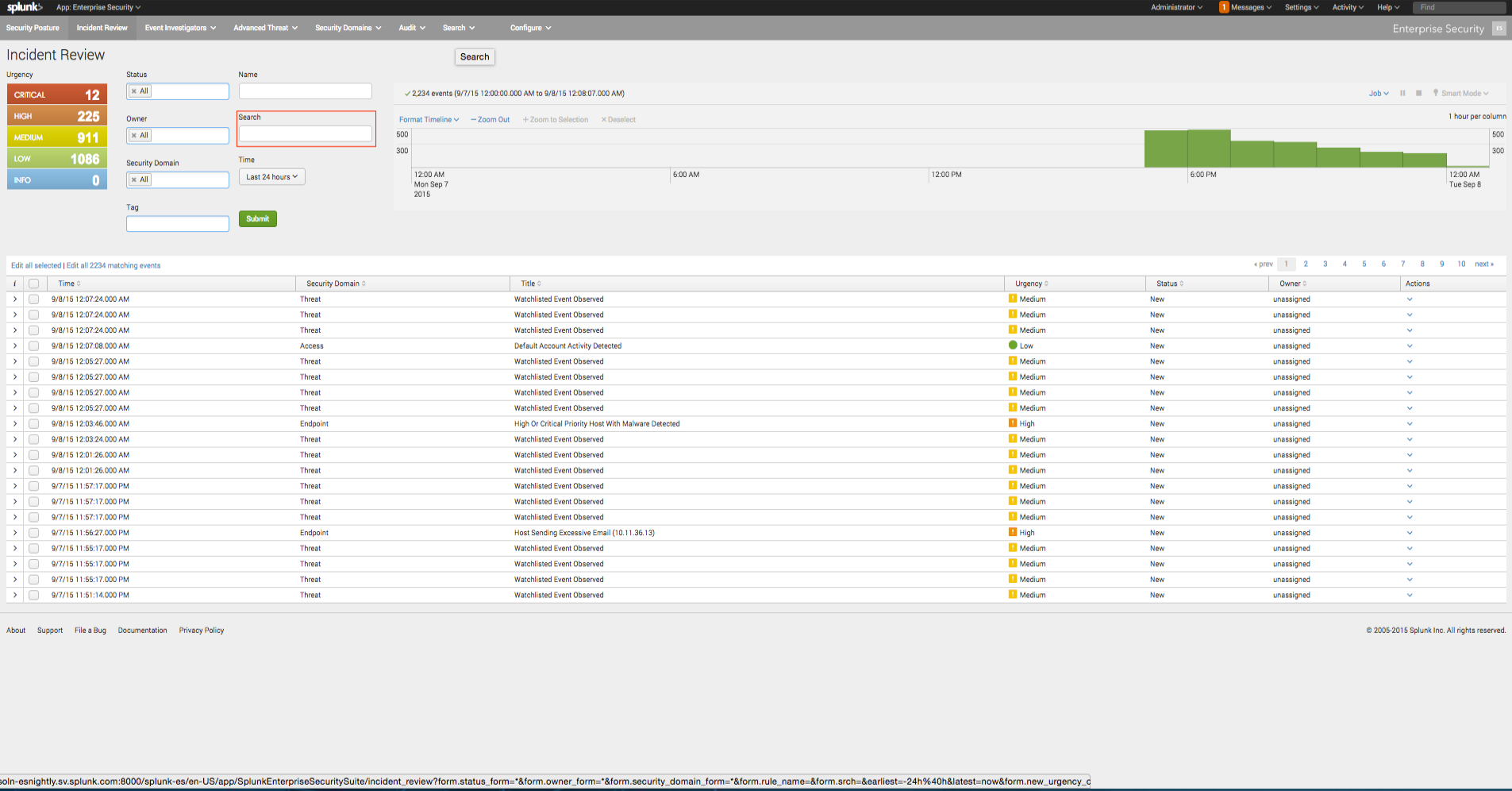
« prev 1 2 next »

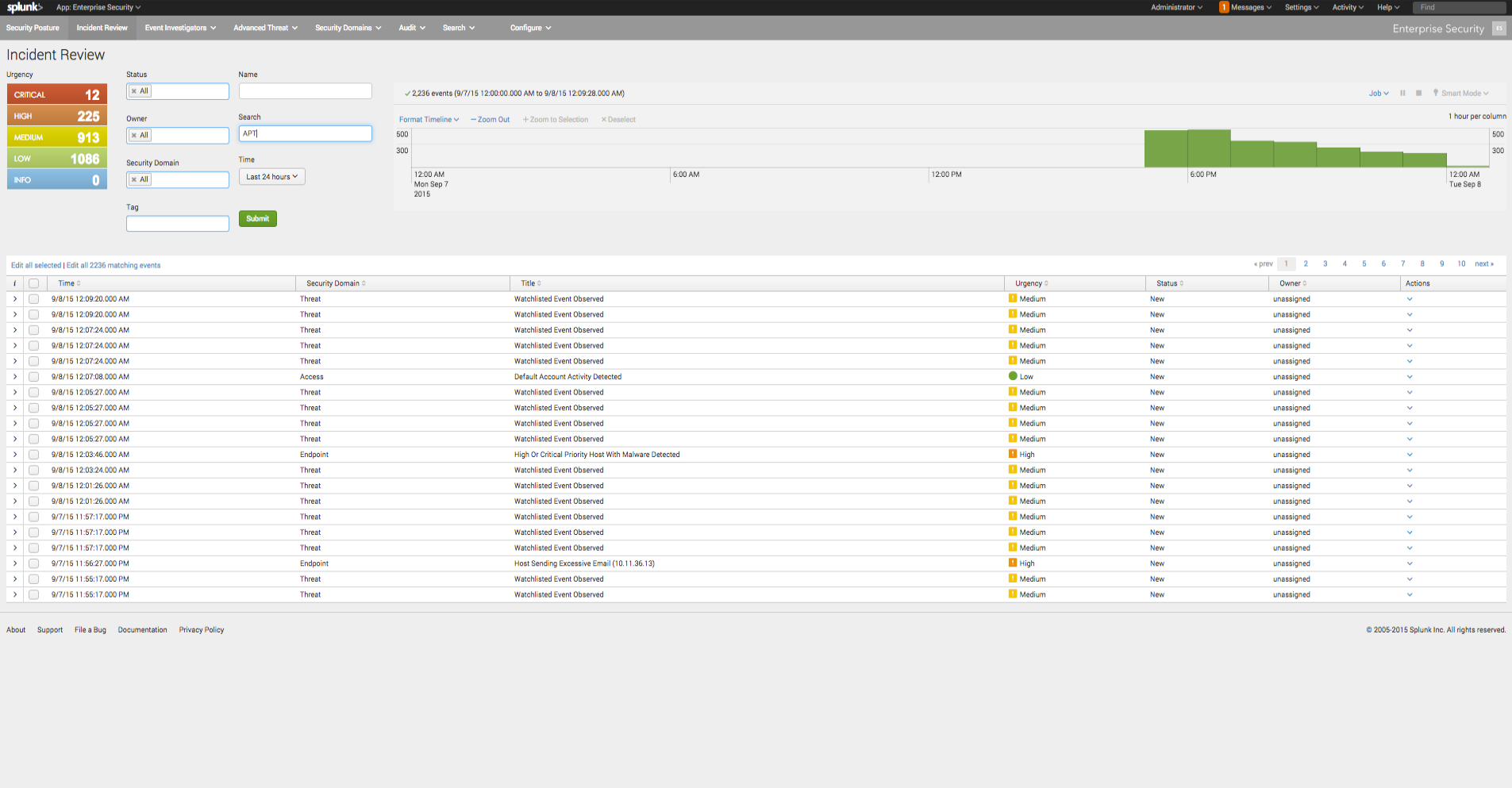

splunk> App: Enterprise Security
Administrator
1 Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Threat Artifacts
Edit
More Info
Threat Artifact
Certificate
Serial Number
Subject
Issuer
Validity Not After
Validity Not Before
Submit
Threat Overview
Network
Endpoint
Certificate
Email
Email Intelligence
i
alias
received_time
src_user
actual_src_user
recipient
actual_recipient
subject
src
attachment_type
threat_group
threat_category
source_id
body
unknown (and 3 more)
to.threat.com
- (and 1 more)
0.0.0.0 (and 3 more)
abc.js
Email APT
APT
c32ab7b5-49c8-40cc-8a12-ef5c9ba91311
Hello Test
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.

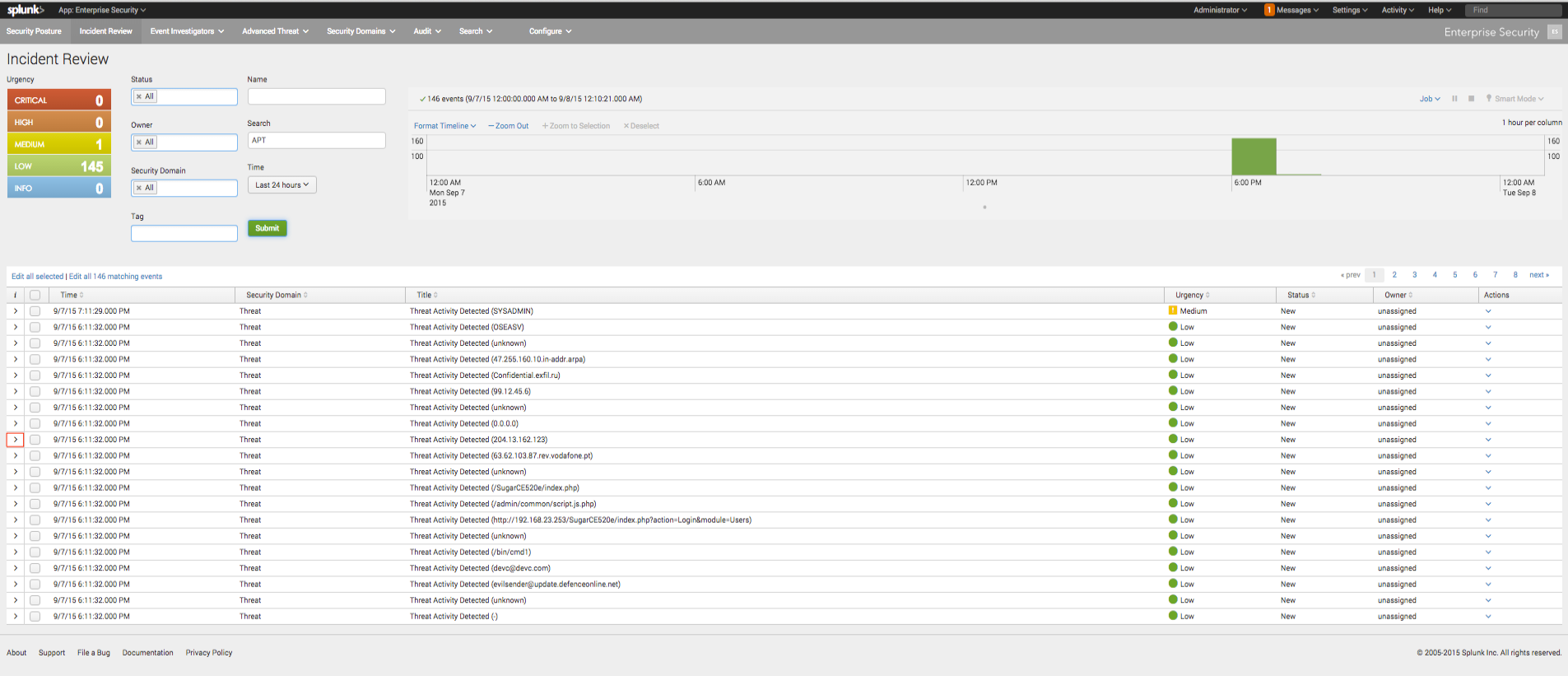


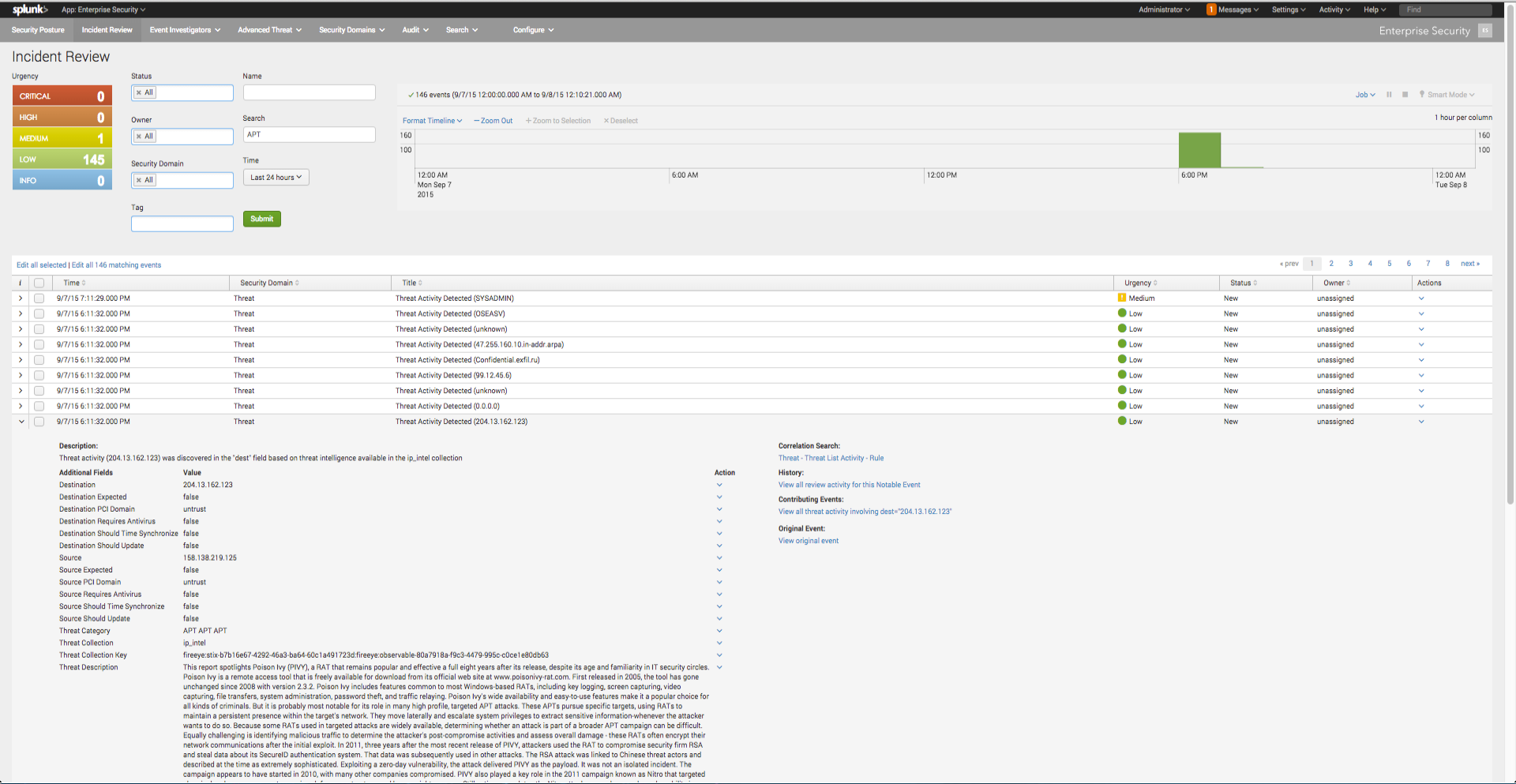
soln-esnightly.sv.splunk.com:8000/splunk-es/en-US/app/SplunkEnterpriseSecuritySuite/threat_artifacts?form.threat_category=&form.threat_group=&form.malware_alias=&form.threat_source_id=&form.threat_source_path=&form.ip=&form.domain=&form.file_name=&form.file_extension=&form.file_path=&form.file_hash=&form.process=&form.process_arguments=&


splunk> App: Enterprise Security
Administrator
1 Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Threat Artifacts
Edit
More Info
Threat Artifact
File
File Name
File Extension
File Path
File Hash
Submit
Threat Overview
Network
Endpoint
Certificate
Email
Email Intelligence
i
alias
received_time
src_user
actual_src_user
recipient
actual_recipient
subject
src
attachment_type
threat_group
threat_category
source_id
body
unknown (and 3 more)
to.threat.com
- (and 1 more)
0.0.0.0 (and 3 more)
abc.js
Email APT
APT
c32ab7b5-49c8-40cc-8a12-ef5c3ba91311
Hello Test
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.


splunk> App: Enterprise Security
Administrator Messages Settings Activity Help Find
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Incident Review
Search
Urgency
CRITICAL 12
HIGH 225
MEDIUM 911
LOW 1086
INFO 0
Status
All
Name
Owner
All
Search
Security Domain
All
Time
Last 24 hours
Tag
Submit
2,234 events (9/7/15 12:00:00.000 AM to 9/8/15 12:08:07.000 AM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
500
300
12:00 AM Mon Sep 7 2015
6:00 AM
12:00 PM
6:00 PM
12:00 AM Tue Sep 8
Edit all selected | Edit all 2234 matching events
« prev 1 2 3 4 5 6 7 8 9 10 next »
i
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/8/15 12:07:24.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:07:24.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:07:24.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:07:08.000 AM Access Default Account Activity Detected Low New unassigned
9/8/15 12:05:27.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:05:27.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:05:27.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:05:27.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:03:46.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/8/15 12:03:24.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:01:26.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:01:26.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:57:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:57:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:57:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:56:27.000 PM Endpoint Host Sending Excessive Email (10.11.36.13) High New unassigned
9/7/15 11:55:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:55:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:55:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:51:14.000 PM Threat Watchlisted Event Observed Medium New unassigned
About Support File a Bug Documentation Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.
soln-esnightly.sv.splunk.com:8000/splunk-es/en-US/app/SplunkEnterpriseSecuritySuite/incident_review?form.status_form=*&form.owner_form=*&form.security_domain_form=*&form.rule_name=&form.srch=&earliest=-24h%40h&latest=now&form.new_urgency_c


splunk> App: Enterprise Security
Administrator
1 Messages
Settings
Activity
Help
Find
Security Posture
Incident Review
Event Investigators
Advanced Threat
Security Domains
Audit
Search
Configure
Enterprise Security
Incident Review
Urgency
CRITICAL 12
HIGH 225
MEDIUM 913
LOW 1086
INFO 0
Status
All
Name
Owner
All
Search
APT
Security Domain
All
Time
Last 24 hours
Tag
Submit
2,236 events (9/7/15 12:00:00.000 AM to 9/8/15 12:09:28.000 AM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
500
300
12:00 AM Mon Sep 7 2015
6:00 AM
12:00 PM
6:00 PM
12:00 AM Tue Sep 8
Edit all selected | Edit all 2236 matching events
« prev 1 2 3 4 5 6 7 8 9 10 next »
i
Time
Security Domain
Title
Urgency
Status
Owner
Actions
9/8/15 12:09:20.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:09:20.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:07:24.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:07:24.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:07:24.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:07:08.000 AM Access Default Account Activity Detected Low New unassigned
9/8/15 12:05:27.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:05:27.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:05:27.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:05:27.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:03:46.000 AM Endpoint High Or Critical Priority Host With Malware Detected High New unassigned
9/8/15 12:03:24.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:01:26.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/8/15 12:01:26.000 AM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:57:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:57:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:57:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:56:27.000 PM Endpoint Host Sending Excessive Email (10.11.36.13) High New unassigned
9/7/15 11:55:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
9/7/15 11:55:17.000 PM Threat Watchlisted Event Observed Medium New unassigned
About Support File a Bug Documentation Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.


splunk> App: Enterprise Security
Administrator Messages Settings Activity Help Find
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Incident Review
Urgency
CRITICAL 0
HIGH 0
MEDIUM 1
LOW 145
INFO 0
Status
All
Name
Owner
All
Search
APT
Security Domain
All
Time
Last 24 hours
Tag
Submit
146 events (9/7/15 12:00:00.000 AM to 9/8/15 12:10:21.000 AM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
160
100
12:00 AM Mon Sep 7 2015
6:00 AM
12:00 PM
6:00 PM
12:00 AM Tue Sep 8
Edit all selected | Edit all 146 matching events
« prev 1 2 3 4 5 6 7 8 next »
i Time Security Domain Title Urgency Status Owner Actions
9/7/15 7:11:29.000 PM Threat Threat Activity Detected (SYSADMIN) Medium New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (OSEASV) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (unknown) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (47.255.160.10.in-addr.arpa) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (Confidential.exfil.ru) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (99.12.45.6) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (unknown) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (0.0.0.0) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (204.13.162.123) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (63.62.103.87.rev.vodafone.pt) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (unknown) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (/SugarCE520e/index.php) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (/admin/common/script.js.php) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (http://192.168.23.253/SugarCE520e/index.php?action=Login&module=Users) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (unknown) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (/bin/cmd1) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (devc@devc.com) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (evilsender@update.defenceonline.net) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (unknown) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (-) Low New unassigned
About Support File a Bug Documentation Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.


splunk> App: Enterprise Security
Administrator Messages Settings Activity Help Find
Security Posture Incident Review Event Investigators Advanced Threat Security Domains Audit Search Configure
Enterprise Security
Incident Review
Urgency
CRITICAL 0
HIGH 0
MEDIUM 1
LOW 145
INFO 0
Status
All
Name
Owner
All
Search
APT
Security Domain
All
Time
Last 24 hours
Tag
Submit
146 events (9/7/15 12:00:00.000 AM to 9/8/15 12:10:21.000 AM)
Job
Smart Mode
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
160
100
12:00 AM Mon Sep 7 2015
6:00 AM
12:00 PM
6:00 PM
12:00 AM Tue Sep 8
Edit all selected | Edit all 146 matching events
« prev 1 2 3 4 5 6 7 8 next »
i Time Security Domain Title Urgency Status Owner Actions
9/7/15 7:11:29.000 PM Threat Threat Activity Detected (SYSADMIN) Medium New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (OSEASV) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (unknown) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (47.255.160.10.in-addr.arpa) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (Confidential.exfil.ru) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (99.12.45.6) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (unknown) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (0.0.0.0) Low New unassigned
9/7/15 6:11:32.000 PM Threat Threat Activity Detected (204.13.162.123) Low New unassigned
Description:
Threat activity (204.13.162.123) was discovered in the "dest" field based on threat intelligence available in the ip_intel collection
Additional Fields Value Action
Destination 204.13.162.123
Destination Expected false
Destination PCI Domain untrust
Destination Requires Antivirus false
Destination Should Time Synchronize false
Destination Should Update false
Source 158.138.219.125
Source Expected false
Source PCI Domain untrust
Source Requires Antivirus false
Source Should Time Synchronize false
Source Should Update false
Threat Category APT APT APT
Threat Collection ip_intel
Threat Collection Key fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d:fireeye:observable-80a7918a-f9c3-4479-995c-c0ce1e80db63
Threat Description This report spotlights Poison Ivy (PIVY), a RAT that remains popular and effective a full eight years after its release, despite its age and familiarity in IT security circles. Poison Ivy is a remote access tool that is freely available for download from its official web site at www.poisonivy-rat.com. First released in 2005, the tool has gone unchanged since 2008 with version 2.3.2. Poison Ivy includes features common to most Windows-based RATs, including key logging, screen capturing, video capturing, file transfers, system administration, password theft, and traffic relaying. Poison Ivy's wide availability and easy-to-use features make it a popular choice for all kinds of criminals. But it is probably most notable for its role in many high profile, targeted APT attacks. These APTs pursue specific targets, using RATs to maintain a persistent presence within the target's network. They move laterally and escalate system privileges to extract sensitive information whenever the attacker wants to do so. Because some RATs used in targeted attacks are widely available, determining whether an attack is part of a broader APT campaign can be difficult. Equally challenging is identifying malicious traffic to determine the attacker's post-compromise activities and assess overall damage - these RATs often encrypt their network communications after the initial exploit. In 2011, three years after the most recent release of PIVY, attackers used the RAT to compromise security firm RSA and steal data about its SecureID authentication system. That data was subsequently used in other attacks. The RSA attack was linked to Chinese threat actors and described at the time as extremely sophisticated. Exploiting a zero-day vulnerability, the attack delivered PIVY as the payload. It was not an isolated incident. The campaign appears to have started in 2010, with many other companies compromised. PIVY also played a key role in the 2011 campaign known as Nitro that targeted
Correlation Search:
Threat - Threat List Activity - Rule
History:
View all review activity for this Notable Event
Contributing Events:
View all threat activity involving dest="204.13.162.123"
Original Event:
View original event

9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (0.0.0.0)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (204.13.162.123)		Low	New	unassigned	

Description:
Threat activity (204.13.162.123) was discovered in the "dest" field based on threat intelligence available in the ip_intel collection

Correlation Search:
Threat - Threat List Activity - Rule

History:
View all review activity for this Notable Event

Contributing Events:
View all threat activity involving dest="204.13.162.123"

Original Event:
View original event

Additional Fields	Value	Action
Destination	204.13.162.123	
Destination Expected	false	
Destination PCI Domain	untrust	
Destination Requires Antivirus	false	
Destination Should Time Synchronize	false	
Destination Should Update	false	
Source	158.138.219.125	
Source Expected	false	
Source PCI Domain	untrust	
Source Requires Antivirus	false	
Source Should Time Synchronize	false	
Source Should Update	false	
Threat Category	APT APT APT	
Threat Collection	ip_intel	
Threat Collection Key	fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d:fireeye:observable-80a7918a-f9c3-4479-995c-c0ce1e80db63	
Threat Description	This report spotlights Poison Ivy (PIVY), a RAT that remains popular and effective a full eight years after its release, despite its age and familiarity in IT security circles. Poison Ivy is a remote access tool that is freely available for download from its official web site at www.poisonivy-rat.com. First released in 2005, the tool has gone unchanged since 2008 with version 2.3.2. Poison Ivy includes features common to most Windows-based RATs, including key logging, screen capturing, video capturing, file transfers, system administration, password theft, and traffic relaying. Poison Ivy's wide availability and easy-to-use features make it a popular choice for all kinds of criminals. But it is probably most notable for its role in many high profile, targeted APT attacks. These APTs pursue specific targets, using RATs to maintain a persistent presence within the target's network. They move laterally and escalate system privileges to extract sensitive information-whenever the attacker wants to do so. Because some RATs used in targeted attacks are widely available, determining whether an attack is part of a broader APT campaign can be difficult. Equally challenging is identifying malicious traffic to determine the attacker's post-compromise activities and assess overall damage - these RATs often encrypt their network communications after the initial exploit. In 2011, three years after the most recent release of PIVY, attackers used the RAT to compromise security firm RSA and steal data about its SecureID authentication system. That data was subsequently used in other attacks. The RSA attack was linked to Chinese threat actors and described at the time as extremely sophisticated. Exploiting a zero-day vulnerability, the attack delivered PIVY as the payload. It was not an isolated incident. The campaign appears to have started in 2010, with many other companies compromised. PIVY also played a key role in the 2011 campaign known as Nitro that targeted chemical makers, government agencies, defense contractors, and human rights groups. Still active a year later, the Nitro attackers used a zero-day vulnerability in Java to deploy PIVY in 2012. Just recently, PIVY was the payload of a zero-day exploit in Internet Explorer used in what is known as a "strategic web compromise" attack against visitors to a U.S. government website and a variety of others. RATs require live, direct, real-time human interaction by the APT attacker. This characteristic is distinctly different from crimeware (malware focused on cybercrime), where the criminal can issue commands to their botnet of compromised endpoints whenever they please and set them to work on a common goal such as a spam relay. In contrast, RATs are much more personal and may indicate that you are dealing with a dedicated threat actor that is interested in your organization specifically.	
Threat Group	F admin338 japanorus nitro th3bug wl menupass	
Threat Key	fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d|fireeye-pivy-report-with-indicators.xml	
Threat Match Field	dest	
Threat Match Value	204.13.162.123	
Threat Source ID	fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	
Threat Source Path	/usr/local/bamboo/splunk-install/current/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	
Threat Source Type	stix	

Event Details:

event_id	E2D06EE6-8CC1-4CE2-AB10-53F9E054A2B9@@notable@@456a5e9f65285c7dca922bef3a359c1ea6bf817a
event_hash	456a5e9f65285c7dca922bef3a359c1ea6bf817a
eventtype	suppress_threat_match_field:threat_match_value
	notable

9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (63.62.103.87.rev.vodafone.pt)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (unknown)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (/SugarCE520e/index.php)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (/admin/common/script.js.php)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (http://192.168.23.253/SugarCE520e/index.php?action=Login&module=Users)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (unknown)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (/bin/cmd1)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (devc@devc.com)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (evilsender@update.defenceonline.net)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (unknown)		Low	New	unassigned	
9/7/15 6:11:32.000 PM	Threat	Threat Activity Detected (-)		Low	New	unassigned	

Takeaways

Takeaways

Not all Threat Intel is created equal!

Takeaways

- Not all Threat Intel is created equal!
- Threat Intelligence Manager

Takeaways

- Not all Threat Intel is created equal!
- Threat Intelligence Manager
- Threat Activity / Incident Review

Takeaways

- Not all Threat Intel is created equal!
- Threat Intelligence Manager
- Threat Activity / Incident Review
- Threat Artifacts Dashboard

Takeaways

- Not all Threat Intel is created equal!
- Threat Intelligence Manager
- Threat Activity / Incident Review
- Threat Artifacts Dashboard
- Targeted Intel > OS-INT

Questions

THANK YOU

splunk>