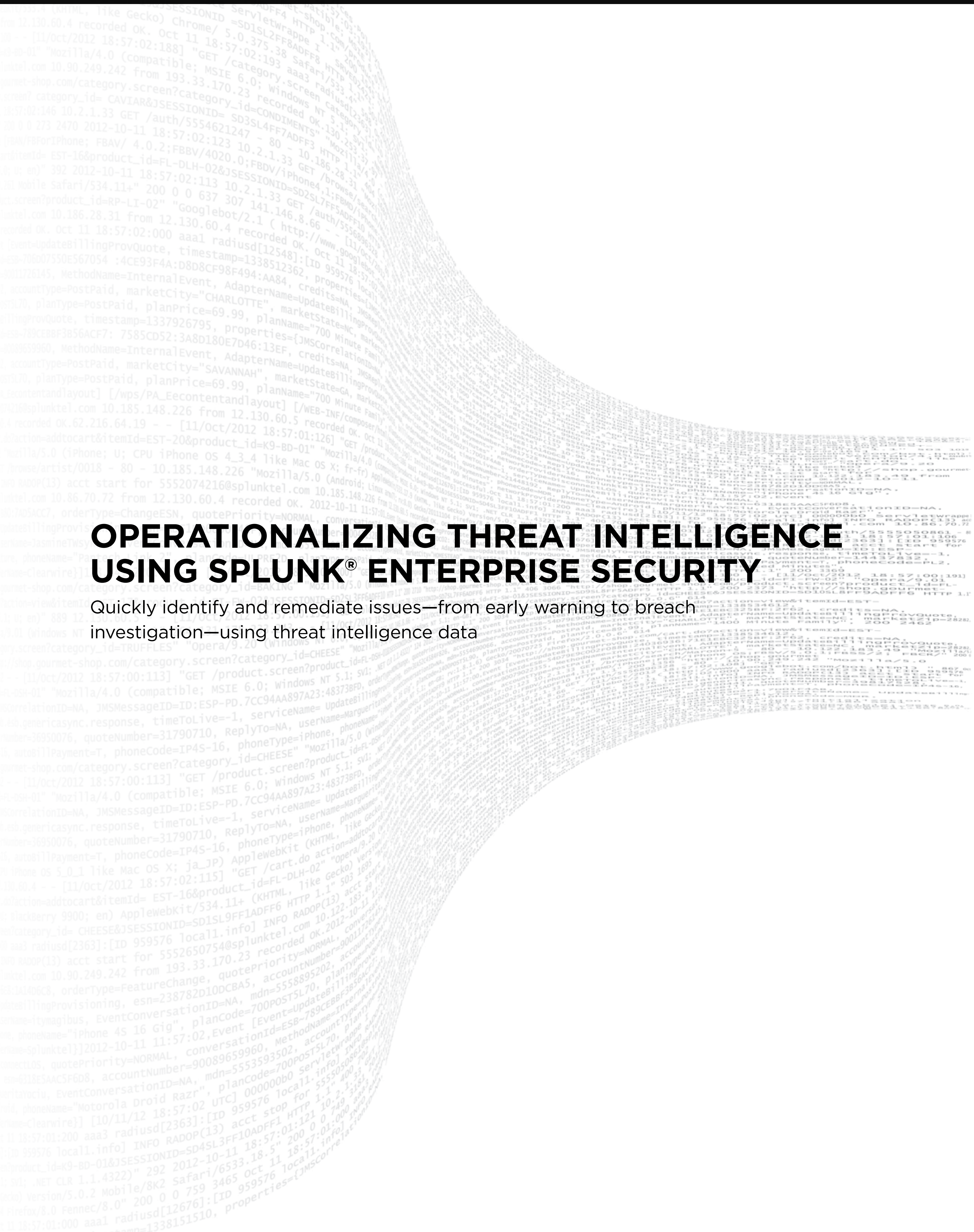
WHITE PAPER



OPERATIONALIZING THREAT INTELLIGENCE USING SPLUNK® ENTERPRISE SECURITY

Quickly identify and remediate issues—from early warning to breach investigation—using threat intelligence data

Table of Contents

Executive Summary

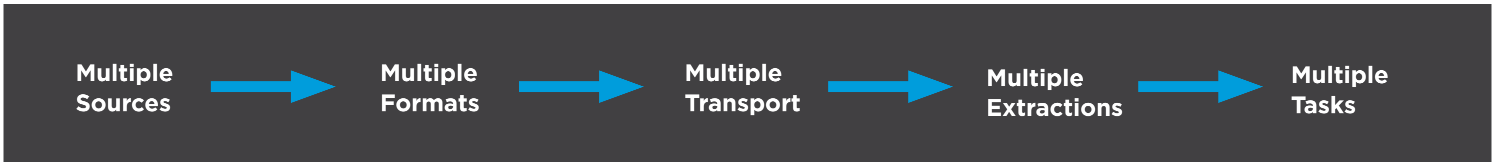
"Threat intelligence" (TI) is evidence-based knowledge — including context, mechanisms, indicators, implications and actionable advice — about an existing or emerging menace or hazard to IT or information assets. It can be used to inform decisions regarding the subject's response to that menace or hazard.[1] Threat intelligence can provide critical security perspective needed to inform an organization about current threats and to help develop a strategy against future threats. Threat intelligence can enable security teams to:

- Detect Malicious Activities
- Prevent Malicious Activities
- Accelerate Response Times
- Save Time and Resources
- Gain Visibility
- Strengthen Security

However, despite its high value as a security technology, operationalizing threat intelligence, or making it readily and easily available to users, is a multi-faceted challenge:

Challenge	Requirement
Maximize coverage	Handle multiple sources
Different formats, mechanisms, tools	Enable use from a central location
Varying confidence levels	Provide a way to prioritize
Difficult to extract value for different tasks	Provide a way to enable faster decisions
Multiple responsibilities and levels of knowledge	Deliver threat context into any operational process

In a nutshell, the challenge to overcome is essentially:



Multiple Sources → Multiple Formats → Multiple Transport → Multiple Extractions → Multiple Tasks

Splunk Enterprise Security (ES) enables security teams to quickly realize the benefits of a high-coverage threat source strategy by providing a threat intelligence platform that can help streamline the delivery of threat context into security operational processes.

This document will describe the challenges and requirements of implementing high-coverage threat intelligence, and how Splunk helps organizations achieve operational maturity with threat intelligence.

[1] "Market Guide for Security Threat Intelligence Services," Gartner, Rob McMillan and Khushbu Pratap, Oct. 22. 2015.

The Need for Threat Intelligence

Modern attacks are perpetrated as a chain of events, comprising multiple activities and components. A limitation of most threat detection technologies is that each solution only handles a particular attack activity or component, thereby burdening users to figure out where an alert sits in the broader sequence of activities.

Threat intelligence provides context from previously seen evidence of attacks, as well as additional context across a range of technologies. Such context can be applied to gain broader perspective of any threat. Applied effectively, threat intelligence can be used to:

- **Detect Malicious Activitie**s – uncovering attacks that originate from compromised systems or are part of an extended, advanced persistent threat (APT); identifying activity against previously seen evidence
- **Prevent Malicious Activities** – providing actionable intelligence to scope and disrupt threats; enabling prioritization of actions to be taken on security devices (e.g., firewalls, web proxies, endpoint devices)
- **Accelerate Response Times** – improving the ability to investigate and perform incident response across all SOC tiers to quickly scope and close out a breach; anticipate and mitigate subsequent malicious activities
- **Save Time and Resources** – eliminating overhead of managing multiple feeds for ad hoc searches and investigations; streamlining processes to investigate, compare and analyze data, across multiple sources
- **Gain Visibility** – making it easy for security operations to access threat intelligence; weighing differing quality and confidence levels of data sources via risk scores; enabling better focus and prioritization
- **Strengthen Security** – improving detection accuracy and coverage via network, host and file attributes; helping deployed products better protect resources through contextual and actionable information

Threat Intelligence Requirements to Derive Maximum Benefits

In an ideal world, a threat intelligence deployment delivers the following benefits:

- **Maximum coverage**, to ensure as many types of threats are included
- **Easy to manage**, regardless of where the threat intelligence is coming from
- **Environmentally relevant,** to ensure context is directly applicable to that organization’s needs
- **Flexible,** to ensure threat context can be operationalized without significant effort
- **Customizable,** to ensure that threat context can be operationalized for any/all teams

In reality, a closer look at some of the challenges associated with deploying threat intelligence reveals multiple critical challenges (see Figure 1).

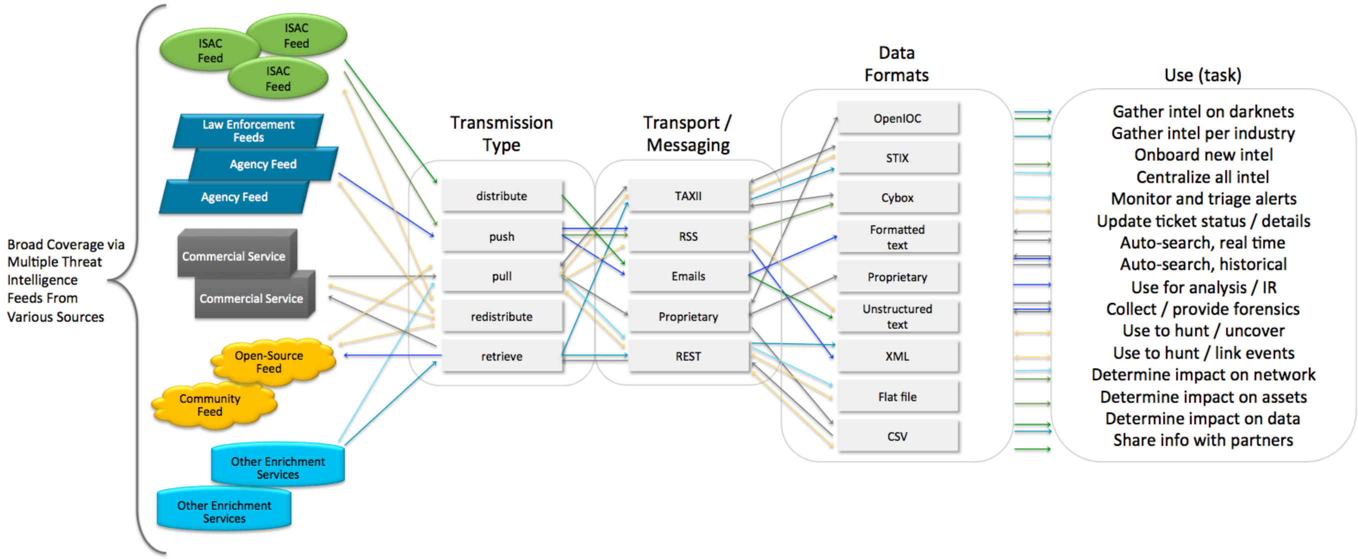


Figure 1: Complexity associated with operationalizing a high-coverage threat source strategy

Each of these challenges translates to a specific requirement that present completely different types of problems at the root.

Challenge	Requirement	Type of Problem
Maximize coverage via a variety of threat intelligence sources, since no single source has the best coverage	Handle multiple threat intelligence sources or feeds from a wide range of organizations	Data management
Threat intelligence sources have different formats and transport mechanisms, can require multiple tools	Handle ingestion and automation required for use from a central location	Interoperability
Threat intelligence translates to varying confidence levels depending on the source, user, other factors	Provide a way to prioritize or assign weights to different threat intelligence sources	Risk modeling
Value of threat intelligence data is difficult to extract for proper use in a wide range of operational tasks	Provide field extraction, ability to create detection rules, correlations in an organization-wide context, and other user-configurable mechanisms to help make faster decisions	Search / rule flexibility
Range of operational tasks that must be supported include different people, groups, responsibilities, levels of knowledge	Extract threat intelligence in a way that can be inserted into operational processes regardless of department, level of responsibility or skill	Reporting / alert customizability

These requirements can be summed up in the following manner:

In order to maximize threat intelligence for coverage, a variety of threat data must be pulled together, be easy to use and easy to operationalize, in order to enable teams to do their jobs better and faster and improve overall security posture with confidence and efficiency.

The following section looks at the requirements in more detail:

Collecting All the Pieces
Threat intelligence is locked within the multiple threat sources that are deployed to maximize coverage. Many organizations want to utilize these threat sources, or "feeds," because each provides a unique perspective on the threat; each provides different benefits and coverage. Examples include:

- External commercial feeds provide their unique approach to capture threat activities, which include trapping threat actors (e.g., within crime syndicates or compromised accounts). They might have honeynets, monitor attacker forums or provide analytics on threat data (e.g., Seculert).
- External law enforcement provides context from criminal and agency investigations, with focus on threat profiles based on victims, offenders and other case aspects.
- External Information Sharing and Analytics Centers (ISACs) focus on a common vertical or research area, e.g. FS-ISAC (Financial Service), REN ISAC (Research & Education Network), NH-ISAC (National Health) where attackers might use the same technique to attack similar entities, or attackers may be targeting specific verticals – the perspective provides the common "assets, devices, victim profiles" to enable security teams to more easily map and prioritize threat activities.
- External vendor-provided reputation lists derive intelligence from feedback collected by deployed products, for example: firewalls, network IPS, endpoint protection.
- OSINT / open-source or crowdsourced – may be specific to certain types of attack techniques or mechanisms, for example: botnets, crimeware, exploit kits.
- Internal teams or results from internal investigations provide information about what has been seen in the immediate environment.

Threat intelligence sources are bound to have different formats and retrieval and transmission mechanisms to distribute, obtain and parse feeds. Furthermore, separate threat intelligence services have vendor-specific UIs and can require work to retrieve, causing inefficiencies. Therefore, effective threat intelligence solutions should be able to:

- Handle data from multiple sources and aggregate those into a single view: IT and security systems, apps, AAA, endpoints, as well as subscription and open source threat feeds, law enforcement reports, industry sharing forums
- Handle data in multiple formats and a range of mechanisms and interfaces to ingest feeds, including but not limited to flat files, unformatted text, XML, Cybox, STIX, TAXII, OpenIOC and Department of Homeland Security's Automated Indicator Sharing (AIS)

Helping Manage Information Flow
It can be challenging to extract value from threat intelligence for use in operational tasks, which typically include: detecting events that match threat context; using threat intelligence for investigations; running reports against use for investigations. Predefined searches are only effective if teams know what to look for, and custom searches can have a steep learning curve. Threat intelligence needs to enable intuitive exploration and analysis of both immediate, localized incidents as well as help paint

the broader picture of threat actors and activities over time. Therefore the solution should:

- Support ad-hoc searches, reports, analysis, visualizations and workflows to make it easy to access and use data, share insights and close the loop, in support of all security, incident response, compliance and auditing activities – for admins, analysts, architects, auditors, etc.
    - In the most basic case, admins will need to be able to create alerts based on results
    - There also needs to be a way to create alert + action (automatic blocking , e.g.)
    - Available for any SecOps personnel to use during both breach investigation and IR
    - Enable threat intelligence fields and values to be available for SecOps teams to view, search and use for operations and analysis, including threat intelligence insight into past data and activities.

Categorizing Data to Identify Risks
Not all data is created equal. Organizations may value each threat intelligence feed differently, based on how data is sourced, created, analyzed and even packaged. For example, a public transit organization may value PT-ISAC (public transportation) since it is focused on defending transportation infrastructure, whereas a bank may value in-house-derived threat context and treat it with higher confidence.

Effective threat intelligence solutions will allow “value association” (e.g., risk scoring and weighting) to enable threats to be accurately identified, categorized and prioritized for downstream use (for example, automation). The threat intelligence solution should:

- Provide mechanisms to determine the accuracy and relevancy of security information – for example, identifying number of “hits” to help identify which feeds are the most reliable
- Weigh and index data based on source, time, location, asset and other factors
- Enrich the data and provide additional context that can be used by the entire security team to determine the nature of the activity in the environment

Correlating the Data to Help Make Sense of It
Correlating data is not limited to finding commonalities and links – attackers use sophisticated methods to hide and perpetrate attacks unnoticed, so it is critical to make sense of those links to see what is really going on. A threat intelligence solution must enable security teams to determine which events pose a real risk so they can remediate a breach and anticipate and prevent subsequent malicious activities. It should:

- Identify malicious intent hiding in seemingly legitimate activities
- Help uncover the scope of a breach, including all impacted devices, systems, applications, users
- Support appropriate action to contain and minimize the impact of a breach
- Improve ongoing monitoring by automatically applying threat intelligence (either learned or from packaged feeds) to detect malicious activities in the environment going forward

Supporting the Ability to Act Selectively
Information is great, but improved security posture is better. The ability to convert data into a prioritized list of actionable tasks is key. However, prioritization of actions depends on context, for example, use of certain credentials may have a different meaning when part of a cascading set of alerts. Based on assigned risk scores, SecOps may take different actions depending on how those credentials were used. Operationalizing threat intelligence includes the ability to automate actions to an enforcement solution by sending information to those devices with supporting command. The devices that receive this information can include:

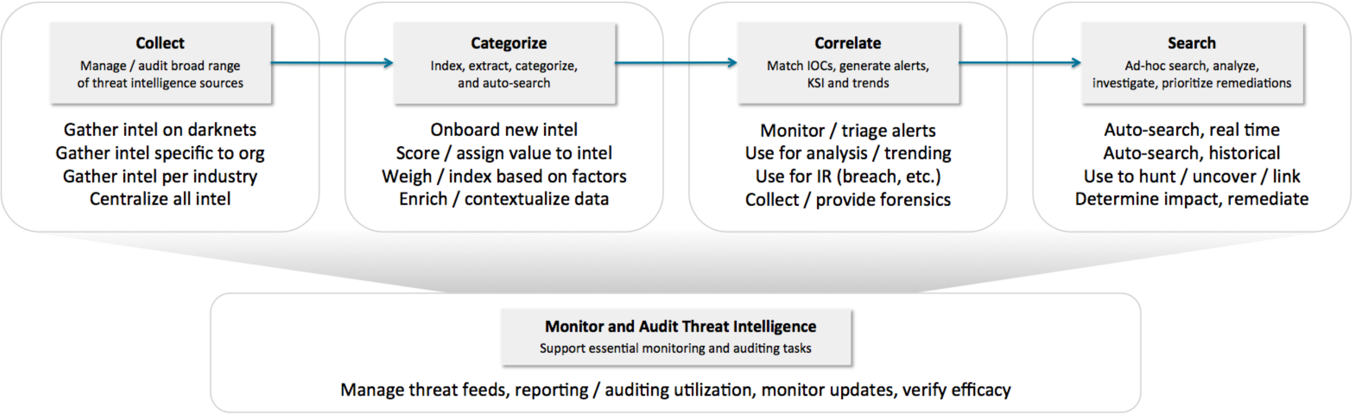
- Firewalls
- Intrusion detection and prevention systems (IDS/IPS)
- Web and email gateways
- Endpoint threat detection solutions

Monitoring and Auditing Threat Intelligence

A threat intelligence platform must also be able to support essential monitoring and auditing tasks as part of the security operations workflow, such as:

- Turning on and off threat feeds
- Reporting and auditing number of hits, utilization, and other metrics
- Monitoring threat intelligence updates – ensuring updates/retrievals are executed
- Verifying efficacy of threat intelligence

In summary, the system has to:


Collect
Manage / audit broad range of threat intelligence sources
Gather intel on darknets
Gather intel specific to org
Gather intel per industry
Centralize all intel
Categorize
Index, extract, categorize, and auto-search
Onboard new intel
Score / assign value to intel
Weigh / index based on factors
Enrich / contextualize data
Correlate
Match IOCs, generate alerts, KSI and trends
Monitor / triage alerts
Use for analysis / trending
Use for IR (breach, etc.)
Collect / provide forensics
Search
Ad-hoc search, analyze, investigate, prioritize remediations
Auto-search, real time
Auto-search, historical
Use to hunt / uncover / link
Determine impact, remediate
Monitor and Audit Threat Intelligence
Support essential monitoring and auditing tasks
Manage threat feeds, reporting / auditing utilization, monitor updates, verify efficacy

The following section explains how the threat intelligence framework within Splunk Enterprise Security (ES) can help operationalize threat intelligence within a security organization. This paper also describes specific details on the threat intelligence capabilities and benefits delivered by ES.

The Splunk Enterprise Security Threat Intelligence Framework

ES helps operationalize threat intelligence to ensure you can identify and mitigate attacks in the environment and support broader security and compliance objectives. Splunk ES:

- **Collects and Aggregates Threat Information** – bringing in all the pieces of information you need to see the complete picture, by collecting data from a variety of threat intelligence sources and providing them for use. ES can ingest, automatically or manually, and aggregate threat intelligence data, removing any duplication, to provide a clean, searchable data set. ES also includes a number of pre-configured threat intelligence sources.
- **Manages and Audits the Data** – ensuring the data is easily usable to support every aspect of your security operations. ES provides the access and controls that ensure everyone can use the data to support their operational activities; it also improves the confidence levels associated with the threat feeds brought into the solution
- **Categorizes Indicators of Compromise to Identify Risks** – extracting values from fielded and coded data sets, indexing them and then making them available for reporting, correlation, searching and analysis. ES extracts and categorizes the indicators of threat activity into collections so it's easier to correlate against different security domains (data types); these collections of indicators are easily searchable through pre-defined dashboards

as well as a search interface that supports ad hoc investigation and analysis.

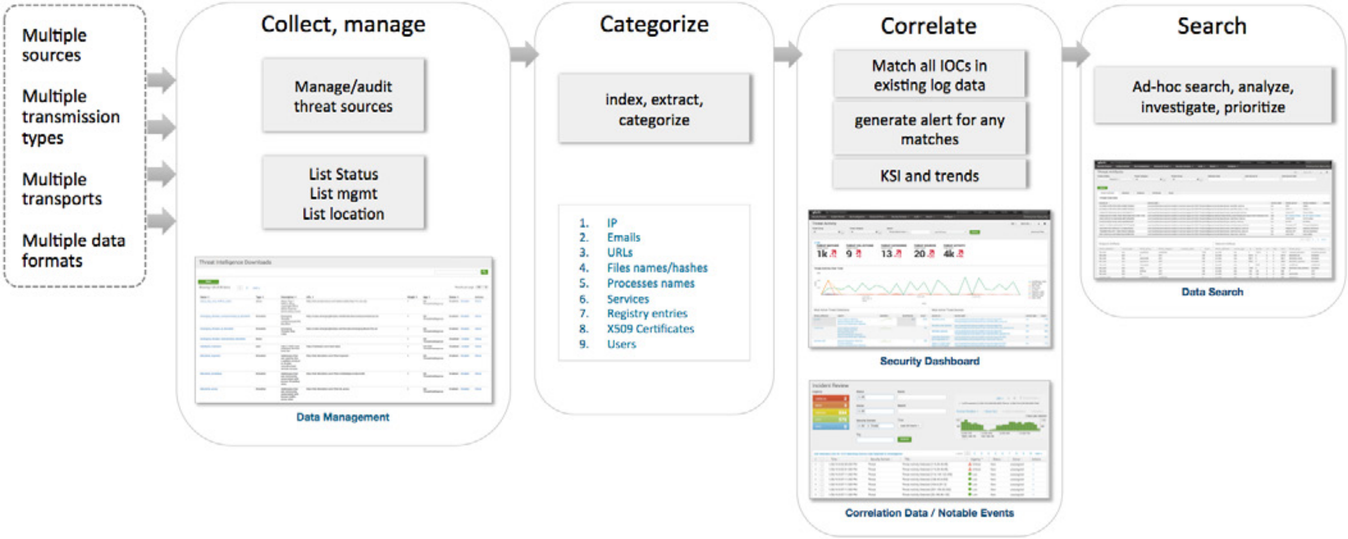
- **Correlates Indicators** – helping you identify threat indicators and understand how they are related to uncover advanced attacks and malicious insider activity. ES identifies matches between content from threat intelligence sources and events, thereby enabling analysts to search the indexed data for threat indicators and associate them with other attack activities to provide a complete picture of what is going on across the organization.

- **Streamlines Threat Intelligence Usage** – once all the steps are performed on top, ES will help improve security by enabling security teams to:

  1. Detect threats based on threat intelligence by setting up correlation searches. Those matches will show up in the alert management screen for further correlation or triaging.

  2. Respond to threats using threat intelligence that is categorized and intuitively displayed within a single interface for fast access or via ad hoc searches.

View of Splunk Enterprise Security Threat Intelligence Framework



Collecting Threat Information

It is vital to get as much high-confidence threat intelligence as possible to support your team's wide variety of security operations. Splunk Enterprise Security is able to collect threat information from a broad set of sources, including data from:

- Commercial threat intelligence systems (both dedicated and derived)
- Open source threat intelligence feeds and platforms
- File hash lookups (for example, from vendors such as VirusTotal)
- Law enforcement reports
- Applicable organizations (peers) and industry forums
- Threat streams and subscriptions

Each of these sources may use a different format or make its data available in a different way. ES can accept flat files in a CSV format, retrieve info via XML (extensible markup language) or TAXII (trusted automated exchange of indicator information), from STIX™ (structured threat information expression) and CybOX™ (cyber observable expression) docs or Open IOC files.

ES not only aggregates all this information from all these different sources, in all these different formats, but also removes duplications to ensure the data set is clean and easily searchable. ES can collect data automatically or manually. To automate its collection, you simply navigate to the Threat Intelligence Download Settings and input the access information for the source, which includes:

- URL
- File type(s)
- Frequency of the collection
- Credentials

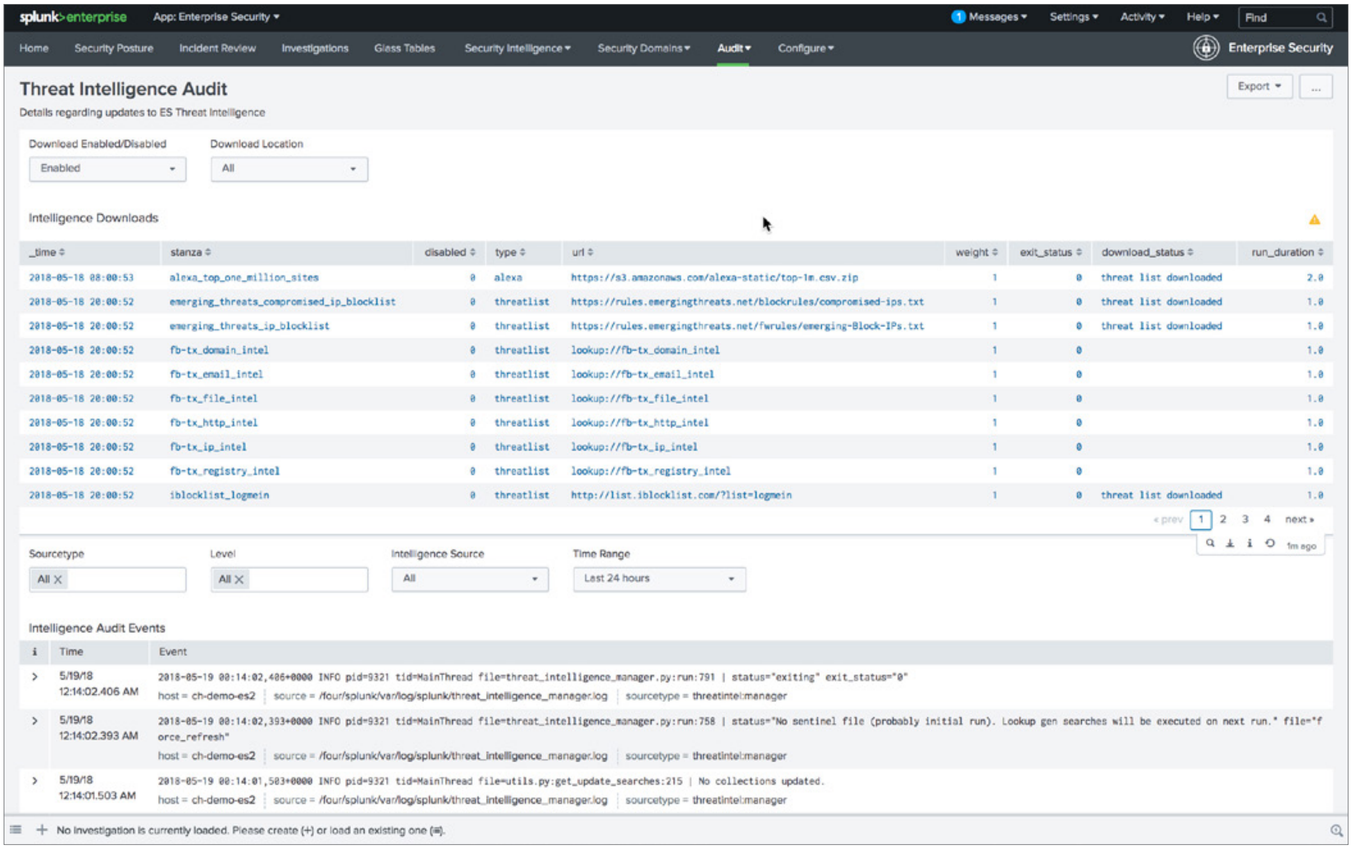
Managing and Auditing Data

If it is easy to access and manage the threat intelligence, it will be easy to derive benefits from it. ES manages and audits the data that is brought into the solution. It provides centralized access and controls to ensure everyone can use the threat intelligence to support their operational activities.

The Threat Intelligence Audit pane provides a central place to:

- **Verify/audit download by sources** - view audit data related to your threat intelligence sources, so you can see if they were successfully downloaded, if there were any errors, etc.
- **Enable/Disable sources** – enable or disable lists as needed.
- **Weighting for prioritization** - These threat lists can also be given a weight to indicate the level of confidence in the data, which can be adjusted based on the number of threat intelligence "hits" the solution identifies for that list.

This pane shows you the last time a threat list was updated, downloaded or if it is local to the solution. It also enables you to quickly see the last time it was run against the data, with the ability to drill into the results. You can search the data by the type of list, source of information and time frame to support tracking and reporting on different threat lists.



Threat Intelligence Audit

Details regarding updates to ES Threat Intelligence

Download Enabled/Disabled: Enabled

Download Location: All

Intelligence Downloads

_time	stanza	disabled	type	url	weight	exit_status	download_status	run_duration
2018-05-18 08:00:53	alexa_top_one_million_sites	0	alexa	https://s3.amazonaws.com/alexa-static/top-1m.csv.zip	1	0	threat list downloaded	2.0
2018-05-18 20:00:52	emerging_threats_compromised_ip_blocklist	0	threatlist	https://rules.emergingthreats.net/blockrules/compromised-ips.txt	1	0	threat list downloaded	1.0
2018-05-18 20:00:52	emerging_threats_ip_blocklist	0	threatlist	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt	1	0	threat list downloaded	1.0
2018-05-18 20:00:52	fb-tx_domain_intel	0	threatlist	lookup://fb-tx_domain_intel	1	0		1.0
2018-05-18 20:00:52	fb-tx_email_intel	0	threatlist	lookup://fb-tx_email_intel	1	0		1.0
2018-05-18 20:00:52	fb-tx_file_intel	0	threatlist	lookup://fb-tx_file_intel	1	0		1.0
2018-05-18 20:00:52	fb-tx_http_intel	0	threatlist	lookup://fb-tx_http_intel	1	0		1.0
2018-05-18 20:00:52	fb-tx_ip_intel	0	threatlist	lookup://fb-tx_ip_intel	1	0		1.0
2018-05-18 20:00:52	fb-tx_registry_intel	0	threatlist	lookup://fb-tx_registry_intel	1	0		1.0
2018-05-18 20:00:52	iblocklist_logmein	0	threatlist	http://list.iblocklist.com/?list=logmein	1	0	threat list downloaded	1.0

Sourcetype: All ×

Level: All ×

Intelligence Source: All

Time Range: Last 24 hours

Intelligence Audit Events

i	Time	Event
>	5/19/18 12:14:02.406 AM	2018-05-19 00:14:02,406+0000 INFO pid=9321 tid=MainThread file=threat_intelligence_manager.py:run:791 | status="exiting" exit_status="0" host = ch-demo-es2 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager
>	5/19/18 12:14:02.393 AM	2018-05-19 00:14:02,393+0000 INFO pid=9321 tid=MainThread file=threat_intelligence_manager.py:run:758 | status="No sentinel file (probably initial run). Lookup gen searches will be executed on next run." file="force_refresh" host = ch-demo-es2 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager
>	5/19/18 12:14:01.503 AM	2018-05-19 00:14:01,503+0000 INFO pid=9321 tid=MainThread file=utils.py:get_update_searches:215 | No collections updated. host = ch-demo-es2 | source = /four/splunk/var/log/splunk/threat_intelligence_manager.log | sourcetype = threatintel:manager

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).

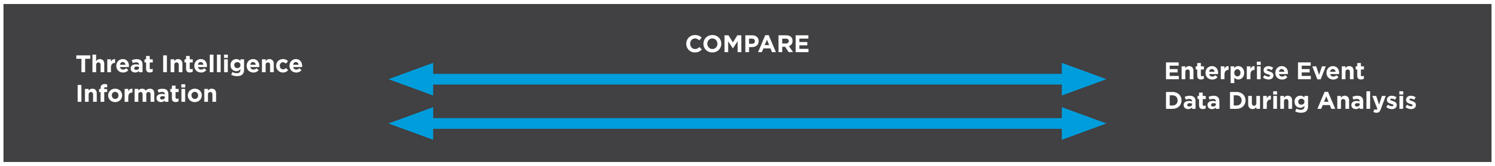
Categorizing Indicators of Compromise to Identify Risks

Finding threats in your big data can be like finding a needle in a haystack. Splunk ES streamlines the process by extracting indicators of compromise (IOCs) in your threat intelligence data to help you pinpoint potential attack activity in your enterprise. When ES ingests new threat intelligence, it can automatically search for IOCs to ensure you have the most up-to-date information on potential risks in your environment.

There are a variety of types of IOCs that are extracted and stored by ES as Collections, including but not limited to:

1. IP Address
2. HTTP headers, UAs, referrers and URLs
3. Email
4. File names/hashes
5. Process names and handles
6. Service (a service running in the host)
7. Registry info
8. Certificate info
9. User names

The Collections of IOCs are grouped as Threat Artifacts by ES. These artifacts allow investigators and analysts to search and filter, through a simple dialog box to give novices and experts alike rapid access to the threat intelligence they need.



Threat Intelligence Information

COMPARE

Enterprise Event Data During Analysis

The table below shows the fields extracted from threat intelligence to the data

Sample of Data Sources Collected by Splunk

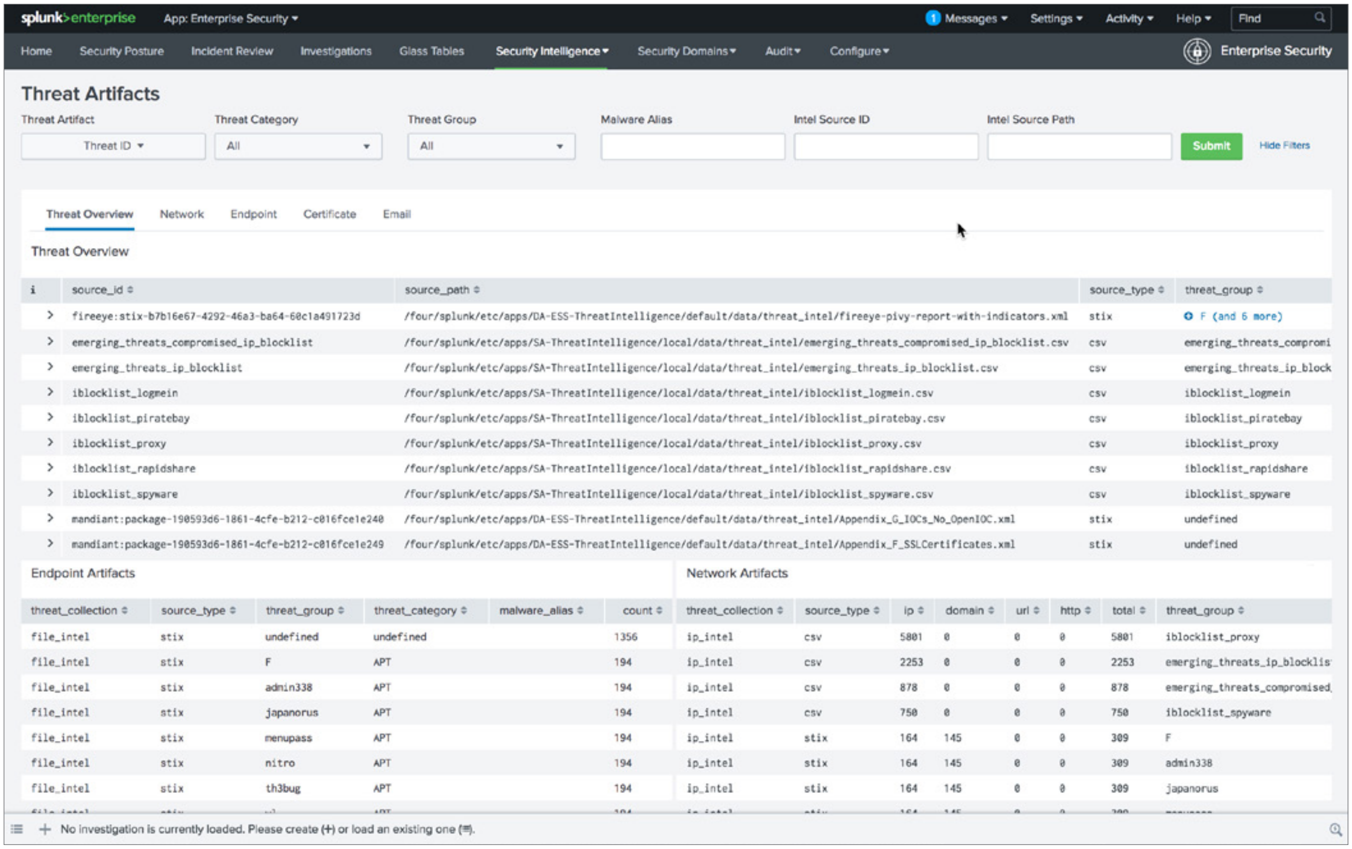
SAMPLE set of threat intelligence data for network and endpoint.
See Splunk product documentation for complete listing

Sample of Extracted Fields	Format / Type	Sample of Data Sources
IP-address, Domain of the dest-host	IP/Domain	Firewall, IPS, web gateway, host firewall, email gateways
Source-user, Subject, Source-user, Subject, File-name, File-hash, Embedded-domain, Embedded-IP	Email	Next-generation firewalls (NGFWs), Intrusion detection and prevention systems (IDS/IPS), proxies

Sample of Extracted Fields	Format / Type	Sample of Data Sources
File hash value, File-name, File-extension, File-path, File-size (in Bytes)	File Information	Universal forwarders, Sandboxing technologies
Process, Process-file-name, Process-handle-name, Process-handle-type, Process-arguments, Src, Dest, dest port	Process	Universal forwarders, endpoint forensic agents (e.g. FireEye's MIR), sandbox technologies, endpoint threat detection (ETD) (e.g. CarbonBlack and Tanium)
Service, Description, Status, Service Type, Service-file-path, Service-file-name, Service-file-hash, Service-dll-file-hash	Services	Universal forwarders, endpoint forensic agents, sandboxes, endpoint threat detection
Registry-path, Registry-hive, Registry-key-name, Registry-value-name, Registry-value-data, Registry-value-text, Registry-value-type, Registry-modified-time, Registry username	Registry	Universal forwarders, endpoint forensic agents, sandboxes, endpoint threat detection

These glance-able collections can also be searched and explored from the ES dashboards.

For a view of the overall threat intelligence repository, you can go to the Threat Artifacts page (under Advanced Threats within ES). You can search and filter the IOC collections to get more contextual information; the results facilitate further investigations and a deeper understanding of the threat activity in your environment.



Threat Artifacts

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

Threat Overview

i	source_id	source_path	source_type	threat_group
>	fireeye:stix-b7b16e67-4292-46a3-ba64-60c1a491723d	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/fireeye-pivy-report-with-indicators.xml	stix	F (and 6 more)
>	emerging_threats_compromised_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_compromised_ip_blocklist.csv	csv	emerging_threats_compromi
>	emerging_threats_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_threats_ip_blocklist.csv	csv	emerging_threats_ip_block
>	iblocklist_logmein	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_logmein.csv	csv	iblocklist_logmein
>	iblocklist_piratebay	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_piratebay.csv	csv	iblocklist_piratebay
>	iblocklist_proxy	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_proxy.csv	csv	iblocklist_proxy
>	iblocklist_rapidshare	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_rapidshare.csv	csv	iblocklist_rapidshare
>	iblocklist_spyware	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/iblocklist_spyware.csv	csv	iblocklist_spyware
>	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e240	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_G_IOCs_No_OpenIOC.xml	stix	undefined
>	mandiant:package-190593d6-1861-4cfe-b212-c016fce1e249	/four/splunk/etc/apps/DA-ESS-ThreatIntelligence/default/data/threat_intel/Appendix_F_SSLCertificates.xml	stix	undefined

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

Network Artifacts

threat_collection	source_type	ip	domain	url	http	total	threat_group
ip_intel	csv	5801	0	0	0	5801	iblocklist_proxy
ip_intel	csv	2253	0	0	0	2253	emerging_threats_ip_blocklis
ip_intel	csv	878	0	0	0	878	emerging_threats_compromised
ip_intel	csv	750	0	0	0	750	iblocklist_spyware
ip_intel	stix	164	145	0	0	309	F
ip_intel	stix	164	145	0	0	309	admin338
ip_intel	stix	164	145	0	0	309	japanorus

No investigation is currently loaded. Please create (+) or load an existing one (≡).

For example, if you get an alert, you can quickly identify the indicators within that alert and look across your data to see all activity that matches those indicators to understand what is going on in your network. Or, if another organization publishes a threat feed about an attack that hit their network, you can quickly search for the attributes of that attack to see if it is active in your environment. This helps you rapidly identify the "bad actors" (in the threat group field) and trends in your environment (a count represents the number of matchable threat artifacts for that entry) that can help you further prioritize efforts and activities.

ES provides tabs in the Threats Artifacts dashboard that group the IOC artifacts based on where they originate to make it easier to filter the indicators and results. You can observe IOCs for:

- **Network** – for example, network artifacts include but are not limited to IP, domain, URL, HTTP headers, UAs, referrers
- **Endpoint,** for example, details on endpoint intelligence such as files, registry, processes, services and users
- **Certificate,** for example, details on threats that use or steal certificates to encrypt command and control (CnC) traffic or sign malware, such as certificate's serial number, issuer and subject

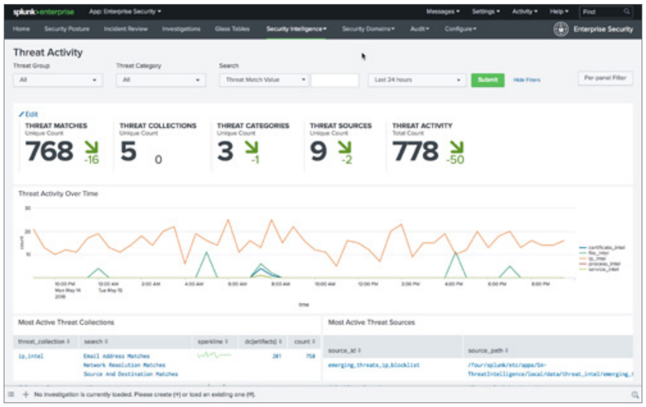
Correlating Indicators of Compromise

ES gives you visibility into the threat indicators present in your network and helps you see how they are related to uncover advanced attacks and malicious insider activity in your network. ES runs predefined correlation searches to match indicators against all your indexed data to identify potential threats.

In addition, ES delivers valuable insights into the threat activity in your network, including insights into how the activity is changing over time through dashboards. The dashboards provide high-level information on the state of the threat activity in your environment. They provide glance-able information on key security indicators (KSIs), including:

- **Threat matches** – the count of the all the IOCs identified in your environment.
- **Threat collections** – the collections of IOC artifacts in your environment.
- **Threat categories** – the types of threats identified in your environment.
- **Threat sources** – the active sources of the IOCs in your environment.
- **Threat activity** – the amount of threat activity in your environment, with a trend-line that shows whether it is increasing or decreasing.

You can also add other indicators based on your role or preference to help you spot threat activity that needs to be addressed.



Threat Activity

Threat Group: All
Threat Category: All
Search: Threat Match Value
Last 24 hours

THREAT MATCHES
Unique Count
768 -16

THREAT COLLECTIONS
Unique Count
5 0

THREAT CATEGORIES
Unique Count
3 -1

THREAT SOURCES
Unique Count
9 -2

THREAT ACTIVITY
Total Count
778 -50

Most Active Threat Collections

threat_collection	search	sparkline	dc(artifacts)	count
ip_intel	Email Address Matches Network Resolution Matches Source And Destination Matches		281	758

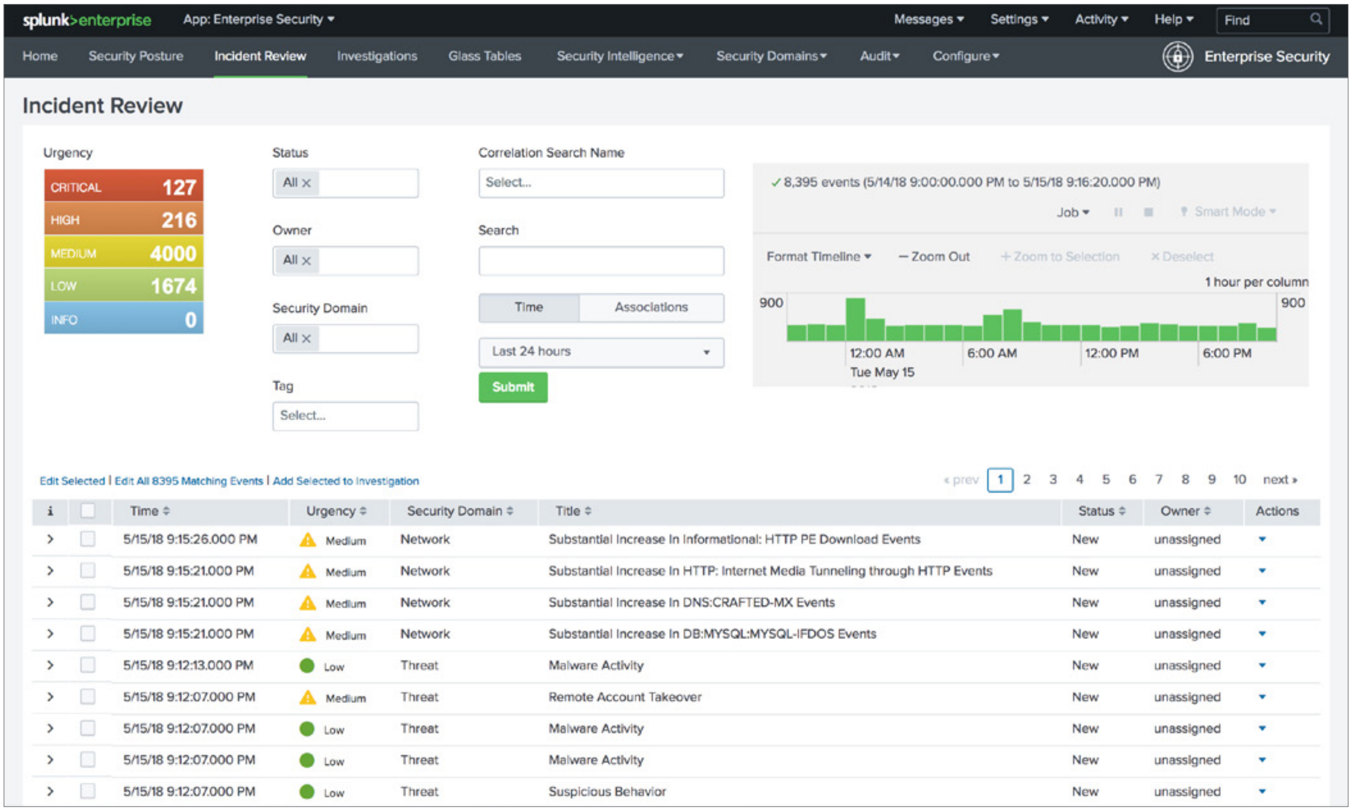
Most Active Threat Sources

source_id	source_path
emerging_threats_ip_blocklist	/four/splunk/etc/apps/SA-ThreatIntelligence/local/data/threat_intel/emerging_t

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Correlating Threat Intelligence

The value of threat intelligence is to improve the overall security of your network by mitigating the threats it has uncovered. ES helps translate threat intelligence into actionable alerts (Notables) that can be used to respond and contain attacks. Notables help you cut through the data and understand where to focus your efforts and how to close out incidents.



Incident Review

Urgency	
CRITICAL	127
HIGH	216
MEDIUM	4000
LOW	1674
INFO	0

Status: All ×

Owner: All ×

Security Domain: All ×

Tag: Select...

Correlation Search Name: Select...

Search:

Time | Associations

Last 24 hours

✓ 8,395 events (5/14/18 9:00:00.000 PM to 5/15/18 9:16:20.000 PM)

i	□	Time	Urgency	Security Domain	Title	Status	Owner	Actions
>	□	5/15/18 9:15:26.000 PM	⚠ Medium	Network	Substantial Increase In Informational: HTTP PE Download Events	New	unassigned	▾
>	□	5/15/18 9:15:21.000 PM	⚠ Medium	Network	Substantial Increase In HTTP: Internet Media Tunneling through HTTP Events	New	unassigned	▾
>	□	5/15/18 9:15:21.000 PM	⚠ Medium	Network	Substantial Increase In DNS:CRAFTED-MX Events	New	unassigned	▾
>	□	5/15/18 9:15:21.000 PM	⚠ Medium	Network	Substantial Increase In DB:MYSQL:MYSQL-IFDOS Events	New	unassigned	▾
>	□	5/15/18 9:12:13.000 PM	● Low	Threat	Malware Activity	New	unassigned	▾
>	□	5/15/18 9:12:07.000 PM	⚠ Medium	Threat	Remote Account Takeover	New	unassigned	▾
>	□	5/15/18 9:12:07.000 PM	● Low	Threat	Malware Activity	New	unassigned	▾
>	□	5/15/18 9:12:07.000 PM	● Low	Threat	Malware Activity	New	unassigned	▾
>	□	5/15/18 9:12:07.000 PM	● Low	Threat	Suspicious Behavior	New	unassigned	▾

From the ES Incident Review page, you can investigate and work to shut down the threat activity that poses the greatest risk to your organization. You can filter and sort the intelligence, search for tags and add hyperlinks (to wikis, a playbook, etc.) to Notable event notes or descriptions to accelerate investigations.

You can also build scripts that can use the data to trigger actions by your security infrastructure. For example, if a malicious URL has been identified, you can have your firewall block traffic to and from that URL. Or you can develop a script, so when a host has been identified as being compromised, it will trigger your authentication server to suspend access to network resources to quarantine and contain the attack.

Threat Intelligence Use Cases

ES provides the advanced, analytics-driven security you need to improve your ability to detect and prevent attacks on your resources. The next-generation security intelligence platform enables you to:

- **Identify Attacks** – searching for IOCs and identifiable attack information that has been observed in your environment will quickly turn up any hits (matches) across all your data sources to accelerate the detection of attacks within your environment.
- **Conduct Analysis and Scoping** – looking for multiple hits across data sources enables you to verify whether or not an attack has penetrated your environment and follow its trail to understand all the activities associated with that threat, including all the actors and compromised systems. The simple to use interface allows you to explore the data to uncover threats; once you identify one clue, you can quickly run correlation searches to look for additional hits to understand the extent of a breach in your network.
- **Strengthen Security** – providing actionable information (Notables), so you can take the steps you need to mitigate the impact of attacks in your network, as well as make changes to your defenses in anticipation of subsequent attacks.
- **Support Compliance and Auditing** – offering reports and dashboards that document the threat activity and investigations in your environment to support forensics, compliance and auditing efforts.

- **Improve and Automate Incident Analysis and Breach Response and Investigation** – automating tasks with threat intelligence around the following fields: IP reputation, web domain reputation, traffic anomalies, malware analysis, endpoint security (ETD, FIM, etc.), forensic analysis. The solution can be used to answer questions such as: Does the file exists in the organization? Has the files associated with the malware been executed? Is there traffic coming from or going to a domain/IP?

Summary

To improve your ability to respond to attacks and minimize their impact, you need to be able to quickly hone in on attack activity in your environment and understand its scope, so you can take appropriate steps to protect your resources. Splunk Enterprise Security delivers the threat intelligence framework you need to accelerate the detection of threats that your existing security tools are not able to catch in your network and arm your analysts with the actionable information they need to respond. With ES, you can improve your visibility and collaboration to strengthen your overall security stance, save time and money and support your compliance objectives.

	Collect	Manage/Audit	Categorize	Investigate	Correlation
Splunk App for Enterprise Security Collect	Data can be automatically or manually collected, from all types of sources (formats); the data is aggregated and de-duped to provide a clean data set.	Access and controls that ensure everyone can use the data to support their operational activities; improves the efficacy and confidence levels of threat feeds. Correlation	Indicators are extracted, categorized (indexed) and displayed in easy to read dashboards and panels.	Indicators in the indexed data can be searched and associated with other attack activity.	Notables (alerts) are raised on malicious activity that enable analysts to take action to mitigate the impact of the incident.
Benefits	Ensures all information is available for an investigation.	Ensures the data is easily useable to support security operations.	Accelerates and simplifies the identification of key threat indicators within the network.	Provides visibility into attack activity and improves the detection of advanced threats and malicious insiders.	Delivers actionable intelligence to stop known, unknown and advanced attacks and take steps in anticipation of subsequent malicious activity.

Try Splunk Enterprise Security now. Experience the power of Splunk Enterprise Security – with no downloads, no hardware set-up and no configuration required. The Splunk Enterprise Security Online Sandbox is a 7-day evaluation environment with pre-populated data, provisioned in the cloud, enabling you to search, visualize and analyze data, and thoroughly investigate incidents across a wide range of security use cases. You can also follow a step-by-step tutorial that will guide you through the powerful visualizations and analysis enabled by Splunk software. **Learn More**

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com