Using threat intelligence in Splunk Enterprise Security

Within an increasingly aggressive threat landscape, security professionals and executives need to explore and implement threat intelligence programs to understand cyber-attacks and remain ahead of the curve. Using threat intelligence data to your advantage is an essential component to any organization's risk remediation and security program.

Your ability to defend against the modern landscape of dangers such as ransomware, malware, and a multitude of other sophisticated malicious activity is essential in assessing and managing risk. Threat intelligence does exactly that, enabling cyber security teams to inform the security operations center (SOC) and incident response teams of potential and impending harmful activities and business risks.

This article is part of Splunk's Use Case Explorer for Security, which is designed to help you identify and implement prescriptive use cases that drive incremental business value. In the Security maturity journey described in the Use Case Explorer, this article is part of Threat intelligence.

What's the value of using threat intelligence with Splunk Enterprise Security?

Threat intelligence can provide huge advantages if it works effectively. Quality threat intelligence goes beyond just providing data-based indicators of compromise you can add to a match list in your SIEM or SOAR platform, it also provides actionable information regarding vulnerabilities, insider threats, leaked credentials and more. Using this information, security teams can reduce the chance of experiencing data breaches and prevent attempts, resulting in measurable savings.

Cybercriminals, fraudulent actors, and malicious insiders alike utilize many tactics, techniques, and procedures (TTP's) to carry out attacks to reach their end goals (which are often, but not always, to benefit financially). Threat actors are becoming more advanced in their attacks and methods, making it even more important that organizations improve their defense capabilities.

Technical threat intelligence provides the details that enable your security teams to create defense practices and help prevent attacks. With the right data incorporated, cyber security teams can immediately notify appropriate resource owners when they become aware of illicit schemes, such as an insider attempting to sell access to company systems or a threat actor claiming to have collections of the organization's credentials. By investigating and addressing these kinds of situations before they escalate, organizations can make threat intelligence actionable while seeing positive impacts on their ROI.

Where do I get threat intelligence?

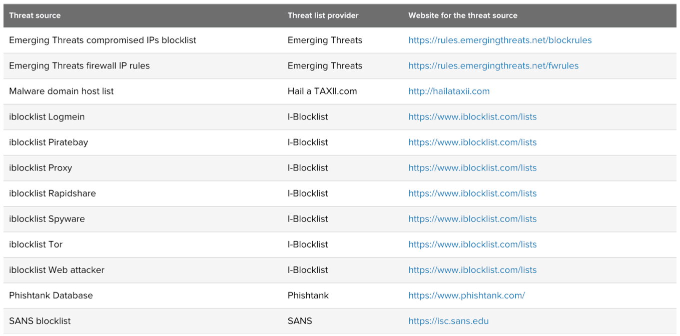
Having access to good quality technical intelligence can be tricky since most of the rich data out there isn't indexed by search engines. Actionable data is often found on multiple mediums, including illicit marketplaces, forums, blogs, social media, and more. This dynamic ocean of data consists of too many sources for most organizations to track and monitor themselves. Additionally, accessing data sources on the deep web and dark web can bring unforeseen risk and exposure to the organization in their attempts to explore and leverage it.

Splunk helps organizations by bringing together threat intelligence sources from across the internet into the Splunk Enterprise Security platform, out of the box and at no extra cost. The threat intelligence sources are parsed for threat indicators and added to the relevant KV Store collections.

The following generic or non-threat intelligence sources are enabled by default:

- Mozilla Public Suffix List
- MITRE ATT&CK Framework
- ICANN Top-level Domains List

Additionally, several other quality sources of threat data are available and just need to be enabled for use:



Threat source	Threat list provider	Website for the threat source
Emerging Threats compromised IPs blocklist	Emerging Threats	https://rules.emergingthreats.net/blockrules
Emerging Threats firewall IP rules	Emerging Threats	https://rules.emergingthreats.net/fwrules
Malware domain host list	Hail a TAXII.com	http://hailataxii.com
iblocklist Logmein	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Piratebay	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Proxy	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Rapidshare	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Spyware	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Tor	I-Blocklist	https://www.iblocklist.com/lists
iblocklist Web attacker	I-Blocklist	https://www.iblocklist.com/lists
Phishtank Database	Phishtank	https://www.phishtank.com/
SANS blocklist	SANS	https://isc.sans.edu

How do I start using threat intelligence to my advantage?

Now that you have data, where should your organization start? The threat intelligence gathering process can be cumbersome, resource-intensive, and highly technical, which is why some businesses choose not to incorporate it into their risk-remediation program. Using curated vendor threat intelligence or Splunk's own threat intelligence management capabilities can help ease you into this complex task.

If done right, even one person can replicate the workflows of a more mature team. One way to have both actionable and scalable threat intelligence is to include this information as part of the correlation search activity performed by Splunk Enterprise Security. Leveraging your threat information to build your search and defense strategies can save you time and resources, and help point your security analysts in the right direction.

If you can build the right foundations, an effective risk-remediation and security program is within your reach.

How to add threat intelligence to Splunk Enterprise Security

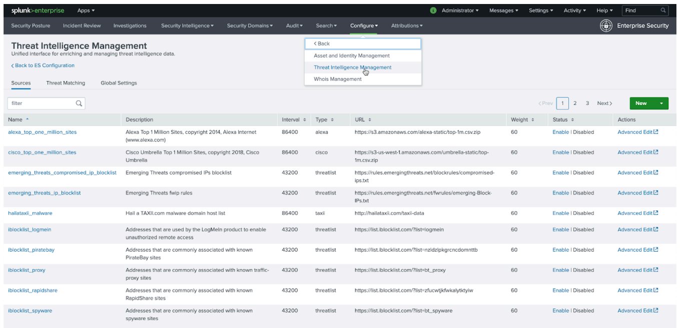
As an Splunk Enterprise Security administrator, you can correlate indicators of suspicious activity, known threats, or potential threats with your events by adding threat intelligence to your deployment. Adding threat intelligence enhances your analysts' security monitoring capabilities and adds context to their investigations.

Splunk Enterprise Security also supports multiple types of threat intelligence so that you can add your own threat intelligence.

Splunk Enterprise Security administrators can add threat intelligence by downloading a feed from the Internet, uploading a structured file, or inserting the threat intelligence directly from events into your deployment.

Before you get started, you should review the types of threat intelligence that Splunk Enterprise Security supports. See Supported types of threat intelligence in Splunk Enterprise Security.

1. Configure the threat intelligence sources included with Splunk Enterprise Security.



Threat Intelligence Management

Unified interface for enriching and managing threat intelligence data.

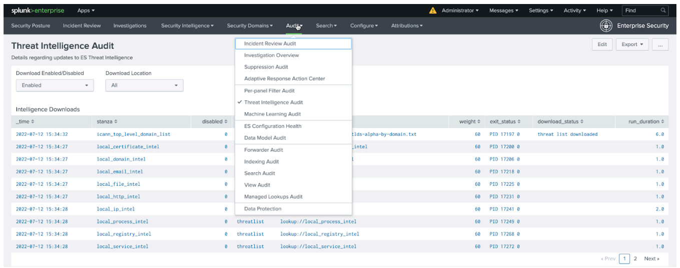
< Back to ES Configuration

Name	Description	Interval	Type	URL	Weight	Status	Actions
alexa_top_one_million_sites	Alexa Top 1 Million Sites, copyright 2014, Alexa Internet (www.alexa.com)	86400	alexa	https://s3.amazonaws.com/alexa-static/top-1m.csv.zip	60	Enable | Disabled	Advanced Edit
cisco_top_one_million_sites	Cisco Umbrella Top 1 Million Sites, copyright 2018, Cisco Umbrella	86400	cisco	https://s3-us-west-1.amazonaws.com/umbrella-static/top-1m.csv.zip	60	Enable | Disabled	Advanced Edit
emerging_threats_compromised_ip_blocklist	Emerging Threats compromised IPs blocklist	43200	threatlist	https://rules.emergingthreats.net/blockrules/compromised-ips.txt	60	Enable | Disabled	Advanced Edit
emerging_threats_ip_blocklist	Emerging Threats fwip rules	43200	threatlist	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt	60	Enable | Disabled	Advanced Edit
hailataxii_malware	Hail a TAXII.com malware domain host list	86400	taxii	http://hailataxii.com/taxii-data	60	Enable | Disabled	Advanced Edit
iblocklist_logmein	Addresses that are used by the LogMeIn product to enable unauthorized remote access	43200	threatlist	https://list.iblocklist.com/?list=logmein	60	Enable | Disabled	Advanced Edit
iblocklist_piratebay	Addresses that are commonly associated with known PirateBay sites	43200	threatlist	https://list.iblocklist.com/?list=nzldzlpkgrcncdomnttb	60	Enable | Disabled	Advanced Edit
iblocklist_proxy	Addresses that are commonly associated with known traffic-proxy sites	43200	threatlist	https://list.iblocklist.com/?list=bt_proxy	60	Enable | Disabled	Advanced Edit
iblocklist_rapidshare	Addresses that are commonly associated with known RapidShare sites	43200	threatlist	https://list.iblocklist.com/?list=zfucwtjkfwkalytktyiw	60	Enable | Disabled	Advanced Edit
iblocklist_spyware	Addresses that are commonly associated with known spyware sites	43200	threatlist	https://list.iblocklist.com/?list=bt_spyware	60	Enable | Disabled	Advanced Edit

2. For each additional threat intelligence source not already included with Splunk Enterprise Security, follow the procedure to add threat intelligence that matches the source and format of the intelligence that you want to add:

    - Upload a STIX or OpenIOC structured threat intelligence file
    - Upload a custom CSV file of threat intelligence
    - Add threat intelligence from Splunk events in Splunk Enterprise Security
    - Add and maintain threat intelligence locally in Splunk Enterprise Security
    - Add threat intelligence with a custom lookup file in Splunk Enterprise Security
    - Upload threat intelligence using REST API

3. Verify that you have added threat intelligence successfully in Splunk Enterprise Security.



Threat Intelligence Audit

Details regarding updates to ES Threat Intelligence

Download Enabled/Disabled: Enabled

Download Location: All

Intelligence Downloads

_time	stanza	disabled			weight	exit_status	download_status	run_duration
2022-07-12 15:34:32	icann_top_level_domain_list	0		tlds-alpha-by-domain.txt	60	PID 17197 0	threat list downloaded	6.0
2022-07-12 15:34:27	local_certificate_intel	0		_intel	60	PID 17200 0		1.0
2022-07-12 15:34:27	local_domain_intel	0		l	60	PID 17206 0		1.0
2022-07-12 15:34:27	local_email_intel	0			60	PID 17218 0		1.0
2022-07-12 15:34:27	local_file_intel	0			60	PID 17225 0		1.0
2022-07-12 15:34:27	local_http_intel	0			60	PID 17231 0		1.0
2022-07-12 15:34:28	local_ip_intel	0			60	PID 17241 0		2.0
2022-07-12 15:34:28	local_process_intel	0	threatlist	lookup://local_process_intel	60	PID 17249 0		1.0
2022-07-12 15:34:28	local_registry_intel	0	threatlist	lookup://local_registry_intel	60	PID 17268 0		1.0
2022-07-12 15:34:28	local_service_intel	0	threatlist	lookup://local_service_intel	60	PID 17272 0		1.0

Next steps

Now that you're doing more with Splunk Enterprise Security, get even more value through implementing use cases, or for additional information see some of these great resources:

- .Conf Talk: Expect more from your threat intelligence in Splunk Enterprise Security and Splunk SOAR
- Docs: Threat intelligence framework in Splunk ES
- Docs: Add threat intelligence to Splunk Enterprise

Still having trouble? Splunk has many resources available to help get you back on track. We recommend the following:

- Splunk OnDemand Services: Credit-based services that allow direct access to Splunk technical consultants for a variety of technical services from a pre-defined catalog. Many Splunk customers already have OnDemand credits included as part of their software license. To request OnDemand Services, file a ticket through the Support Portal.
- Splunk Answers**:** Ask your question to the Splunk Community, which has provided over 50,000 user solutions to date.
- Splunk Customer Support: Contact Splunk to discuss your environment and receive customer support.