Threat Sources within Splunk Enterprise Security

Splunk Enterprise Security (ES) includes various pre-configured threat intelligence sources. Splunk ES uses these threat sources for monitoring and investigation purposes by comparing the contents of multiple threat sources to indexed events. The table below is a listing of the available threat sources as well as the current configuration settings within the QA-Lab version of Splunk ES. NOTE: The entries in the table that are **bolded** are the currently enabled threat sources.

Threat Sources Table

| **Threat Source** | **Threat Provider** | **Source Site** | **Current Setting** |
| --- | --- | --- | --- |
| **Alexa Top 1 Million Sites** | **Alexa Internet** | [**http://s3.amazonaws.com/alexa-static**](http://s3.amazonaws.com/alexa-static) | **Enabled** |
| Emerging Threats compromised IPs blocklist | Emerging Threats | <http://rules.emergingthreats.net/blockrules> | Disabled |
| Emerging Threats fwip rules | Emerging Threats | <http://rules.emergingthreats.net/fwrules> | Disabled |
| Malware domain host list | Hail a TAXII.com | <http://hailataxii.com> | Disabled |
| **iblocklist Logmein** | **I-Blocklist** | [**http://list.iblocklist.com**](http://list.iblocklist.com) | **Enabled** |
| **iblocklist Piratebay** | **I-Blocklist** | [**http://list.iblocklist.com**](http://list.iblocklist.com) | **Enabled** |
| **iblocklist Proxy** | **I-Blocklist** | [**http://list.iblocklist.com**](http://list.iblocklist.com) | **Enabled** |
| **iblocklist Rapidshare** | **I-Blocklist** | [**http://list.iblocklist.com**](http://list.iblocklist.com) | **Enabled** |
| **iblocklist Spyware** | **I-Blocklist** | [**http://list.iblocklist.com**](http://list.iblocklist.com) | **Enabled** |
| **iblocklist Tor** | **I-Blocklist** | [**http://list.iblocklist.com**](http://list.iblocklist.com) | **Enabled** |
| **iblocklist Web attacker** | **I-Blocklist** | [**http://list.iblocklist.com**](http://list.iblocklist.com) | **Enabled** |
| **ICANN Top-level Domains List** | **IANA** | [**http://data.iana.org**](http://data.iana.org) | **Enabled** |
| **local\_certificate\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_certificate\_intel** | **Enabled** |
| **local\_domain\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_domain\_intel** | **Enabled** |
| **local\_email\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_email\_intel** | **Enabled** |
| **local\_file\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_file\_intel** | **Enabled** |
| **local\_http\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_http\_intel** | **Enabled** |
| **local\_ip\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_ip\_intel** | **Enabled** |
| **local\_process\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_process\_intel** | **Enabled** |
| **local\_registry\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_registry\_intel** | **Enabled** |
| **local\_service\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_service\_intel** | **Enabled** |
| **local\_user\_intel** | **DA-ESS-ThreatIntelligence** | **lookup://local\_user\_intel** | **Enabled** |
| **Malware Domain Blocklist** | **Malware Domains** | [**http://mirror1.malwaredomains.com**](http://mirror1.malwaredomains.com) | **Enabled** |
| MaxMind GeoIP ASN IPv4 Database | MaxMind | <http://download.maxmind.com> | Disabled |
| MaxMind GeoIP ASN IPv6 Database | MaxMind | <http://download.maxmind.com> | Disabled |
| **Mozilla Public Suffix List** | **Mozilla** | [**https://publicsuffix.org**](https://publicsuffix.org) | **Enabled** |
| abuse.ch Palevo C&C IP Blocklist | abuse.ch | <https://palevotracker.abuse.ch> | Disabled |
| Phishtank Database | Phishtank | <http://data.phishtank.com> | Disabled |
| **SANS blocklist** | **SANS** | [**http://isc.sans.edu**](http://isc.sans.edu) | **Enabled** |
| abuse.ch ZeuS blocklist (bad IPs only) | abuse.ch | <https://zeustracker.abuse.ch> | Disabled |
| abuse.ch ZeuS blocklist (standard) | abuse.ch | <https://zeustracker.abuse.ch> | Disabled |