EclecticIQ splunk>

SOLUTIONS BRIEF

Time to Soar with EclecticIQ and Splunk

Make your CTI analyst the Splunk team's hero with the Splunk Apps for EclecticIQ Intelligence Center.

www.eclecticiq.com

Splunk Apps Features

Automated Integration

EclecticIQ Intelligence Center includes built-in integration with Splunk Enterprise and Splunk SOAR.

Prioritize Threat Response

Splunk Enterprise analyzes and filters EclecticIQ's cyber threat data to identify your organization's most relevant threats.

Instant Operations

The Splunk Enterprise App ships with a default set of dashboard gauges. The dashboard facilitates Splunk users analyzing threats and performing triage on any Indicators of Compromise (IOCs) the data analysis yields.

Team Benefits

Benefit to CTI

CTI Teams automatically receive critical sightings from Splunk to enrich and help prioritize ongoing threat analysis.

Benefit to SOC/Incident Response

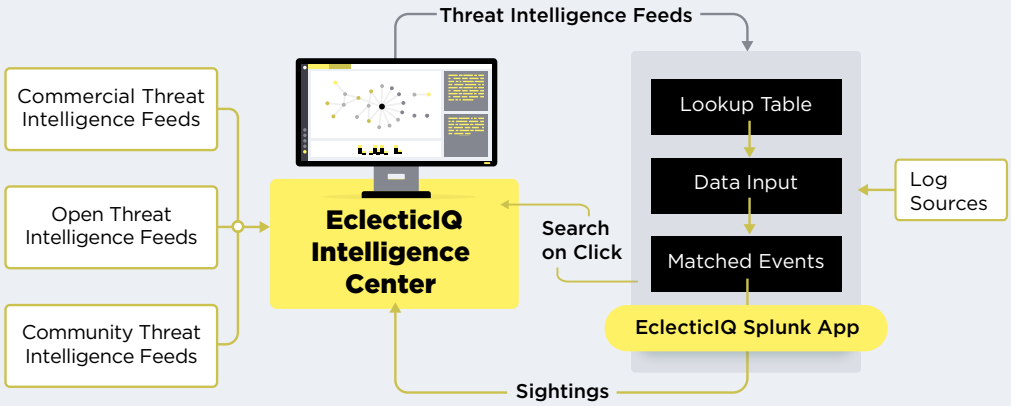
SOC/IR teams gain context from EclecticIQ Intelligence Center, driving more effective and efficient Splunk alert analysis.

Benefit to Security Leaders

Tight integration of CTI and SOC operations drives down mean time to detect (MTTD) and respond (MTTR) by dropping investigation times significantly.

Integrate EclecticIQ Intelligence Center with Splunk Enterprise

Relevant Feed (Half-Life, Relevancy, TLP, Confidentiality, Maliciousness, Tagging)



EclecticIQ and Splunk Enterprise Use Cases

SOC Augmentation

The challenge

According to the Ponemon Institute, more than half of all organizations believe its SOC is ineffective at gathering evidence and investigating and finding the source of threats.[1]

SOCs need the right data at the right time, with the right context to successfully identify, prioritize, and respond to threats. SOCs need to aggregate and prioritize CTI to make proactive decisions on what threats pose the greatest risk.

The Solution

EclecticIQ Intelligence Center includes built-in integration with Splunk to augment the SOC's use of Splunk as its SIEM.

The Splunk Enterprise App facilitates:

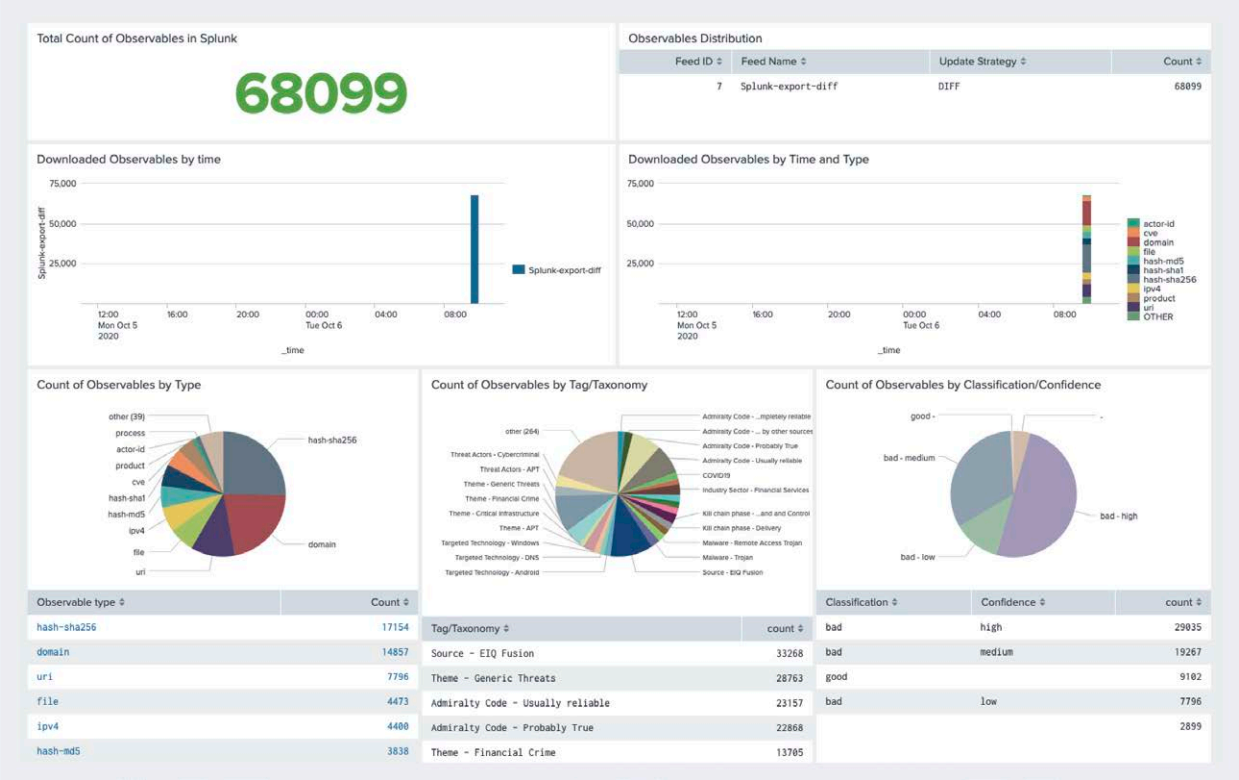
- Granular control of sources, entities, and observables
- Filtering of integrated intelligence based on content, tags, maliciousness, decay rates, TLP, and much more
- Integrations for multiple security controls and workflow systems
- TLP management to filter and overwrite sharing designations for specific integrations

The Outcome

EclecticIQ's enrichment of alerts and telemetry ensures that SOC analysts focus on what matters:

- Enrichment of threat intelligence for qualification and reduction of false positives. EclecticIQ transfers all data without losing any context
- Anonymization of fields to protect the confidentiality of data and comply with GDPR
- Analysts easily view incident context in powerful graph visualization and search tools for exceptionally fast analysis and response.

Focus on What Matters With EclecticIQ SOC Augmentation



EclecticIQ and Splunk SOAR Use Cases

SOAR Integration

The challenge

CTI can enhance multiple SOAR use cases, including alert triage, incident response (IR), IOC Hunting, vulnerability management (VM), and intelligence sharing. However, to successfully implement these use cases, organizations need to turn critical CTI practices into SOC team workflows. These practices include augmenting security controls, automatically updating watchlists, and leveraging sightings.

The Solution

The Splunk SOAR App for EclecticIQ Intelligence Center seamlessly integrates into Splunk SOAR. Through this integration, CTI analysts can trigger playbooks directly from EclecticIQ Intelligence Center. And it's a two-way street with sightings from Splunk enhancing CTI actions. This seamless integration is the essence of intelligence-driven security. The Splunk SOAR App facilitates:

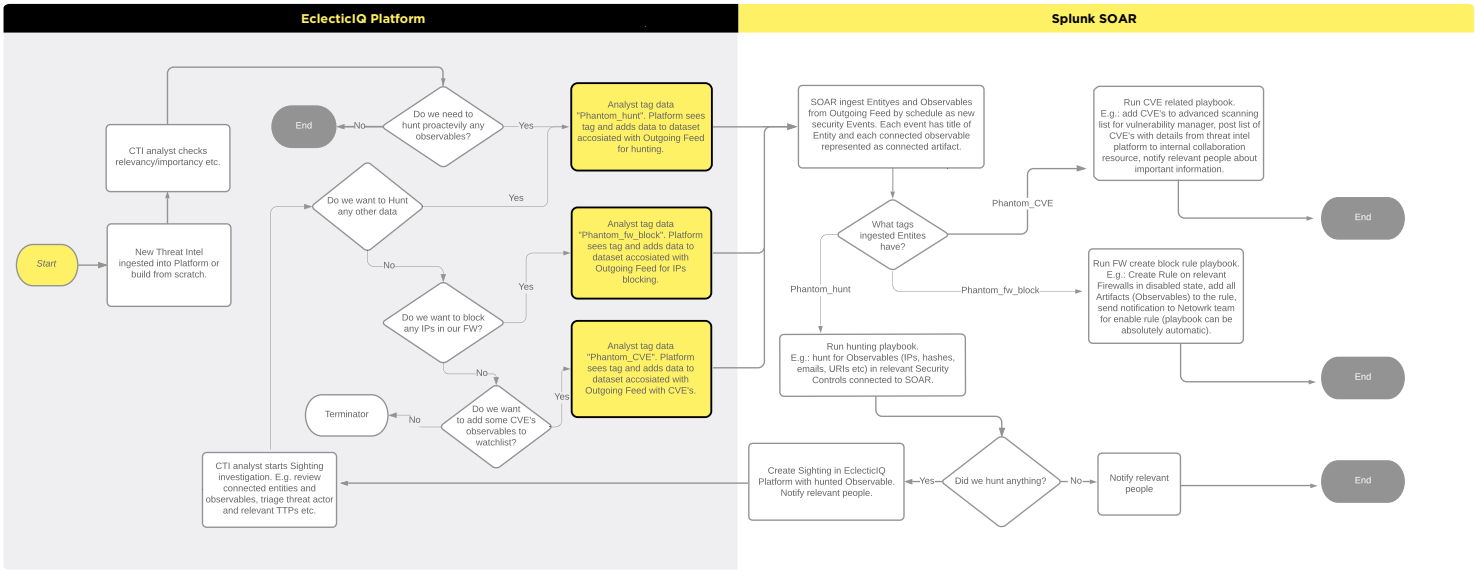
- Proactively hunting threat intelligence and data
- Automating security control integration: block IPs (FW), blacklist hashes (EDR)
- Adding CVE's observables to watchlists

The Outcome

Integrating Splunk SOAR with EclecticIQ Intelligence Center decreases the mean time to detect (MTTD), respond (MTTR), and remediate incidents. Benefits include:

- Faster investigations because EclecticIQ delivers high confidence threat intelligence that improves the effectiveness of the playbooks
- Fewer false positives due to automated enrichment of indicators
- Powerful threat hunting by automatically correlating high confidence threats with existing IOCs and vulnerabilities
- Threat Intel team adjusts cybersecurity controls safely via Phantom automations
- Triggering investigations from sighting to triage threat actor and relevant TTPs

Improve Playbook Effectiveness With EclecticIQ and Splunk SOAR



 |

About EclecticIQ

EclecticIQ is a global provider of threat intelligence, hunting and response technology and services.

Stay ahead of rapidly evolving threats and outmaneuver your adversaries by embedding Intelligence at the core™ of your cyberdefenses.

We operate worldwide with offices and teams across Europe and UK, North America, India and via value-add partners.

Contact us at:
info@eclecticiq.com
www.eclecticiq.com

Download the apps from:
eclecticiq.com/splunk-enterprise-app
eclecticiq.com/splunk-soar-app

About Splunk

The Splunk platform removes the barriers between data and action, empowering observability, IT and security teams to ensure their organizations are secure, resilient and innovative.

Founded in 2003, Splunk is a global company — with over 7,500 employees, Splunkers have received over 1,020 patents to date and availability in 21 regions around the world — and offers an open, extensible data platform that supports shared data across any environment so that all teams in an organization can get end-to-end visibility, with context, for every interaction and business process. Build a strong data foundation with Splunk.

For more information visit splunk.com