Data Sheet

EclecticIQ | splunk>

Time to Soar with EclecticIQ and Splunk

Make your CTI analyst the Splunk team's hero with the Splunk App for EclecticIQ Platform

Splunk App Features

Automated Integration

EclecticIQ Platform includes built-in integration with Splunk Enterprise and Splunk Phantom.

Prioritize Threat Response

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

Instant Operations

The 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

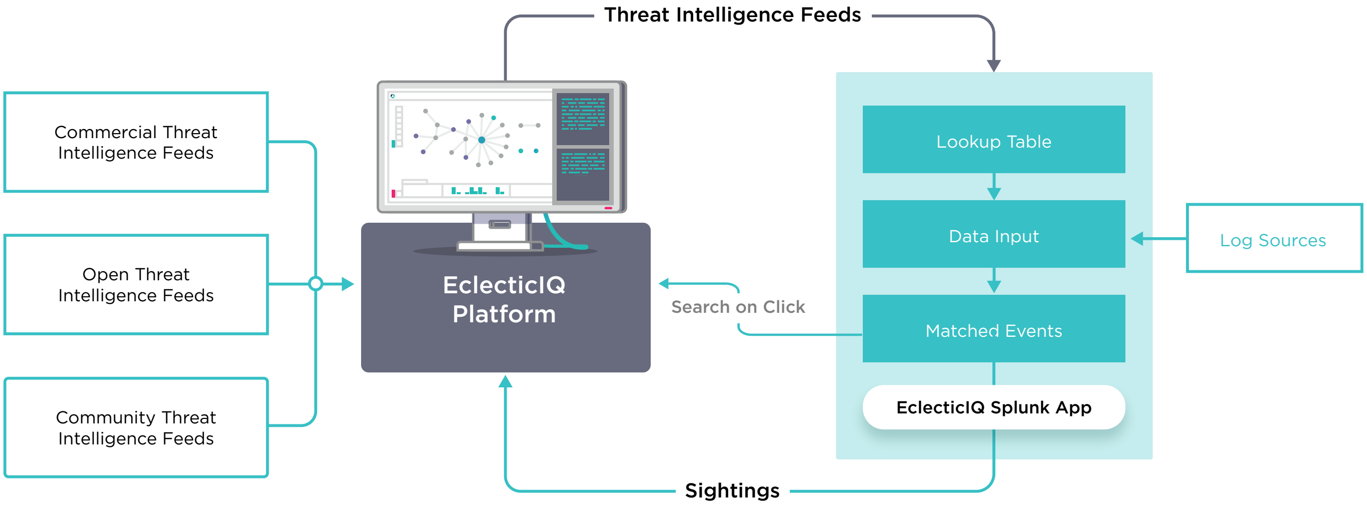
SOC/IR teams gain context from EclecticIQ Platform, driving more effective and efficient Splunk alert analysis.

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 Platform with Splunk

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


Threat Intelligence Feeds
Commercial Threat Intelligence Feeds
Open Threat Intelligence Feeds
Community Threat Intelligence Feeds
EclecticIQ Platform
Search on Click
Lookup Table
Data Input
Matched Events
EclecticIQ Splunk App
Log Sources
Sightings

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

The Splunk App facilitates:

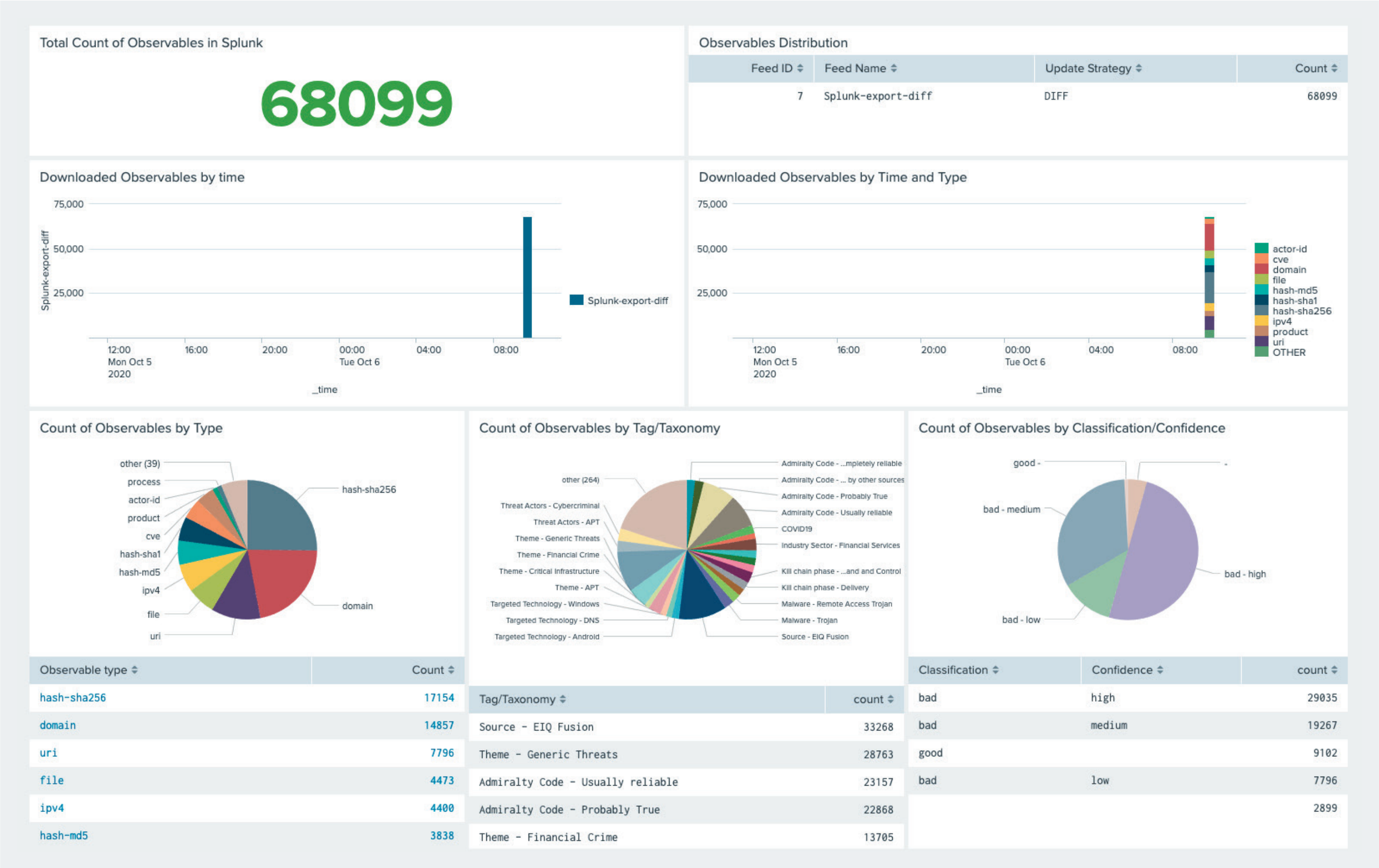
- Granular control of sources, entities, and observables
- Filtering of integrated intelligence based on content, tags, maliciousness, decay rates, TLP, and much more
- Integrations for multiple security controls and workflow systems
- TLP management to filter and overwrite sharing designations for specific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



Total Count of Observables in Splunk

68099

Observables Distribution

Feed ID	Feed Name	Update Strategy	Count
7	Splunk-export-diff	DIFF	68099

Downloaded Observables by time

Downloaded Observables by Time and Type

Count of Observables by Type

Observable type	Count
hash-sha256	17154
domain	14857
uri	7796
file	4473
ipv4	4400
hash-md5	3838

Count of Observables by Tag/Taxonomy

other (264)
Threat Actors - Cybercriminal
Threat Actors - APT
Theme - Generic Threats
Theme - Financial Crime
Theme - Critical Infrastructure
Theme - APT
Targeted Technology - Windows
Targeted Technology - DNS
Targeted Technology - Android
Admiralty Code - ...mpletely reliable
Admiralty Code - ... by other sources
Admiralty Code - Probably True
Admiralty Code - Usually reliable
COVID19
Industry Sector - Financial Services
Kill chain phase - ...and and Control
Kill chain phase - Delivery
Malware - Remote Access Trojan
Malware - Trojan
Source - EIQ Fusion

Tag/Taxonomy	count
Source - EIQ Fusion	33268
Theme - Generic Threats	28763
Admiralty Code - Usually reliable	23157
Admiralty Code - Probably True	22868
Theme - Financial Crime	13705

Count of Observables by Classification/Confidence

Classification	Confidence	count
bad	high	29035
bad	medium	19267
good		9102
bad	low	7796
		2899

EclecticIQ and Splunk 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 Phantom App for EclecticIQ Platform seamlessly integrates into Splunk Phantom. Through this integration, CTI analysts can trigger Phantom playbooks directly from EclecticIQ Platform. 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 Phantom App facilitates:

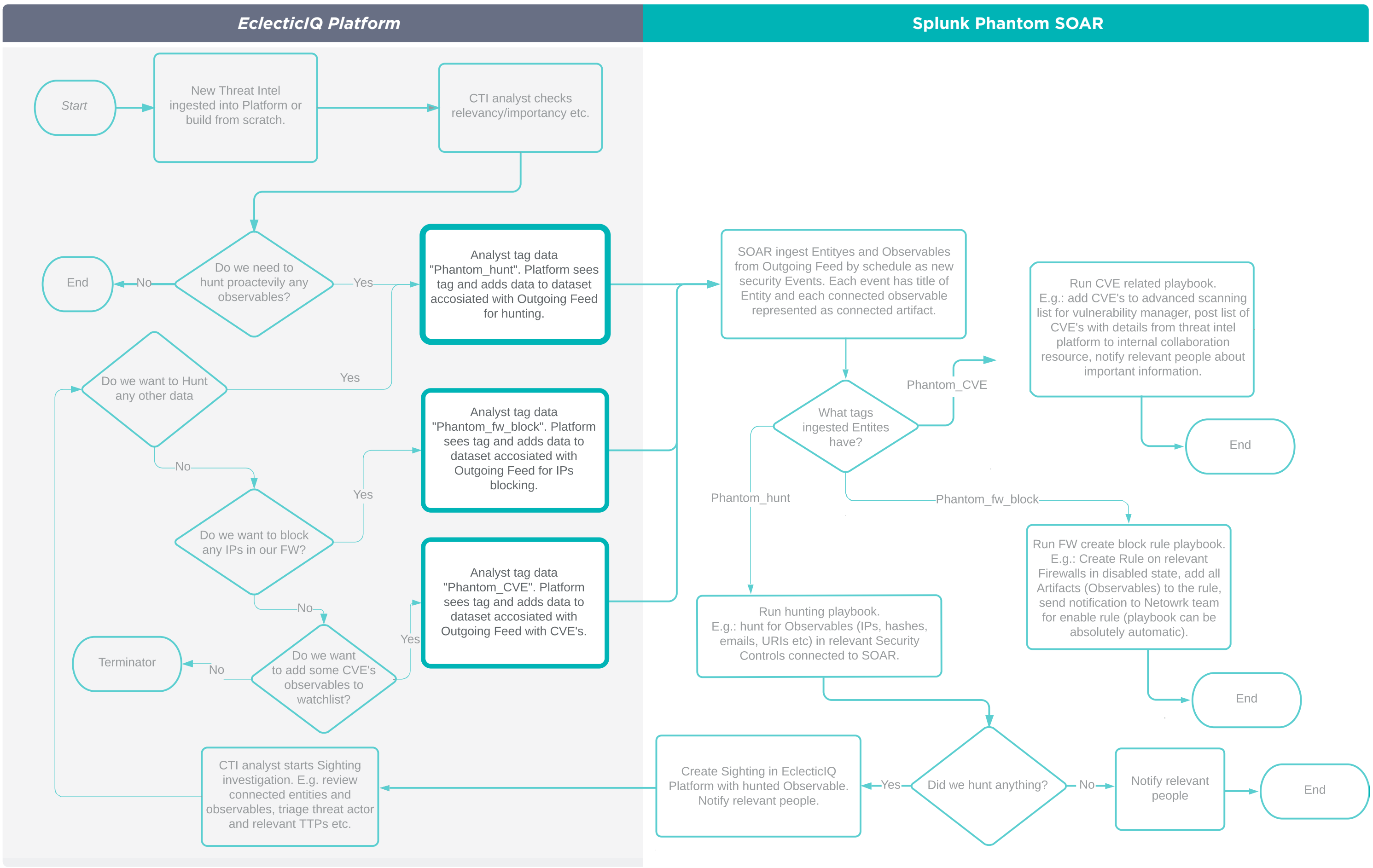
- Proactively hunting threat intelligence and data
- Automate security control integration: block IPs (FW), blacklist hashes (EDR)
- Adding CVE's observables to watchlists

The Outcome

Integrating Splunk Phantom with EclecticIQ Platform 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 Phantom


EclecticIQ Platform
Splunk Phantom SOAR
Start
New Threat Intel ingested into Platform or build from scratch.
CTI analyst checks relevancy/importancy etc.
End
No
Do we need to hunt proactevily any observables?
Yes
Analyst tag data "Phantom_hunt". Platform sees tag and adds data to dataset accosiated with Outgoing Feed for hunting.
Do we want to Hunt any other data
Yes
No
Analyst tag data "Phantom_fw_block". Platform sees tag and adds data to dataset accosiated with Outgoing Feed for IPs blocking.
Yes
Do we want to block any IPs in our FW?
No
Analyst tag data "Phantom_CVE". Platform sees tag and adds data to dataset accosiated with Outgoing Feed with CVE's.
Yes
Terminator
No
Do we want to add some CVE's observables to watchlist?
CTI analyst starts Sighting investigation. E.g. review connected entities and observables, triage threat actor and relevant TTPs etc.
SOAR ingest Entityes and Observables from Outgoing Feed by schedule as new security Events. Each event has title of Entity and each connected observable represented as connected artifact.
Run CVE related playbook. E.g.: add CVE's to advanced scanning list for vulnerability manager, post list of CVE's with details from threat intel platform to internal collaboration resource, notify relevant people about important information.
Phantom_CVE
What tags ingested Entites have?
End
Phantom_hunt
Phantom_fw_block
Run FW create block rule playbook. E.g.: Create Rule on relevant Firewalls in disabled state, add all Artifacts (Observables) to the rule, send notification to Netowrk team for enable rule (playbook can be absolutely automatic).
Run hunting playbook. E.g.: hunt for Observables (IPs, hashes, emails, URIs etc) in relevant Security Controls connected to SOAR.
End
Create Sighting in EclecticIQ Platform with hunted Observable. Notify relevant people.
Yes
Did we hunt anything?
No
Notify relevant people
End

About EclecticIQ

EclecticIQ is an official Splunk Technology Alliance Partner. We enable intelligence-powered cybersecurity for government organizations and commercial enterprises. We develop analyst-centric products and services that align our clients' cybersecurity focus on their threat reality. The result is intelligence-led security, improved detection and prevention, and cost-efficient security investments.

For more information on the Splunk App, please go to **https://splunkbase.splunk.com/app/4176/**

Please contact us for a demo:
info@eclecticiq.com
+31 (0) 20 737 1063

[1] Ponemon Institue, LLC, "Improving the Effectiveness of the Security Operations Center," June 2019, 9.

EclecticIQ
INTELLIGENCE POWERED DEFENSE