EclecticIQ

Intelligence
at the core

Intelligence
Hunting
Response

DATA SHEET

EclecticIQ Intelligence Center

Analyst-centric intelligence management
and workflow automation

www.eclecticiq.com

Introduction

The stark reality is that cyberattacks – and the resulting breaches – are now commonplace. The adversaries are highly organized and adept at side-stepping attempts to stop them.

Security professionals must defend against an ever-increasing threat landscape. A daunting task, it's not feasible or economically viable for governments or enterprises to defend against every single exploit or threat vector.

Overcoming these challenges requires harnessing the power of cyber threat intelligence (CTI) for smart allocation of resources to strengthen the security posture against the attacks most likely to occur.

This approach is intelligence led security operations that provides workflow leading to faster and better-informed business decisions.

Key Benefits

Identify the most critical threats faster

- Process structured and unstructured threat data by automating qualification and discovery.
- Collaborate using dynamic workspaces to sort intelligence automatically.
- Investigate sophisticated threats better and speed up investigations through powerful analyst tools and collaboration.

Improve detection, hunting, and response

- Add queries, graphs, free text, and assign tasks for faster response.
- Curation and integration of intelligence and threat detection content into third-party security controls.

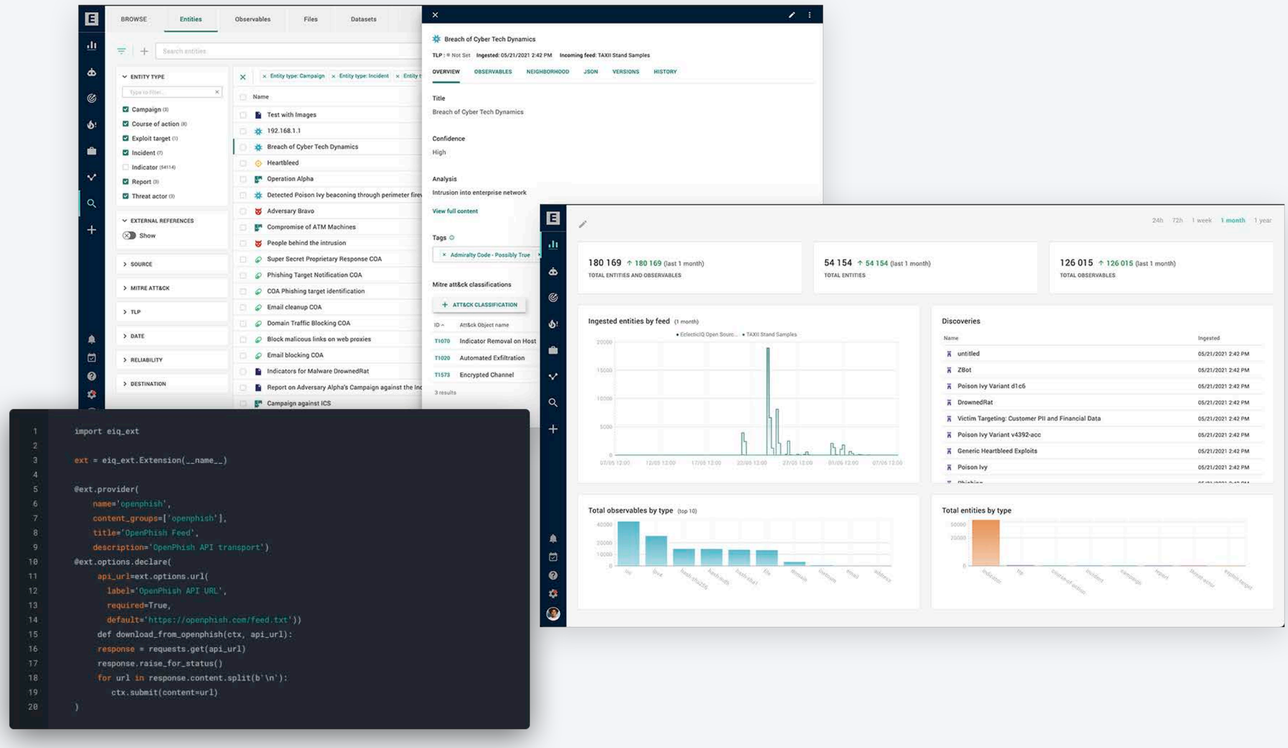
Disseminate and exchange actionable intelligence at machine-speed

- Achieve enhanced decision-making and industry collaboration with advanced workflows and shared workspaces to better triage, analyze, process, and disseminate intelligence.

Product Overview

EclecticIQ Intelligence Center is the only threat intelligence solution that unites machine-powered threat data processing and dissemination with human-led data analysis without compromising analyst control, freedom, or flexibility. Using an advanced threat intelligence manager, curated intelligence feeds and a collaborative analyst workbench, your analysts, can collect and process data, create and share cyberthreat intelligence, and supercharge detection and response.

EclecticIQ Intelligence Center



☑ Campaign (3)
☑ Course of action (8)
☑ Exploit target (1)
☑ Incident (7)
□ Indicator (54114)
☑ Report (3)
☑ Threat actor (3)

Test with Images
192.168.1.1
Breach of Cyber Tech Dynamics
Heartbleed
Operation Alpha
Detected Poison Ivy beaconing through perimeter firev
Adversary Bravo
Compromise of ATM Machines
People behind the intrusion
Super Secret Proprietary Response COA
Phishing Target Notification COA
COA Phishing target identification
Email cleanup COA
Domain Traffic Blocking COA
Block malicous links on web proxies
Email blocking COA
Indicators for Malware DrownedRat
Report on Adversary Alpha's Campaign against the Inc
Campaign against ICS

Breach of Cyber Tech Dynamics

TLP : Not Set Ingested: 05/21/2021 2:42 PM Incoming feed: TAXII Stand Samples

Title
Breach of Cyber Tech Dynamics

Confidence
High

Analysis
Intrusion into enterprise network

View full content

Tags
× Admiralty Code - Possibly True

Mitre att&ck classifications

+ ATT&CK CLASSIFICATION

ID	Att&ck Object name
T1070	Indicator Removal on Host
T1020	Automated Exfiltration
T1573	Encrypted Channel

3 results

```
import eiq_ext

ext = eiq_ext.Extension(__name__)

@ext.provider(
    name='openphish',
    content_groups=['openphish'],
    title='OpenPhish Feed',
    description='OpenPhish API transport')
@ext.options.declare(
     api_url=ext.options.url(
       label='OpenPhish API URL',
       required=True,
       default='https://openphish.com/feed.txt'))
     def download_from_openphish(ctx, api_url):
     response = requests.get(api_url)
     response.raise_for_status()
     for url in response.content.split(b'\n'):
        ctx.submit(content=url)
)
```

180 169 ↑ 180 169 (last 1 month)
TOTAL ENTITIES AND OBSERVABLES

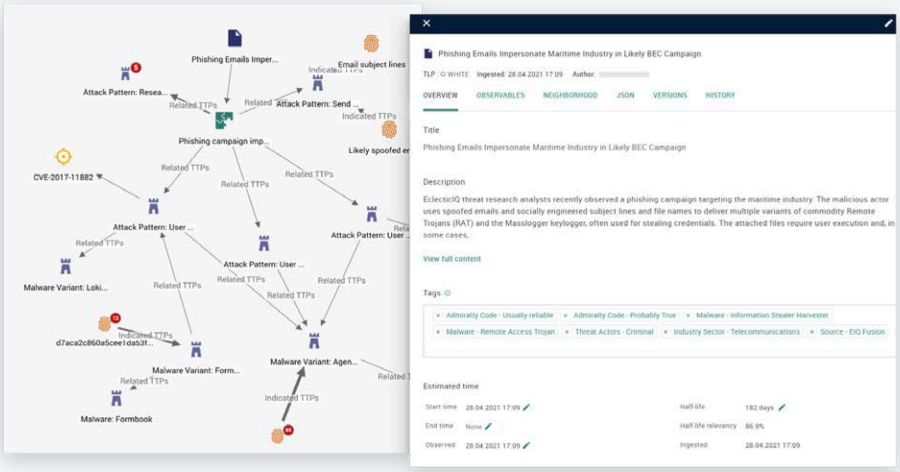
54 154 ↑ 54 154 (last 1 month)
TOTAL ENTITIES

126 015 ↑ 126 015 (last 1 month)
TOTAL OBSERVABLES

Discoveries

Name	Ingested
untitled	05/21/2021 2:42 PM
ZBot	05/21/2021 2:42 PM
Poison Ivy Variant d1c6	05/21/2021 2:42 PM
DrownedRat	05/21/2021 2:42 PM
Victim Targeting: Customer PII and Financial Data	05/21/2021 2:42 PM
Poison Ivy Variant v4392-acc	05/21/2021 2:42 PM
Generic Heartbleed Exploits	05/21/2021 2:42 PM
Poison Ivy	05/21/2021 2:42 PM

EclecticIQ Curated Feeds



Phishing Emails Impersonate Maritime Industry in Likely BEC Campaign

TLP : WHITE Ingested: 28.04.2021 17:09 Author: [redacted]

Title
Phishing Emails Impersonate Maritime Industry in Likely BEC Campaign

Description
EclecticIQ threat research analysts recently observed a phishing campaign targeting the maritime industry. The malicious actor uses spoofed emails and socially engineered subject lines and file names to deliver multiple variants of commodity Remote Trojans (RAT) and the Masslogger keylogger, often used for stealing credentials. The attached files require user execution and, in some cases,

View full content

Tags
× Admiralty Code - Usually reliable × Admiralty Code - Probably True × Malware - Information Stealer Harvester
× Malware - Remote Access Trojan × Threat Actors - Criminal × Industry Sector - Telecommunications × Source - EIQ Fusion

Estimated time

Start time	28.04.2021 17:09	Half-life	182 days
End time	None	Half-life relevancy	86.9%
Observed	28.04.2021 17:09	Ingested	28.04.2021 17:09

Supporting the CTI Lifecycle

By using a core set of workflows and processes within a collaborative workspace, analysts can quickly discern actionable and relevant intelligence. EclecticIQ Intelligence Center consolidates, normalizes, and enriches threat content so that analysts can focus on threat data triage, analysis, collaboration, and production of intelligence.

EclecticIQ Intelligence Center efficiently supports threat intelligence analysts to execute an effective CTI lifecycle supporting critical stakeholders, including SOCs, CERTs, information resources, vulnerability management, IT architects, businesses and organizational leaders.

Planning and Collection

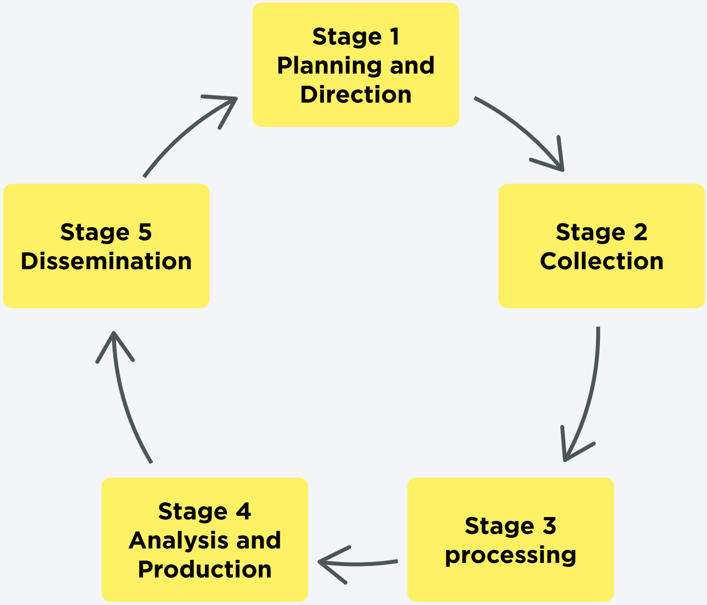
- Intelligence data from multiple sources.
- Structured STIX-compatible and unstructured entities.
- A large diversity of supported data formats: CSV, PDF, proprietary, and STIX.
- Automatically pull data from active web sessions.

Analysis and Collaboration

- Automated qualification, triage, and discovery processes.
- Collaborative workspaces with intuitive graphs, search, pivoting tools, and tasking.
- Capture data from websites via the browser extension to feed it directly into the data repository.

Production and Dissemination

- Reports for dissemination to both human and machine consumers.
- Daily digests and full intelligence reports.
- Dissemination with controls to manage data sensitivity and privacy.



EclecticIQ Intelligence Center Products

Intelligence Manager

Create a single source of truth for collaboration and analysis. Move beyond the time-consuming manual processing of multiple feeds to increase your team's productivity, accuracy, and responsiveness.

Core features:

- Automatic data ingestion, normalization, transformation, and enrichment.
- Combine internal, open and commercial sources and industry partnership feeds.
- Native support of industry standards (e.g., STIX/TAXII, MITRE ATT&CK).
- Disseminate human- and machine-readable intelligence as reports to stakeholders or direct input to security controls.

Key benefits:

- Highly scalable and cost effective with a unique ingestion data pipeline.
- Identify the most critical threats faster with a single source of truth repository for collaboration and analysis.
- Quickly cut through the noise to focus on what attack vectors are most pertinent.
- Improve detection, hunting, and response by delivering machine-readable intelligence feeds to an extensive catalog of third-party security controls.

Analyst Workbench

Conduct deep threat investigations using advanced search queries, intuitive graphical link analysis, and support for leading CTI frameworks to help your analysts identify the TTPs of sophisticated threat actors.

Core features:

- Prioritize intelligence and easily align indicators with MITRE ATT&CK.
- Comprehensive dashboard and dynamic workspaces providing workflow-oriented views.
- Powerful search queries, intuitive graphical link analysis, and support for leading CTI frameworks, standards, and libraries.
- Develop professional reports for threat intelligence dissemination.

Key benefits:

- Identify the TTPs of sophisticated threat actors with MITRE ATT&CK search and mapping.
- Shorten investigations by quickly sharing dynamic results around a specific topic or area of interest with team members via collaborative workspaces,
- Leverage a browser extension to build on existing intelligence by easily adding missing or editing existing STIX-compatible data.

Integrations, API & SDK

Open and extendable integrations with any security control with pre-built integrations or through the use of powerful developer tools.

Core features:

- Detection, hunting, and response for major SIEMs.
- Unique bi-directional MISP integration to ingest and synchronize MISP community threat intelligence.
- Use industry standards like STIX, CSV, and EclecticIQ JSON to integrate into third-party security controls.

Key benefits:

- Quick start with out-of-the-box integrations.
- Boost SIEM effectiveness with direct integration.
- Take immediate action through automatic delivery of YAML files to security controls.
- Quickly integrate custom tools with an extensible SDK and deep developer support.

EclecticIQ Intelligence Center Use Cases

Expedite Detection, Hunting, and Response

The challenge:

- It is difficult for overwhelmed SOC analysts to get the right threat data with the right confidence, context, and clarity to succeed at hunting, detection, and response.

The solution:

- With EclecticIQ Intelligence Center, the SOC can ingest high-quality indicators and hunting data rich with context and filter based on tags, threat expiration date, maliciousness, confidence, TLP, and more.

Outcome:

- The SOC leverages timely threat data and intelligence synchronized with EclecticIQ source datasets to expedite and streamline hunting, detection, and response.

Collaboration and Dissemination

The challenge:

- Open source and homegrown tools lack rich collaboration, analyst workflows, and dissemination capabilities. These tools also lack controls to protect the confidentiality of an organization's data.

The solution:

- EclecticIQ Intelligence Center provides robust analyst workflows that allow analysts, intelligence teams, and threat hunting teams to quickly establish and prioritize relevant intelligence, collaborate with other analysts and groups, and disseminate information with external communities.

Outcome:

- The CTI team identifies active threats quickly and with high confidence to trigger an automated threat response.

Government and Enterprise Ready

EclecticIQ supports the most targeted organizations in the world. For this reason, we deliver deployment models and core capabilities to meet the needs of high-security government and enterprise deployments.

- Flexible deployment options: single instance to multi-tier on virtual machines or physical hardware: on-premises, hosted, and hybrid environments.
- Retention policies for compliance with the General Data Protection Regulation (GDPR) and agency policies.
- Highly configurable and easily integrates with existing security infrastructure.
- Robust authorization and authentication controls.
- Data diodes for unclassified to classified data transfer.
- Flexible inter- and intra-organization collaboration models including hierarchical, flat, hub-and-spoke, and hybrid.

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**