eclectic iq

EclecticIQ Platform. The Analyst-centric Threat Intelligence Platform Based on STIX/TAXII that Meets the Full Spectrum of Intelligence Needs

Go beyond automation. Empower your threat analysts to investigate threats and assemble seemingly distant dots into a bigger picture.

Introduction

Cyber threats have forced enterprises and governments to improve cyber defenses across CERTs, SOCs, IT departments, and functional areas within organizations. The diffuse spending makes it difficult to maintain budgets at a reasonable and predictable level, and the dispersed responsibility slows down the effectiveness of a response.

By centralizing Cyber Threat Intelligence (CTI) through a human-led, technology-enabled Threat Intelligence Practice (TIP), organizations can improve the overall effectiveness of cyber defenses while regaining control of budgets.

Within a TIP, threat analysts gather and analyze both technical and strategical intelligence, make recommendations on threat mitigation, advise the business to implement changes, and collaborate with external parties on how to improve the overall security posture. This approach allows organizations to better ensure that their IT security efforts and investments are aligned against the reality of their threat exposure.

EclecticIQ Platform, our analyst-centric Threat Intelligence Platform (TIP), sits at the center of a threat intelligence practice by collecting intelligence data from open sources, commercial suppliers, and industry partnerships into a single collaborative analyst workbench. EclecticIQ Platform eliminate manual and repetitive work involved with processing multiple intelligence feeds, allowing analysts to discern the most critical threats, take timely action, advise the organization on how to respond, and collaborate with industry peers. EclecticIQ Platform is based on industry best practice and built with threat intelligence workflows and tradecraft at its core.

At a glance:

- Collection, Enrichment and Exchange
- Relevancy, Qualification and Analysis
- Analysis and Exploration
- Collaboration
- Knowledge basing and Production
- Dissemination and Integration

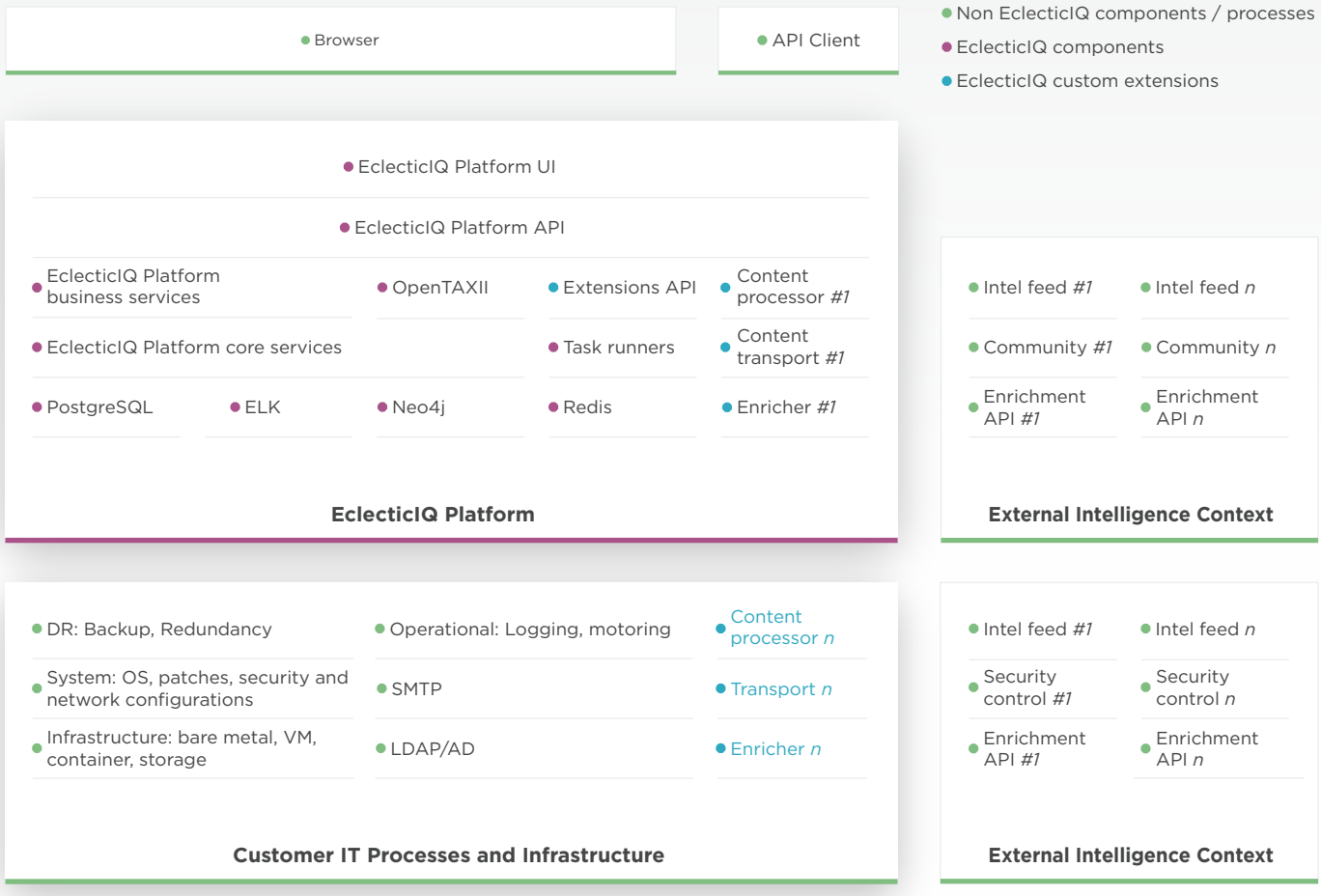
CTI, TIP and EclecticIQ at a Glance

The ability of threat intelligence analysts to quickly understand their threat reality and assist organizations in protecting themselves from cyber attacks depends on how well, and how efficiently, they can make use of the full range of Cyber Threat Intelligence (CTI).

EclecticIQ Platform connects and interprets intelligence data from open sources, commercial suppliers, and industry partnerships. By using a core set of workflows and processes within a collaborative workspace, analysts can quickly discern actionable and relevant intelligence. EclecticIQ consolidates, normalizes, and enriches threat content, so that analysts can focus on triage, analysis, collaboration, and defensive strategies.

EclecticIQ Platform efficiently supports threat intelligence analysts to inform stakeholders including SOCs, CERTs, Information Resources, Vulnerability Management, IT architects, businesses, and organizational leaders.

Technical Architecture



Key Messages

Relevancy

Consolidates incoming intelligence from open sources, communities, and commercial intelligence suppliers.

Determines relevance of threat intelligence through real-time collaboration, accelerating the time to come up with a suitable response.

Allows analysts to easily determine the relevancy of threat intelligence to the organization.

Analyst Empowerment

Eliminates repetitive work and facilitates complex analysis, allowing analysts to concentrate on improving security.

Enables analysts to deal with large amounts of Threat Intelligence on a day-to-day basis.

Provides ad-hoc support during breaches with rapid access to diverse sources of research, supporting creation of Intelligence for their organization.

Enterprise Integration

Keeps pace with evolving threats through live integration of threat intelligence to and from detection, prevention, and response technologies.

Identifies and distributes actionable threat indicators for immediate detection and prevention throughout an organization.

Disseminates intelligence and analyst insights to other security teams and stakeholders.

Intelligence Sourcing

Maintains an up-to-date portfolio of threat intelligence providers.

Acquires new and relevant sources of Cyber Threat Intelligence and integrates them into your environment.

Manages the ongoing process of ingesting structured and unstructured data formats on your behalf.

Relevancy	Analyst Empowerment	Enterprise Integration	Intelligence Sourcing
Key Features			
Intelligence collection, enrichment, and exchange Data fusion, normalization, correlation, and de-duplication Out-of-box connectivity with intelligence providers (e.g., DHS AIS, Flashpoint, FireEye iSIGHT, Group-IB, Intel 471), and enrichment services (e.g. Crowdstrike, DomainTools, Geo-IP, Recorded Future, VirusTotal)	Qualification, triage, and discovery Scoring by threat confidence, reliability, time, kill chain Graphical exploration and analysis Powerful search Workflows based on industry best practices Collaborative workspaces for cases, campaigns, threats, analyses, and tasks	Integration with HPE Security ArcSight, IBM QRadar, Splunk and other SIEM solutions Integration with IDS, IDP and related Security Control and Analysis tools Dissemination to business and security stakeholders over email and/or workflow systems Authentication and authorization using internal protocols or LDAP	Standards-based support for STIX/TAXII APIs for intelligence feeds, intelligence enrichment and search Extensible plugin library and SDK for data formats
Benefits			
Reduce “mean-time-to-know” for awareness of new threats Improve discovery of hidden threats Eliminate unnecessary, duplicative, or irrelevant indicators before they clog your workflow	Improve response time with fast search for specific types of Indicators of Compromise (IOCs) over any time range Real-time risk analysis of IOCs based on severity Understand threat context quickly for adequate response and resource focus. Easy-to-use interface	Direct SIEM integration Increase productivity with bootstrapped workflow of intelligence-related processes such as triage, threat hunting, proactive research, and exposure/ integration of IOC management. Integrate intelligence into existing security investments	Faster on-boarding of new intelligence feeds Get started easily with 24/7 guidance. Accelerate usage of machine-readable threat intelligence (MRTI)

Use Cases

1 Workflow Management

Stakeholders: Keep track of the interests of stakeholders to ensure that they receive intelligence in the cadence and format they expect. Provide complete support for technical security personnel, security analysts, business analysts, incident responders, risk managers and executives.

Tasks: Ensure an adequate schedule of planned and ad-hoc production of automated and analyst-driven intelligence.

2 Collection, Enrichment and Exchange

Central repository: Integrate, normalize, and consolidate existing sources of cyber threat intelligence from multiple formats into a central intelligence repository.

Enrichment: Tap into supplementary data sources to enrich intelligence for easier review by threat analysts.

Discovery: Allow analysts to search through the central repository with user-defined criteria.

Communities: Exchange relevant findings with ISACs, ISAO's, interest groups, and other sharing communities.

3 Qualification and Analysis

Qualification: Assess relevant intelligence regarding:

- Correlations with known TTPs, Actors, Indicators, and Reports
- Enriched intelligence based on external data sources such as passive DNS information, actor databases, virus databases, public databases, and internal databases
- Confidence statements
- Kill-chain associations
- Time relevancy components (e.g. observed vs. ingested; threat start/stop times)
- Related campaigns

Tagging: Uncover correlations within intelligence data using user-generated tags or pre-defined taxonomies.

Search: Use tags and search terms to explore the full collection of intelligence in the repository.

Visualization: Advanced link analysis using intuitive, easy-to-use tools.

4 Collaboration

Catalog: Use a well-defined, standards-based taxonomy to share concerns about cases, campaigns, target models and/or analytic lines.

Collaborate: Share and comment on intelligence findings. For a given analytic line, analysts can contribute to centralized intelligence sources, produce custom reports, and exchange comments. The solution also supports file sharing, task management, auditing access and archiving content.

5 Creation of Intelligence

Structured: Intelligence analysts can produce multi-paragraph reports for a central repository; reports on specific tools, techniques, and procedures; actor profiles, campaign profiles, incident reports, and indicator reports.

Unstructured: Analysts can include unstructured intelligence reports contained within the context of structured information.

6 Dissemination and Integration

Human Stakeholders: Distribute intelligence reports to approved and audited recipients.

Security Controls: Integrate structured intelligence and IOC/IOA feeds into security controls such as SIEMs, Intrusion Detection systems and Incident workflow tools.

Integration: Consolidate, institutionalize, and structure insights and intelligence within a single platform, facilitating the processing of incoming and outgoing feeds.

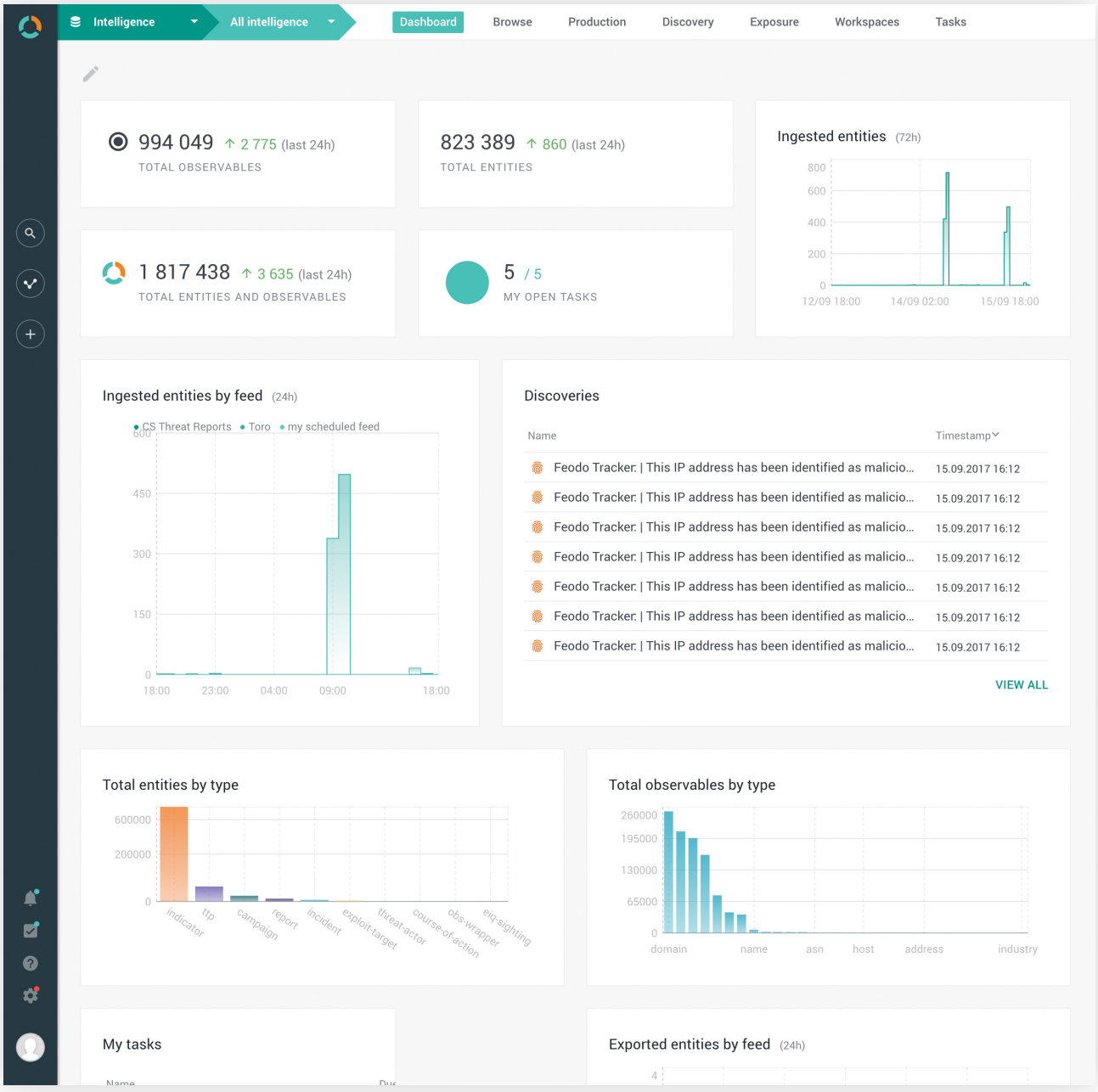
Triage: Automatic quality determination for IOCs, improving the effectiveness and relevance of IOC databases.

Discovery: Correlate new, incoming intelligence with existing intelligence and research; discover new intelligence related to previously published advisories; and automatically correlate data from various reports.

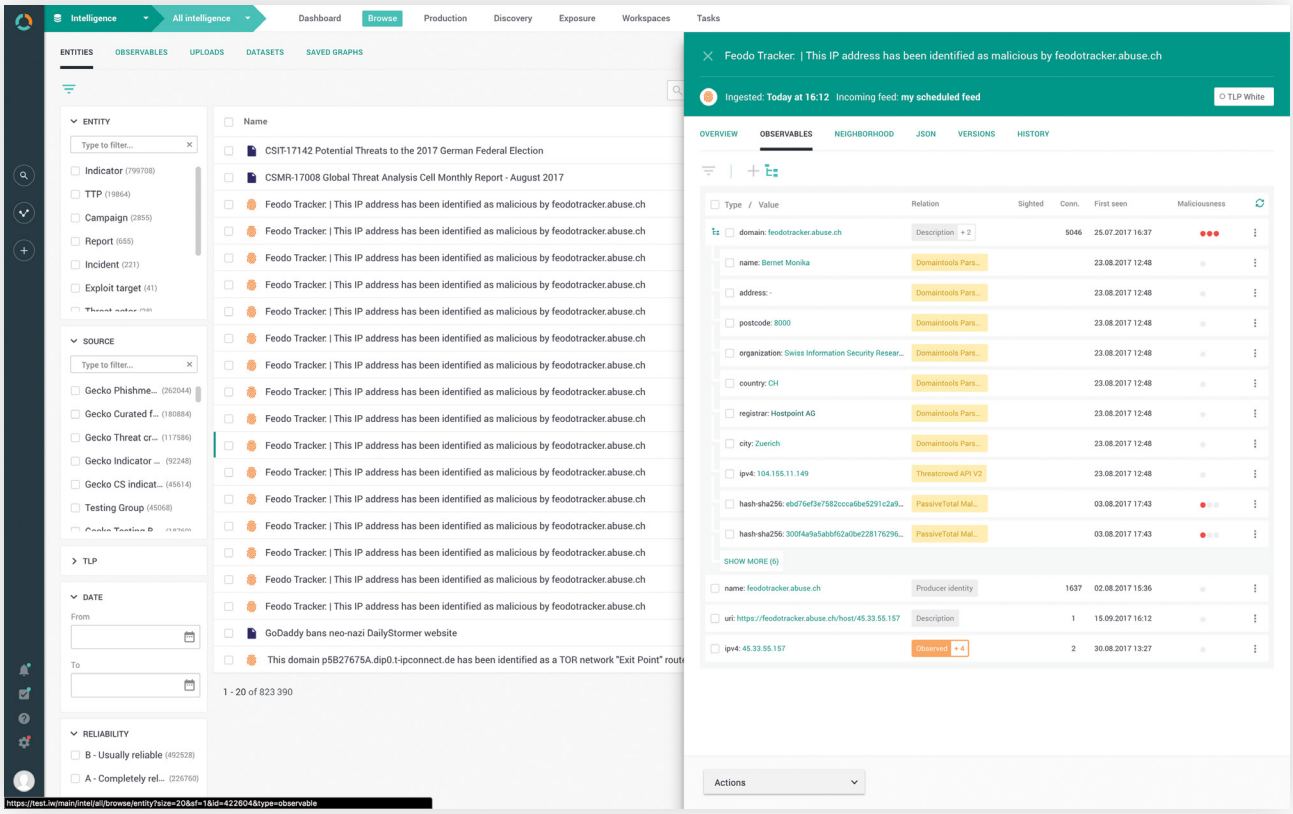
Teamwork: Enable analysts to collaborate during analysis, and during the creation of briefings or advisories, with tools including workflow, file-sharing, and task management.

MISP integration: Automatic enrichment of Malware Information Sharing Project (MISP) indicators to improve overall situational awareness.

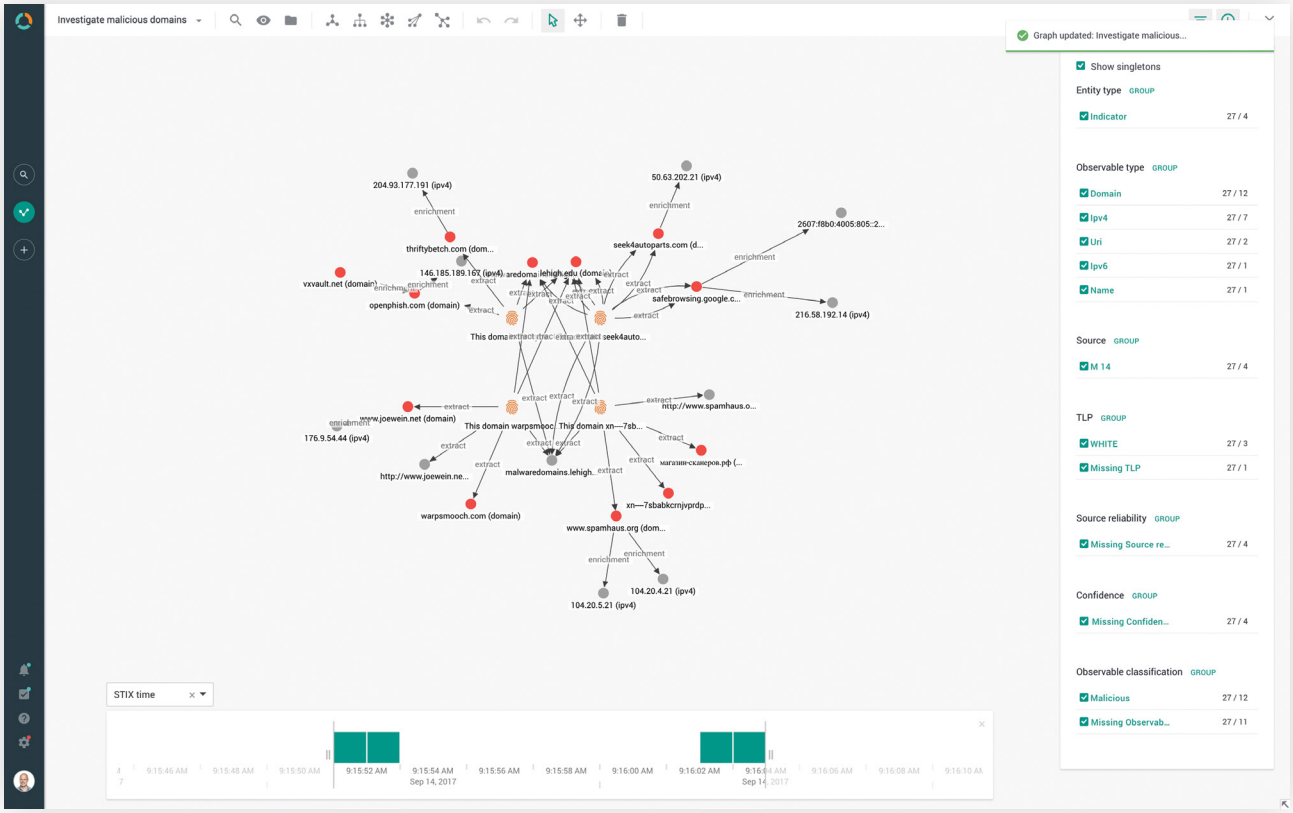
EclecticIQ Platform Screenshots



Dashboard: all your intelligence at a glance



Aggregate, normalize and enrich your intelligence automatically



Perform faster, better investigations with the most advanced graph-capability in the market

Mission Statement

EclecticIQ's mission is to restore balance in the fight against cyber adversaries. EclecticIQ Platform enables operationalization of security information exchange, empowers collaborative analyst workflow, and ensures timely integration of cyber threat intelligence detection, prevention and response capabilities.

Special offer for Threat Intelligence Analysts

Try EclecticIQ Platform. Experience what it brings to your mission.

EclecticIQ allows analysts to collect an expanded range of sources into an advanced workbench. Customizable workflows allow analysts to deliver deeper and smarter insights to front-line employees faster than ever before.

Using EclecticIQ Platform, analysts can improve the quality of their contributions to the organization and to the intelligence community, while bolstering their own skillsets.

About EclecticIQ

EclecticIQ helps organizations to turn cyber threat intelligence into business value through products built for cyber security professionals in threat intelligence, threat hunting, SOC, and Incident Response.

EclecticIQ Platform is the analyst-centric threat intelligence platform based on STIX/TAXII that meets the full spectrum of intelligence needs.

EclecticIQ Fusion Center enables the acquisition of thematic bundles of cyber threat intelligence from leading suppliers with a single contract.

The company won Deloitte's Technology FAST50 Rising Star Award for "Most Disruptive Innovator".

EclecticIQ is headquartered in Amsterdam, The Netherlands.

For more information or to schedule a personal demo, please visit www.eclecticiq.com.