Data Sheet

EclecticIQ Platform

for enterprise

Harnessing the power of threat intelligence - moving from reactive to adaptive with intelligence-led security

Introduction

Addressing ongoing cyber security threats is a challenge for every enterprise. As threats continue to escalate, consumers, insurers and investors are demanding better cyber security protection. This is where Cyber Threat Intelligence (CTI) can make a difference.

Using a Threat Intelligence Platform (TIP), organizations can uncover invaluable insights into identifying and prioritizing the most relevant vulnerabilities and cyber threats.

EclecticIQ Platform is the analyst-centric TIP, optimized for the collection of intelligence data from open sources, commercial suppliers and industry partnerships into a single collaborative analyst workbench. EclecticIQ Platform eliminates the manual and repetitive work involved with processing multiple intelligence feeds. This means analysts can focus on identifying the most critical threats, take timely action, advise the organization on how to respond and collaborate with industry peers.

Whether you're wanting to bootstrap CTI into the organization to improve the effectiveness of your Security Operations Center (SOC) or if you want to use the power of threat intelligence to guide decisions at all levels to minimize business risk, EclecticIQ Platform provides you with the ability to introduce and/or grow intelligence-led security in your organization.

Key Benefits

Analyst-centric: enabling collaboration, analysis and production

EclecticIQ Platform lets analysts work with large amounts of threat intelligence on a day-to-day basis by automating the qualification and discovery processes. Dynamic workspaces drive collaboration by helping analysts automatically sort intelligence around a topic or area of interest with the ability to add queries, graphs, free text and assign tasks. The result is an actionable threat reality knowledge base. Armed with this, you can align your IT security controls and defenses with known threats, dramatically reducing the mean time to remediation.

Delivering actionable intelligence to drive faster response

EclecticIQ Platform is the only TIP enabling analysts to create structured and unstructured intelligence within the platform itself. Reports can be sent via email and/or directly to IT security controls. The links within the unstructured reports let decision makers see the context within EclecticIQ Platform, driving better situational awareness and quicker responses.

Intelligence-led security and business decisions

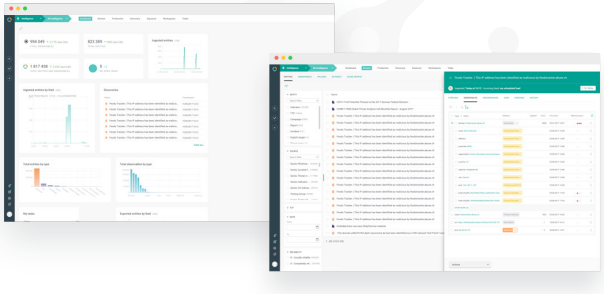
Our solution is unique, in that it allows for workflow and data-types across the entire organization. Threat intelligence from different departments and external sources is unified and enhanced with cases created. This allows the enterprise to introduce intelligence-led security and in turn aids faster and better-informed business decisions.

EclecticIQ

Data Sheet

Product Overview

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



Collect and correlate

- Intelligence data from multiple sources
- Structured STIX-compatible and unstructured entities
- Large diversity of supported data formats: csv, pdf, proprietary and STIX

Analyze and collaborate

- Automated qualification, triage and discovery processes
- Collaborative workspaces with intuitive graphs, search, pivoting tools and tasking
- CTI clipboard to capture data from websites and feed it directly into TIP

Produce and disseminate

- Reports for dissemination to both human and machine consumers
- Daily digests and full intelligence reports
- Only TIP to support sending human-readable reports via email

Enterprise ready

- Horizontally scalable to support enterprises of all sizes
- RHEL, CentOS and Ubuntu operating systems are supported
- Flexible deployment options: single instance to multi-tier on virtual machines or physical hardware
- Available on-premise or as a hosted solution.
- Highly configurable and easily integrates with existing security infrastructure
- Ever-expanding catalog of integrations to different security systems and intelligence sources: SIEM, endpoint solutions, intelligence feeds, data enrichers etc

EclecticIQ