EclecticIQ Platform

Empowering analysts to take back control of their threat reality and drive down mean time to remediation from days to minutes.

Cyber threats have forced governments and enterprises to improve cyber defenses across NCSCs, CERTs, SOCs, IT departments and other functional areas within organizations. Cyber Threat Intelligence (CTI) has transitioned from a nice to have, to a basic necessity for a security portfolio.

Introduction

The stark reality is that cyber-attacks are now commonplace. The adversaries are smart, highly-organized and adept at making changes to side-step attempts to stop them. Security professionals are expected to plan and prepare not only for existing threats but also ones that may emerge in the future. This is a daunting task. After all, it's not feasible or economically viable for governments or enterprises to protect against every single exploit or threat vector. Instead, it's about the smart allocation of resources to strengthen the security posture against the attacks most likely to occur.

By harnessing the power of cyber threat intelligence, governments and enterprises are able to cut across the noise and discern the most relevant threats to them. With a Threat Intelligence Platform (TIP) analysts are able to generate actionable intelligence. Precise and accurate threat intelligence helps drive better informed strategic, tactical and operational decisions, ensuring the most effective remedial action is implemented. The result is that the impact of breaches on the organization is minimized

.

EclecticIQ Platform is the analyst-centric TIP. It ingests 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, allowing analysts to identify 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, compatible with STIX & TAXII, and developed with CTI workflows and tradecraft at its core.

Key Benefits

Increasing the productivity of your analysts by enabling them to do what they love

With EclecticIQ Platform, analysts are aided by a TIP that speeds up their entire workflow. The discovery automation and data enrichment eliminate the repetitive and mundane aspects of the role, such as processing multiple feeds or sorting through Indicators of Compromise (IOCs). Instead, analysts can focus on what they love: delivering unique insights and more effective threat identification.

Delivering actionable intelligence to drive faster response

Threat data is only valuable to the business if it's accurate, timely and contextual. Our extensive data ingestion capability and entity editor ensure that analysts quickly create STIX-compatible actionable intelligence for both human and machine consumption. EclecticIQ Platform is the only TIP that enables analysts to create structured and unstructured intelligence within the platform itself. Reports and data are sent via email and/or directly to IT security controls. The links within the unstructured reports let decision makers see the context in EclecticIQ Platform driving better informed and timely responses.

Aligning security efforts across the reality of your threat landscape

By using EclecticIQ Platform, organizations can determine what attack vectors are most pertinent. Armed with relevant actionable intelligence, organizations can allocate resources where they are most needed and can focus their attention on appropriate courses of action. This use of effective threat intelligence lets an organization achieve more with the allocated budget and resources and safeguards business assets from existing and emerging threats.

Improving the effectiveness of your CTI practice

The intelligence disseminated by a CTI practice lets the organization improve defenses adaptively rather than reactively. Providing dynamic collaborative workspaces, intuitive graphs, search and pivoting tools help analysts decipher large amounts of data to identify relationships, patterns and trends. As more hypotheses are validated, you can respond in a timely manner to intelligence requests within the organization.

Increasing the Return on Investment of CTI

EclecticIQ Platform is an extension of your security team. With its automation and enrichment capabilities, EclecticIQ Platform increases the return on investment by offloading the manual overhead. It frees up analysts to deliver more effective threat identification, increasing their productivity. From an IT perspective, EclecticIQ Platform is highly configurable and easily integrates with your existing security infrastructure. There is an ever-expanding catalog of existing integrations to different security systems: SIEM, endpoint solutions, intrusion detection systems, firewalls etc. What's more, the software development kit (SDK) gives you the power to add bespoke systems as quickly as you need.

Product Overview

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

EclecticIQ Platform efficiently supports threat intelligence analysts to inform stakeholders including SOCs, CERTs, information resources, vulnerability management, IT architects, businesses and organizational leaders.

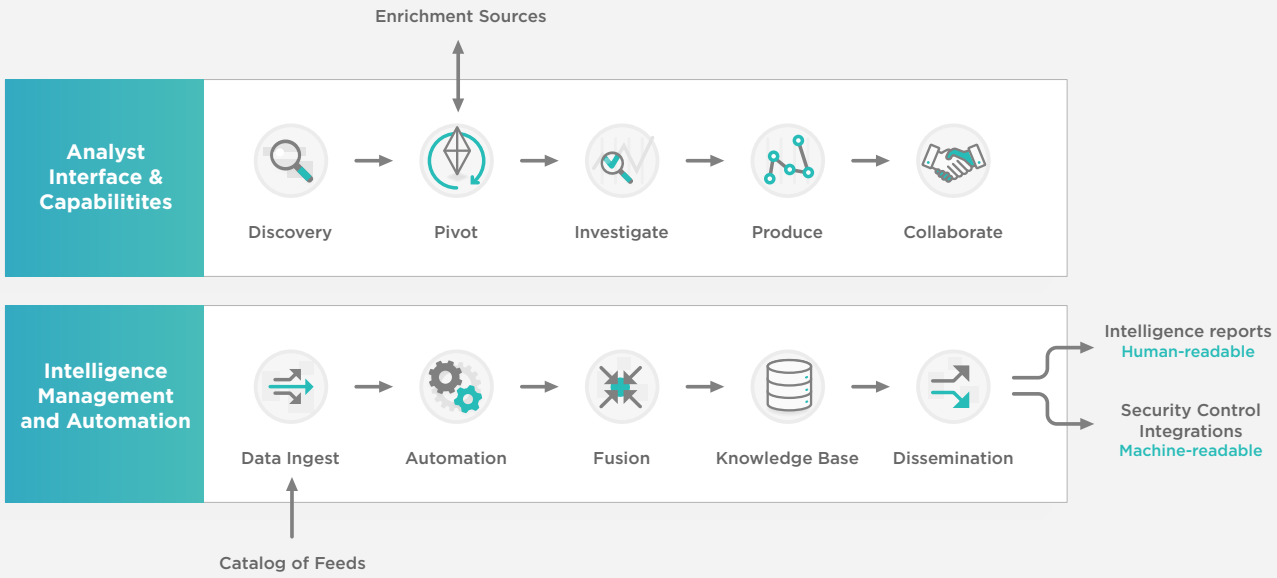

Figure 1: High level overview of EclecticIQ Platform key capabilities

EclecticIQ

Collect and correlate

EclecticIQ Platform collects intelligence data from multiple sources: open source, commercial suppliers, internal sources and industry partnerships. New feed sources are added on a regular basis, ensuring that the very latest information is available. Next to automated ingestion, intelligence can be created inside the platform by using the entity editor, which saves analysts time by allowing them to create structured and unstructured STIX-compatible intelligence without leaving EclecticIQ Platform.

The data ingestion capability of EclecticIQ Platform offers analysts the largest diversity of data formats to work with in the industry. Ingestion supports multiple formats, including pdf, csv, proprietary and STIX. As a result, the threat intelligence generated is of a higher fidelity and is more accurate due to the broad range of sources used. This provides a more exhaustive view of your threat reality and improves anticipation of relevant threats.

With data fusion, the triage process is enriched, providing immediate insight into the connections and relationships within the data. It is powered by de-duplication, extraction of relevant information and use of the rule engine for automated enrichment, tagging, grouping and manipulation. Data fusion removes the labor-intensive part of the process, allowing the analysts to more quickly obtain a comprehensive view of the threat landscape. Meanwhile, automation minimizes the risk of human oversight when dealing with such large quantities of data.

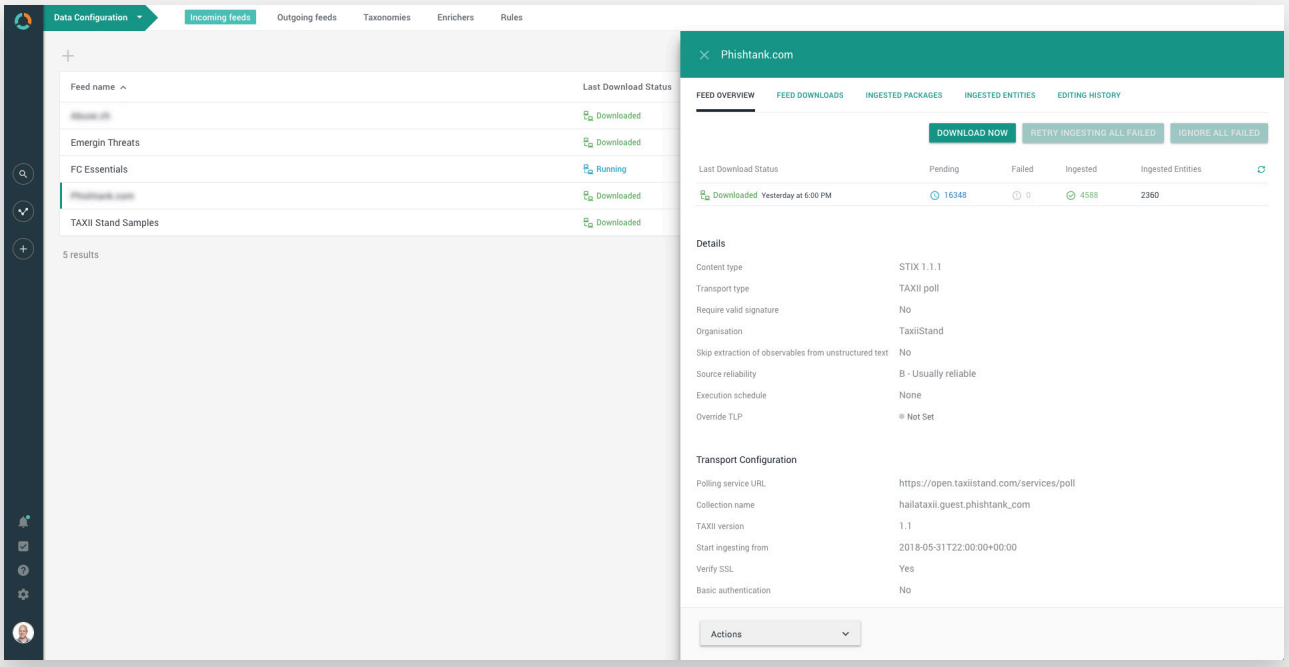

Figure 2: Clear overview of incoming feeds

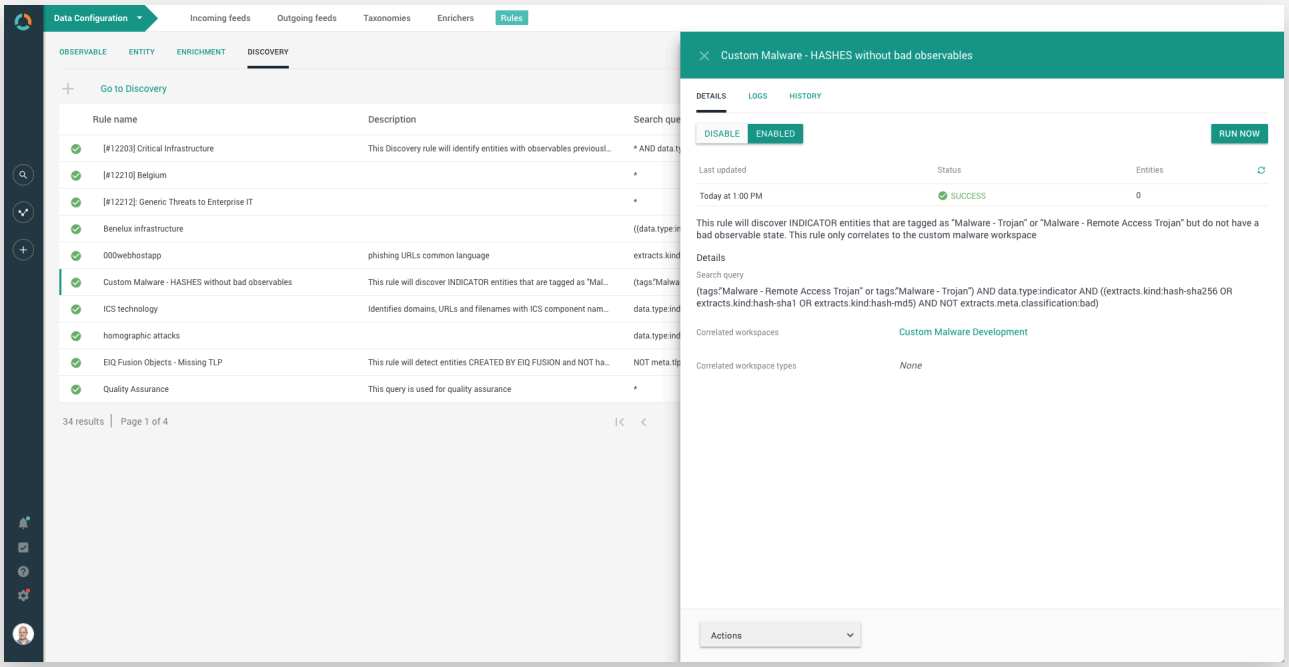

Figure 3: Intuitive rules engine

Analyze and collaborate

EclecticIQ Platform lets analysts deal with large amounts of threat intelligence on a day-to-day basis by automating the qualification, triage and discovery processes. With discovery, for instance, near real-time feeds and alerts can be configured. In addition, EclecticIQ Platform provides the capability for analysts to set tasks within the platform, either for themselves or a colleague to follow up on actions. This introduces efficiencies within the CTI practice by streamlining the process, facilitating collaboration and enabling analysts to cover more ground.

Collaboration is further enhanced by dynamic workspaces that provide a workflow-oriented view of the knowledge base. Dynamic workspaces allow analysts to cluster intelligence based on business process (e.g. intelligence requirements or team design) without organizing data into siloes. Adding data into EclecticIQ Platform has been made simpler with the introduction of the CTI clipboard add-on. This provides analysts with the capability to capture data directly from a website without leaving their browser, giving them an effective way to save and input straight into the platform.

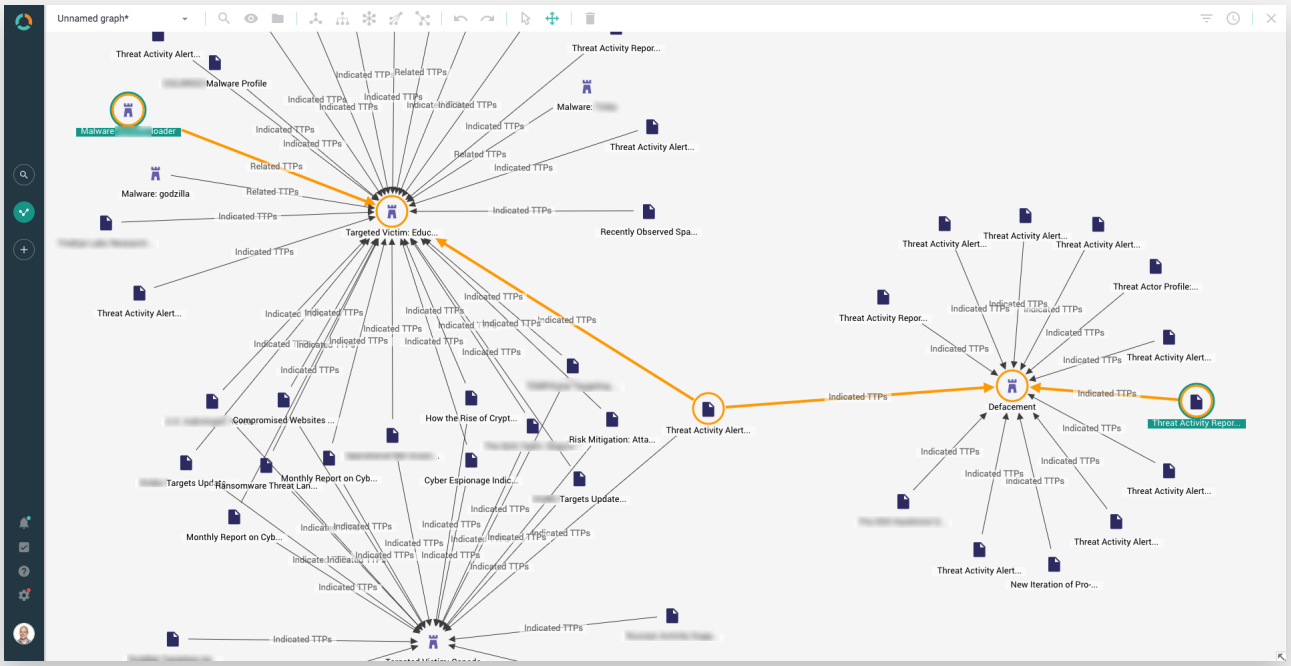

Figure 4: Analyzing relationships is made easier

Produce and disseminate

With EclecticIQ Platform, analysts can produce both human-readable and machine-readable reports which rely on the same data source, ensuring consistency and accuracy. Creating reports within the platform is quick and simple. The workspaces and dynamic datasets mean that analysts no longer need to collect or copy and paste information from different tools or locations. Everything is within the platform, which significantly reduces the time it takes to generate reports.

Reports for machine consumption are delivered automatically to the IT security controls. With the human-readable reports, analysts can supply daily digests as well as full intelligence reports. With EclecticIQ Platform, links can be embedded in the reports which provide the decision maker with access to the context of the intelligence directly within the platform. What's more, EclecticIQ Platform is the only TIP which supports the dissemination of human-readable reports via email, making it easier for the rest of the organization to consume vital threat intelligence.

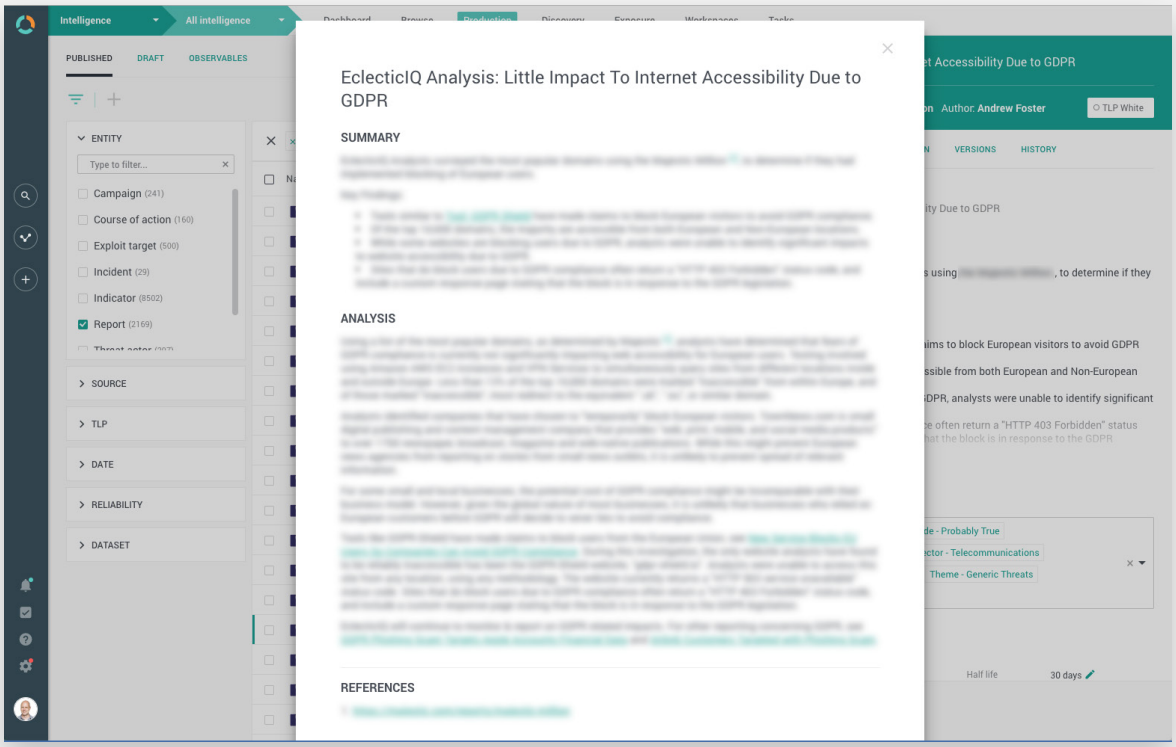

Figure 5: Time saving report generation supporting machine- and human-readable requirements

Enterprise readiness

Whether you're a government with multiple constituents or a growing enterprise, EclecticIQ Platform provides you with flexible and multiple means of deployment from a single instance to multi-tier on virtual machines or physical hardware. It is available on-premise, where various topologies of deployment are an option. Deployment ranges from a single instance to multiple nodes with different levels of access with inter-platform exchange of intelligence. For organizations who prefer a managed solution, there is the option for EclecticIQ to host the platform.

EclecticIQ Platform supports RHEL, CentOS and Ubuntu operating systems, providing your IT administrator with a flexible solution that is easy to integrate into your existing IT infrastructure.

INTELLIGENCE POWERED DEFENSE

www.eclecticiq.com