Intelligent Cyber Threat Response

Cyber security professionals know there are fundamental gaps in most cyber operations centers, one of which is the overwhelming level of effort required to understand cyber threat information. As a result, cyber analysts are rarely allowed to produce their primary work product: actionable intelligence. The operative descriptor is actionable—wholistic intelligence delivered to the right people at the right time to make informed actions to protect their networks. Analyst1 bridges the gap between threat information and actionable intelligence. Analyst1 serves as a platform with a contextualized knowledge base that reciprocally enriches data with various cyber security tools found in enterprise environments. Teams within cyber operations centers are therefore brought together with Analyst1. By sharing a comprehensive view into cyber threat activity, they are together empowered to act.

Cyber Defense: It's Worse Than You Think...

On a monthly basis, analysts spend more than 80% of their time manually researching and understanding cyber threat information. They typically navigate a myriad of cyber threat intelligence sources, copying and pasting the context from these intelligence reports into spreadsheets and then exchanging the content of their analysis through portals or emails. This manual process is duplicative across multiple teams and across all organizations. From sources, to reports, gathering, and reporting, intelligence is overwhelming and, in many cases, not comprehensive nor up to date. As a result, networks are left unprotected from the "known bad".

Simplifying Cyber Security

Inefficient operating procedures coupled with vulnerable networks in an increasingly complex cyber environment will inevitably have an impact on the cost to defend your infrastructure. From

this financial perspective, Analyst1 provides significant cost savings through efficiency gains. Analyst1 automates the collection, correlation, and enrichment of cyber threat information and establishes a shared and trusted knowledge base that provides the context that analysts require. Analyst1 utilizes a vendor-agnostic approach that enables network defenders to integrate their existing tools, automate laborious tasks, and orchestrate cyber operation business processes. Modernizing information sharing, Analyst1 implements machine-to-machine interactions and supports STIX and TAXII data exchange standards. Analyst1 modernizes cyber information sharing to empower cyber analysts, net defenders, vulnerability analysts, and incident responders to take action to effectively detect, understand, and respond to cyber threat activity. Within a few clicks of the mouse anyone can quickly identify actionable intelligence, understand what happened, who the targets are, who the threat actors are, what malware is being used, what vulnerabilities are being exploited, prescribe mitigation actions, validate actions occurred, and share critical information with mission partners. Analyst1 provides analysts with customizable dashboards that provide insights into trends and changes in adversarial activity over time.

Empowering Analysts to Take Effective Action

Analyst1 provides a comprehensive threat understanding for the entire security team to include intelligence, operations, malware, and vulnerability analysts as well as sensor owners.

- **Intelligence analysts** gain the ability to quickly access automated extracted, correlated, and aggregated intelligence allowing them to conduct analysis and capture it in one location.
- The analysis and actionable information that is captured, allows **operations analysts** the trusted insight and context surrounding cyber threat activity to conduct intelligence-based network hunting and prioritized operations for effective command and control.
- **Malware analysts** have access to a correlated and enriched malware family, negating the need to navigate to multiple sites to gain an understanding of all the actionable information to take action against malware.
- Similarly, **vulnerability analysts** are provided with pre-prioritized CVE listing to all known exploiting actors and malware, via trusted and verified threat intelligence to filter the scope of vulnerabilities. Continuous, automated updates to threat posture with integrated data analysis from other roles and teams allows for a threat driven approach for calculating risk.
- Utilizing a streamlined workflow capability in Analyst1 to create signatures and counter-measures, **sensor owners** have the ability to task and maintain configuration management of all connected sensors.
- Additionally, **any user or analyst** utilizing Analyst1 can rapidly identify what signature and/or counter-measure is deployed to any sensor, with the context and insight back to the original piece of evidence as to why that mitigation was created.

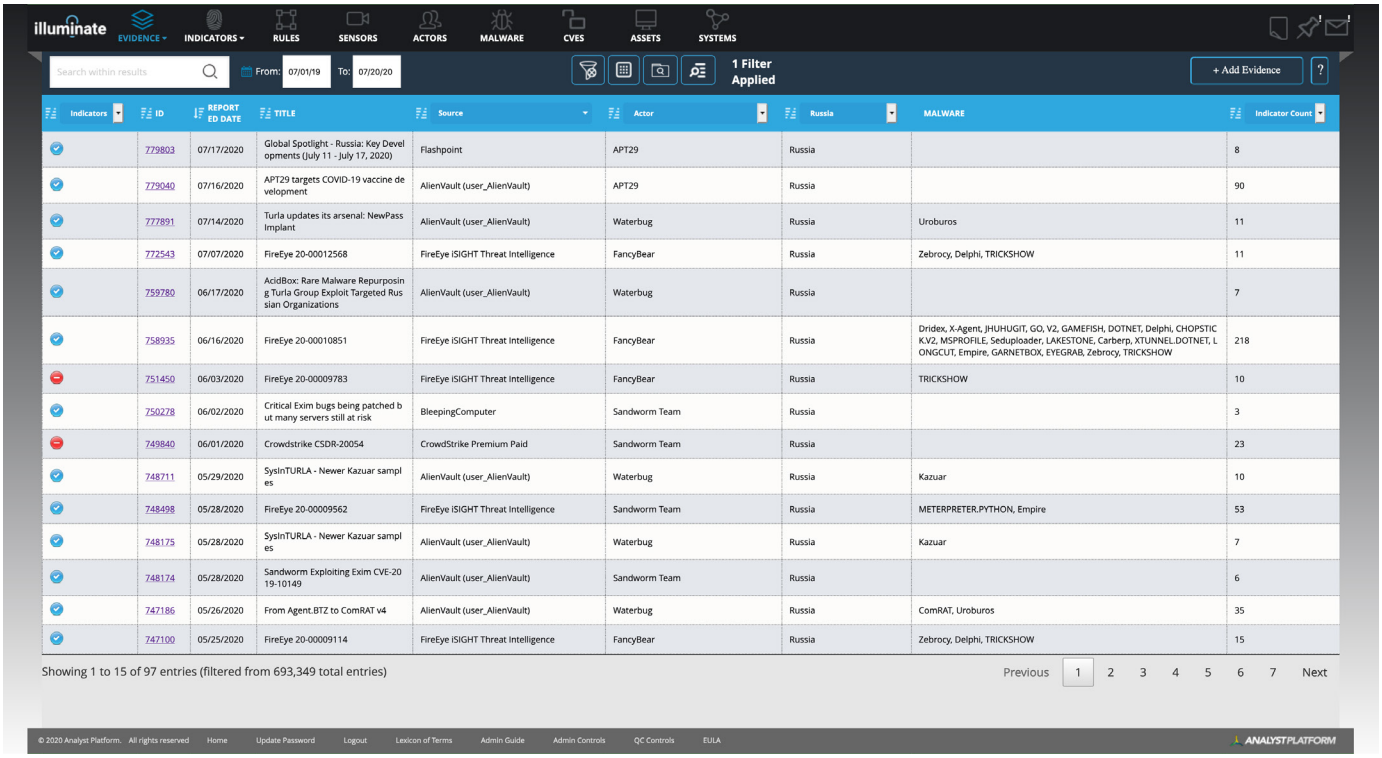

Figure 1. Reporting is sorted and prioritized

Analyst1 automates the aggregation, extraction, correlation and enrichment of actionable cyber threat information to establish a shared knowledge base of correlated vulnerabilities, threats, Indicators of Compromise (IOCs), and malware to provide the context that analysts require. For example, Analyst1 auto-ingests hundreds of cyber threat intelligence reporting sources to include: free commercial and open-source sources (e.g., AlienVault, Securelist, PhishMe), paid commercial reporting sources (e.g., FireEye iSight Threat Intelligence, CrowdStrike), and classified reporting sources (e.g., Pulse, IADaily, CIAwire). Regarding classified reporting sources, Analyst1 has the ability to extract classified information in paragraph and portion marked reporting and assign the specific classification to the actionable information. The knowledge base is established through automated collection and processing of the information produced by the trusted sources.

Analyst1 provides the ability to ingest both structured and unstructured data

Analyst1 provides the ability to ingest both structured and unstructured data formats without requiring any additional costs beyond standard licensing. New data can be added to Analyst1 through automatic consumption, API integrations, published to the Analyst1 TAXII endpoint, or uploaded through the user interface., Analysts can configure Analyst1 to automatically consume structured and unstructured content from any source, as well as enable analysts to upload content in multiple formats, such as spreadsheets, slide presentations, images, PCAP samples, text documents, XML, PDF and others.

Analyst1 auto-correlates all extracted information across its database holdings establishing a shared and trusted knowledgebase. This auto-extraction and auto-correlation allows analysts to discover other correlated reporting that would otherwise be tedious and time consuming to identify interconnected actionable information.

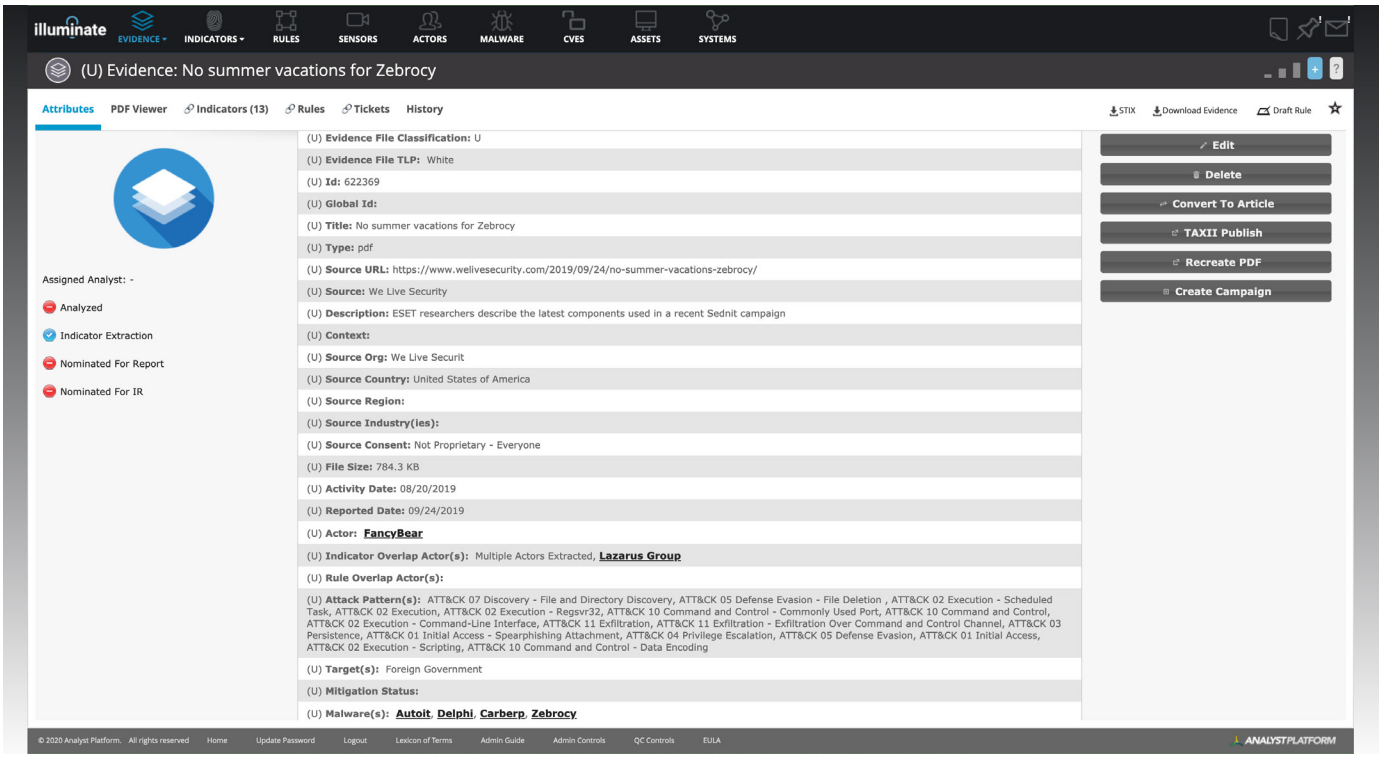

Figure 2. Actionable information auto-extracted

Analyst1's natural language processing engine automates the extraction of actionable and contextual information from the source data, which includes all indicators, cyber threat actors, employed malware families, exploited/targeted vulnerabilities, attack patterns, target/victim information, activity dates, and existing countermeasures or signatures.

Analyst1 has a comprehensive means of extracting content from any text-based data source, discovering Indicators of Compromise (IOCs), related metadata to IOCs (activity dates, ports, protocols, file names, etc.), and the relevant threat intelligence in Actors, Malware, CVEs, and Targets. This extraction engine is tuned from experienced analysts over 5+ years of open source threat intelligence assessment and can be further tuned by operational analysts within the Analyst1 web interface. IOCs such as domains, IP addresses, http requests, mutexes, email addresses, files, hashes, and strings are all traceable back to each artifact they originated from and then auto-enriched to obtain additional detail from external sources such as Virus Total and Domain Tools.

Analysts no longer need to manually correlate IOCs with other information or perform countless search's attempting to discover the presence of IOCs on their network because Analyst1 provides a repository of IOCs and automates hunting and tracking the IOCs detected on the network.

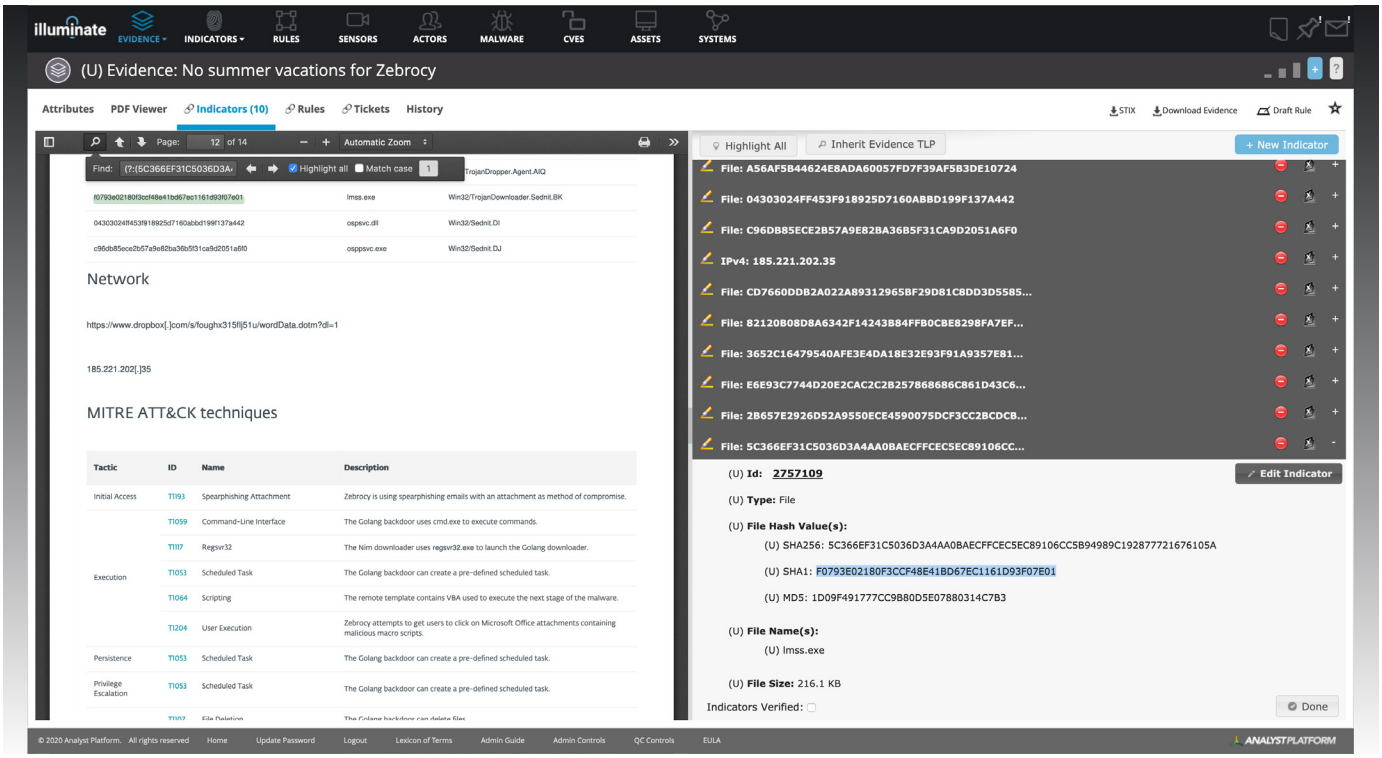

Figure 3a. Indicators of compromise auto-extracted

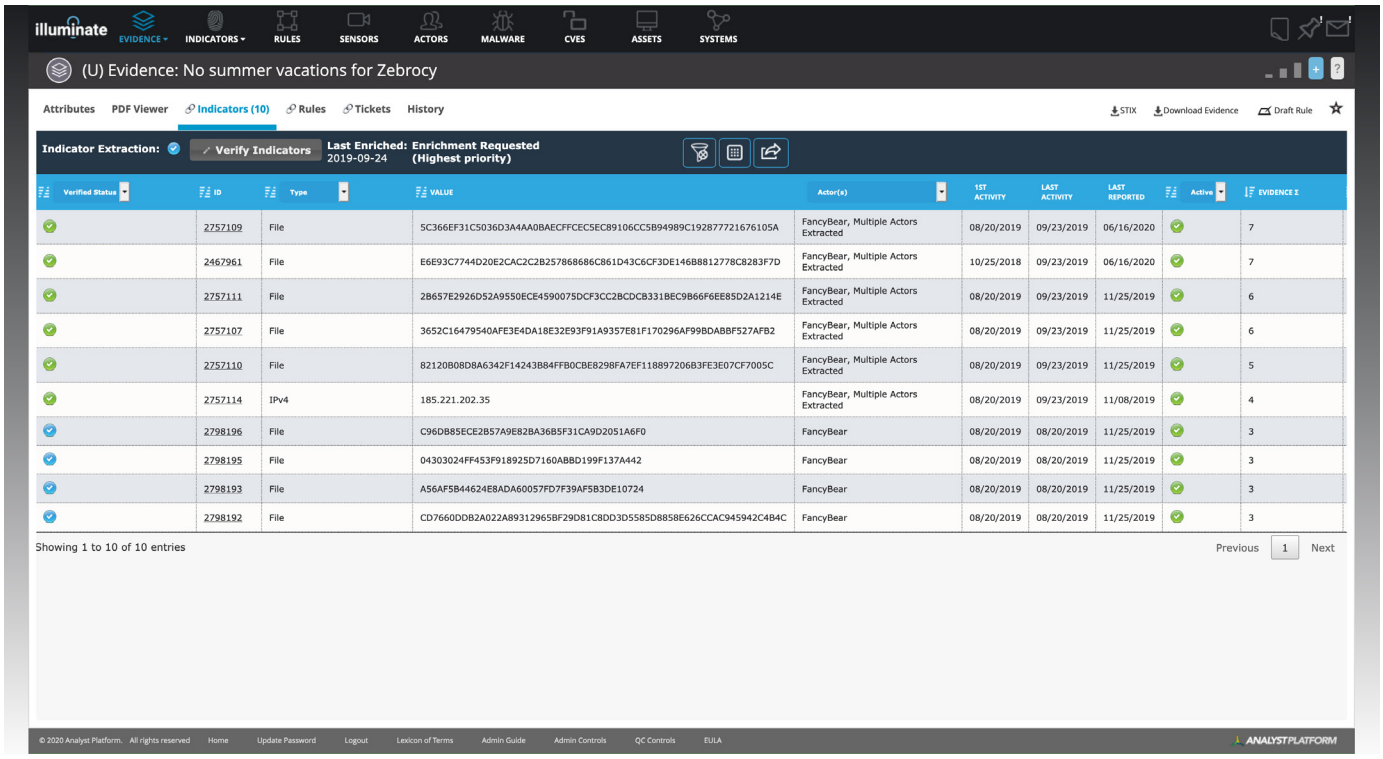

Figure 3b. Indicators of compromise auto-extracted

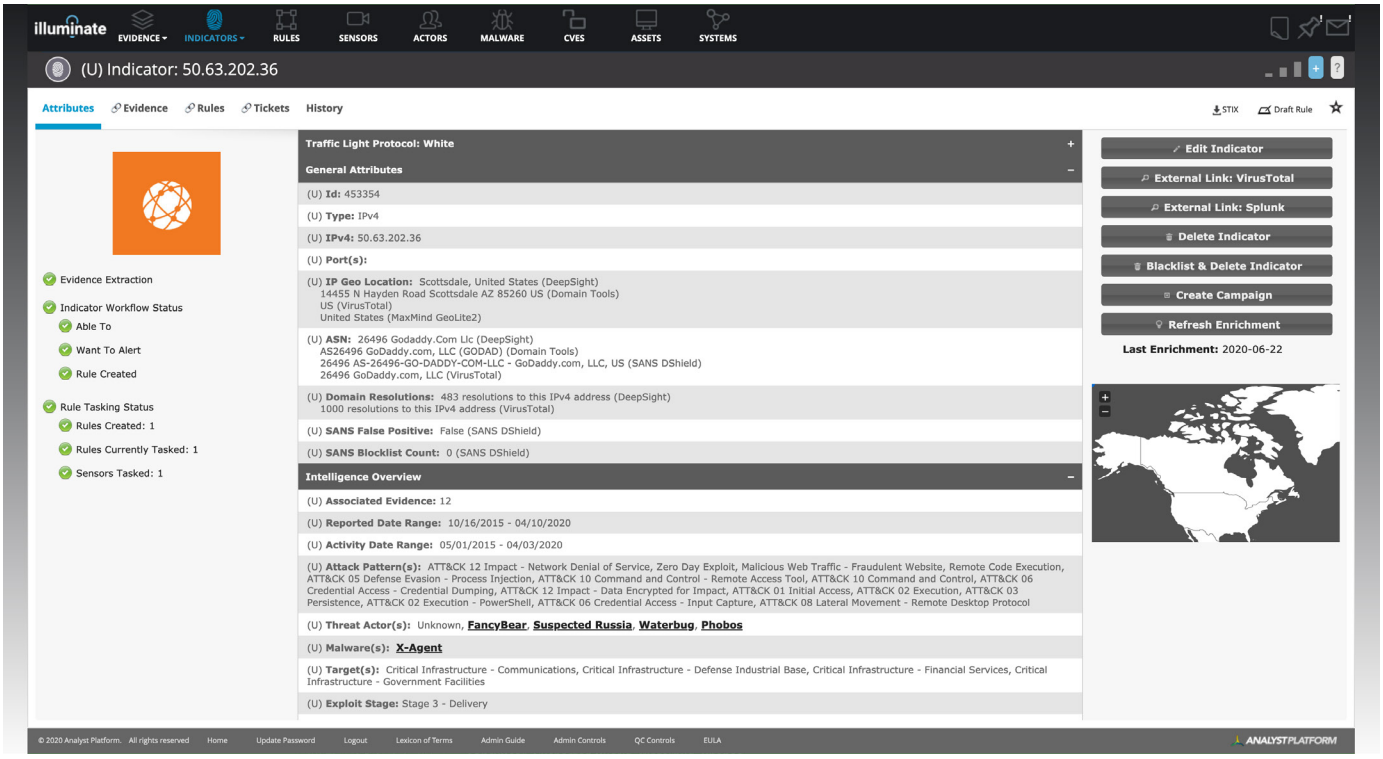

Figure 4. IOCs linked to additional context

Using the above process, Analyst1 can provide context to classified reporting to downgrade actionable information to the lowest classification to enable analysts, net defenders, and incident responders to take action at the lowest levels possible.

Any user of Analyst1 can create and quickly identify what rule and/or signature with context back to the original evidence file and the indicator it detects and/or protects the network. Analyst1's rule management system enables any format of signature and countermeasure rules to be added, stored, tested, and tasked. Within Analyst1 analysts can upload samples of PCAP to run through the test rule to reduce the number of false positives prior to deploying the signature, which eliminates the need for analysts to attempt to create simulated network traffic to test the signature. Once within Analyst1, rules and metadata about rules are searchable and viewable by any authorized user. Rule test results and rule versions are tracked over time and visible through a rule history timeline. When viewing a rule within Analyst1, analysts can identify what sensors, if any, the rule is running on, and when the last rule change was made.

As with rule creation and discovery, any user in Analyst1 can quickly identify what each sensors' configuration is and the rules that are currently tasked with context back to the original source. Sensor owners can easily update the security policies through exports of the security configuration. Analyst1 integrates with McAfee ePO HIPS, Palo Alto, Juniper, and Sourcefire sensors to identify the devices and systems with specific vulnerable configurations (vendor/product/version) that are associated with cyber threat actors and malware.

Deploying Analyst1 to Your Environment

Analyst1 is a web-based application that consists of a web server and a database server that can be hosted on-premise, in the cloud, or in hybrid cloud-premise environments. Analyst1 is currently in use across customers who have each deployed Analyst1 into a diverse set of environments which include running on-premise in virtual machines, on bare metal, in commercial cloud, government-based cloud, and hybrid environments. For instance, The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) hosts Analyst1 within their on-premise environment on their Mission Operational Environment (MOE) network. Organizations within the DOD host Analyst1 within the Secret Internet Protocol Router Network (SIPRNet) MilCloud cloud-based environment. Organizations within the Intelligence Community employ a hybrid approach where Analyst1 resides in a hosted unclassified commercial cloud, then sends threat, IOCs, and context information up to the on-premise network where Analyst1 runs on physical servers on the Top Secret Joint Worldwide Intelligence Communications System (JWICS) network.

Analyst1 Integrations in Your Environment

Analyst1 natively supports the ingestion of threat intelligence via API connections from numerous free sources, paid sources and classified sources of threat intelligence without requiring any additional costs beyond standard licensing. In addition to the API, Analyst1 is a TAXII endpoint that can consume published content from one or more sources of STIX sources. And for the sources of threat intelligence that do not have an API or TAXII endpoint, such as internal SharePoint sites, or external sources like the Dell SecureWorks and PaloAlto Blogs, Analyst1 can consume the available threat intelligence from an RSS feed.

Analyst1 natively supports the ingestion of threat intelligence via API connections.

The natural language processing engine within Analyst1 identifies and extracts the actionable information from threat intelligence independent of any source formatting. Analyst1 comes pre-configured to consume information from hundreds of different sources of information, and customers can easily add new sources of information within minutes without requiring any support. Further, Analyst1's REST API allows customers to push threat intelligence reports from their internal, proprietary systems.

Analyst1 provides indicators to SIEMs via the native Analyst1 API and the SIEMs' APIs, Common Event Format (CEF), and/or defined Common Information Model (CIM). Analysts can specify how often IOCs and the enriched contextual information flow into the SIEM. If any activity is identified within a SIEM, the number of hit detections is shared with Analyst1 via machine-to-machine communication. Utilizing this communication method, analysts no longer have to manually hunt for each IOC attempting to discover network activity. Without having to run searches, analysts can quickly identify, filter, and prioritize based on contextual

threat, malware, and vulnerability activity that has been pre-identified to be present within their network.

Analyst1 categorizes data about threat actors, targets, victims, assets and systems with amplifying information such as location, type and industry. Analyst1 natively identifies nation state threats and other hacktivist groups (actors) by their multiple known names and country of origin; it further auto-correlates the malware, CVEs, indicators, and other details from threat intelligence to the actor so that the comprehensive view of the threat is immediately known.

This same model is applied to victim discovery. Values within threat intelligence which identify victims by named groups (such as industry or government agency) are auto-extracted also as targets within Analyst1 and through the threat intelligence auto-associated to the known threats. The same auto-extraction and auto-association model applies to customer domains, machines, and infrastructure as Analyst1 identifies customer assets (a unique on- network device or identity) and systems (a group of assets to serve a function) contained within threat information.

In this automated approach, seeded by the multi-year archive of data, it takes minimal customization at each Analyst1 instance so that threat intelligence is uniquely processed for that customer's active knowledge and defense needs. Each automatically extracted value self-discovers related metadata through the common threat intelligence in addition to the in-built analyst specified values of country of origin, malware category, exploit stage, attack patterns, owning victim organizations, asset type and purpose, system names, and other values.

To learn more about Analyst1, to calculate your ROI, or to request a demo, please contact us at info@analyst1.com.

(888) 4-ANLYST | info@analyst1.com
11921 Freedom Dr #550, Reston, VA 20190