ANOMALI LENS™

Instant Insights into Action for Cybersecurity Analysts

FACING THE THREAT DATA TSUNAMI

Attackers inevitably set the agenda for cybersecurity analysts. Yet CISOs want answers and actions from those same analysts—and they want them now. Analysts are constantly racing against the clock to understand attacks and how to prevent threats from harming their networks.

This process often involves researching, evaluating, and analyzing tactics, techniques, and procedures (TTPs) to produce reports for the C-suite. TTPs often come in the form of unstructured data like research papers, blogs, and incident response (IR) reports. TTPs are much harder to fake than indicators of compromise (IoCs) like IP addresses but requires more work from the analysts. Working with TTP requires switching between multiple public and internal content locations for research and reporting. This process is tedious and involves error-prone manual copying and pasting of data.

Speed and efficiency are key when even the best research and reports are of limited use if they can't be presented to leadership in a timely and accurate manner that is relevant to the business. Amid the mounting costs of data breaches, executives insist upon a big-picture view of the cyber threat landscape, risk-based assessments, and actionable intelligence nearly instantly.

SUPERCHARGING THREAT RESEARCH AND REPORTING

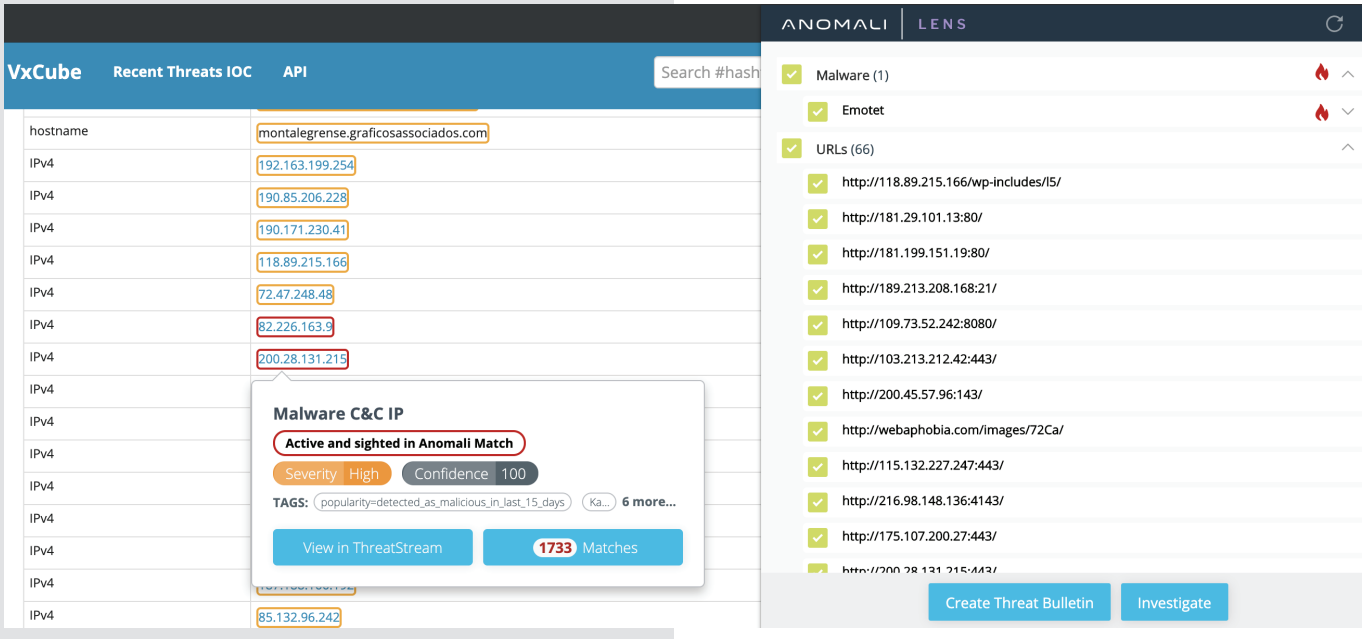
Anomali Lens enables analysts to work and stay in any single web-content location for faster research and to communicate cyber risk better to the executive leadership. This is especially critical in high-pressure environments such as widespread cyber attacks and high-profile data breaches.

Anomali Lens scans and converts unstructured data, such as news stories, social media, research papers, blogs, paste sites, coding repositories, and internal content sources like SIEM user interfaces, into actionable intelligence. Anomali Lens leverages natural language programming (NLP) that takes unstructured data and identifies threat actors, malware families, and attack techniques as they relate to threat intelligence.

Security Operations teams, Threat Intelligence teams, and Managed Security Service Providers (MSSPs) can execute the entire research and reporting process from any single web-content resource.

By helping streamline the entire process of researching and reporting cyber threats, Anomali Lens gives analysts the ability to communicate to management quickly and effectively, clearly demonstrating the value of the organization's cyber defense and highlighting the analysts' essential contributions.

Without a tool like Anomali Lens, an analyst may require hours—or even days—to provide an executive summary with a clear analysis and risk assessment for the organization.



CASE STUDY: ENABLING CISOS TO RESPOND TO CYBERATTACKS

BUSINESS CHALLENGE:

Tina, a threat intelligence analyst, receives a website address for a security vendor blog from the CISO about a new attack. The CISO asks if their organization currently has (or has had) any activity associated with the threat actors, Indicators of Compromise (IOCs) or methods associated with it. The challenge with questions like these is that most tools are not designed to assist in this kind of historical analysis. In addition, the research involves working with TTPs, which is tedious and involves error-prone manual copying and pasting of data.

SOLUTION:

Tina navigates to the security vendor's blog site and uses Anomali Lens to scan the web page. Anomali Lens immediately highlights the presence of the threat in the organization by leveraging the Anomali[1] detection capability. In this case, Anomali[1] draws on over a year's worth of an organization's cybersecurity event logs to uncover evidence of compromise utilizing Anomali's vast database[1] of high fidelity threat indicators.

Tina then pivots into Anomali to investigate and enrich the observable. The analyst completes the investigation and immediately starts the creation of an incident report to inform response and remediation efforts, all starting from within the blog post they first received from the CISO. Detailed information starts to flow immediately to the CISO about the organization's status with this breach.

CUSTOMER BENEFIT:

Tina, with a single click, can confirm whether or not their organization is being attacked and provide an assessment on who has attacked them and whether the attacks are successful. Tina can pinpoint malicious activity caused by known threats in a matter of seconds instead of hours or days.

CASE STUDY: INSTANT THREAT RESEARCH

BUSINESS CHALLENGE:

As part of the daily work routine, a threat intelligence analyst works with multiple external and internal content resources for research. The analyst switches between multiple locations and often has to copy and paste raw data and information from one location to another to contextualize it. The analyst may require hours—or even days—to process and analyze the tactical indicators related to available finished intelligence. For example, the analyst reads about APT28, Fancy Bear, and Sofacy in multiple articles only to find out that these terms are used interchangeably to describe the same threat group after spending time researching each individually.

SOLUTION:

Anomali Lens draws upon the power of Anomali[2] to instantly highlight and consolidate threat intel at the source of content. Anomali[2] links multiple tactical indicators to finished intelligence products, for example, IP addresses of threat actors that are associated with APT28, Fancy Bear and Sofacy, which are all one and the same. Anomali Lens uses natural language processing capabilities to provide context that ensures the information provided is security-related. For instance, a search for Fancy Bear will result in intelligence related to the threat group and not to a circus bear or social media posting of a bear in a dress.

CUSTOMER BENEFIT:

The analyst now works directly from the content source for research, instead of clicking, copying, and pasting various content sources. The analyst will spend minutes instead of hours—or even days—to research and correlate the tactical indicators to related finished intelligence.

[1] Anomali Match functionality
[2] Anomali ThreatStream functionality

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI®