ANOMALI LENS™

Empowering Executives to Manage Cyber Risk

KEEPING A CONSISTENT SECURITY POSTURE AMIDST LABOR SHORTAGE

Executives and CISOs often struggle to hire qualified security personnel to maintain a proper and consistent security posture. But even success in meeting those staffing goals isn't enough. Data feeds must be translated into boardroom-ready presentations—an often complex and time-consuming process in itself.

As a result, CISOs often try to access analyst tools directly just to stay informed. However, most cyber tools are not designed to directly alert CISOs that their organization is at risk of being victimized by the threats appearing in online news sources on a daily basis.

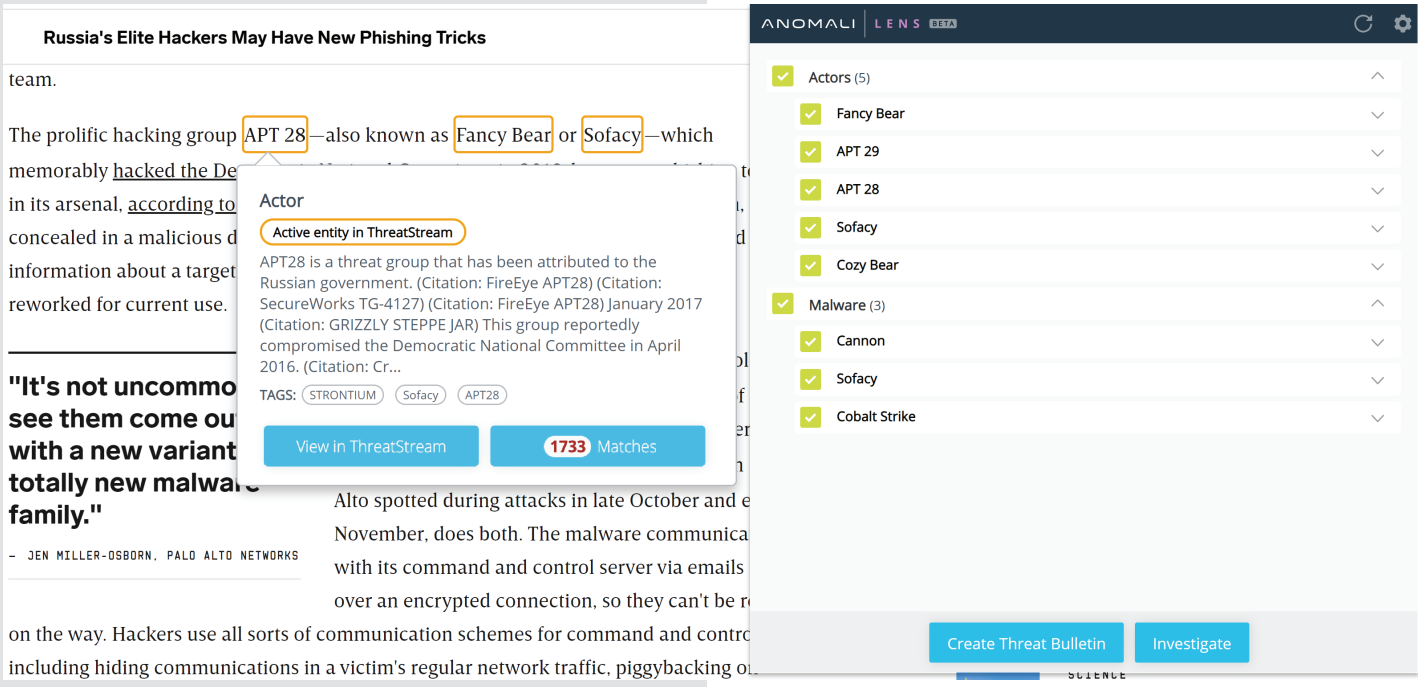
That can lead to frustration in the C-suite and make it more difficult for leaders to respond when the next wave of cyberattacks comes—be it a ransomware outbreak, a denial of services onslaught or a data breach at a similar enterprise. If the cyber analysts can't provide prompt and precise intelligence products at critical junctures, they'll be unable to achieve a central goal of their job: providing leadership with the ability to make intelligence-driven decisions about cyber threats.

SUPERCHARGING ANALYSTS AND CISOS

Anomali Lens will raise the level of every security analyst to that of an experienced veteran. Anomali Lens—part of the Anomali Altitude platform— streamlines the entire process of researching and reporting cyber threats. Anomali Lens amplifies the productivity of even junior frontline Security Operations Center staff, enabling them to produce intelligence products with the quality of seasoned cyber professionals.

Anomali Lens also puts the power directly into the hands of the CISO. With a Lens-enabled Web browser, CISOs can determine the relevance of online cyberattack reports, by leveraging Anomali detection capabilities. Anomali[1] searches an organization's historic cyber security event logs to uncover evidence of compromise by comparing them against Anomali's vast database[1] of high fidelity threat indicators. Lens gives CISOs a direct look at the relevant data with a single click.

What's more, Anomali[2] enriches threat data, thereby speeding analyst investigations, incident response and reporting. CISOs stay in the thick of the action by viewing the threat to their organization in the context of online reports of the attack.



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

CASE STUDY: CYBERSECURITY LABOR SHORTAGE

BUSINESS CHALLENGE:

Charles, a CISO has not been able to fill multiple security analyst positions due to the tight labor market. There's a low probability of finding experienced analysts who understand both the day-to-day cyber defender tasks —researching, evaluating and analyzing tactics, techniques, and procedures (TTPs)—and delivering accurate, usable information for the C-suite.

SOLUTION:

Instead of hiring hard to find skilled analysts, Charles enlists other analysts within the organization to help. Charles provides Anomali Lens to these new security analysts to streamline the analytic process of delivering the type of high-level intelligence products that management expects.

With Anomali Lens, any analyst can now navigate to the security blog site and scan the web page. Anomali Lens immediately highlights the presence of the threat in the organization by leveraging Anomali[3] threat detection capability. Analysts also leverage Anomali[4] to investigate and enrich data with context to produce actionable and relevant intelligence to secure the organization.

CUSTOMER BENEFIT:

Charles restores the security posture of the organization by using tools to enhance team productivity. Every analyst can now pinpoint malicious activity caused by known threats in a matter of seconds instead of hours or days; while also investigating emerging threats to determine relevance to your business.

[3] Anomali Match functionality
[4] Anomali ThreatStream functionality
[5] Anomali Match functionality

CASE STUDY: INSTANT EXECUTIVE ACCESS TO THREAT AND BREACH DATA

BUSINESS CHALLENGE:

An industry peer in the financial sector just confirmed a breach of its mission-critical database. Board members, regulators and customers want to know: Is our own bank impacted? If so, how? What steps are needed for remediation? How long will it take? Can we be sure it won't happen again? The CEO asks Charles, the CISO, for an evaluation of the threat data—in real time, in clear language. Meanwhile, IT executives need a more technical analysis to determine their next steps in the hours and days ahead.

SOLUTION:

Anomali Lens enables Charles to immediately determine that a threat actor is present in the environment.[5] Rather than wait for an analyst to report this breach, Charles initiates the investigation with a simple point and click so his team can start responding and remediating the breach. The team quickly get the perspective they need about the attack implications, accessing the SIEM tool that they're already accustomed to using.

CUSTOMER BENEFIT:

Charles takes immediate action and the CEO confidently passes on timely, relevant, and accurate information to stakeholders while cybersecurity teams shore up their defenses.

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

ANOMALI®