FINDING THE RELEVANT IOCS AMONG MILLIONS AND TAKING ACTION

With Indicators of Compromise (IoCs) increasing exponentially year after year, security operations teams are inevitably overwhelmed. Even leading security tools with powerful automation can reliably ingest only a fraction of that data.

Without the proper tools to handle the massive volume of information, alerts are often set aside to undergo later analysis—or simply ignored. Hours, days—or more—may pass before security operations teams determine whether those threats are relevant and potentially present in the environment. At the same time, management—from the CISO to other C-suite leaders—are following key developments in the media and seeking answers from security teams about whether an action is required.

That's why the Anomali Altitude platform enables organizations to instantly identify what matters most to them, and empower executives to quickly distill that data into actionable intelligence. The Anomali Altitude platform consists of the following three products.

- **Anomali ThreatStream** improves efficiency when handling large volume and/or multiple threat intelligence feeds with full integration with top cybersecurity tools.

- **Anomali Match** accelerates forensics activities with a powerful engine to compare that threat data with information throughout your environment—not just today, but in previous periods to see whether a newly discovered threat has already been present.

- **Anomali Lens** puts threat intelligence literally into the hands of senior leadership and analysts, with monitoring of cyber threats in news and social media feeds and an innovative, easy-to-use color-coded indicator of whether that threat is relevant to—or already present within—the organization's internal networks.
THREATSTREAM: ENHANCING SECOPS BY AUTOMATING THREAT INTELLIGENCE

Alarms sound off when someone breaks in—a control that no organization can do without. But in cybersecurity, detective controls, while essential, can come far too late to protect systems and data. What’s needed is threat intelligence—information about known malicious actors likely to attempt a break-in, or who might have already breached the perimeter.

Anomali ThreatStream provides organizations with access to the most reliable sources of threat intelligence—and then closes the gap between analysis and taking action. That’s because ThreatStream is built to work with key cyber defense tools: intrusion detection systems/intrusion protection systems (IDS/IPS), Next-Generation Firewalls (NGFW) and Security Incident and Event Management (SIEM) platforms. Information about threat actors can quickly be ingested by those tools to strengthen defenses against known threat actors even before they take aim at an organization.

With ThreatStream, organizations can accumulate many different sources of intelligence without creating more work for the threat intel team. ThreatStream automates the core functions of a dedicated team: aggregating threat intel stories, de-duplicating data, curating information and invoking machine learning to remove false positives. All this reduces the signal-to-noise ratio. The results are thoroughly vetted—and far more useful than free threat intelligence feeds off the Web.

The capabilities of ThreatStream make it possible for security operations teams to get the benefits of a dedicated threat intelligence practice without having to augment personnel. What’s more, ThreatStream information sharing capability is similar to your neighborhood watch program. It allows organizations to share information with peers and continuously evolve best practices in responding to threats and denying attackers the element of surprise.
MATCH: USING THREAT INTELLIGENCE FOR IMMEDIATE INCIDENT RESPONSE

With nearly a billion active IOCs, security operations teams need the ability to parse and analyze that data to bolster cyber defense. Yet the tools that can consume those IOCs—can handle a comparatively tiny amount—thousands for a leading next-generation firewall, and hundreds of thousands for a SIEM. Organizations find themselves trying to reconcile two imperatives—tapping the threat intelligence from leading private and public feeds and ISACs, but sifting through them effectively to tune SIEMs and firewalls for what is most relevant.

*Anomali Match empowers security operations teams* to make use of all of that vast threat intelligence by comparing it to what is most relevant to—and even present within—their IT environment. A zero-day exploit may be new to defenders, but it may have been active in an organization’s environment for weeks, days or even years.

A SIEM may provide some context for timely incident response. But because of cost considerations, SIEMs are typically configured to retain log data for no more than six months—and most for only 90 days or less.

By contrast, Match can provide much longer context—for example, five years—on the day it is deployed. That information builds each week, allowing your security operations team to respond to changes in threats and threat actor profiles.

Match’s automation capabilities allow that information to be brought into play immediately. Rather than being overwhelmed by the upswing in threat intelligence data, security operations teams can use Match to identify and act upon what is most relevant.
LENS: ZEROING IN ON ZERO-DAYS WITH COLOR-CODED CONTEXT

High-profile data breaches and ransomware attacks keep threat intelligence and security operations teams working hard to keep up. Meanwhile, CISOs and other executives are expected by their boards and other stakeholders to take responsibility for their organization’s response. But the time lag between real-time defense and management-level reporting can lead to costly delays in deciding upon the appropriate response.

Anomali Lens closes that gap by providing critical information and context directly in the hands of leaders and analysts. Lens follows decision-makers and analysts as Lens read through news feeds about cyber threats of all kinds. Lens provides executives and analysts with a real-time, color-coded notice of just what is relevant.

A red alert informs the reader that the threat is active—right now—within the organization’s network. A click takes the viewer directly to a timeline of the attack via Anomali Match.

An orange alert signifies an active campaign, based on input from ThreatStream threat intelligence feeds.

A yellow alert indicates a threat that was active in the past but has not been seen in 30 days or more in ThreatStream.

A blue alert indicates a possible zero-day—a threat that’s being seen for the first time in the cyber defense community but is not yet present in threat intelligence feeds.

With Lens, managers are better equipped to engage with security operations teams and their industry peers to decide upon incident response, making use of state-of-the-art threat intelligence instantly.