REPORT REPRINT

Anomali puts a new lens on threat intelligence at Detect '19

OCTOBER 15 2019

By Scott Crawford

With cyber threat intelligence becoming increasingly central to a wide range of security initiatives – as well as to vendors across the market – Anomali re-brands its key products and introduces a new offering for correlating threat intelligence with web content.

451 Research®

Introduction

Cyber threat intelligence (CTI) has long been a largely human-driven affair, representing the investment of expertise in recognizing and responding to the actions of intelligent adversaries. But that emphasis on the uniquely human aspects of cybersecurity doesn't mean that CTI can't benefit from advances in technology. At Detect '19, its annual event for threat intelligence analysts, customers and partners, Anomali, a provider of technologies that help organizations realize the benefits of CTI, highlighted how its efforts helps businesses make the most of precious cybersecurity expertise.

451 TAKE

If there is one trend above others that has characterized the information security (infosec) market in recent years, it's a seemingly unending thirst for information. It's not raw data that security organizations need; they are often overwhelmed with volume and can ill afford putting precious expertise on problems that technology can solve. Turning insight into action is key to driving security response and, increasingly, supporting strategic decisions. Modern analytics at cloud scale have been a primary enabler for meeting this demand across the infosec market, while the application (and, sometimes, abuse) of concepts such as machine learning have become pervasive.

Participants in the world of CTI have played a central role in these trends. Among these, Anomali has maintained a solid footing, and at Detect '19, it introduced new innovations to further the actionability of threat intelligence, including Anomali Lens, which harnesses natural language processing (NLP) to correlate threat intelligence with web content. As the sheer scope of the security industry's integration of actionable data expands, however, boundaries in the CTI market are blurring. Anomali has an advantage in both well-established partnerships and a solid customer base in a primary area of focus for putting CTI to work. Its opportunity – as well as its challenge – is to maintain its distinctions if it is to navigate the growing penetration of both CTI and analytics across the infosec market.

Context

Detect '19 is Anomali's fourth annual user conference. Its setting in the greater Washington DC area puts it near a center of gravity for CTI, attracting a number of noteworthy attendees as well as industry luminaries. Speakers included Admiral Michael S. Rogers, former NSA director and head of US Cyber Command, and journalist Joseph Menn, author of the definitive story of one of infosec's pioneering hacker groups, Cult of the Dead Cow.

The conference also gives Anomali the opportunity to showcase its own contributions to threat intelligence. While 42% of organizations surveyed in 2019 by 451 Research's Voice of the Enterprise already report some implementation of CTI, an additional 15% have new CTI implementations currently in pilot or proof of concept. Another 16% plan to deploy new investments in the next 12 months, while a further 9% plan to do so in the next two years. Anomali has benefited from that continued interest and investment.

Founded in 2013 as ThreatStream, Redwood City, California-based Anomali was one of the first commercial vendors of threat intelligence platform (TIP) technology, which began with consolidation and rationalization of CTI information to make intelligence more readily consumable and actionable by analysts, security operations teams and threat defense. Today, that focus has been raised even higher, recognizing the role of CTI in cybersecurity decision-making and risk mitigation.

Anomali has been led since 2014 by CEO Hugh Njemanze, a co-founder of ArcSight and former Entrepreneur in Residence with Kleiner Perkins Caufield & Byers. Wei Huang, a leading ArcSight architect, also joined Anomali in 2014 as VP of engineering and today serves as CTO. With $96.3m in funding, Anomali is backed by Google Ventures, General Catalyst, Paladin, Institutional Venture Partners (IVP), Lumina and In-Q-Tel, and has grown to roughly 350 customers and more than 300 employees. Recent additions to the executive team include chief customer officer Sunil Nagdev, CFO Jon Skoglund and chief revenue officer Bijan Hafezi.

Products, technology and partnerships

At Detect '19, Anomali introduced its combined platform as Anomali Altitude, whose three main components include Anomali Match, which is the re-branded Anomali Enterprise with new features and capabilities, and a new offering, Anomali Lens, in addition to Anomali ThreatStream, the company's long-standing CTI sharing platform.

Anomali ThreatStream is arguably the most recognized of the three, the foundational TIP technology long familiar among CTI analysts and security operations teams for providing a unified view that consolidates findings from multiple sources, both open source CTI (OSINT) as well as commercial intelligence feeds. Anomali ThreatStream provides analytics for supporting security investigations, prioritizing security investments, sharing intelligence within a community and integrating CTI with incident response and ongoing defense. Anomali ThreatStream is available as a fully in-cloud offering, an on-premises deployment or in a hybrid model to enable organizations to meet their unique needs.

Anomali Match is the new branding for Anomali Enterprise, which enables businesses to correlate large volumes of CTI with evidence in an organization's security monitoring, detection and remediation functions. This allows organizations to identify threats previously unknown to researchers or unrecognized in enterprise security monitoring. Integrations include security information and event management (SIEM), vulnerability management and other enterprise security management systems. New Anomali Match capabilities introduced at Detect '19 include heightened accuracy for domain generation algorithm (DGA) detection, high-volume retrospective search for evidence over a year or more using Elasticsearch, new data visualizations in the Anomali Match Analysis Dashboard and integration with what is arguably Anomali's most provocative debut at Detect '19, Anomali Lens.

Anomali Lens is a new and innovative offering that scans Web-based content, recognizes and identifies threat intelligence-related information, and automatically provides links to insight delivered via Anomali Altitude. If, for example, web content includes references to threat intelligence or attack data already cataloged in Anomali ThreatStream, those items will be highlighted automatically by Lens to allow the analyst to drill down into that content and discover relevant information. Threats already seen within a specific enterprise can be linked by Lens to information in Anomali Match. Lens also offers the ability to automate the production of reports, which can be published as bulletins to ThreatStream.

Anomali Lens serves three key objectives of CTI analysts: the need to produce rapid and responsive insight into new threats relevant to a given constituency, correlation of threats with evidence seen in the enterprise environment and linkages to action for containing and resolving threats as they arise. These have historically been highly time- and human-intensive activities and are still reflected in premium services that highlight the contribution of human analysts to analyzed intelligence. At a time when human expertise is at a premium in cybersecurity, reliance on human effort for the production of

intelligence findings is less sustainable than ever. Anomali Lens represents a response to that need in a way distinctive to the CTI community, harnessing tools such as natural language processing (NLP) to leverage automation in a key area for cyber defense. Currently available as a browser plug-in, Anomali Lens will also be available for mobile devices.

Because CTI is a community affair, with insight accessed from both open and commercial sources, partnerships are central to the Anomali strategy. Many of Anomali's commercial partners participate in the Anomali Preferred Partner (APP) program and offer packaged integrations via the Anomali APP Store, which makes it easy for Anomali customers to add providers to the intelligence managed via the Altitude platform. At Detect '19, Anomali announced a further level of partner participation in the APP Store, with trials of partner offerings providing a subset of full capabilities or premium feed volume. Six partners announced their support for this new level at Detect '19: DomainTools, Farsight Security, Flashpoint, Intel 471, ReversingLabs and Sixgill.

Competition and market dynamics

In recent years, CTI has become more pervasive across the security vendor landscape, and more broadly integrated in a wide range of products and services. While Anomali continues to face competition in the TIP market from the likes of EclecticIQ, ThreatConnect and ThreatQuotient, providers of commercial CTI such as LookingGlass and FireEye (through its iSIGHT Partners acquisition) also provide some measure of CTI management, while AT&T recently acquired AlienVault and its Open Threat Exchange. Within the TIP space, ThreatConnect is a competitor broadening its focus with emphasis on security automation and orchestration (SAO). A more recent and provocative entrant in CTI is ThreatBook, distinctive as a Chinese vendor, which provides TIP functionality as part of a wider portfolio that includes threat detection, sandboxing and secure DNS.

Anomali's many partnerships are a counterweight to competition in multiple fields. Partners such as Blueliv combine threat intelligence management with intelligence gathering and complement the Anomali portfolio. More recently, CTI-centric defense has appeared in the threat intelligence gateway (TIG) functionality of another Anomali partner, Bandura Cyber, which can filter traffic based on the volume or nature of CTI indicators. This represents an evolution in CTI actionability alongside initiatives in addition to SAO such as the MITRE ATT&CK framework and its roots in the STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated eXchange of Indicator Information) specifications for defining machine-readable CTI structure and communication.

While this widening of emphasis is good for the broader CTI landscape – and Anomali partnerships – it also blurs distinctions between potential partners and possible competitors, especially given how pervasive the application (or at least the buzz) of analytics and automation have become in infosec. This blurring has particularly evident among strategic security vendors. Automation, for example, has been a recent acquisition theme for both Palo Alto Networks, whose CTI initiatives include its Unit 42 operations, and another CTI player, FireEye (which acquired both ISIGHT Partners and Mandiant). With Verodin, FireEye took on automation in security assessment, while with Demisto, Palo Alto Networks embraced SAO for security operations. These CTI players are all partners of Anomali, and partner as well with SIEM to align intelligence with security operations. Yet Demisto competes in SAO with SIEM vendors such as IBM, which acquired SAO via Resilient Systems in 2016, and Splunk, which did so via Phantom Cyber two years later. As the security market continues to evolve, the boundaries between these players may become even less distinct.

SWOT Analysis

STRENGTHS

Anomali has a substantial share of the TIP market and as such represents an anchor for CTI in security operations. Its expanded offerings leverage this position to sustain and enhance its value in an evolving security landscape.

WEAKNESSES

Threat intelligence is valued by enterprises, but the CTI market is dependent on the customer's ability and need to invest – which may restrict substantial investment to the most mature security organizations. Anomali's challenge is to sustain and expand its appeal across its addressable market.

OPPORTUNITIES

Never before has access to insight at scale been as available as it is today. As a focus of threat intelligence for the enterprise, Anomali and its partners have opportunities to forge new ways for making CTI relevant and actionable.

THREATS

Threat intelligence and platform plays are increasingly common interests of strategic vendors. Anomali must maintain its differentiation to keep its footing as large vendors and hyperscalers see increased opportunity in CTI.