ESG Economic Validation

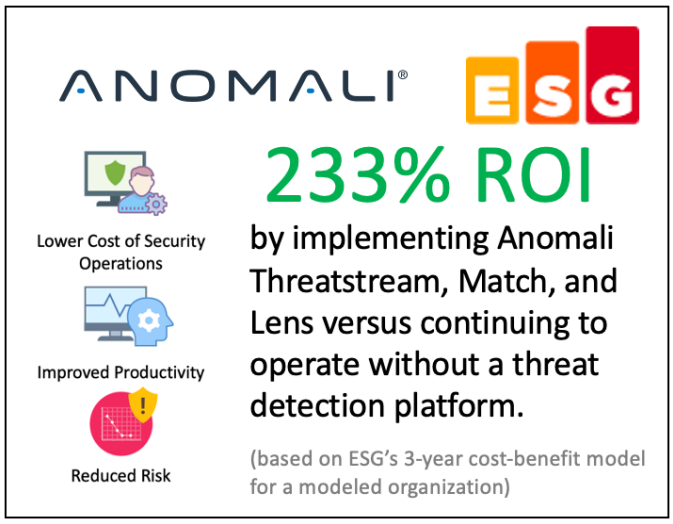
Analyzing the Economic Benefits of the Anomali Threat Intelligence Platform

By Aviv Kaufmann and Alex Arcilla, Senior Validation Analysts

July 2020

Executive Summary

Never before has it been so critical for enterprises to effectively empower an increasingly remote workforce with access to applications and resources across a number of geographic regions, networks, and devices. Enterprises have been forced to quickly implement solutions, ease restrictions and policies, and remove barriers to entry, placing an even greater burden on their security teams to operate effectively and efficiently to protect the organization and its assets. Security teams must work smarter and more efficiently to incorporate as much threat intelligence information as possible to identify and remediate threats.



ESG validated that Anomali's suite of intelligence-driven security products has helped to streamline security operations, automate workflows, reduce false positives, improve internal and external collaboration, and reduce time to detection and remediation. ESG validated the benefits that Anomali's customers had experienced through a series of interviews and used the information to create a modeled scenario that shows how an organization can save $93K per month through improved productivity, avoidance of risk, and value gained from included products. ESG's model predicts a return on investment of 233% and a payback period of only 11 months for an organization with a security team of 10 individuals choosing to implement Anomali versus continuing to operate without a threat intelligence platform.

Introduction

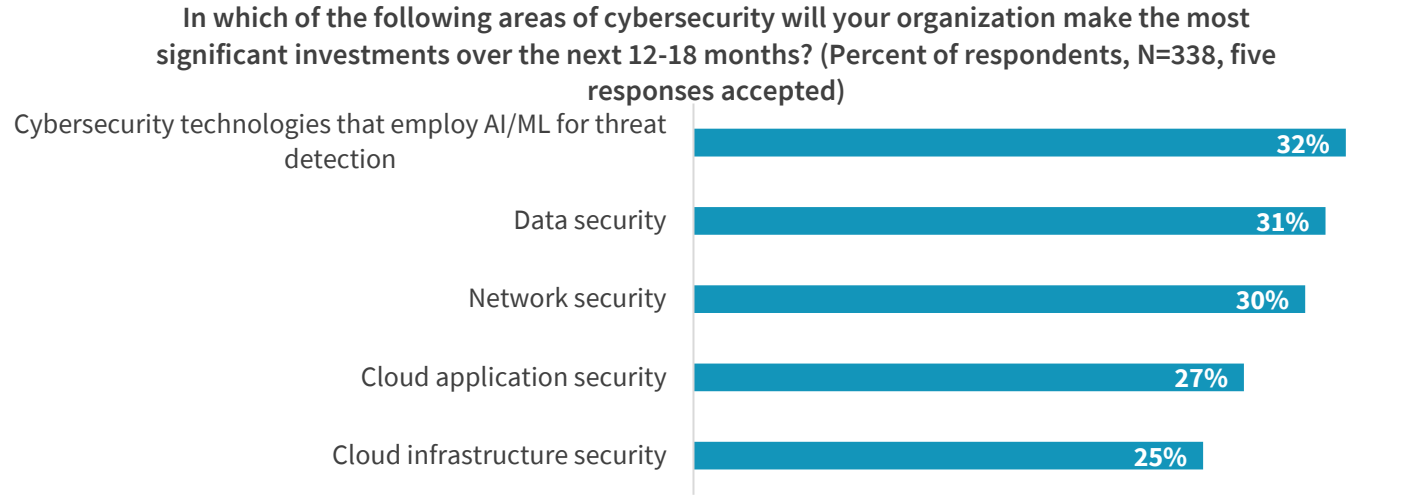
This ESG Economic Validation focused on the quantitative and qualitative benefits organizations can expect by empowering their security operations teams with Anomali's suite of intelligence-driven security products to analyze, detect, investigate, and respond to potential threats faster and more efficiently. These products include Anomali ThreatStream (threat intelligence platform), Anomali Match (threat detection), and Anomali Lens (threat knowledge).

Challenges

Cybersecurity is a top concern for any business. Security operations teams have evolved from reactively responding to alerts and "plugging holes" to proactively leveraging the exponentially growing volumes of threat intelligence to stay better protected. ESG research shows that 62% of organizations expect to increase cybersecurity services spending over the next 12-18 months.[1] The availability of so many threat intelligence sources has placed a burden on security professionals, who struggle to find ways to efficiently bring in, manage, analyze, and take appropriate action based on this intelligence. These organizations will simply never have the human resources to utilize all of the intelligence that is available to them. Automation and analytics are required to effectively prioritize and extract the actionable intelligence needle from the ever-growing threat intelligence haystack.

Many larger organizations have, over time, deployed a broad set of security technologies, and grown their team of security professionals to support these solutions. The implementation of a security operations center (SOC) has brought the combined knowledge and experience of this team to a common operation that is better equipped to deal with threat detection and response, but security experts are a finite resource that is difficult and expensive to find, train, and retain. Similarly, the deployment of security information and event management (SIEM) promise to detect threats more effectively by consolidating the intelligence and information generated by a number of servers and devices, but SIEMs have a limit to the volume of data they can effectively search and manage, and produce quite a lot of false positives that require the team's attention, limiting the organization's visibility into threats. It comes as no surprise therefore that organizations are looking to help their overwhelmed SOC teams better pinpoint real threats and accelerate their response to these threats. ESG research identifies the use of technologies that employ artificial intelligence (AI) and machine learning (ML) for threat detection as the most often cited area of cybersecurity in which organizations will make the most significant investment during 2020 (see Figure 1).

Figure 1. Top 5 2020 Cybersecurity Spending Priorities



Source: Enterprise Strategy Group

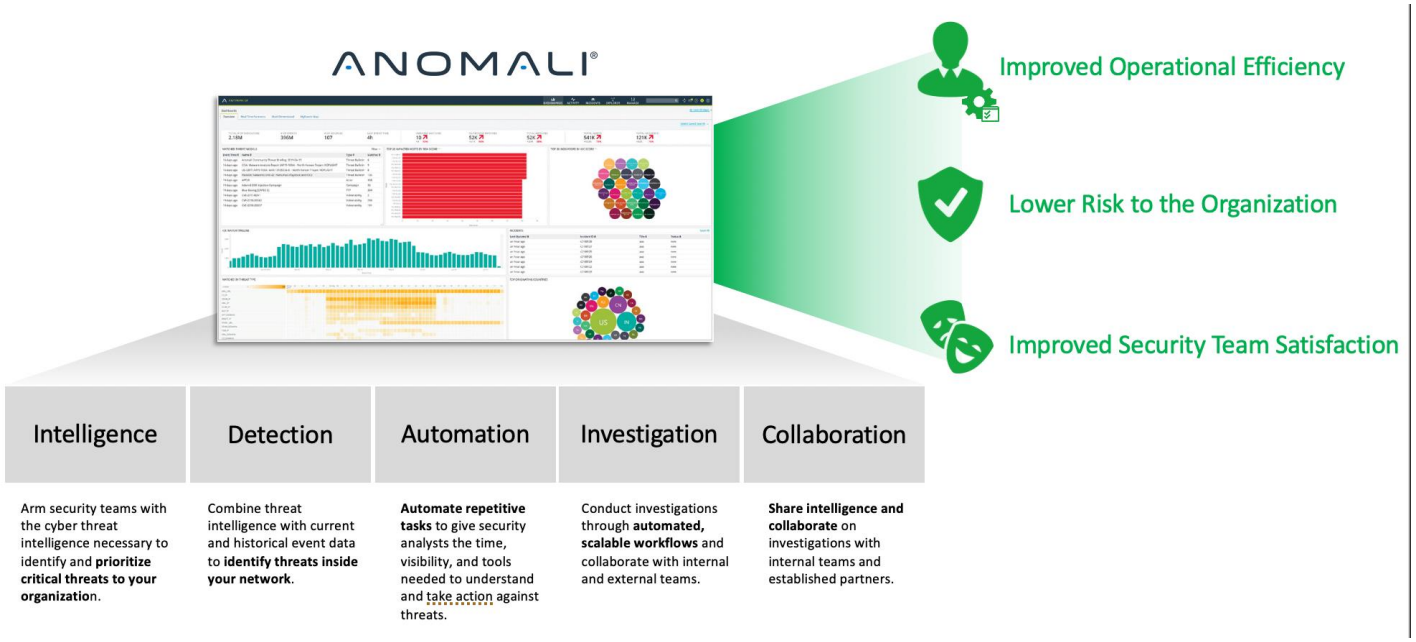
[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020. All ESG research references and charts in this economic validation have been taken from this master survey results set.

While the availability of massive volumes of threat intelligence and system telemetry hold out the promise of better security, more effective protection can only be achieved when organizations are better able to free up and optimize communication between their most valuable weapons, which are their SOC and cyber threat intelligence personnel.

The Anomali Solution

Anomali offers a suite of intelligence-driven security products providing unmatched threat visibility, accelerated detection, faster response, and improved productivity. Anomali products help organizations automate the collection, management and deployment of multiple internal and external streams of threat intelligence, filter out false positives, identify threats in their environments, and operate more efficiently to focus on the most important security needs.

Figure 2. The Anomali Threat Intelligence Platform



Source: Enterprise Strategy Group

Anomali can be deployed in the cloud, on-premises, or air gapped (on-premises, but disconnected from public data). The platform consists of three main products: Anomali ThreatStream, Anomali Match, and Anomali Lens.

Anomali ThreatStream – Unifies threat data and information into high-fidelity intelligence, automatically disseminates it to security controls, and integrates a suite of research tools to support efficient threat investigations. ThreatStream automates the collection of threat intelligence data from hundreds of external and internal sources, including open source threat intelligence, commercial threat feeds, shared intelligence, and internal intelligence from investigations, sandbox detonations, etc. The product normalizes and deduplicates these feeds into a common taxonomy, leveraging machine-learning algorithms to remove false positives, enrich the data, and risk score the intelligence for severity and confidence. ThreatStream then operationalizes the intelligence via automated distribution of machine-readable threat indicators to security controls (e.g., SIEM, firewall, EDR, IPS, SOAR, etc.). The product also provides tools for analysts and SOC teams to do model-based investigations using the Diamond, Kill Chain, STIX, or MITRE ATT&CK frameworks. The investigations workbench includes a comprehensive set of data enrichment sources, a powerful visual Explorer tool for indicator expansion and pivoting, integrated sandbox detonation for malware and phishing URLs, and threat bulletin collaboration, authoring, and publication.

Anomali Match – Automates the detection of threats in the network by correlating all available threat intelligence against all network activity logs. Match accomplishes this by indexing all SIEM logs and other event sources to maintain a year or more of historical data that is continuously analyzed against new and existing threat intelligence, automatically delivering alerts back to the SIEM, SOAR, or ticketing system for response and remediation. Real-time forensics allows analysts to track evidence of past breaches back to "Patient Zero," hunt for threats based on actor, vulnerability, or TTP, and prioritize responses based on risk score and asset criticality.

Anomali Lens – Provides threat knowledge at your fingertips, automatically identifying threat data in any web content using natural language processing (NLP). Lens does this by scanning web pages, social media platforms, and SIEM and other security logs to identify indicators of compromise (IOCs), threat actors, malware families, and attack techniques. Threat intelligence identified by Lens is automatically associated with the MITRE ATT&CK framework and can be imported into Anomali ThreatStream for further investigation and analysis at the click of a button. Lens also integrates with Anomali Match to highlight scanned threat intelligence present in the network, providing instant understanding of the level of severity and impact it has on your environment.

ESG Economic Validation

ESG completed a quantitative economic validation and modeled analysis on the Anomali suite of products.

ESG's Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages ESG's core competencies in market and industry analysis, forward-looking research, and technical and economic validation. ESG reviewed the results of existing case studies and end-user surveys and conducted in-depth interviews with end-users to better understand and quantify how Anomali has impacted their organizations, particularly in comparison with how they used to operate prior to deploying Anomali or previous experiences at other organizations. The qualitative and quantitative findings were used as the basis for a simple ROI model comparing the expected savings and benefits that a modeled organization might expect versus the expected cost of deploying Anomali.

Anomali Economic Overview

ESG's economic analysis revealed that customers who had deployed Anomali were very satisfied with the product and felt that they had greatly streamlined their security operations, were operating more efficiently, and were doing a better overall job at protecting the organization. ESG found that Anomali provided its customers with significant savings and benefits in the following categories:

- Lower Operational Cost of SecOps – Organizations significantly streamlined security operations and made better use of their security resources through Anomali's automation and orchestration capabilities, and its well-designed and effective security tools and features.
- Improved Security Effectiveness and Reduced Risk to the Organization – Customers reported that Anomali helped to better arm the security team and operationalized the security process, making teams more effective, and reducing the time to identify and remediate security issues.
- Improved SecOps Productivity and Satisfaction – Anomali helps improve both productivity and satisfaction for security professionals by automating repetitive or time-consuming tasks, freeing them to focus on higher value security operations. Skills are quickly improved, collaboration and visibility are improved, and synergetic value with other security products is amplified.

Lower Operational Cost of Security Operations

ESG found that security teams that deployed Anomali products reported that their security operations had been greatly simplified through operationalization, automation, and orchestration. Users reported significant time savings or reductions in a number of areas including deployment of new technologies, researching threats, enhancing data, responding to false positives, and correlating information from multiple sources (as well as in many other areas). This allowed teams to get more from every security analyst, improve the capabilities of junior analysts, onboard quicker, and reduce the time spent on lower value tasks, allowing the team to focus on the higher value activities like remediation.

- Reduced Administrative Complexity – Customers reported that ThreatStream reduced the administrative complexity of managing multiple security threat intelligence streams and point security products. There are fewer interfaces to manage, simple app-store-like trials and deployment of new premium feeds, and integrated management of IOCs. This saved organizations the time and complexity of deploying, managing, and integrating multiple products using several different interfaces.

- Faster Time to Value – ThreatStream was quick and easy to deploy for organizations, as was integration with IOCs and adding or removing premium feeds. The strong partner ecosystem and software development kits (SDKs) allowed organizations to quickly incorporate the internal and external threat intelligence tools and feeds that best meet their needs. "Freemium" options allow customers to subscribe to commercial intelligence partner feeds to better optimize their threat intelligence programs. Procurement was simplified, and organizations felt they spent less time dealing with integration and support issues. This means that organizations were able to test and integrate security strategies and tools faster. One customer commented, "Anomali saves us time and effort in procuring and installing streams, and we know it's already set up and ready to go with no integration needed – that saves us hours to days depending on the complexity."

"I could spend hours researching and collecting context, with Anomali, I can just type in the URL or pivot with Lens and know exactly what my containment actions need to be."

- Streamlined Workflow – Anomali helped organizations to streamline their security workflows to reduce the amount of time spent on investigations by the SOC, CTI, and incident response teams by bringing them all together in one platform. Simplified workflows, tight integration with other security feeds and solutions, and enrichment of threat intelligence and research minimized the time spent by security team members on all aspects of threat detection, investigation, and response.

- Automation of Tasks – Users reported having to perform significantly fewer manual tasks after deploying ThreatStream. Anomali automated many of the repetitive or time-consuming tasks that take up much of security analysts' days, including normalization of sources, investigating and understanding the risk profile, formatting and enriching threat intelligence, and creating reports. Anomali also orchestrated many of the configuration, integration, and bidirectional security-related tasks between security solutions like SIEMs, firewalls, and network devices. Anomali Match processed log information for one customer that Anomali users estimated would have taken up to

"For a task where we would have otherwise needed to restore SIEM logs from tape, it would take longer than 2 weeks to respond to a request that Anomali Match allowed us to do in under an hour."

2.5x more people to accomplish: "We have four guys doing the job that would have otherwise taken maybe ten people."

- Less Wasted Time – Organizations that had deployed Anomali reported that they now had to deal with far fewer false positives and suffered from far less "alert fatigue." Users felt that this gave them additional time to focus on more important tasks. The automation of threat intelligence research and enrichment resulted in less time spent trying to figure the situation out, a lower risk of having to repeat tasks, and less troubleshooting due to human error. One user stated, "I don't have to go start hunting and trying to figure out what an indicator means or why it is bad which was like 90% of the job that I had to do before."

Improved Security Effectiveness and Reduced Risk to the Organization

Anomali works in conjunction with other security products to deliver a streamlined solution that is more effective at identifying IOCs, reducing false positives, and providing context and insight to help understand and remediate threats. Customers whom we spoke with believe that Anomali has greatly increased the overall effectiveness of their security operations, with some reporting that they believe Anomali has made them up to 90% more effective at identifying and remediating threats.

- Faster Time to Insight – End-users felt that Anomali, when used in conjunction with their other tools, provided them with a noticeably improved time to insight. Customers reported greater feed agility, increased visibility, and IOC-enriched data that helped to speed time to awareness and threat detection, ultimately resulting in improved mean time to response (MTTR) and remediation. One user reported that Anomali Match helped drive an improvement in MTTR from more than nine days down to only ten minutes to validate IOCs. Customers agreed that Anomali enabled them to detect, investigate, and remediate a greater volume and variety of threats and IOCs in less time.

"Without Anomali there are so many threats that would have been missed, or taken far longer to identify and remediate. It has become a critical part of our security monitoring."

- Machine Learning-powered Intelligence – Anomali uses machine learning algorithms to provide enrichment of threat context, help prioritize threats, and perform historical evaluation of events. This provides organizations with more holistic, effective, and timely intelligence than could be achieved through hours of human effort. Teams reported that this helped them to identify, research, and respond to threats much faster, and felt that they now had a security operations team that was far more effective than before. One user commented, "Anomali represents the first time that we can exponentially grow and manage the ability to collect and incorporate information from the internet—to the point where the human is no longer the limit."

- More Threat Intelligence Processing – ThreatStream allowed teams to process a greater volume and variety of threat intelligence than they would have before. They could test and manage more external feeds as well as combine with near-real-time threat bulletins and internally produced threat intelligence. The ability to perform threat actor profiling and track an actor over a longer period of time was extremely valuable. One customer stated, "There are other TIPs out there that do things like take in feeds and perform correlation, but Anomali really delivers value to us by giving us the ability to ingest our own data as well."

- More Effective Security Response – All of the users whom we spoke with agreed that Anomali helped them to be far more effective at responding to security threats. Not only did ThreatStream help to process a greater volume of intelligence and identify threats faster, but it greatly reduced the busy work that analysts used to perform by automating the updating of feeds, correlation of indicators, and breach analysis to figure out which ones tie together, and suggesting research and remediation actions up front. One customer said, "Rather than just indicating that an IP is bad, I can see why the IP is bad, what activity it was doing, and what steps I should take."

"Instead of me checking each one of these emails or each one of these IPs one by one I can get this big global view and see that 90% of them come from one breach, or one indicator type, or one tag."

Why This Matters

It's the goal of every organization to provide more effective security for the business.

Anomali customers stated that they felt Anomali was up to 90% more effective at identifying and remediating threats. One organization reported that Anomali was the reason that they avoided over $400K in stolen user credits by proactively identifying and taking cross-functional action to protect users' accounts against a breach attempt.

- More Informed Security-related Decision Making – Users reported that Anomali provides a number of simple yet effective dashboards to help teams visualize threats, prioritize decision making, and share information with other teams in a useful manner. The built-in sandboxing capabilities, availability of Anomali's expert threat intelligence support teams, and ability to share information with peers helped to provide additional information that was useful in making internal decisions. Users agreed that Anomali provided the ability to make more informed and timely decisions, helping to reduce risk to the organization.

Improved SecOps Productivity and Satisfaction

Every organization that we spoke with felt that Anomali had helped them transform their organization to make the most of the resources they had. They reported that their teams were far more productive, but also that they were more satisfied in their roles, and that the organization was better able to communicate with the business and their peers.

- More Productive Security Professionals – ThreatStream enables everyone to be more productive and focus on where they bring the most value. Teams reported that less experienced members onboarded and contributed earlier, learned faster, and quickly gained more experience performing higher value roles. This is a benefit to both the organization and to the individual's career.

"With Anomali we are able to have two people performing the work that [named organization] dedicates a very large team to – and we are doing a better job at it."

- More Satisfied Security Team – End-users indicated that because Anomali helps them to do a better job, they sleep better at night, progress faster in their careers, and feel that they have achieved more to protect the company. Overall, they reported that they now view their job as a more positive experience. Organizations felt that Anomali helped them to build a stronger team and create an environment where it is easier to retain workers in a field where people are struggling to find and keep talent.

- Improved Business Processes – Customers stated that ThreatStream has allowed them to better share information between security organizations, and facilitated far more effective discussions between security teams, business units, and end-users. One organization stated: "We have been able to build some really cool processes around Anomali. We have worked with our fraud team, our red team (testing) and threat intelligence team, even our compliance team and give them a view of what we actively see." Customers felt they educated their users better because they were better able to show what threats were observed in an easy-to-consume manner. They felt without Anomali, they did not have a way to communicate to the business without spending hours writing up detailed explanations.

"Anomali is improving some of the processes that were already there, but it's also building new avenues for us because we are able to talk to them in a more effective manner."

- Better Collaboration with Peers – Customers felt that Anomali provided them with a means to share internally collected threat intelligence and remediation suggestions with peer groups in a trusted manner. This allows the organization to contribute to or even be recognized as leaders among their peers while making the peer group more effective at identifying and remediating threats and saving valuable time by not having to repeat investigations that others have already performed. One customer said, "Being able to share intelligence with other groups has been extremely helpful…we do not have to dig as deep or experience the pain sometimes because we are able to share intelligence."

ESG Analysis

ESG leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to create a three-year ROI model that compares the costs and benefits of implementing Anomali ThreatStream, Match, and Lens with continuing to operate without a threat analysis and detection platform. ESG's interviews with Anomali's customers, combined with experience and expertise in economic modeling and technical validation of Anomali products helped to form the basis for our modeled scenario.

ESG's modeled organization consisted of a team of 10 threat intelligence analysts with varying degrees of experience providing security services to an organization with 1,500 employees. ESG factored in the expected cost to install, implement, and train employees to use the Anomali platform, as well as annual subscription costs, hardware nodes, infrastructure costs, and support and maintenance over a three-year period.

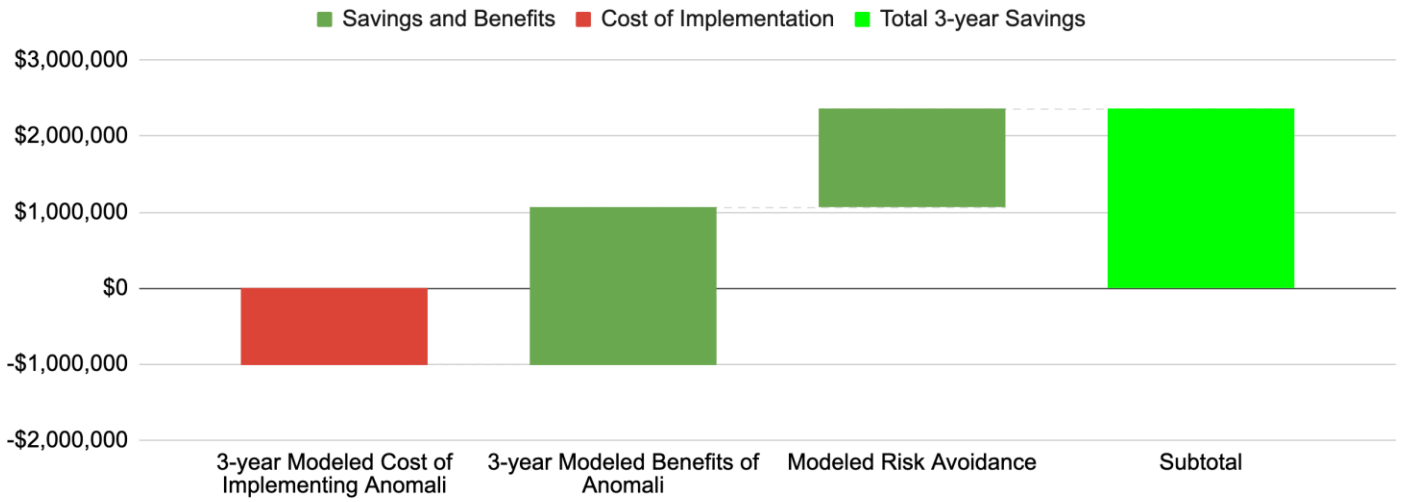
On the benefits side, ESG modeled the expected avoided cost or benefit of improved productivity across the security team based on an expected 20% to 70% improvement on tasks related to managing and curating feeds, performing and reporting the results of investigations, integrating with other security systems, sharing threat intelligence with collaborative organizations, and sharing and reporting intelligence internally across the organization. ESG conservatively estimated that only 35% of the security team's total man hours were spent performing these tasks. ESG's model resulted in a 58% improvement in productivity while performing these tasks and a total three-year savings of $969K. These savings manifest themselves as man hours that are now available for additional security-related tasks that were not there before Anomali.

ESG's models predicated cost savings provided through 40% reduction in false positives ($608K), value associated with the security products that Anomali provides (sandboxing, freemium and premium threat intelligence feeds, responsive Anomali support, and training through Anomali University) for a total value of $452K, and other cost savings provided by the avoidance of professional services, training, and certification, and simplified procurement and integration ($53K).

ESG also modeled the avoidance of risk provided by a lower chance of data breach based on increased probability of earlier detection, increased total efficacy, and faster remediation of issues, as well as a lower expected cost of a data breach

based on the ability to detect and take automated action faster and more effectively. ESG's probability and cost assumptions of a data breach are based on publicly available data published by the Ponemon Institute. ESG calculated that Anomali could lower risk to an organization, avoiding up to $1.292M in expected cost of a data breach over three years. The results of ESG's modeled cost benefit analysis are shown in Figure 3.

Figure 3. Results of ESG's Three-year Cost-benefit Analysis on Anomali Threat Intelligence Platform



Source: Enterprise Strategy Group

What the Numbers Mean

ESG's modeled analysis predicted substantial savings and benefits for our modeled organization. While no modeled scenario could ever accurately represent the economics behind every deployment, ESG encourages organizations to perform their own analysis to see how much they can save. ESG suggests that organizations consider the following costs that were included in our analysis:

- Cost of Implementing the Anomali Solution – Includes cost of Anomali subscriptions; FTE and professional service man hours to deploy, test, and train on the solution; appliances to run Anomali, power/cooling/floorspace costs; and support and maintenance on the hardware.
- Value of Included Threat Intelligence Products – Dollar value assigned to the equivalent solutions for sandboxing, TIP Intel, included freemium and premium threat intelligence feeds, training with Anomali University, expert support, etc.
- Avoided Cost of Dealing with False Positives – ESG assumed 50 false positives per day per analyst, 2 minutes spent per false positive, and a 40% reduction in false positives with Anomali.
- Productivity Improvement to Security Operations – ESG's detailed conservative models considered the expected number of man hours spent before Anomali against the expected improvement for feed collection (70% improvement), feed management and curation (70% improvement), investigations and reporting (60% improvement), integration with operational security systems (20% improvement), external collaboration (50% improvement), and internal sharing and operations (60% improvement).
- Quantification of Reduced Risk – ESG calculated a reduced risk of data breach versus the industry average proportional to a 70% improvement in detection and response, as well as a reduced expected cost of data breach for automated systems (both numbers are reported by the Ponemon Institute).

The Bigger Truth

Strengthening cybersecurity has consistently topped ESG research respondents' list of business drivers for technology spending for several years. As organizations continue to grow their teams, organize their teams, and invest in new solutions, one thing is clear: The problem is not a lack of security tools and threat intelligence, but a lack of human power to effectively manage, interpret, and take action based on the intelligence and alerts. Modern security organizations require a threat intelligence platform that can help streamline the security process, automate repetitive tasks, provide AI-driven intelligence, and allow the human resources to become more operationally efficient.

ESG validated that Anomali ThreatStream, Match, and Lens have provided customers with a platform that helps them get the most out of their security investments. Security teams are far more empowered, productive, and focused on the most important tasks; their investments in their SIEM and other security products are easily integrated and enhanced to provide even greater value; and their threat intelligence feeds are ready to evaluate, purchase, and integrate. Customers reported considerably improved visibility and a greater ability to share threat intelligence internally with other divisions of the company, and externally with their peers and security organizations.

ESG's modeled cost benefit analysis shows how an organization that implements Anomali can expect to save through improved security team productivity, value added from included threat intelligence products, and avoidance of risk. The key assumptions in the model were based on ESG's validation with Anomali's customers. ESG's model calculated an expected total savings of up to $93K per month with an expected return on investment (ROI) of 233%.

Anomali is not competing with an organization's existing security products or looking to functionally change the way teams need to operate. Instead, Anomali serves to operationalize and enhance threat intelligence, tools, and solutions to make security teams more efficient and to expand the security discussion to other parts of the business. Every organization that ESG spoke with felt they accomplished far more with a smaller team and scaled operations far beyond what was realistically achievable through manpower alone. Some had even brought Anomali with them into new roles: "I had used Anomali in a previous role, and when I came here, I said If we don't have Anomali we are not going to be able to accomplish our goals." As an analyst, you quickly learn that a statement like that is the mark of a transformative technology. If you are looking to transform and streamline your security operations and get the most from your threat intelligence, ESG recommends that you contact Anomali to see if it is the right threat intelligence platform for your team.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.