Wirtschaftliche Betrachtung von ESG

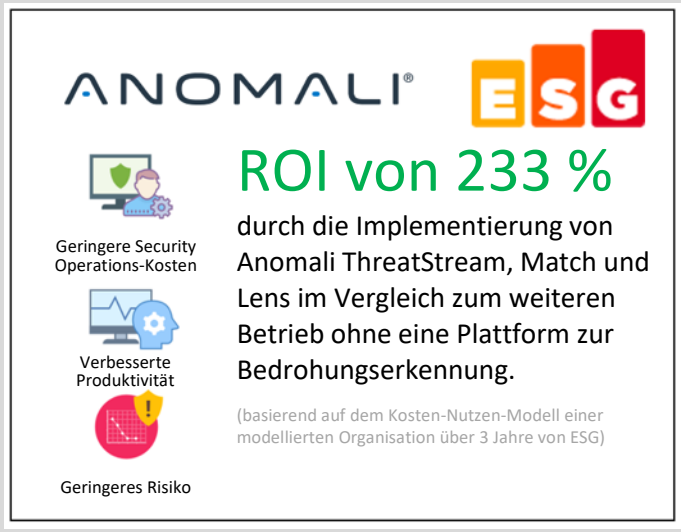
# Analyse der wirtschaftlichen Vorteile der Threat Intelligence-Plattform von Anomali

Von Aviv Kaufmann und Alex Arcilla, Senior Validation Analysts

Juli 2020

## Zusammenfassung

Noch nie zuvor war es für Unternehmen so wichtig, eine wachsende Anzahl an Remote-Mitarbeitern effektiv mit Zugriff auf Anwendungen und Ressourcen über eine Reihe geografischer Regionen, Netzwerke und Geräte hinweg zu unterstützen. Unternehmen sahen sich gezwungen, Lösungen schnell zu implementieren, Einschränkungen und Richtlinien zu vereinfachen und Zugangsbarrieren zu beseitigen. Dies setzte ihre Sicherheitsteams unter zusätzlichen Druck, noch effektiver und effizienter zu arbeiten, um das Unternehmen und seine Ressourcen zu schützen. Sicherheitsteams müssen intelligenter und effizienter vorgehen, um so viele Bedrohungsinformationen wie möglich zu integrieren, um so Bedrohungen zu erkennen und zu beheben.




ESG bestätigt, dass die Suite an intelligenten Sicherheitsprodukten von Anomali dazu beigetragen hat, Sicherheitsvorgänge zu optimieren, Workflows zu automatisieren, Fehlalarme zu reduzieren, die interne und externe Zusammenarbeit zu verbessern und die Zeit bis zur Erkennung und Behebung zu verkürzen. ESG bestätigte die Vorteile für Anomali-Kunden in einer Reihe von Interviews und nutzte diese Informationen, um ein modelliertes Szenario zu erstellen, das zeigt, wie ein Unternehmen durch eine verbesserte Produktivität, Risikovermeidung und Wertschöpfung aus im Lieferumfang enthaltenen Produkten 93.000 USD pro Monat einsparen kann. Zudem prognostiziert das ESG-Modell für ein Unternehmen mit einem Sicherheitsteam aus zehn Personen, das sich für die Implementierung von Anomali entscheidet, eine Investitionsrendite von 233 % und eine Amortisationszeit von nur elf Monaten (im Vergleich zum weiteren Betrieb ohne eine Plattform zur Bedrohungserkennung).

## Einführung

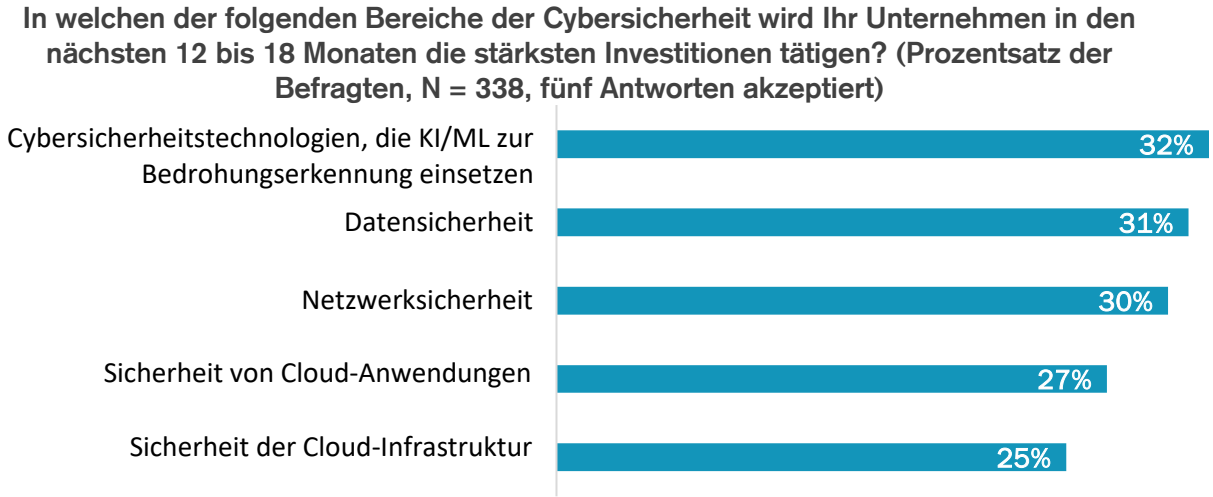
Diese wirtschaftliche Betrachtung von ESG konzentriert sich auf die quantitativen und qualitativen Vorteile, die Unternehmen erwarten können, wenn sie ihre Sicherheitsteams mit den intelligenten Sicherheitsprodukten von Anomali ausstatten, um potenzielle Bedrohungen schneller und effizienter zu analysieren, zu erkennen, zu untersuchen und darauf zu reagieren. Zu diesen Produkten gehören Anomali ThreatStream (Plattform zur Bedrohungserkennung), Anomali Match (Bedrohungserkennung) und Anomali Lens (Threat Intelligence).

### Herausforderungen

Cybersicherheit ist für jedes Unternehmen ein Hauptanliegen. Moderne Sicherheitsteams reagieren nicht nur auf Warnungen und „stopfen Löcher", sondern nutzen die exponentiell wachsende Menge an Threat Intelligence proaktiv, um einen besseren Schutz zu erreichen. Laut ESG-Studien rechnen 62 % der Unternehmen damit, dass sich ihre Ausgaben für Cybersicherheitsdienste in den nächsten 12 bis 18 Monaten erhöhen.[1] Die schiere Menge an Bedrohungsquellen setzt Sicherheitsexperten unter Druck. Viele tun sich schwer damit, diese Informationen effizient einzubringen, zu verwalten, zu analysieren und entsprechende Maßnahmen zu ergreifen. Diese Unternehmen verfügen einfach nicht über die erforderlichen personellen Ressourcen, um die ihnen zur Verfügung stehenden Informationen angemessen zu nutzen. Automatisierung und Analysen sind erforderlich, um die Nadel, d. h. nutzbare Informationen, im ständig wachsenden Heuhaufen an Threat Intelligence effektiv zu priorisieren und zu extrahieren.

Viele größere Unternehmen haben im Laufe der Zeit eine breite Palette von Sicherheitstechnologien eingeführt und ihr Team von Sicherheitsexperten ausgebaut, um diese Lösungen zu unterstützen. Die Implementierung eines Security Operations Center (SOC) hat das Wissen und die Erfahrung dieses Teams zu einem gemeinsamen Betrieb zusammengeführt, der besser für die Erkennung und Reaktion von Bedrohungen gerüstet ist. Sicherheitsexperten sind jedoch eine begrenzte Ressource, die schwer und teuer zu finden, zu schulen und zu binden ist. Ebenso verspricht die Bereitstellung von SIEM-Systemen (Security Information and Event Management), Bedrohungen effektiver zu erkennen, indem die von einer Reihe von Servern und Geräten generierten Informationen konsolidiert werden. SIEMs sind jedoch im Hinblick auf die Datenmenge, die sie efektiv durchsuchen und verwalten können, eingeschränkt und verursachen eine Menge Fehlalarme, die die Aufmerksamkeit des Teams erfordern, wodurch die Sichtbarkeit von Bedrohungen im Unternehmen beeinträchtigt wird. Daher ist es keine Überraschung, dass Unternehmen ihren überforderten SOC-Teams helfen möchten, echte Bedrohungen besser zu erkennen und schneller auf diese Bedrohungen zu reagieren. ESG-Untersuchungen haben den Einsatz von Technologien, die künstliche Intelligenz (KI) und maschinelles Lernen (ML) zur Bedrohungserkennung einsetzen, als den am häufigsten genannten Bereich der Cybersicherheit identifiziert, in dem Unternehmen im Jahr 2020 die bedeutendste Investition tätigen werden (siehe Abbildung 1).

**Abbildung 1. Die 5 wichtigsten Prioritäten bei Cybersicherheitsausgaben 2020**




*Quelle: Enterprise Strategy Group*

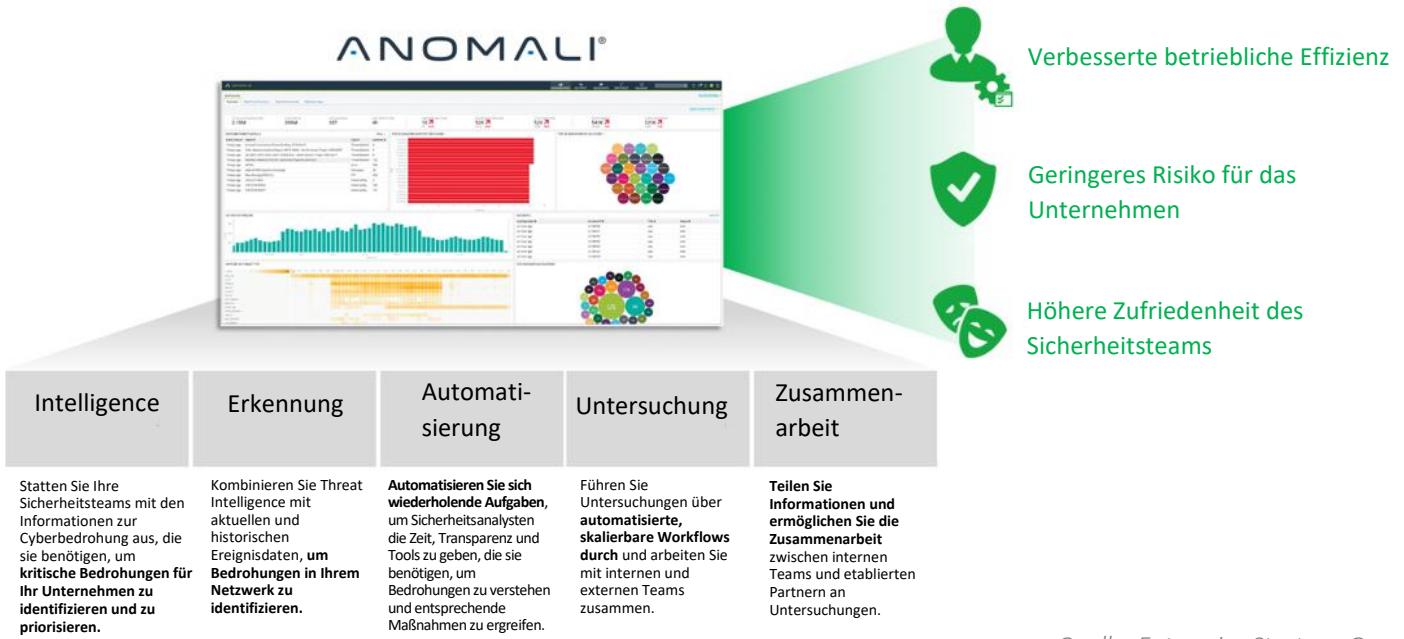
[1] Quelle: ESG Master Survey Results, *Umfrage zu geplanten Technologieausgaben 2020*, Januar 2020. Alle ESG-Forschungsreferenzen und -Diagramme in dieser wirtschaftlichen Betrachtung wurden diesem Master-Umfrageergebnissatz entnommen.

Während die Verfügbarkeit riesiger Mengen an Threat Intelligence und Systemtelemetrie eine bessere Sicherheit verspricht, kann ein effektiverer Schutz nur dann erreicht werden, wenn Unternehmen die Kommunikation zwischen ihren wertvollsten Waffen, nämlich dem SOC und den CTI-Mitarbeitern (Cyber Threat Intelligence), besser freisetzen und optimieren können.

## Die Lösung von Anomali

Anomali bietet eine Suite von intelligenten Sicherheitsprodukten, die unübertroffene Bedrohungstransparenz, beschleunigte Erkennung, schnellere Reaktion und eine verbesserte Produktivität bieten. Mit den Produkten von Anomali können Unternehmen die Erfassung, Verwaltung und Bereitstellung mehrerer interner und externer Threat Intelligence automatisieren, Fehlalarme herausfiltern, Bedrohungen in ihren Umgebungen identifizieren und effizienter arbeiten, um sich auf die wichtigsten Sicherheitsanforderungen zu konzentrieren.

**Abbildung 2. Die Threat Intelligence-Plattform von Anomali**




*Quelle: Enterprise Strategy Group*

Anomali kann in der Cloud, lokal oder physisch getrennt (lokal, aber von öffentlichen Daten getrennt) bereitgestellt werden. Die Plattform besteht aus drei Hauptprodukten: Anomali ThreatStream, Anomali Match und Anomali Lens.

Anomali ThreatStream – Vereint Bedrohungsdaten und -informationen zu zuverlässigen Daten, verteilt sie automatisch an Sicherheitskontrollen und integriert eine Suite von Forschungstools zur Unterstützung effizienter Bedrohungsuntersuchungen. ThreatStream automatisiert die Erfassung von Threat Intelligence aus Hunderten von externen und internen Quellen, einschließlich Open-Source-Bedrohungsinformationen, kommerziell erhältlichen Feeds, gemeinsam genutzte Informationen und interne Erkenntnisse aus Untersuchungen, Sandbox-Entschärfungen usw. Das Produkt normalisiert und dedupliziert diese Feeds in einer gemeinsamen Taxonomie. Dabei kommen Machine-Learning-Algorithmen zum Einsatz, um Fehlalarme zu entfernen, die Daten anzureichern und eine Risikobewertung der Informationen hinsichtlich Schweregrad und Vertrauen vorzunehmen. Anschließend operationalisiert ThreatStream die Informationen durch die automatisierte Verteilung von maschinenlesbaren Bedrohungsindikatoren an Sicherheitskontrollen (z. B. SIEM, Firewall, EDR, IPS, EAR usw.). Das Produkt bietet außerdem Tools für Analysten und SOC-Teams, um modellbasierte Untersuchungen mit den Frameworks Diamond, Kill Chain, STIX oder MITRE ATT&CK durchzuführen. Die Untersuchungs-Workbench umfasst eine umfassende Reihe von Datenanreicherungsquellen, ein leistungsstarkes Visual Explorer-Tool für Indikatorerweiterung und Pivoting, integrierte Sandbox-Entschärfung für Malware und Phishing-URLs sowie Zusammenarbeit, Authoring und Veröffentlichung von Bedrohungsanalysen.

Anomali Match – Automatisiert die Bedrohungserkennung im Netzwerk durch kontinuierliche Korrelierung aller verfügbaren Bedrohungsinformationen mit allen Netzwerkaktivitäts-Protokollen. Match erreicht dies, indem alle SIEM-Protokolle und andere Ereignisquellen indiziert werden, um historische Daten aus einem Jahr oder länger zu pflegen und kontinuierlich anhand von neuen und vorhandenen Bedrohungsinformationen zu analysieren. Dabei werden automatisch Warnungen an das SIEM-, SOAR- oder Ticketerstellungssystem ausgegeben, um eine entsprechende Reaktion und Behebung zu ermöglichen. Dank der Echtzeit-Forensik können Analysten Beweise für vergangene Verstöße bis auf „Patient Null" zurückverfolgen, auf der Grundlage von Akteur, Schwachstelle oder TTP nach Bedrohungen suchen und die Reaktion basierend auf der Risikobewertung und Asset-Kritikalität priorisieren.

Anomali Lens – Bietet Threat Intelligence auf Knopfdruck und identifiziert automatisch Bedrohungsdaten in Webinhalten mithilfe von Natural Language Processing (NLP). Zu diesem Zweck scannt Lens Webseiten, Social-Media-Plattformen sowie SIEM- und andere Sicherheitsprotokolle, um Gefährdungsindikatoren (Indicators of Compromise, IOCs), Bedrohungsakteure, Malware-Familien und Angriffstechniken zu identifizieren. Durch Lens identifizierte Bedrohungsinformationen werden automatisch mit dem MITRE ATT&CK-Framework verknüpft und können mit einem Mausklick in Anomali ThreatStream importiert werden, um weitere Untersuchungen und Analysen durchzuführen. Lens lässt sich auch in Anomali Match integrieren, um gescannte Bedrohungsinformationen im Netzwerk hervorzuheben und ein sofortiges Verständnis des Schweregrads und der Auswirkungen auf Ihre Umgebung zu vermitteln.

## Wirtschaftliche Betrachtung von ESG

ESG hat eine quantitative wirtschaftliche Betrachtung durchgeführt und eine Analyse auf Grundlage der Produktsuite von Anomali modelliert.

Die wirtschaftliche Betrachtung von ESG ist eine bewährte Methode, um die wirtschaftlichen Wertversprechen eines Produkts oder einer Lösung zu verstehen, zu validieren, zu quantifizieren und zu modellieren. Der Prozess nutzt die Kernkompetenzen von ESG in den Bereichen Markt- und Branchenanalysen, zukunftsorientierte Forschung sowie technische und wirtschaftliche Betrachtung. ESG hat die Ergebnisse bestehender Fallstudien und Endbenutzerumfragen geprüft und ausführliche Interviews mit Endbenutzern durchgeführt, um besser zu verstehen und zu quantifizieren, wie sich Anomali auf ihre Unternehmen ausgewirkt hat, insbesondere im Vergleich zum Betrieb vor der Implementierung von Anomali oder früheren Erfahrungen in anderen Unternehmen. Die qualitativen und quantitativen Ergebnisse wurden als Grundlage für ein einfaches ROI-Modell herangezogen, bei dem die erwarteten Einsparungen und Vorteile, die ein modelliertes Unternehmen erwarten kann, mit den erwarteten Kosten für die Bereitstellung von Anomali verglichen wurden.

### Überblick über die Wirtschaftlichkeit von Anomali

Die Wirtschaftlichkeitsanalyse von ESG ergab, dass Kunden, die Anomali bereitgestellt haben, mit dem Produkt sehr zufrieden waren und der Meinung waren, dass die Lösung ihre Sicherheitsabläufe erheblich optimiert, einen effizienteren Betrieb ermöglicht und insgesamt zu einem besseren Schutz des Unternehmens beiträgt. ESG stellte fest, dass Anomali seinen Kunden erhebliche Einsparungen und Vorteile in den folgenden Kategorien bot:

- Geringere Betriebskosten von SecOps – Unternehmen konnten die Sicherheitsabläufe erheblich optimieren und ihre Sicherheitsressourcen dank der Automatisierungs- und Orchestrierungsfunktionen von Anomali sowie der gut konzipierten und effektiven Sicherheitstools und -Funktionen besser nutzen.

- Verbesserte Sicherheitseffektivität und geringeres Risiko für das Unternehmen – Kunden gaben an, dass sie ihr Sicherheitsteam mit Anomali besser unterstützen und den Sicherheitsprozess operationalisieren konnten, was die Effektivität der Teams erhöhte und die benötigte Zeit zur Erkennung und Behebung von Sicherheitsproblemen verkürzte.

- Höhere SecOps-Produktivität und -Zufriedenheit – Anomali trägt dazu bei, die Produktivität und Zufriedenheit von Sicherheitsexperten zu steigern, indem wiederholte oder zeitaufwändige Aufgaben automatisiert werden, sodass sie sich auf höherwertige Sicherheitsabläufe konzentrieren können. Die Fähigkeiten werden schnell verbessert, die Zusammenarbeit und Transparenz verbessert und der synergetische Wert mit anderen Sicherheitsprodukten erhöht.

## Geringere Security Operations-Betriebskosten

ESG stellte fest, dass die Sicherheitsabläufe in Sicherheitsteams, die Produkte von Anomali einsetzen, durch die Operationalisierung, Automatisierung und Orchestrierung erheblich vereinfacht wurden. Benutzer meldeten erhebliche Zeiteinsparungen in einer Reihe von Bereichen, einschließlich der Bereitstellung neuer Technologien, Untersuchung von Bedrohungen, Anreicherung von Daten, Reaktion auf Fehlalarme und Korrelation von Informationen aus verschiedenen Quellen (sowie in vielen weiteren Bereichen). Dadurch konnten Teams ihre einzelnen Sicherheitsanalysten optimaler einsetzen, die Fähigkeiten von Junior-Analysten verbessern, ein schnelleres Onboarding gewährleisten und den Zeitaufwand für Aufgaben mit geringerem Wert reduzieren, sodass sich das Team auf wertvollere Aktivitäten wie die Problembehebung konzentrieren konnte.

- **Unkompliziertere Verwaltung** – Kunden gaben an, dass ThreatStream die administrative Komplexität bei der Verwaltung mehrerer Threat Intelligence-Streams und punktueller Sicherheitsprodukte reduziert hat. Sie profitieren von weniger zu verwaltenden Schnittstellen, einfachen Testversionen und der Bereitstellung neuer Premium-Feeds mit einer App-Store-ähnlichen Erfahrung sowie einer integrierten Verwaltung von IOCs. Dadurch sparten Unternehmen Zeit und Komplexität bei der Bereitstellung, Verwaltung und Integration mehrerer Produkte über verschiedene Schnittstellen hinweg.

- **Schnellere Amortisierungszeit** – Die Unternehmen empfanden die Bereitstellung von ThreatStream als schnell und einfach, ebenso wie die Integration mit IOCs und das Hinzufügen oder Entfernen von Premium-Feeds. Dank des starken Partner-Ökosystems und der Software Development Kits (SDKs) konnten Unternehmen die internen und externen Threat Intelligence-Tools und Feeds, die ihren Anforderungen am besten entsprachen, schnell integrieren. Über „Freemium"-Optionen können Kunden Feeds von Business Intelligence-Partnern abonnieren, um ihre Threat Intelligence-Programme besser zu optimieren. Die Beschaffung wurde vereinfacht und Unternehmen hatten das Gefühl, dass sie seit der Implementierung weniger Zeit mit Integrations- und Supportproblemen verbringen. Das bedeutet, dass Unternehmen Sicherheitsstrategien und -tools schneller testen und integrieren konnten. Ein Kunde merkte an: „Anomali spart uns Zeit und Aufwand bei der Beschaffung und Installation von Streams. Zudem wissen wir, dass die Lösung ohne komplizierte Integration bereits eingerichtet und einsatzbereit ist. Das spart uns, je nach Komplexität Stunden bis Tage."

  ***„Bisher habe ich Stunden damit verbracht, den Kontext zu untersuchen und zu erfassen. Mit Anomali kann ich einfach die URL eingeben oder ein Pivoting mit Lens durchführen und weiß genau, welche Eindämmungsmaßnahmen ich umsetzen muss."***

- **Rationalisierter Workflow** – Anomali half Unternehmen, ihre Sicherheitsabläufe zu optimieren, um den Zeitaufwand für Untersuchungen durch SOC-, CTI- und Vorfallsreaktionsteams über eine zentrale Plattform zu reduzieren. Vereinfachte Workflows, die enge Integration in andere Sicherheits-Feeds und -Lösungen sowie die Anreicherung von Threat Intelligence und Recherchen minimierten den Zeitaufwand für Sicherheitsteams in allen Aspekte der Bedrohungserkennung, -untersuchung und -reaktion.

- **Automatisierung von Aufgaben** – Benutzer gaben an, nach der Implementierung von ThreatStream deutlich weniger manuelle Aufgaben ausführen zu müssen. Anomali automatisierte viele der repetitiven oder zeitaufwändigen Aufgaben, die einen Großteil des Tages vieler Sicherheitsanalysten verschlingen, einschließlich der Normalisierung von Quellen, der Untersuchung und des Verständnisses des Risikoprofils, der Formatierung und Anreicherung von Threat Intelligence und der Erstellung von Berichten. Anomali orchestrierte außerdem viele der Konfigurations-, Integrations- und bidirektionalen sicherheitsbezogenen Aufgaben zwischen Sicherheitslösungen wie SIEMs, Firewalls und Netzwerkgeräten. Bei einem Kunden verarbeitete Anomali Match Protokollinformationen, die nach Einschätzung der Anomali-Benutzer mit anderen Lösungen bis zu 2,5 Mal mehr Mitarbeiter erfordert hätten: „Nur vier Leute haben die Arbeit erledigt, die sonst vielleicht zehn Personen beschäftigt hätte."

  ***„Eine Anfrage, für die wir im Normalfall SIEM-Protokolle von Bandlaufwerken wiederherstellen mussten und deren Beantwortung mehr als 2 Wochen gedauert hätte, ließ sich mit Anomali Match in weniger als einer Stunde erledigen."***

- **Weniger Zeitverschwendung** – Unternehmen, die Anomali eingesetzt hatten, mussten sich nun mit weitaus weniger Fehlalarmen auseinandersetzen und litten deutlich seltener unter „Alarmermüdung“. Benutzer waren der Meinung, dass ihnen dadurch mehr Zeit blieb, sich auf wichtigere Aufgaben zu konzentrieren. Die Automatisierung von Threat Intelligence-Recherche und -Anreicherung führt zu einem geringeren Zeitaufwand für die Erfassung der Situation, einem geringeren Risiko für sich wiederholende Aufgaben und einem geringeren Fehlerbehebungsaufwand aufgrund menschlicher Fehler. Ein Benutzer gab Folgendes an: „Ich muss nicht mehr Informationen hinterherjagen und erstmal herausfinden, was ein Indikator bedeutet oder warum er schlecht ist, was früher etwa 90 % meiner Arbeit ausmachte.“

## Verbesserte Sicherheitseffektivität und geringeres Risiko für das Unternehmen

Anomali arbeitet mit anderen Sicherheitsprodukten zusammen, um eine optimierte Lösung zu schaffen, die IOCs effektiver identifiziert, Fehlalarme reduziert und Kontext und Einblicke bietet, um Bedrohungen besser zu verstehen und zu beheben. Kunden, mit denen wir gesprochen haben, sind der Meinung, dass Anomali die Gesamteffektivität ihrer Sicherheitsabläufe erheblich erhöht hat. Einige Kunden berichten, dass Anomali ihre Effektivität bei der Erkennung und Behebung von Bedrohungen um bis zu 90 % verbesserte.

- **Schnellere Einblicke** – Endbenutzer hatten das Gefühl, dass Anomali in Kombination mit anderen Tools ihnen deutlich schnellere Einblicke verschafft hat. Kunden berichteten von einer höheren Feed-Flexibilität, einer höheren Transparenz und mit IOC angereicherten Daten, die dazu beitrugen, die Zeit bis zur Erkennung von Bedrohungen zu verkürzen, was letztendlich zu einer verbesserten mittleren Reaktionszeit (MTTR) und einer besseren Behebung führte. Ein Benutzer berichtete, dass er mit Anomali Match die MTTR von mehr als neun Tagen auf nur zehn Minuten für die Betrachtung der IOCs verkürzen konnte. Die Kunden waren sich einig, dass sie mit Anomali größere Mengen und eine breitere Vielzahl an Bedrohungen und IOCs in kürzerer Zeit erkennen, untersuchen und beheben konnten.

***„Ohne Anomali hätten wir so viele Bedrohungen übersehen oder es hätte viel länger gedauert, um sie zu identifizieren und zu beheben. Anomali ist zu einem wichtigen Teil unserer Sicherheitsüberwachung geworden.“***

- **Durch maschinelles Lernen unterstützte Informationen** – Anomali verwendet Algorithmen für maschinelles Lernen, um den Bedrohungskontext anzureichern, Bedrohungen zu priorisieren und historische Ereignisse auszuwerten. Dadurch erhalten Unternehmen ganzheitlichere, effektivere und zeitnahe Informationen, als dies durch stundenlange menschliche Eingriffe möglich wäre. Die Teams berichteten, dass sie so Bedrohungen schneller identifizieren, untersuchen und auf sie reagieren konnten, und ihre Sicherheitsteams nun weitaus effektiver als zuvor seien. Ein Benutzer merkte an: „Dank Anomali können wir jetzt erstmals exponentiell wachsen und Informationen aus dem Internet kontrolliert erfassen und integrieren, sodass wir nicht mehr durch menschliche Faktoren eingeschränkt werden.“

- **Umfassender Verarbeitung von Threat Intelligence** – Mit ThreatStream konnten Teams eine größere Menge und Vielfalt an Threat Intelligence verarbeiten als zuvor. Sie konnten mehr externe Feeds testen und verwalten und diese nahezu in Echtzeit mit Bedrohungsanalysen und intern erstellter Threat Intelligence kombinieren. Die Fähigkeit, ein Profil von Bedrohungsakteurs zu erstellen und einen Akteur über einen längeren Zeitraum zu verfolgen, erwies sich als äußerst wertvoll. Ein Kunde sagte: „Es gibt weitere TIPs, die eine Erfassung von Feeds und Korrelation bieten, aber Anomali liefert uns einen echten Mehrwert, indem wir damit auch unsere eigenen Daten integrieren können.“

- **Effektivere Sicherheitsreaktion** – Alle Benutzer, mit denen wir gesprochen haben, sind sich einig, dass Anomali sie bei der Reaktion auf Sicherheitsbedrohungen unterstützt. ThreatStream kann nicht nur eine größere Menge an Informationen verarbeiten und Bedrohungen schneller identifizieren, sondern auch traditionelle „Fleißarbeiten" von Analysten durch automatisierte Aktualisierung von Feeds, Korrelation von Indikatoren und der Analyse von Sicherheitsverstößen reduzieren, sodass sie Zusammenhänge besser nachvollziehen können und im Vorfeld Vorschläge für Recherche- und Abhilfemaßnahmen erhalten. Ein Kunde sagte: „Anomali gibt nicht nur an, dass eine IP-Adresse schädlich ist, sondern informiert mich auch, warum sie schädlich ist, welche Aktivität ausgeführt wurde und welche Schritte ich ergreifen sollte."

***„Statt jede einzelne E-Mail oder jede IP-Adressen einzeln zu überprüfen, erhalte ich einen globalen Überblick und kann sofort erkennen, dass 90 % der Aktivitäten mit einem bestimmten Verstoß, Indikatortyp oder Tag zusammenhängen."***

## Bedeutung

Das Ziel jedes Unternehmens besteht darin, eine effektivere Sicherheit für das Geschäft zu gewährleisten.

Kunden von Anomali schätzten, dass Anomali bis zu 90 % effektiver bei der Erkennung und Behebung von Bedrohungen ist. Ein Unternehmen meldete, dass es mit Anomali den Diebstahl von Benutzerguthaben im Wert von über 400.000 US-Dollar durch eine proaktive Identifizierung und Umsetzung funktionsübergreifender Maßnahmen zum Schutz von Benutzerkonten vor einem Sicherheitsverstoß vermeiden konnte.

- **Fundiertere Entscheidungen in Bezug auf die Sicherheit** – Benutzer gaben an, dass Anomali eine Reihe einfacher und dennoch effektiver Dashboards bereitstellt, um Teams dabei zu helfen, Bedrohungen zu visualisieren, Entscheidungen zu priorisieren und Informationen auf nützliche Weise mit anderen Teams zu teilen. Die integrierten Sandboxing-Funktionen, die Verfügbarkeit von Expertenteams für Threat Intelligence von Anomali und die Möglichkeit, Informationen mit Kollegen auszutauschen, haben dazu beigetragen, zusätzliche Informationen bereitzustellen, die für interne Entscheidungen nützlich waren. Die Benutzer waren sich einig, dass sie mit Anomali fundiertere und zeitnahe Entscheidungen treffen und so das Risiko für das Unternehmen reduzieren können.

### Höhere SecOps-Produktivität und -Zufriedenheit

Alle Unternehmen, mit denen wir gesprochen haben, hatten das Gefühl, dass Anomali ihnen dabei geholfen hat, ihr Unternehmen zu transformieren, um ihre vorhandenen Ressourcen optimal zu nutzen. Sie berichteten, dass ihre Teams jetzt viel produktiver, aber auch mit ihren Rollen zufriedener sind und dass das Unternehmen besser mit den einzelnen Geschäftsbereichen und seinen Kollegen kommunizieren kann.

- **Produktivere Sicherheitsexperten** – Mit ThreatStream können alle produktiver arbeiten und sich auf Bereiche konzentrieren, in denen sie den größten Nutzen liefern. Die Teams berichteten, dass weniger erfahrene Mitglieder schneller eingearbeitet werden können, schneller lernen und schneller mehr Erfahrung in der Ausübung höherwertigere Aufgaben sammeln. Dies ist sowohl für das Unternehmen als auch für die Karriere der einzelnen Mitarbeiter von Vorteil.

***„Mit Anomali können zwei Personen die Arbeit ausführen, wo woanders ein sehr großes Team arbeitet – und wir sind dabei auch noch bessebesser."***

- **Zufriedeneres Sicherheitsteam** – Endbenutzer gaben an, dass Anomali ihnen hilft, bessere Arbeit zu leisten, nachts besser zu schlafen, schneller in ihrer Karriere voranzukommen, da sie das Gefühl haben, einen besseren Beitrag zum Schutz des Unternehmens geleistet zu haben. Insgesamt berichteten sie, dass sie ihre Arbeit jetzt als positivere Erfahrung wahrnehmen. Unternehmen waren der Meinung, dass sie mit Anomali ein stärkeres Team aufbauen und eine Umgebung schaffen konnten, die Mitarbeiter in einem Bereich bindet, in dem Talentknappheit ein dauerhaftes Problem darstellt.

- Verbesserte Geschäftsprozesse – Kunden gaben an, dass sie mit ThreatStream einfacher Informationen über Sicherheitsorganisationen hinweg auszutauschen und Diskussionen zwischen Sicherheitsteams, Geschäftseinheiten und Endnutzern wesentlich effektiver gestalten können. Ein Unternehmen erklärte: „Wir haben einige wirklich coole Prozesse rund um Anomali entwickelt. Wir haben mit unserem Fraud-Team, unserem Red Team (Testteam) und dem Threat Intelligence-Team zusammengearbeitet. Sogar unser Compliance-Team wurde involviert und weiß jetzt, was wir aktiv sehen." Kunden hatten das Gefühl, ihre Benutzer besser ausbilden zu können, da sie ihnen genau und auf verständliche Weise zeigen konnten, welche Bedrohungen beobachtet wurden. Nach eigenen Angaben hatten sie vor Anomali keine Möglichkeit, mit dem Geschäftsbereich zu kommunizieren, ohne stundenlang detaillierte Erklärungen zu verfassen.

***„Anomali verbessert einige unserer bestehenden Prozesse, eröffnet uns aber auch neue Wege, weil wir jetzt effektiver mit ihnen interagieren können."***

- Bessere Zusammenarbeit mit Kollegen – Kunden waren der Meinung, dass Anomali ihnen die Möglichkeit gab, intern gesammelte Threat Intelligence und Vorschläge zur Behebung auf vertrauenswürdige Weise an Peergruppen weiterzugeben. Dadurch können die Unternehmen einen Beitrag zu ihrer Peergruppe leisten oder diese sogar anführen. Gleichzeitig kann die Peergroup so Bedrohungen effektiver erkennen und beheben und wertvolle Zeit sparen, da Untersuchungen, die andere bereits durchgeführt haben, nicht wiederholt werden müssen. Ein Kunde sagte: „Die Fähigkeit, Informationen mit anderen Gruppen zu teilen, war extrem hilfreich ...Wir müssen nicht mehr so tief graben oder das Problem selbst durchmachen, weil wir in der Lage sind, Informationen auszutauschen."

## ESG-Analyse

ESG nutzte aus den vom Anbieter bereitgestellten Materialien, öffentlichen und Branchenkenntnissen über Wirtschaftlichkeit und Technologien sowie den Ergebnissen von Kundeninterviews erfasste Informationen, um ein ROI-Modell über drei Jahre zu erstellen und so die Kosten und Vorteile der Implementierung von Anomali ThreatStream, Match und Lens im Vergleich zum weiteren Betrieb ohne eine Plattform zur Bedrohungserkennung zu ermitteln. Die von ESG durchgeführten Interviews mit Kunden von Anomali zusammen mit Erfahrungen und Fachkenntnissen in der Wirtschaftsmodellierung und technischen Betrachtung von Anomali-Produkten dienten als Grundlage unseres modellierten Szenarios.

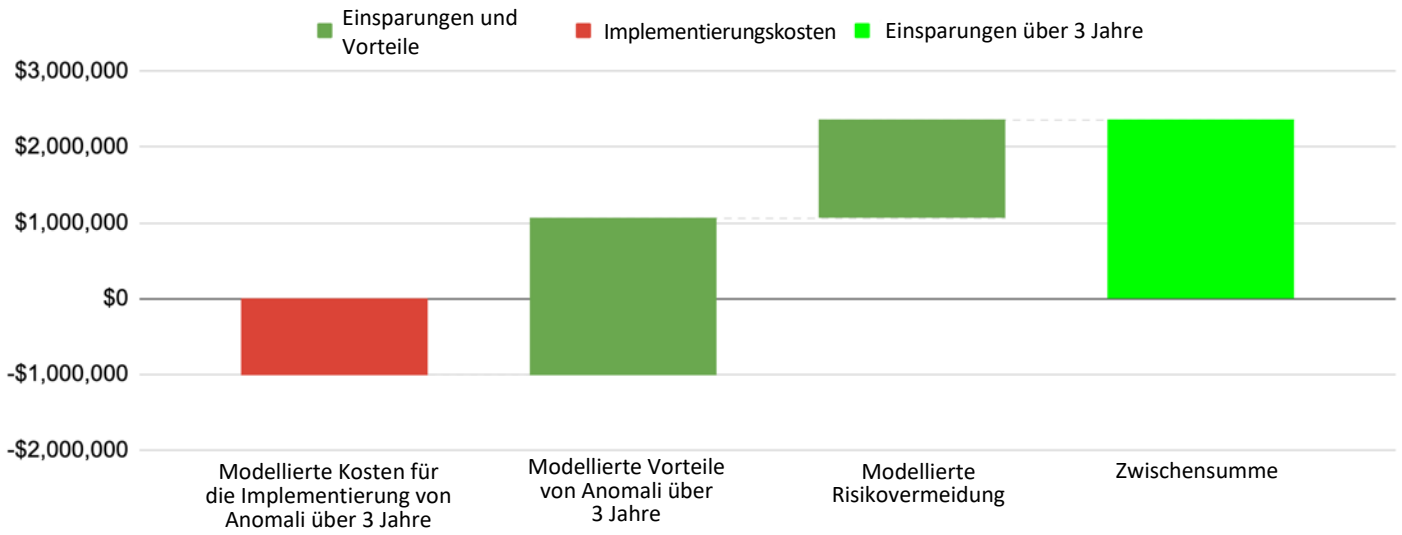
Das von ESG modellierte Unternehmen bestand aus einem Team von zehn Threat Intelligence-Analysten mit unterschiedlicher Erfahrung in der Bereitstellung von Sicherheitsdiensten für ein Kundenunternehmen mit 1.500 Mitarbeitern. ESG berücksichtigt die erwarteten Kosten für Installation, Implementierung und Schulung von Mitarbeitern in der Verwendung der Anomali-Plattform, jährliche Abonnementkosten, Hardwareknoten, Infrastrukturkosten sowie Support und Wartung über einen Zeitraum von drei Jahren.

Im Hinblick auf die Vorteile modellierte ESG die erwarteten vermiedenen Kosten oder Vorteile einer verbesserten Produktivität im gesamten Sicherheitsteam basierend auf einer erwarteten Verbesserung von 20 % bis 70 % bei Aufgaben im Zusammenhang mit der Verwaltung und Pflege von Feeds, der Durchführung und Berichterstattung der Untersuchungsergebnisse und der Integration in andere Sicherheitssysteme, Weitergabe von Bedrohungsinformationen an verbundene Organisationen sowie Weitergabe und Berichterstattung von Informationen innerhalb des Unternehmens. ESG schätzte konservativ, dass nur 35 % der Gesamtarbeitszeit des Sicherheitsteams für diese Aufgaben aufgewendet werden. Das ESG-Modell zu einer Produktivitätssteigerung von 58 % bei der Durchführung dieser Aufgaben und zu Einsparungen von insgesamt 969.000 USD über drei Jahre. Diese Einsparungen zeigen sich als Arbeitsstunden, die jetzt für zusätzliche sicherheitsrelevante Aufgaben verfügbar sind und vor der Implementierung von Anomali nicht vorhanden waren.

Zudem prognostizierten die ESG-Modelle Einsparungen durch eine 40%ige Reduzierung von Fehlalarmen (608.000 USD), einen Mehrwert der von Anomali angebotenen Sicherheitsprodukte (Sandboxing, Freemium- und Premium-Threat Intelligence-Feeds, reaktionsschneller Anomali-Support und Schulungen über die Anomali University) im Gesamtwert von 452.000 USD. Weitere Kosteneinsparungen ergaben sich durch den Wegfall von Professional Services, Schulungen und Zertifizierungen sowie eine vereinfachte Beschaffung und Integration (53.000 USD).

ESG modellierte auch die Risikovermeidung durch eine geringere Wahrscheinlichkeit einer Datenschutzverletzung aufgrund einer erhöhten Wahrscheinlichkeit einer früheren Entdeckung, einer erhöhten Gesamtwirksamkeit und schnelleren Behebung von Problemen, sowie geringere erwartete Kosten für eine Datenschutzverletzung, da automatisierte Maßnahmen schneller und effektiver erkannt und ergriffen werden können. Die von ESG angegebenen Wahrscheinlichkeits- und Kostenannahmen für einen Datenschutzvorfall basieren auf öffentlich verfügbaren Daten, die vom Ponemon Institute veröffentlicht wurden. Die ESG-Analyse ergab, dass Anomali das Risiko für ein Unternehmen senken und so erwartete Kosten einer Datenschutzverletzung über drei Jahre in Höhe von bis zu 1.292 Mio. USD vermeiden kann. Die Ergebnisse der von ESG modellierten Kosten-Nutzen-Analyse sind in Abbildung 3 dargestellt.

**Abbildung 3: Ergebnisse der Kosten-Nutzen-Analyse von ESG für die Threat Intelligence-Plattform von Anomali über drei Jahre**




*Quelle: Enterprise Strategy Group*

## Bedeutung der Zahlen

Die von ESG modellierte Analyse prognostizierte erhebliche Einsparungen und Vorteile für das Modellunternehmen. Obwohl ein modelliertes Szenario niemals die Wirtschaftlichkeit jeder Bereitstellung präzise darstellen kann, ermutigt ESG Unternehmen, ihre eigenen Analysen durchzuführen, um zu sehen, wie viel sie durch die Lösung sparen können. ESG schlägt vor, die folgenden Kosten berücksichtigen, die auch in unserer Analyse enthalten waren:

- **Kosten für die Implementierung der Anomali-Lösung** – Beinhaltet Kosten für Anomali-Abonnements, VZÄ und Professional Service-Arbeitsstunden für Bereitstellung, Test und Schulung der Lösung, Appliances für die Ausführung von Anomali, Strom-/Kühlungs-/Raumkosten sowie Support und Wartung der Hardware.
- **Wert der enthaltenen Threat Intelligence-Produkte** – Bezieht sich auf den monetären Wert der entsprechenden Lösungen für Sandboxing, TIP-Informationen aus Freemium- und Premium-Threat Intelligence-Feeds, Schulungen an der Anomali University, Expertenunterstützung usw.
- **Vermeidung von Kosten für die Handhabung von Falschmeldungen** – ESG ging von 50 Falschmeldungen pro Tag pro Analytiker, 2 Minuten Bearbeitungszeit pro Falschmeldung und 40 % weniger Falschmeldungen mit Anomali aus.
- **Produktivitätssteigerung bei Sicherheitsvorgängen** – Die detaillierten und konservativen Modelle von ESG berücksichtigten die erwartete Anzahl an Arbeitsstunden vor Anomali im Vergleich zur erwarteten Verbesserung bei Feed-Erfassung (70 % Verbesserung), Feed-Management und -Anpassung (70 % Verbesserung), Untersuchungen und Berichterstattung (60 % Verbesserung), Integration in betriebliche Sicherheitssysteme (20 % Verbesserung), externer Zusammenarbeit (50 % Verbesserung) und interne Weitergabe und Betriebsabläufe (60 % Verbesserung).

- Quantifizierung des reduzierten Risikos – ESG berechnete ein geringeres Risiko von Datenschutzverletzungen im Vergleich zum Branchendurchschnitt, das proportional zu einer Verbesserung der Erkennung und Reaktion um 70 % ist, sowie geringere erwartete Kosten für Datenschutzverletzungen bei automatisierten Systemen (beide Zahlen wurden vom Ponemon Institute gemeldet).

## Die übergreifende Erkenntnis

Die Stärkung der Cybersicherheit wird von ESG-Forschungsteilnehmern seit mehreren Jahren durchgehend als führender Geschäftsfaktor für Technologieausgaben genannt. Während Unternehmen ihre Teams weiter ausbauen, organisieren und in neue Lösungen investieren, wird eines deutlich: Das Problem ist nicht der Mangel an Sicherheitstools und Threat Intelligence, sondern ein Mangel an personellen Ressourcen, um diese effektiv zu verwalten, zu interpretieren und basierend auf den Informationen und Warnungen Maßnahmen zu ergreifen. Moderne Sicherheitsorganisationen benötigen eine Threat Intelligence-Plattform, die dazu beitragen kann, den Sicherheitsprozess zu optimieren, sich wiederholende Aufgaben zu automatisieren, KI-gestützte Informationen bereitzustellen und Mitarbeitern zu mehr betrieblicher Effizienz zu verhelfen.

ESG bestätigte, dass Anomali ThreatStream, Match und Lens Kunden eine Plattform bieten, mit der sie ihre Sicherheitsinvestitionen optimal ausschöpfen können. Ihre Sicherheitsteams fühlen sich deutlich befähigter, werden produktiver und können sich auf die wichtigsten Aufgaben konzentrieren. Ihre Investitionen in SIEM und andere Sicherheitsprodukte lassen sich einfach integrieren und erweitern, um einen noch größeren Mehrwert zu schaffen. Zudem lassen sich Threat Intelligence-Feeds problemlos bewerten, erwerben und integrieren. Kunden berichteten von einer deutlich besseren Transparenz und einer größeren Fähigkeit, Threat Intelligence intern mit anderen Geschäftsbereichen des Unternehmens und extern mit Kollegen und anderen Sicherheitsorganisationen zu teilen.

Die von ESG modellierte Kosten-Nutzen-Analyse zeigt, wie ein Unternehmen, das Anomali implementiert, durch eine verbesserte Produktivität des Sicherheitsteams, einen Mehrwert durch integrierte Threat Intelligence-Produkte und die Vermeidung von Risiken Einsparungen erwarten kann. Die wichtigsten Annahmen im Modell basierten auf der Betrachtung von ESG anhand von Interviews mit Kunden von Anomali. Im ESG-Modell wurden erwartete Gesamteinsparungen von bis zu 93.000 USD pro Monat und eine erwartete Investitionsrendite (ROI) von 233 % berechnet.

Anomali konkurriert nicht mit den vorhandenen Sicherheitsprodukten eines Unternehmens und zielt auch nicht darauf ab, die Arbeitsweise von Teams zu verändern. Stattdessen dient Anomali zur Operationalisierung und Anreicherung von Threat Intelligence, Tools und Lösungen, um Sicherheitsteams effizienter zu gestalten und die Sicherheitsdiskussion auf andere Bereiche des Unternehmens auszuweiten. Jedes Unternehmen, mit dem ESG gesprochen hat, hatte das Gefühl, nach der Implementierung mit einem kleineren Team viel mehr zu erreichen und seinen Betrieb auf ein Maß skalieren zu können, das allein durch Personalkraft realistisch nicht möglich wäre. Einige von ihnen haben Anomali sogar in neue Stellen mitgebracht: „Ich hatte Anomali in einer früheren Position verwendet. Als ich hierher kam, sagte ich, dass wir unsere Ziele ohne Anomali nicht erreichen können.“ Analysten erkennen, dass eine solche Aussage eindeutig auf eine transformative Technologie schließen lässt. Wenn Sie Ihre Sicherheitsabläufe transformieren und optimieren und Ihre Threat Intelligence optimal nutzen möchten, empfiehlt ESG, dass Sie sich an Anomali wenden, um zu erfahren, ob diese Threat Intelligence-Plattform für Ihr Team geeignet ist.



**Enterprise Strategy Group** ist ein Unternehmen für IT-Analysen, Forschung, Validierung und Strategien, das Marktinformationen und umsetzbare Erkenntnisse für die globale IT-Community bereitstellt.