Validação Econômica da ESG

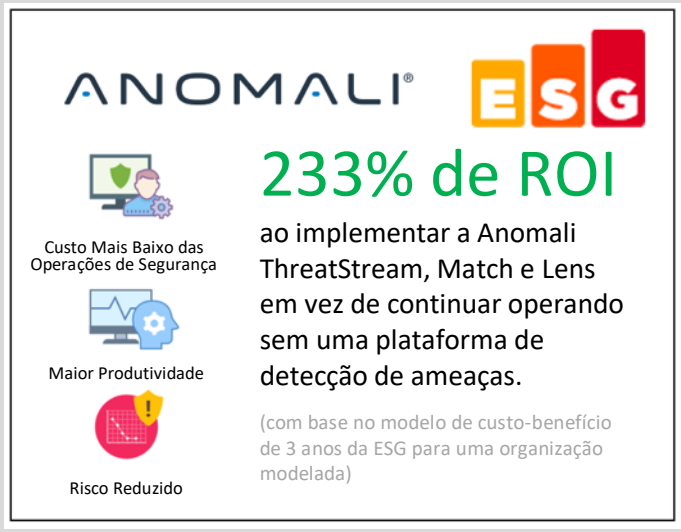
Análise dos benefícios econômicos da plataforma de inteligência contra ameaças da Anomali

Por Aviv Kaufmann e Alex Arcilla, Analistas de Validação Sênior

Julho de 2020

Resumo Executivo

Nunca antes foi tão importante para as empresas capacitar com eficiência uma força de trabalho cada vez mais remota com acesso a aplicativos e recursos em várias regiões geográficas, redes e dispositivos. As empresas foram forçadas a implementar rapidamente soluções, relaxar restrições e políticas, e remover barreiras de entrada, colocando uma carga ainda maior sobre suas equipes de segurança para operar de forma eficaz e eficiente, protegendo a organização e seus ativos. As equipes de segurança devem trabalhar de forma mais inteligente e eficiente para incorporar o máximo possível de informações de inteligência contra ameaças para identificar e remediar as ameaças.



A ESG validou que o conjunto de produtos de segurança orientados por inteligência da Anomali ajudou a simplificar as operações de segurança, automatizar fluxos de trabalho, reduzir falsos positivos, melhorar a colaboração interna e externa, e reduzir o tempo de detecção e correção. A ESG validou os benefícios que os clientes da Anomali haviam experimentado por meio de diversas entrevistas e utilizou as informações para criar um cenário modelado que mostra como uma organização pode economizar US$ 93 mil por mês por meio de uma maior produtividade, redução de risco e geração de valor com produtos incluídos. O modelo da ESG prevê um retorno do investimento de 233% e um período de retorno de apenas 11 meses para uma organização com uma equipe de segurança de 10 pessoas optando por implementar a Anomali em vez de continuar operando sem uma plataforma de inteligência contra ameaças.

Introdução

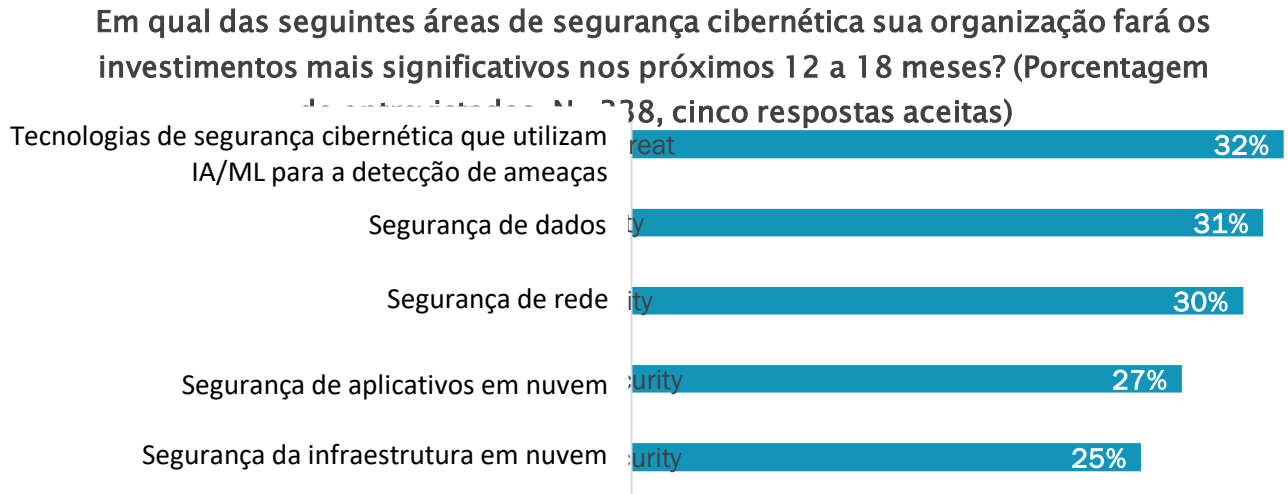
Esta análise econômica feita pela ESG, enfocou nos benefícios quantitativos e qualitativos que as organizações podem esperar capacitando suas equipes de operações de segurança com o conjunto de produtos de segurança orientados por inteligência da Anomali para analisar, detectar, investigar e responder a ameaças potenciais de forma mais rápida e eficiente. Esses produtos incluem a Anomali ThreatStream (plataforma de inteligência contra ameaças, conhecido em inglês como Threat Intelligence Platform ou simplesmente pela sigla "TIP"), o Anomali Match (detecção de ameaças) e o Anomali Lens (conhecimento sobre ameaças).

Desafios

A segurança cibernética é uma das principais preocupações de qualquer empresa. As equipes de operações de segurança evoluíram de uma resposta reativa a alertas e "tapando buracos" para alavancar proativamente os volumes exponencialmente crescentes de inteligência contra ameaças para permanecerem melhor protegidas. A pesquisa da ESG mostra que 62% das organizações esperam aumentar os gastos com serviços de segurança virtual nos próximos 12 a 18 meses.[1] A disponibilidade de tantas fontes de inteligência contra ameaças tem colocado uma carga sobre os profissionais de segurança, que se esforçam para encontrar maneiras de incorporar, gerenciar, analisar e tomar medidas apropriadas com base nessa inteligência. Essas organizações simplesmente nunca terão os recursos humanos para utilizar toda a inteligência que está disponível para elas. A automação e a análise são necessárias para priorizar e extrair efetivamente a agulha da inteligência acionável do palheiro de inteligência contra ameaças que não para de crescer.

Muitas organizações maiores implantaram, com o passar do tempo, um amplo conjunto de tecnologias de segurança e aumentaram sua equipe de profissionais de segurança para dar suporte a essas soluções. A implementação de um SOC (Security Operations Center, centro de operações de segurança) trouxe o conhecimento e a experiência combinados dessa equipe para uma operação comum que está melhor equipada para lidar com a detecção e resposta contra ameaças. No entanto, os especialistas em segurança são recursos limitados, difíceis e caros de serem encontrados, treinados e preservados. Da mesma forma, a implantação de um SIEM (Security Information and Event Management, sistema de gerenciamento de eventos e informações de segurança) prometeu detectar ameaças de forma mais eficaz, consolidando a inteligência e as informações geradas por vários servidores e dispositivos, mas os SIEMs têm uma limitação quanto ao volume de dados que podem ser pesquisados e gerenciados com eficiência, produzindo muitos falsos positivos que exigem a atenção da equipe, limitando a visibilidade da organização contra ameaças. Portanto, não surpreende que as organizações estejam buscando ajudar suas equipes de SOC sobrecarregadas a identificar com maior precisão as ameaças reais e acelerar sua resposta contra essas ameaças. A pesquisa da ESG identifica o uso de tecnologias que empregam IA (artificial intelligence, inteligência artificial) e ML (machine learning, aprendizado de máquina) para detecção de ameaças como a área de segurança cibernética mais frequentemente citada, em que as organizações farão os investimentos mais significativos durante 2020 (ver Figura 1).

Figura 1. As 5 Principais Prioridades de Investimento em Segurança Cibernética em 2020



[1] Fonte: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, janeiro de 2020. Todas as referências e gráficos da pesquisa da ESG nesta validação econômica foram extraídas deste conjunto de resultados de pesquisa principal.

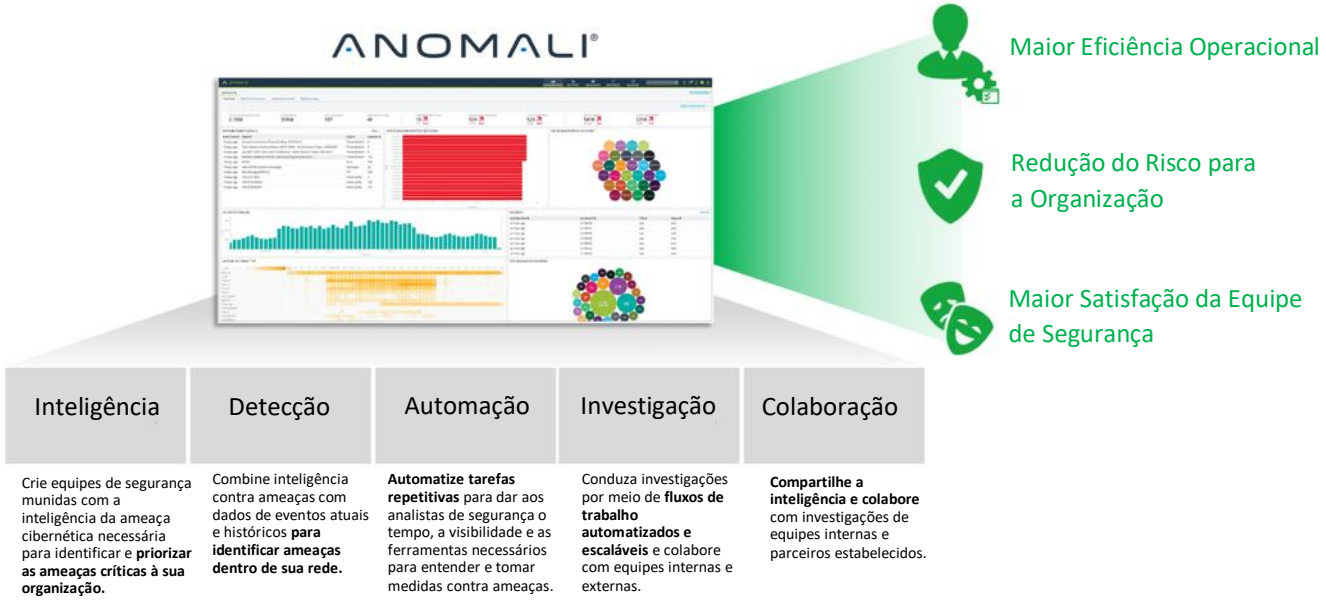
Fonte: Enterprise Strategy Group

Embora a disponibilidade de grandes volumes de inteligência contra ameaças e telemetria de sistemas cumpra a promessa de melhorar a segurança, uma proteção mais eficaz só pode ser alcançada quando as organizações são mais capazes de liberar e otimizar a comunicação entre seus recursos mais valiosos, que são o seu SOC e a equipe de inteligência contra ameaças cibernéticas.

A Solução da Anomali

A Anomali oferece um conjunto de produtos de segurança orientados por inteligência que proporciona visibilidade inigualável das ameaças, detecção acelerada, resposta mais rápida e maior produtividade. Os produtos da Anomali ajudam as organizações a automatizar a coleta, o gerenciamento e a implantação de vários fluxos internos e externos de inteligência contra ameaças, filtrar falsos positivos, identificar ameaças em seus ambientes e operar com mais eficiência para se concentrar nas necessidades de segurança mais importantes.

Figura 2. A Plataforma de Inteligência Contra Ameaças da Anomali



Fonte: Enterprise Strategy Group

A Anomali pode ser implantada na nuvem, no local ou por air gap (no local, mas desconectada de dados públicos). A plataforma consiste em três produtos principais: A Anomali ThreatStream, o Anomali Match e o Anomali Lens.

Anomali ThreatStream – Unifica dados e informações sobre ameaças em inteligência de alta fidelidade, dissemina-os automaticamente para os controles de segurança e integra um conjunto de ferramentas de pesquisa para dar suporte a investigações contra ameaças eficientes. A ThreatStream automatiza a coleta de dados de inteligência contra ameaças de centenas de fontes externas e internas, incluindo inteligência contra ameaças de código-fonte aberto, feeds de ameaças comerciais, inteligência compartilhada e inteligência interna de investigações, detonações de sandbox etc. O produto normaliza os vários feeds e remove indicadores duplicados para criar uma taxonomia comum, potencializando algoritmos de aprendizagem de máquina para remover falsos positivos, enriquecer os dados e pontuar os riscos com inteligência visando a seriedade e confiança. Em seguida, a ThreatStream operacionaliza a inteligência por meio da distribuição automatizada de indicadores de ameaças legíveis por máquina para controles de segurança (por exemplo, SIEM, firewall, EDR, IPS, PLANE etc.). O produto também fornece ferramentas para analistas e equipes SOC fazerem investigações baseadas em modelos usando os frameworks Diamond, Kill Chain, STIX, ou MITRE ATT&CK. O workbench de investigações inclui um conjunto completo de fontes de enriquecimento de dados, uma poderosa ferramenta visual de exploração para expansão e

posicionamento de indicadores, detonação integrada de sandbox para malware e URLs de phishing e colaboração, autoria e publicação de boletins de ameaças.

Anomali Match – Automatiza a detecção de ameaças em sua rede, correlacionando continuamente toda a inteligência contra ameaças disponível a todos os seus registros de eventos. O Match realiza isso indexando todos os registros SIEM e outras fontes de eventos para manter um ano ou mais de histórico de dados que é continuamente analisado contra novas e existentes ameaças de inteligência, entregando automaticamente alertas de volta ao SIEM, SOAR, ou sistema de tíquetes para resposta e correção. A perícia em tempo real permite que os analistas rastreiem as evidências de violações do passado retornando ao "paciente zero", caçando ameaças baseadas em agente, vulnerabilidade ou TTP e priorizem respostas baseadas na pontuação de risco e na criticidade dos ativos.

Anomali Lens – Oferece conhecimento de ameaças na ponta dos seus dedos, identificando automaticamente dados de ameaças em qualquer conteúdo da Web usando processamento de linguagem natural (NLP). O Lens faz isso verificando páginas da Web, plataformas de mídia social, o SIEM e outros registros de segurança para identificar IOCs (indicators of compromise, indicadores de comprometimento), agentes de ameaça, famílias de malware e técnicas de ataque. A inteligência contra ameaças identificada pelo Lens é automaticamente associada na estrutura do MITRE ATT&CK e pode ser importada para a Anomali ThreatStream para investigação e análise adicionais ao clique de um botão. O Lens também se integra ao Anomali Match para destacar a inteligência contra ameaças escaneadas presente na rede, proporcionando uma compreensão instantânea do nível de gravidade e do impacto que ele tem no seu ambiente.

Validação Econômica da ESG

A ESG concluiu uma validação econômica quantitativa e uma análise modelada sobre o conjunto de produtos da Anomali.

O processo de validação econômica da ESG é um método comprovado de compreensão, validação, quantificação e modelagem das propostas de valor econômico de um produto ou solução. O processo aproveita as principais competências da ESG em análise do mercado e do setor, pesquisa voltada para o futuro e validação técnica e econômica. A ESG analisou os resultados de estudos de caso existentes e pesquisas de usuários finais, realizando entrevistas detalhadas com usuários finais para entender e quantificar melhor como a Anomali impactou as organizações, particularmente em comparação com a forma como foi operada antes de implantar o Anomali ou experiências anteriores em outras organizações. As descobertas qualitativas e quantitativas foram usadas como base para um modelo simples de ROI, comparando as economias e os benefícios previstos que uma organização modelada poderia esperar em relação ao custo calculado da implantação do Anomali.

Visão Geral Econômica da Anomali

A análise econômica da ESG revelou que os clientes que implantaram o Anomali estavam muito satisfeitos com o produto e acharam que tinham agilizado muito suas operações de segurança, estavam operando com mais eficiência e estavam fazendo um trabalho geral melhor na proteção da organização. A ESG descobriu que a Anomali forneceu a seus clientes economias e benefícios significativos nas seguintes categorias:

- Menor custo operacional das SecOps – As organizações otimizaram significativamente as operações de segurança e fizeram melhor uso de seus recursos de segurança por meio dos recursos de automação e orquestração da Anomali, além de suas ferramentas e recursos de segurança bem projetados e eficazes.
- Eficácia de Segurança Aprimorada e Risco Reduzido para a Organização – As clientes relataram que a Anomali ajudou a aprimorar a equipe de segurança e operacionalizou o processo de segurança, tornando as equipes mais eficazes e reduzindo o tempo para identificar e corrigir problemas de segurança.
- Melhor Produtividade e Satisfação de SecOps – A Anomali ajuda a melhorar a produtividade e a satisfação dos profissionais de segurança, automatizando tarefas repetitivas ou demoradas, dando mais tempo a eles para se

concentrarem em operações de segurança de maior valor. As habilidades são rapidamente melhoradas, a colaboração e a visibilidade são aprimoradas e o valor sinérgico com outros produtos de segurança é ampliado.

Redução do Custo Operacional das Operações de Segurança

A ESG descobriu que as equipes de segurança que implantaram produtos da Anomali relataram que suas operações de segurança foram simplificadas por meio da operacionalização, automação e orquestração. Os usuários relataram economias significativas de tempo ou reduções em várias áreas, incluindo a implantação de novas tecnologias, pesquisa de ameaças, aprimoramento de dados, resposta a falsos positivos e correlação de informações de várias fontes (além de muitas outras áreas). Isso permitiu que as equipes aproveitassem mais de cada analista de segurança, melhorassem os recursos dos analistas juniores, integrassem mais rapidamente e reduzissem o tempo gasto em tarefas de menor valor, permitindo que a equipe se concentrasse nas atividades de maior valor, como a correção.

- Complexidade Administrativa Reduzida – As clientes relataram que a ThreatStream reduziu a complexidade administrativa do gerenciamento de vários fluxos de inteligência contra ameaças de segurança e produtos de segurança pontuais. Existem menos interfaces para gerenciar, testes simples do tipo loja de aplicativos, implantação de novos feeds premium e gerenciamento integrado de IOCs. Isso economizou tempo e complexidade para as organizações implantar, gerenciar e integrar vários produtos usando várias interfaces diferentes.

- Tempo de Retorno do Investimento Mais Rápido – A ThreatStream foi rápida e fácil de implantar para as organizações, assim como a integração com IOCs e adicionar ou remover feeds premium. O sólido ecossistema de parceiros e os SDKs (software development kits, kits de desenvolvimento de software) permitiram que as organizações incorporassem rapidamente as ferramentas e os feeds internos e externos de inteligência contra ameaças que melhor atendem às suas necessidades. As opções "Freemium" (incluídas) permitem que os clientes assinem feeds de parceiros de inteligência comercial para otimizar melhor seus programas de inteligência contra ameaças. A aquisição foi simplificada e as organizações sentiram que gastaram menos tempo lidando com problemas de integração e suporte. Isso significa que as organizações puderam testar e integrar estratégias e ferramentas de segurança mais rapidamente. Um cliente comentou: "A Anomali nos poupa tempo e esforço na aquisição e instalação de fluxos e sabemos que já está configurado e pronto para operar sem necessidade de integração, o que nos poupa de horas a dias, dependendo da complexidade".

"Eu poderia passar horas pesquisando e coletando contexto. Com o Anomali, posso simplesmente digitar a URL ou girar com o Lens para saber exatamente quais devem ser minhas ações de contenção."

- Fluxo de Trabalho Simplificado – A Anomali ajudou as organizações a simplificar seus fluxos de trabalho de segurança para reduzir o tempo gasto em investigações pelas equipes de SOC, CTI e resposta a incidentes reunindo-as em uma única plataforma. Fluxos de trabalho simplificados, integração estreita com outros feeds e soluções de segurança e enriquecimento de inteligência e pesquisa de ameaças, minimizando o tempo gasto pelos membros da equipe de segurança em todos os aspectos de detecção, investigação e resposta de ameaças.

- **Automação de Tarefas** – Os usuários relataram ter que executar significativamente menos tarefas manuais após a implantação da ThreatStream. A Anomali automatizou muitas das tarefas repetitivas ou demoradas que ocupam grande parte do dia de analistas de segurança, incluindo a normalização de fontes, a investigação e a compreensão do perfil de risco, a formatação e o enriquecimento da inteligência contra ameaças e a criação de relatórios. A Anomali também orquestrou muitas das tarefas relacionadas à configuração, integração e segurança bidirecional entre soluções de segurança, como SIEMs, firewalls e dispositivos de rede. O Anomali Match processou informações de registro para um cliente que os usuários da Anomali estimam que poderia ter sido necessárias até 2,5 vezes mais pessoas para realizar: "Temos quatro funcionários fazendo o trabalho que seria feito por dez pessoas."

"Para uma tarefa em que, de outra forma, precisaríamos restaurar os registros SIEM da fita, demoraria mais de 2 semanas para responder a uma solicitação que o Anomali Match nos permitiu fazer em menos de uma hora."

- **Menos Desperdício de Tempo –** As organizações que implantaram o Anomali relataram que agora tinham que lidar com muito menos falsos positivos e sofreram com muito menos "fadiga de alerta". Os usuários sentiram que isso lhes deu tempo adicional para se concentrarem em tarefas mais importantes. A automação da pesquisa e do enriquecimento de inteligência contra ameaças resultou em menos tempo gasto tentando descobrir a situação, um menor risco de ter que repetir tarefas e menos solução de problemas devido a erro humano. Um usuário disse: "Eu não tenho mais que começar a caçar e tentar descobrir o significado de um indicador ou se ele é ruim, o que era cerca de 90% do trabalho que eu tinha que fazer antes".

Maior Eficácia na Segurança e Menor Risco para a Organização

A Anomali trabalha em conjunto com outros produtos de segurança para oferecer uma solução simplificada que é mais eficaz na identificação de IOCs, na redução de falsos positivos e no fornecimento de contexto e percepção para ajudar a entender e corrigir ameaças. Os clientes com quem conversamos acreditam que a Anomali aumentou muito a eficácia geral de suas operações de segurança, com alguns relatos de que eles acreditam que a Anomali os tornou 90% mais eficazes na identificação e correção de ameaças.

- **Tempo de Percepção Mais Rápido** – Os usuários finais sentiram que o Anomali, quando usado em conjunto com suas outras ferramentas, proporcionou a eles um tempo de percepção visivelmente melhor. Os clientes relataram maior agilidade na alimentação, maior visibilidade e dados enriquecidos pelo IOC que ajudaram a acelerar o tempo de conscientização e detecção de ameaças, resultando, em última análise, em MTTR (improved mean time to response, melhor tempo médio de resposta) e correção. Um usuário relatou que o Anomali Match ajudou a impulsionar uma melhoria no MTTR de mais de nove dias para apenas dez minutos para validar IOCs. Os clientes concordaram que a Anomali permitiu detectar, investigar e corrigir um volume e uma variedade maior de ameaças e IOCs em menos tempo.

"Sem a Anomali haveriam diversas ameaças que teriam sido perdidas ou que teriam levado muito mais tempo para serem identificadas e corrigidas. Isso se tornou uma parte crítica do nosso monitoramento de segurança."

- **Inteligência Baseada em Aprendizado de Máquina** – A Anomali usa algoritmos de aprendizado de máquina para fornecer o enriquecimento do contexto de ameaças, ajudar a priorizar ameaças e realizar a avaliação do histórico

de eventos. Isso proporciona às organizações uma inteligência mais global, eficaz e oportuna do que aquela que poderia ser alcançada com horas de esforço humano. As equipes relataram que isso as ajudou a identificar, pesquisar e responder às ameaças muito mais rapidamente e sentiram que agora tinham uma equipe de operações de segurança muito mais eficiente do que antes. Um usuário comentou: "O Anomali simboliza a primeira vez que podemos crescer exponencialmente e gerenciar a capacidade de coletar e incorporar informações da Internet até o ponto em que o humano não é mais o limite".

- Mais Processamento de Inteligência Contra Ameaças – A ThreatStream permitiu que as equipes processassem um volume e uma variedade maior de inteligência contra ameaças do que antes. Eles poderiam testar e gerenciar mais feeds externos, além de combinar com boletins de ameaça em tempo quase real e a inteligência contra ameaças produzida internamente. A capacidade de fazer o perfil de um agente ameaçador e rastreá-lo durante um período de tempo mais longo foi extremamente valiosa. Um cliente declarou: "Existem outros TIPs que fazem coisas, como ingerir com feeds e realizar correlações, mas o Anomali realmente nos proporciona valor ao nos dar a capacidade de consumir nossos próprios dados também".

- Resposta de Segurança Mais Eficaz – Todos os usuários com quem falamos concordaram que a Anomali os ajudou a ser muito mais eficazes na resposta às ameaças contra a segurança. A ThreatStream não só ajudou a processar um volume maior de inteligência e identificar ameaças mais rapidamente, como também reduziu muito o trabalho que os analistas costumavam realizar, automatizando a atualização dos feeds, a correlação de indicadores e a análise de violações para descobrir quais se unem, e sugerindo pesquisas e ações de remediação de frente. Um cliente disse: "Em vez de apenas indicar que um IP está ruim, eu posso ver o porquê o IP está ruim, que atividade estava fazendo e que medidas eu deveria tomar".

"Em vez de verificar cada um desses e-mails ou cada um desses IPs, posso ter essa visão global e ver que 90% deles vêm de uma violação, um tipo de indicador ou um marcador."

- Tomada de decisões mais informada sobre segurança – Os usuários relataram que o Anomali fornece vários painéis simples, porém eficazes, para ajudar as equipes a visualizar ameaças, priorizar a tomada de decisões e compartilhar informações com outras equipes de maneira útil. Os recursos embutidos para sandbox, a disponibilidade das equipes especializadas de apoio de inteligência contra ameaças do Anomali e a capacidade de compartilhar informações com os colegas ajudaram a fornecer informações adicionais que foram úteis na tomada de decisões internas. Os usuários concordaram que o Anomali forneceu a capacidade de tomar decisões mais informadas e pontuais, ajudando a reduzir os riscos para a organização.

Por Que Isto é Importante

É o objetivo de cada organização oferecer uma segurança mais eficaz para a empresa.

Os clientes afirmaram que sentiam que a Anomali era até 90% mais eficaz na identificação e correção de ameaças. Uma organização informou que a Anomali conseguiu evitar mais de US$ 400 mil em créditos de usuários roubados ao identificar e tomar medidas interfuncionais para proteger as contas dos usuários contra uma tentativa de violação.

Melhor Produtividade e Satisfação de SecOps

Todas as organizações com quem falamos sentiram que o Anomali os ajudou a transformar sua organização para aproveitar ao máximo os recursos que tinham. Elas relataram que suas equipes eram muito mais produtivas, mas também que estavam mais satisfeitas em suas funções e que a organização era podia se comunicar mais com a empresa e seus colegas.

- **Profissionais de segurança mais produtivos** – A ThreatStream permite que todos sejam mais produtivos e se concentrem em onde eles agregam mais valor. As equipes relataram que os membros menos experientes foram incluídos e contribuíram mais cedo, aprenderam mais e ganharam experiência mais rapidamente com funções de maior valor. Isso é um benefício para a organização e para a carreira do indivíduo.

"Com o Anomali, podemos ter duas pessoas realizando o trabalho ao qual [nome da organização] dedica uma equipe muito grande e estamos fazendo um trabalho melhor."

- **Equipe de segurança mais satisfeita** – Os usuários finais indicaram que, como o Anomali os ajuda a fazer um trabalho melhor, eles dormem melhor à noite, progridem mais rapidamente em suas carreiras e sentem que realizaram mais para proteger a empresa. No geral, eles relataram que agora veem seu trabalho como uma experiência mais positiva. As organizações sentiram que o Anomali os ajudou a construir uma equipe mais forte e a criar um ambiente onde é mais fácil manter trabalhadores em um campo onde as pessoas se esforçam para encontrar e manter talentos.

- **Processos de negócios aprimorados –** Os clientes declararam que a ThreatStream permitiu que eles compartilhassem melhor as informações entre as organizações de segurança e facilitou discussões muito mais eficazes entre as equipes de segurança, as unidades de negócios e os usuários finais. Uma organização declarou: "Conseguimos construir alguns processos realmente interessantes em torno do Anomali. Trabalhamos com nossa equipe de fraude, nossa equipe vermelha (testes) e nossa equipe de inteligência contra ameaças, até mesmo nossa equipe de conformidade e fornecemos a eles uma visão do que vemos ativamente." Os clientes sentiram que treinaram melhor seus usuários, porque estavam mais capacitados para mostrar quais ameaças eram observadas de uma maneira fácil de consumir. Eles sentiram que sem o Anomali, não tinham como se comunicar com a empresa sem passar horas escrevendo explicações detalhadas.

"O Anomali está melhorando alguns dos processos que já existiam, mas também está construindo novos caminhos para nós, porque somos capazes de falar com eles de forma mais eficaz."

- **Melhor colaboração com colegas** – As clientes sentiram que a Anomali forneceu a eles um meio de compartilhar informações coletadas internamente sobre ameaças e sugestões de correção com grupos de colegas de maneira confiável. Isso permite que a organização contribua ou até mesmo seja reconhecida como líder entre seus parceiros, ao mesmo tempo em que torna o grupo de colegas mais eficaz na identificação e remediação de ameaças e economiza um tempo valioso ao não ter que repetir investigações que outros já realizaram. Um cliente disse: "Ser capaz de compartilhar inteligência com outros grupos tem sido extremamente útil, pois não temos que nos aprofundar tanto ou enfrentar o mesmo problema porque somos capazes de compartilhar inteligência".

Análise da ESG

A ESG aproveitou as informações coletadas por meio do material disponibilizado pelo fornecedor, de conhecimento público e da indústria sobre economia e tecnologias, e os resultados das entrevistas com clientes para criar um modelo de ROI de três anos que compara os custos e benefícios da implementação da Anomali ThreatStream, Match e Lens com a continuidade da operação sem uma plataforma de análise e detecção de ameaças. As entrevistas da ESG com os clientes da Anomali, combinadas com experiência e especialização em modelagem econômica e validação técnica dos produtos Anomali ajudaram a formar a base de nosso cenário modelado.

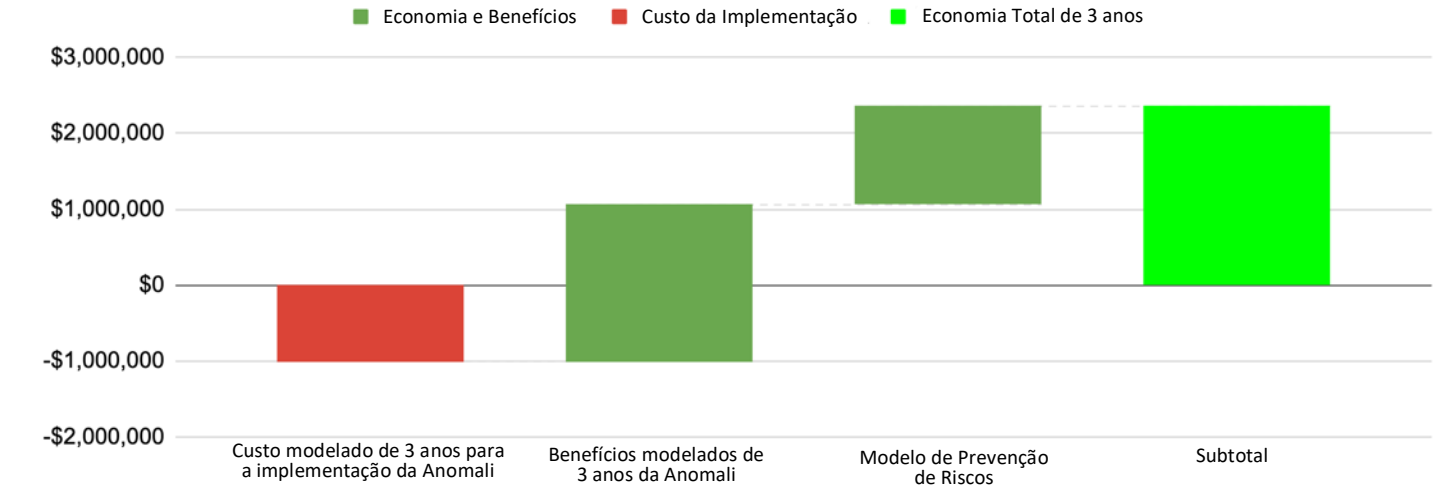
A organização modelada da ESG consistia em uma equipe de 10 analistas de inteligência contra ameaças com diferentes graus de experiência fornecendo serviços de segurança a uma organização com 1.500 funcionários. A ESG considerou o custo esperado para instalar, implementar e treinar funcionários para usar a plataforma Anomali, bem como os custos anuais de assinatura, nós de hardware, custos de infraestrutura, suporte e manutenção durante um período de três anos.

No aspecto dos benefícios, a ESG modelou o custo ou benefício evitado previsto de melhorar a produtividade em toda a equipe de segurança com base em uma melhoria esperada de 20% a 70% nas tarefas relacionadas ao gerenciamento e controle de feeds, execução e relatório dos resultados das investigações, integração com outros sistemas de segurança, compartilhamento de inteligência contra ameaças com organizações colaborativas, e compartilhamento e relatório de inteligência internamente em toda a organização. A ESG estimou, de forma conservadora, que apenas 35% do total de horas de trabalho da equipe de segurança foram gastos na execução dessas tarefas. O modelo da ESG resultou em uma melhoria de 58% na produtividade durante a execução dessas tarefas e uma economia total de US$ 969 mil em três anos. Essas economias se manifestam como horas de trabalho que agora estão disponíveis para tarefas adicionais relacionadas à segurança que não estavam lá antes da Anomali.

Os modelos da ESG pressupõem uma economia de custos graças à redução de 40% nos falsos positivos (US$ 608 mil), valor associado aos produtos de segurança que a Anomali fornece (sandbox, feed de inteligência contra ameaças freemium e premium, suporte responsivo à Anomali e treinamento pela Anomali University) por um valor total de US$ 452 mil e outras economias de custos graças à prevenção de serviços profissionais, treinamento e certificação, além de aquisição e integração simplificadas (US$ 53 mil).

A ESG também modelou a prevenção de riscos proporcionada por uma menor chance de violação de dados com base na maior probabilidade de detecção antecipada, maior eficácia total e correção mais rápida de problemas, além do menor custo esperado de uma violação de dados com base na capacidade de detectar e tomar medidas automatizadas de forma mais rápida e eficaz. As suposições de probabilidade e custo da ESG de uma violação de dados são baseadas em dados publicamente disponíveis divulgados pelo Ponemon Institute. A ESG calculou que a Anomali poderia reduzir o risco para uma organização, evitando até US$ 1,292 milhão em custos esperados de uma violação de dados durante três anos. Os resultados da análise de custo-benefício modelada da ESG são mostrados na Figura 3.

Figura 3. Custo-benefício de Três Anos da Plataforma de Inteligência Contra Ameaças da Anomali



Fonte: Enterprise Strategy Group

O Que os Números Representam

A análise modelada da ESG previa economias e benefícios substanciais para nossa organização modelada. Embora nenhum cenário modelado possa representar com precisão a economia por trás de cada implantação, a ESG incentiva as organizações a realizar sua própria análise para ver o quanto elas podem economizar. A ESG sugere que as organizações consideram os seguintes custos que foram incluídos em nossa análise:

- Custo de Implementação da Solução Anomali – Inclui o custo das assinaturas Anomali; FTE e horas de serviço profissional humano para implantar, testar e treinar a solução; aparelhos para operar o Anomali, custos de energia/refrigeração/espaço físico; e suporte e manutenção no hardware.

- Valor dos Produtos Integrados de Inteligência Contra Ameaças – Valor em dólares atribuído às soluções equivalentes para sandbox, TIP Intel, feeds de inteligência contra ameaças premium e freemium incluídos, treinamento com a Anomali University, suporte especializado etc.

- Custo Evitado de Lidar com Falsos Positivos – A ESG assumiu 50 falsos positivos por dia por analista, 2 minutos gastos por falso positivo e uma redução de 40% em falsos positivos com o Anomali.

- Melhoria da Produtividade para as Operações de Segurança – Os modelos conservadores detalhados da ESG consideraram o número esperado de horas de trabalho gastas antes do Anomali em relação à melhoria esperada para a coleta do feed (melhoria de 70%), gerenciamento de feed e controle (melhoria de 70%), investigações e relatórios (melhoria de 60%), integração com sistemas de segurança operacional (melhoria de 20%), colaboração externa (melhoria de 50%), e compartilhamento interno e operações (melhoria de 60%).

- Quantificação de Risco Reduzido – A ESG calculou um risco reduzido de violação de dados em comparação com a média do setor proporcional a uma melhoria de 70% na detecção e resposta, além de um custo esperado reduzido de violação de dados para sistemas automatizados (ambos os números foram divulgados pelo Ponemon Institute).

A Grande Verdade

O fortalecimento da segurança cibernética tem tido, de forma consistente, o maior número de participantes da pesquisa da ESG na lista de geradores de negócios para gastos com tecnologia por vários anos. À medida que as organizações continuam a desenvolver, organizar e investir em suas equipes com novas soluções, uma coisa se torna clara: o problema não é uma falta de ferramentas de segurança e inteligência contra ameaças, mas uma falta de poder humano para gerenciar, interpretar e tomar medidas com base na inteligência e nos alertas. As organizações de segurança modernas precisam de uma plataforma de inteligência contra ameaças que possa ajudar a simplificar o processo de segurança, automatizar tarefas repetitivas, incluir inteligência orientada por IA e permitir que os recursos humanos se tornem mais eficientes em termos operacionais.

A ESG validou que a Anomali ThreatStream, Match e Lens forneceu aos clientes uma plataforma que os ajuda a extrair o máximo de seus investimentos em segurança. As equipes de segurança são muito mais capacitadas, produtivas e focadas nas tarefas mais importantes; seus investimentos em SIEM e outros produtos de segurança são facilmente integrados e aprimorados para fornecer ainda mais valor; e seus feeds de inteligência contra ameaças estão prontos para avaliar, comprar e integrar. Os clientes relataram uma visibilidade consideravelmente melhor e uma maior capacidade de compartilhar a inteligência contra ameaças internamente com outras divisões da empresa e externamente com seus colegas e organizações de segurança.

A análise de custo-benefício modelada da ESG mostra como uma organização que implementa o Anomali pode esperar economizar por meio de uma maior produtividade da equipe de segurança, valor agregado dos produtos incluídos de inteligência contra ameaças e prevenção de riscos. As principais suposições no modelo foram baseadas na validação da ESG com os clientes da Anomali. O modelo da ESG calculou uma economia total esperada de até US$ 93 mil por mês com um retorno sobre o investimento (ROI) esperado de 233%.

A Anomali não está competindo com os produtos de segurança existentes de uma organização ou procurando mudar funcionalmente a maneira como as equipes precisam operar. Em vez disso, a Anomali trabalha para operacionalizar e aprimorar a inteligência, as ferramentas e as soluções contra ameaças para tornar as equipes de segurança mais eficientes e expandir a discussão sobre segurança para outros setores da empresa. Cada organização com a qual a ESG falou achou que conseguiu muito mais com uma equipe menor e escalou as operações muito além do que era realisticamente possível somente com mão de obra. Alguns haviam até trazido o Anomali com eles para novas funções: "Eu tinha usado o Anomali em um emprego anterior e quando cheguei aqui, disse que se não tivermos o Anomali, não seremos capazes de atingir nossos objetivos." Como analista, você aprende rapidamente que uma afirmação como essa é a marca de uma tecnologia transformadora. Se você está procurando transformar e simplificar suas operações de segurança e extrair o máximo de sua

inteligência contra ameaças, a ESG recomenda que você entre em contato com a Anomali para ver se ela é a plataforma certa de inteligência contra ameaças para sua equipe.

www.esg-global.com contact@esg-global.com Tel.: +1.508.482.0188