paloalto NETWORKS | CORTEX XSIAM®

Guia de compra XSIAM:
Como transformar seu SOC para a era da IA

ÍNDICE

PREENCHENDO O VAZIO:
PREVENÇÃO PROATIVA NOS SOC MODERNOS

O cenário da segurança cibernética evolui rapidamente, apresentando desafios sem precedentes às organizações. Os agentes das ameaças atuais são mais sofisticados e usam técnicas avançadas e IA para contornar as medidas de segurança tradicionais. Como profissional de segurança, é provável que você esteja experimentando em primeira mão como as necessidades do seu centro de operações de segurança (SOC) mudaram drasticamente. As formas antigas de detectar e responder a ameaças não são mais suficientes em uma era em que as violações podem ocorrer em questão de horas — em comparação com 24 horas há apenas um ano[1]— e os requisitos regulamentares estão se tornando cada vez mais rigorosos.

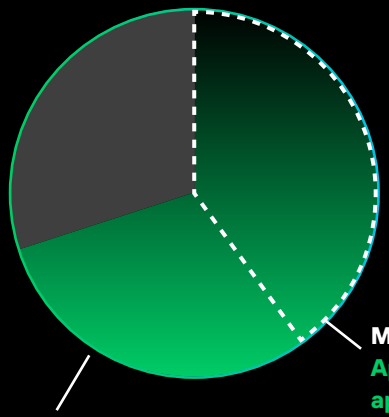
Sempre que ocorre uma violação, a sua equipe de segurança provavelmente pode juntar as peças do que aconteceu após o fato — como o sistema ficou comprometido, quais sistemas estavam envolvidos e quais dados foram exfiltrados. Isso levanta a seguinte questão: Se você tem as informações necessárias para entender um incidente após a violação, por que não pode impedi-la ou detê-la antes que aconteça? Esse vazio entre a análise após o incidente e a prevenção proativa está no centro das necessidades em evolução dos SOCs modernos.

As soluções tradicionais de gerenciamento de eventos e informações de segurança (SIEM), que já foram a base de muitas operações de segurança, estão com dificuldades para acompanhar o ritmo. Você pode se deparar com configurações complexas, integrações demoradas, investimentos pesados em engenharia de detecção e um volume impressionante de alertas.

As táticas de multiextorsão continuam crescendo

O cenário dos ataques de ransomware evoluiu significativamente nos últimos anos, com as táticas de multiextorsão se tornando cada vez mais predominantes.

Roubo de dados em casos de ransomware: [2]



Final de 2022:
Aproximadamente 70% dos casos

Meados de 2021:
Apenas aproximadamente 40% dos casos

Aumento de 75%

na ocorrência de roubo de dados durante ataques de ransomware em um período de 18 meses.

1. *Relatório global de resposta a incidentes da Unit 42 de 2025*, Palo Alto Networks, 25 de fevereiro de 2025.
2. *2023 Unit 42 Ransomware and Extortion Report*, Palo Alto Networks Unit 42, 28 de setembro de 2025.

Esses desafios podem deixar sua equipe sobrecarregada e sua organização vulnerável. A natureza fragmentada de muitas ferramentas de segurança leva a fluxos de trabalho ineficientes, maior carga cognitiva para seus analistas e possível supervisão de ameaças críticas. Além disso, a falta de integração entre funções de segurança proativas (como gerenciamento de vulnerabilidades) e ferramentas reativas dificulta a detecção de ameaças em tempo real e atrasa a resposta a incidentes, colocando sua organização em risco.

Além disso, depender principalmente de regras de correlação estática e de engenharia de detecção extensiva, exacerbadas pelo grande volume de dados, dificulta a identificação de relações expressivas entre os eventos de segurança em seu ambiente, resultando em uma defesa insuficiente contra ameaças. Isso geralmente faz com que os alertas apareçam como pontos de dados desconectados, exigindo esforços de correlação manual por parte da equipe do SOC e levando a altas taxas de falsos positivos. Esse processo desarticulado prejudica a eficácia de sua infraestrutura de segurança e destaca a necessidade de metodologias mais avançadas e adaptáveis de detecção de ameaças.

Impacto quantificado: ROI real da transformação do SOC

Um estudo Total Economic Impact™ da Forrester® Consulting encomendado pela Palo Alto Networks examinou as implantações do Cortex XSIAM® e descobriu que uma organização alcançou resultados mensuráveis e críticos para os negócios:[3]

257% | US$ 5,6 milhões | <6 meses

ROI em 3 anos | Valor presente líquido | Período de retorno

85% | 70% | US$ 3,1 milhões

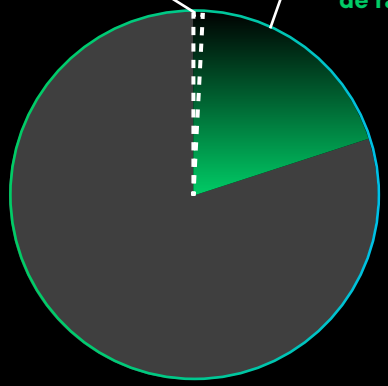
Redução no MTTR | Menos incidentes que exigem investigação do SOC | Economia com a consolidação de ferramentas

As táticas de multiextorsão continuam crescendo (cont.)

Uso de intimidação como tática de extorsão: [4]

Meados de 2021: Presente em menos de 1% dos casos

Final de 2022: Presente em aproximadamente 20% dos casos de ransomware



Aumento de 1.900%

no uso de táticas de intimidação por grupos de ransomware no mesmo período.

Essas estatísticas destacam uma mudança significativa nas estratégias de ransomware, com os agentes de ameaças empregando cada vez mais vários pontos de pressão para extorquir suas vítimas. O aumento drástico nas táticas de roubo de dados e intimidação destaca a complexidade e a gravidade crescentes das ameaças de ransomware enfrentadas pelas organizações.

As vítimas pagam para recuperar o acesso
Criptografia

Hackers ameaçam liberar dados roubados
Roubo de dados

Os ataques DDoS interromperam sites públicos
DDoS

Clientes, parceiros de negócios e mídia contatados
Intimidação

3. *O Total Economic Impact™ da Palo Alto Networks sobre o Cortex XSIAM*, Forrester Consulting, 13 de outubro de 2025.
4. Palo Alto Networks Unit 42, *2023 Unit 42 Ransomware and Extortion Report.*

TRANSFORME AS OPERAÇÕES DE SEGURANÇA

A transformação do SOC começa com o Cortex® Extended Data Lake (XDL), uma base extensível e pronta para IA para SecOps em plataforma. Atuando como a única fonte confiável para o seu SOC, o Cortex XDL integra, normaliza e enriquece todos os seus dados de segurança.

Com base nessa estrutura, o Cortex XSIAM consolida funções críticas de segurança em uma única plataforma transformadora, incluindo:

- Gestão de eventos e informações de segurança (SIEM)
- Resposta e detecção de endpoint (EDR)
- Recursos de detecção e resposta estendidas (XDR)
- Orquestração, automação e resposta de segurança (SOAR)
- Gerenciamento de superfície de ataque (ASM)
- Análise comportamental de usuários e entidades (UEBA)
- Resposta e detecção a ameaças de identidade (ITDR)
- Detecção e resposta na nuvem
- Gerenciamento de inteligência contra ameaças (TIM)
- Plataforma de inteligência de ameaças (TIP)

> Com o XSIAM, temos mais visibilidade e investigações mais rápidas. A integração perfeita de dados e a configuração da automação são divisores de águas.
>
> – Mike Dembek
> Arquiteto de rede, Boyne Resorts

Figura 1. Centro de comando do XSIAM

O Cortex XSIAM transforma as operações de segurança centralizando dados, a defesa alimentada por IA e a automação em uma única plataforma. O XSIAM Command Center apresenta um espectro de fontes de dados, que vão desde endpoint e rede até identidade, nuvem, telemetria de aplicativos e muito mais, ao mesmo tempo em que fornece insights sobre a integridade e o volume de ingestão de dados.

Essa consolidação elimina a necessidade de alternar entre várias ferramentas, reduzindo a complexidade e aumentando a eficiência da sua equipe. Em vez de fazer malabarismos com vários consoles e enfrentar problemas de integração, é possível gerenciar todas as suas operações de segurança em uma única plataforma coerente, projetada especificamente para as necessidades do SOC moderno.

As organizações que implantaram o Cortex XSIAM alcançaram resultados mensuráveis. De acordo com o estudo Total Economic Impact™ da Forrester, uma organização teve uma **redução de 85% no volume de alertas que exigiram atenção do SOC de nível 1 até o terceiro ano**, economizando mais de **US$ 930,000** em triagem e operações de nível 1. Além disso, as organizações tiveram uma **redução de 70% nos casos que exigiram investigação de SecOps,** com uma **diminuição de 85% no tempo médio de correção (MTTR) no terceiro ano**, avaliado em mais de **US$ 1,2 milhão**.[5]

Os recursos simplificados de IA ativa e automação que o XSIAM oferece mudam fundamentalmente a forma como você lida com incidentes de segurança. A plataforma automatiza a integração, a análise e a triagem dos dados, reduzindo significativamente o esforço manual exigido de seus analistas. Essa automação permite que a sua equipe se concentre no que é importante— resolver incidentes de alta prioridade que exigem conhecimento humano.

Os modelos de IA do XSIAM prontos para uso vão além dos métodos tradicionais, conectando eventos em diversas fontes de dados e oferecendo uma visão geral abrangente dos incidentes e riscos em um único local. Ao aproveitar o agrupamento de alertas e a pontuação de incidentes alimentada por IA, o XSIAM conecta perfeitamente eventos de baixa confiança, transformando-os em incidentes de alta confiança. Essa priorização se baseia no risco geral, permitindo que as equipes de segurança concentrem seus esforços de forma eficiente.

A plataforma XSIAM garante a coleta, a união e a normalização contínuas de dados brutos, indo além dos alertas. Isso capacita sua equipe SOC com recursos de investigação superiores e simplificados, permitindo que eles identifiquem e corrijam ameaças de forma mais rápida e eficaz.

Com o Cortex XSIAM, você vai perceber uma melhora significativa na experiência e na produtividade dos seus analistas. A abordagem alimentada por IA da plataforma ajuda a eliminar a confusão, reduzindo a fadiga dos alertas e permitindo que sua equipe se concentre nas ameaças críticas. Essa mudança significa que seus analistas passam menos tempo na triagem rotineira de alertas e mais tempo desenvolvendo suas habilidades, realizando investigações profundas e procurando ameaças de forma proativa.

Além disso, a abordagem de automação do XSIAM acelera a correção de incidentes. Com centenas de pacotes de conteúdo testados e comprovados no Cortex Marketplace, além do suporte nativo ao servidor e cliente MCP, você pode se conectar facilmente a todo o seu ecossistema de segurança para integrar insights e orquestrar respostas. Ao automatizar tarefas anteriormente manuais, a automação incorporada economiza tempo e esforço na resposta a incidentes ou no gerenciamento dos riscos, como exposições a superfícies de ataque.

Você tem a flexibilidade de adicionar, personalizar ou modificar automações de acordo com suas necessidades específicas. Os manuais podem ser programados, executados sob demanda ou acionados automaticamente por alertas para garantir uma resposta oportuna e a mitigação de riscos.

Quando chega a hora de investigar ameaças, o Cortex Agentic Assistant coloca uma equipe de agentes de IA à sua disposição para enfrentar qualquer desafio de segurança. Incorporado ao XSIAM, ele envolve os agentes Cortex AgentiX™ para planejar e executar fluxos de trabalho avançados, convertendo esforços manuais tediosos em ações instantâneas e especializadas. Sua equipe obtém orientação passo a passo, sensível ao contexto, com controles integrados, permitindo que eles ajam mais rapidamente, respondam com determinação e mantenham sua empresa segura.

O Cortex AgentiX fornece agentes de IA personalizados, baseados em experiência do mundo real, para multiplicar a força de cada membro da sua equipe. Desenvolvidos com base em mais de uma década de liderança em automação de segurança, enriquecidos com inteligência global sobre ameaças e informados por 1,2 bilhão de manuais executados, esses agentes funcionam como especialistas em segurança sempre ativos. Os analistas simplesmente usam prompts de linguagem natural, e os agentes planejam e executam instantaneamente tarefas complexas e em várias etapas com rapidez e precisão.

5. Forrester Consulting, *O Total Economic Impact™*.

AVALIANDO O CORTEX XSIAM PARA SUA ORGANIZAÇÃO

Ao considerar o Cortex XSIAM para sua organização, é essencial avaliar vários fatores-chave. Primeiro, avalie o panorama atual de ferramentas de segurança e sua complexidade. Se estiver enfrentando dificuldades com a proliferação de ferramentas e fluxos de trabalho desconexos entre funções de segurança proativas e reativas, a abordagem consolidada do XSIAM pode oferecer benefícios significativos. Considere quanto tempo sua equipe gasta alternando entre diferentes ferramentas e correlacionando informações manualmente. A plataforma unificada XSIAM reduz drasticamente essa sobrecarga e melhora a eficiência da sua equipe.

Em segundo lugar, considere o volume e a variedade de dados que sua organização processa. O XSIAM se destaca no processamento e na análise de grandes quantidades de dados diversos, tornando-o particularmente adequado para organizações com ambientes complexos e ricos em dados. Se você estiver lidando com uma combinação de dados locais e na nuvem, com dificuldades para obter uma visão holística de sua postura de segurança, a capacidade do XSIAM de processar e analisar dados de várias fontes pode ser um divisor de águas.

Se você estiver operando em ambientes de nuvem ou híbridos, a arquitetura nativa da nuvem do XSIAM e a visibilidade abrangente dos ativos locais e de nuvem poderão melhorar significativamente suas operações de segurança. Muitas organizações acham que suas ferramentas de segurança tradicionais têm dificuldades para oferecer visibilidade e proteção adequadas em ambientes de nuvem. O XSIAM estende seu SOC para a nuvem, garantindo visibilidade unificada e operações de segurança em toda a sua infraestrutura.

Em terceiro lugar, analise os requisitos de conformidade, que são outro fator crucial. Os recursos robustos de geração de relatórios e a análise abrangente de dados do XSIAM podem ajudar você a atender a vários padrões regulatórios de forma mais eficaz. Considere quanto tempo a sua equipe gasta atualmente com relatórios de conformidade e como o XSIAM poderia simplificar esse processo.

Em comparação com o SIEM tradicional e outras plataformas de segurança, o XSIAM oferece recursos aprimorados de detecção de ameaças graças à sua abordagem alimentada por IA. É provável que você observe uma redução na complexidade operacional e uma economia de custos potencialmente significativa devido à consolidação de ferramentas e ao aumento da eficiência. Na avaliação do ROI, considere não apenas os custos diretos, mas também o valor do tempo liberado dos analistas e a postura de segurança aprimorada. Pense em quanto mais rápido sua equipe poderia detectar e responder a ameaças com os recursos de triagem e resposta automatizados do XSIAM.

O estudo Total Economic Impact™ da Forrester Consulting documentou resultados financeiros reais. A pesquisa descobriu que as organizações alcançaram um **ROI de 257% em três anos,** com um **período de retorno inferior a seis meses**. Como relatou um vice-presidente de segurança global no estudo: "O tempo médio para detectar e corrigir problemas caiu mais de 80%. O que antes levava quatro horas para detectar e duas horas para corrigir agora leva de 40 a 50 minutos no total."[6]

> "O Cortex XSIAM transformou nossas operações de segurança de uma forma que nosso SIEM anterior não conseguiu. O XSIAM possibilitou a automação e a orquestração de nossos fluxos de trabalho de detecção, investigação e resposta — o que representou uma grande melhoria na produtividade e na postura de segurança do LOLC.
>
> – Prasanna Siriwardena
> Diretor de Informações, LOLC Holdings PLC

6. Forrester Consulting, *O Total Economic Impact™*.

Veja os aprimoramentos que o XSIAM oferece além das soluções SIEM isoladas

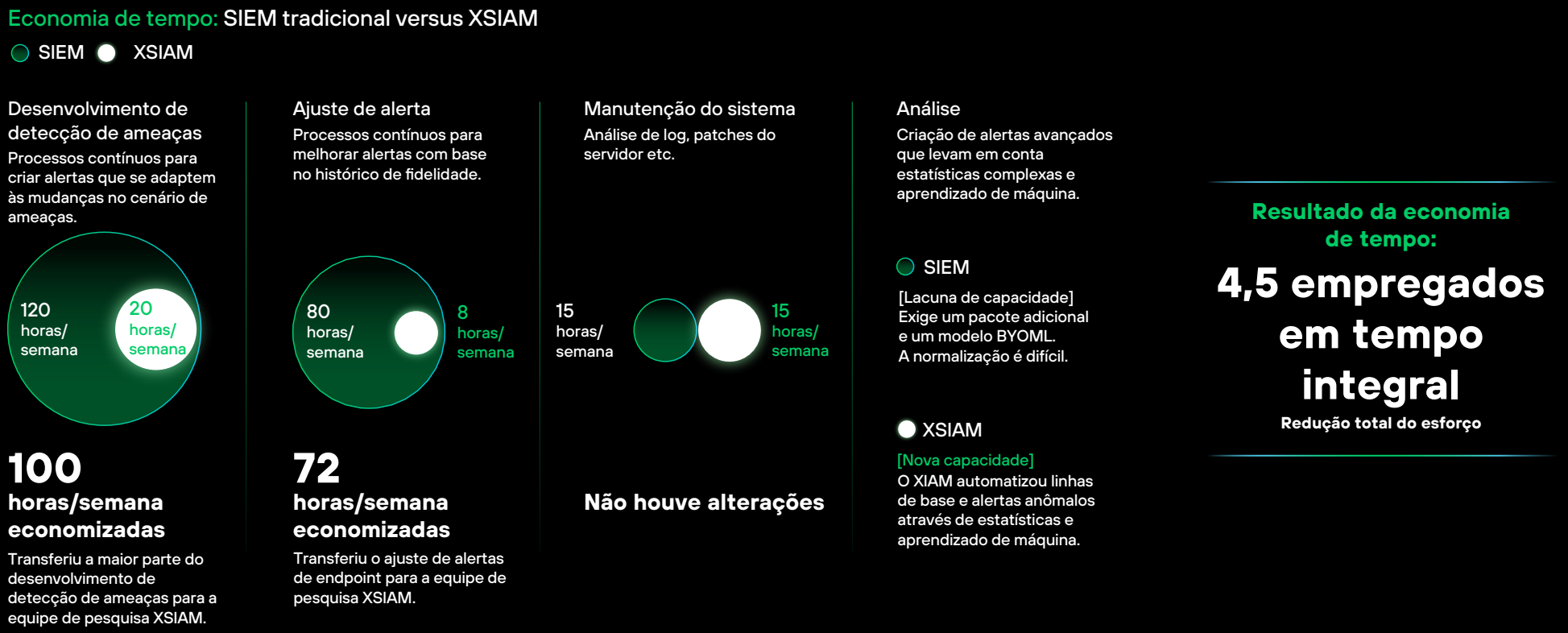


Figura 2. Redução de tempo entre o SIEM tradicional e o XSIAM

Antes de adotar o XSIAM, avalie a prontidão de sua organização nas operações de segurança alimentadas por IA. Considere as habilidades e os processos atuais da sua equipe e esteja preparado para uma mudança na forma de abordar as operações de segurança.

Embora o XSIAM possa melhorar significativamente suas operações de segurança, ele pode exigir alguns ajustes na forma como sua equipe trabalha. Considere os aspectos de treinamento e gerenciamento de mudanças da adoção de uma nova plataforma alimentada por IA.

PREPARANDO SUAS OPERAÇÕES DE SEGURANÇA PARA O FUTURO

O Cortex XSIAM desempenha um papel crucial na evolução de paradigmas de segurança como Confiança Zero, borda de serviço de acesso seguro (SASE) e borda de serviço de segurança (SSE). Sua visibilidade abrangente e seus recursos avançados de análise se alinham bem com essas abordagens modernas de segurança, ajudando a preparar suas operações de segurança para o futuro. À medida que você avança em direção a uma arquitetura de Confiança Zero, a capacidade do XSIAM de fornecer insights profundos sobre o comportamento de usuários e entidades pode ajudar você a implementar e manter um modelo robusto de Confiança Zero.

A plataforma unifica a resposta reativa a incidentes com a gestão proativa da postura de segurança. Ela aborda as duas áreas de risco mais críticas para as empresas, fornecendo:

- **Gerenciamento de exposição do Cortex**: Reduza o ruído de vulnerabilidades em até 99% com priorização orientada por IA e correção automatizada em toda a empresa e na nuvem. Essa abordagem disruptiva se concentra nas vulnerabilidades com explorações ativas e sem controles compensatórios, permitindo que você priorize os 0,01% críticos das ameaças que realmente importam.
- **Análise de e-mails do Cortex:** Impeça tentativas avançadas de phishing e ataques baseados em e-mail com análises baseadas em LLM combinadas com detecção e resposta líderes do setor. Com o e-mail continuando a ser a principal ferramenta de comunicação — com previsão de atingir 5 bilhões de usuários até 2030[7]— e o principal alvo de ataques cibernéticos, esse recurso remove automaticamente e-mails maliciosos, desativa contas comprometidas e isola os endpoints afetados em tempo real.

À medida que sua organização cresce e as ameaças evoluem, a escalabilidade do XSIAM garante que ele consiga lidar com volumes crescentes de dados e se adaptar a novos tipos de ameaças. Os modelos e detectores de IA da plataforma são atualizados continuamente, fornecendo os recursos mais recentes de inteligência e detecção de ameaças sem exigir atualizações manuais da sua equipe. Isso significa que você está sempre protegido contra as ameaças mais recentes, sem a necessidade de ajustes e atualizações manuais constantes das suas ferramentas de segurança.

O XSIAM aprende com as ações manuais dos analistas e fornece recomendações para futuras automações. Isso aumenta a capacidade da plataforma de resolver incidentes de forma automática e melhorar a eficiência e a precisão ao longo do tempo, permitindo que você e a postura de segurança da sua organização melhorem a cada dia.

O XSIAM aproveita modelos de dados de aprendizado de máquina maduros específicos de segurança, que normalizam e combinam automaticamente grandes quantidades de dados de várias fontes para detectar ameaças à segurança. Esses modelos são construídos com base no comportamento aprendido de dezenas de milhares de ambientes, ajudando a diferenciar entre comportamentos anômalos e maliciosos. Isso reduz significativamente os falsos positivos e melhora os recursos de detecção e prevenção, interrompendo os ataques antes que se tornem incidentes de segurança.

Além disso, com o XSIAM Bring Your Own Machine Learning (BYOML), você pode integrar suas próprias ferramentas de aprendizado de máquina à plataforma. Isso permite aproveitar o poder do aprendizado de máquina para caçar ameaças usando dados centralizados e normalizados no XSIAM, aprimorando ainda mais sua capacidade de detectar e responder a ameaças sofisticadas.

Impacto financeiro da consolidação

De acordo com o *The Total Economic Impact™ da Palo Alto Networks sobre o Cortex XSIAM* da Forrester Consulting:[8]

US$ 3,1 milhões
economizados com a eliminação de mais de 20 ferramentas legadas (total em 3 anos)

US$ 2,2 milhões
valor obtido com a melhoria de 60% na postura de segurança

US$ 5,6 milhões
valor presente líquido em 3 anos

Ao adotar o XSIAM, você resolverá os desafios de segurança atuais e posicionando sua organização para atender às necessidades de cibersegurança do futuro. Essa abordagem voltada para o futuro pode dar confiança em sua capacidade de proteger sua organização contra um cenário de ameaças em constante evolução. À medida que novos tipos de ameaças surgem e a infraestrutura de TI da sua organização precisa evoluir para atender às demandas, o XSIAM oferece uma abordagem flexível, orientada por IA, que garante que suas operações de segurança possam se adaptar e responder com eficácia.

O XSIAM permite que as equipes do SOC e a postura de segurança da organização melhorem a cada dia.

Talvez o mais importante seja o fato de o XSIAM oferecer aprimoramento contínuo através da IA e do aprendizado de máquina. A plataforma refina regularmente seus recursos de detecção e resposta com base em novos dados e técnicas de ataque emergentes. Isso significa que suas operações de segurança ficam mais eficazes ao longo do tempo, adaptando-se a novas ameaças e padrões sem ajustes manuais constantes.

7. *Relatório de estatísticas de e-mail 2025-2030*, cloudHQ, 24 de abril de 2025.
8. Forrester Consulting, *O Total Economic Impact™*.

MELHORE SUAS MÉTRICAS CRÍTICAS DO SOC

O Cortex XSIAM oferece uma abordagem revolucionária para reduzir o tempo médio de detecção (MTTD) e o tempo médio de resposta (MTTR), aprimorando drasticamente suas operações de segurança. Ao aproveitar a IA avançada e o aprendizado de máquina, o XSIAM automatiza a tarefa entediante de integração e análise de dados, permitindo que sua equipe identifique ameaças quase em tempo real. Isso significa que você pode detectar possíveis violações mais rápido do que nunca, geralmente capturando os invasores antes que eles possam causar danos significativos à sua organização.

Mas a detecção é apenas metade da batalha. A abordagem de automação em primeiro lugar do XSIAM acelera a resposta a incidentes, transformando horas de investigação manual em minutos de ação automatizada. Imagine sua equipe de SOC não mais atolada em atividades de triagem manual ou gastando um tempo precioso correlacionando dados de fontes diferentes. Em vez disso, capacite seus analistas para se concentrarem no que é importante com a pontuação de incidentes orientada por IA e o agrupamento inteligente de alertas do XSIAM.

A nossa abordagem unificada para segurança reativa e proativa significa que você pode responder a incidentes com mais rapidez e evitar que muitos deles ocorram. Ao integrar a gestão de exposição e a análise de e-mails diretamente na plataforma SOC, o XSIAM aborda dois dos vetores de ataque mais comuns com os mesmos dados unificados, IA e automação.

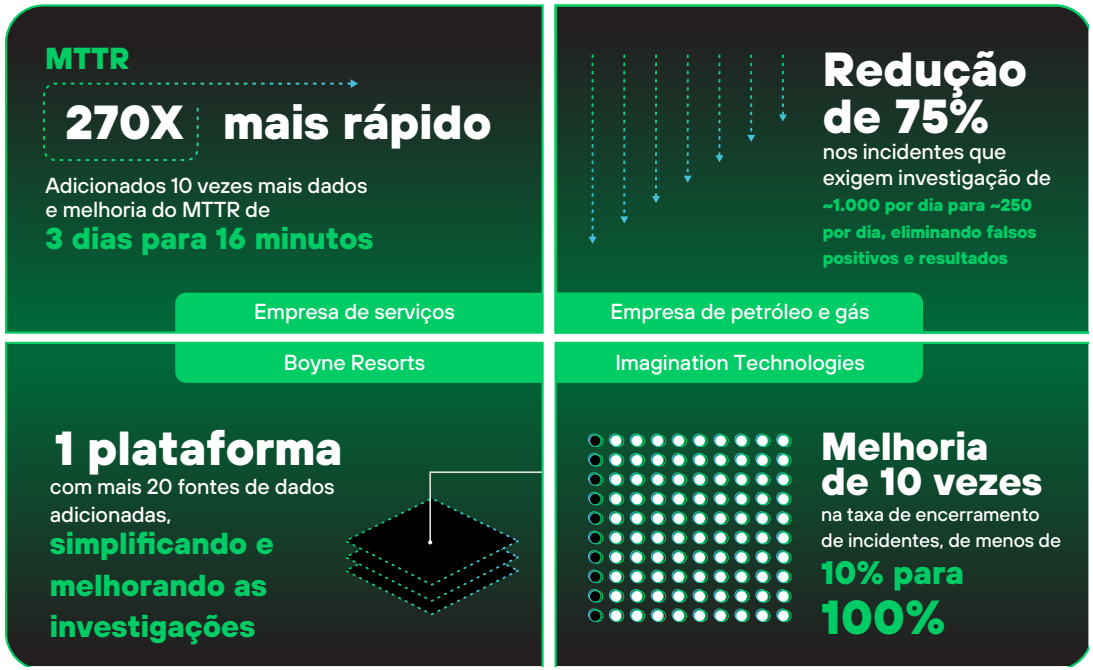


Figura 3. Exemplos de como os clientes obtiveram melhorias mensuráveis usando o XSIAM

Você verá uma redução drástica no MTTR à medida que sua equipe utiliza manuais avançados e agentes Cortex AgentiX, permitindo uma ação rápida e decisiva contra ameaças. Talvez o mais importante seja o fato de que o XSIAM aprende e se adapta continuamente ao seu ambiente, garantindo que sua postura de segurança melhore com o tempo. À medida que você enfrenta ameaças novas e emergentes, os modelos do AI de ponta do XSIAM evoluem continuamente, mantendo você um passo à frente de potenciais adversários.

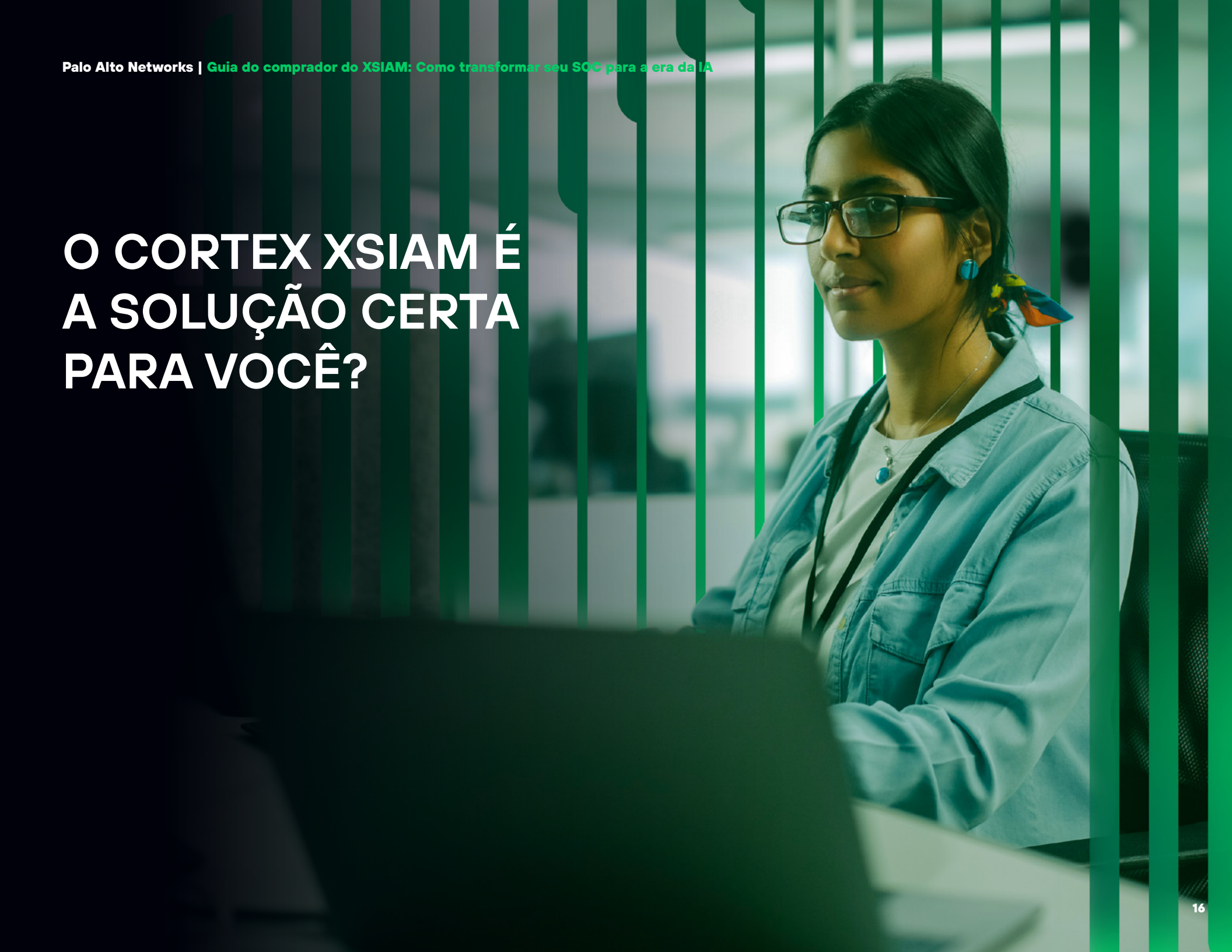
Isso significa que você está melhorando seu MTTD e MTTR hoje, além de preparar suas operações de segurança para os desafios de amanhã. Com o Cortex XSIAM, você pode navegar com confiança no complexo cenário da segurança cibernética, sabendo que suas métricas críticas de SOC são continuamente otimizadas para proteger os ativos mais valiosos da sua organização.

Pesquisas comprovam essas melhorias. Para um varejista especializado, os alertas caíram de **25.000 para 4.500 por trimestre**, de acordo com seu diretor de SecOps. O estudo documentou que, para a organização com base nos clientes entrevistados, a implantação exigiu **três FTEs ao longo de dois meses**, com apenas **0,5 FTE para manutenção anual contínua**.[9]

> “Consideramos o XSIAM como a próxima fronteira na direção de um SOC de última geração, pois integra vários recursos em uma única plataforma unificada. Com o XSIAM, esperamos maior automação e maior capacitação para nossa equipe de operações cibernéticas.
>
> – Rob Jillson
> Diretor de segurança cibernética, Resolution Life Australasia

9. Forrester Consulting, *O Total Economic Impact™*.

O CORTEX XSIAM É A SOLUÇÃO CERTA PARA VOCÊ?



1. Desafios atuais do SOC

- ☐ Você está com dificuldades para realizar configurações complexas em seu SIEM atual?
- ☐ Você enfrenta integrações demoradas entre as ferramentas de segurança?
- ☐ Sua equipe está sobrecarregada por um grande volume de alertas?
- ☐ Você tem fluxos de trabalho ineficientes devido a ferramentas de segurança fragmentadas?
- ☐ Existe uma desconexão entre suas funções de segurança proativas e a resposta reativa a incidentes?

2. Detecção e resposta a ameaças

- ☐ Você depende muito de regras de correlação estática?
- ☐ Você precisa melhorar a detecção de ameaças em tempo real?
- ☐ Seu processo de resposta a incidentes está atrasado devido à falta de integração?
- ☐ Você tem dificuldades com as altas taxas de falsos positivos?

3. Gerenciamento de dados

- ☐ Você lida com grandes volumes de dados de segurança diversos?
- ☐ Está lidando com uma combinação de dados no local e na nuvem?
- ☐ Você precisa de melhores recursos de normalização e recursos de correlação?

4. Necessidades de IA e automação

- ☐ Você está procurando aproveitar a IA para detecção aprimorada de ameaças?
- ☐ Deseja automatizar tarefas rotineiras de segurança?
- ☐ A redução do esforço manual na triagem de incidentes é uma prioridade?
- ☐ Você precisa de priorização de vulnerabilidades orientada por IA para eliminar o excesso de informações?

5. Requisitos da plataforma unificada

- ☐ Você precisa consolidar várias funções de segurança, como SIEM, EDR, XDR, SOAR, gestão de vulnerabilidades e segurança de e-mails?
- ☐ Deseja gerenciar as operações de segurança em uma única plataforma?
- ☐ Deseja preencher a lacuna entre a segurança proativa e a reativa?

6. Nuvem e ambiente híbrido

- ☐ Você está operando em ambientes de nuvem ou híbridos?
- ☐ Você precisa de melhor visibilidade dos ativos no local e na nuvem?

7. Conformidade e relatórios

- ☐ Você precisa simplificar os processos de relatórios de conformidade?
- ☐ Está buscando uma análise de dados mais abrangente para as normas regulamentares?

8. Escalabilidade

- ☐ Sua organização está crescendo e precisa lidar com volumes de dados cada vez maiores?
- ☐ Você precisa de uma solução que possa se adaptar às ameaças em constante evolução?

9. Análise avançada

- ☐ Você está interessado na pontuação de incidentes e no agrupamento de alertas alimentados por IA?
- ☐ Você precisa de uma melhor correlação de eventos em várias fontes de dados?
- ☐ Deseja utilizar IA para priorizar as vulnerabilidades mais críticas?

10. Prontidão da equipe

- ☐ Sua equipe está preparada para se adaptar às operações de segurança alimentadas por IA?
- ☐ Você está disposto a investir em treinamento para uma plataforma nova e avançada?

11. Prova futura

- ☐ Você está se movendo em direção a modelos de segurança de Confiança Zero, SASE ou SSE?
- ☐ Você precisa de uma solução que melhore continuamente através da IA e aprendizado de máquina?

12. Integração de aprendizado de máquina personalizado

- ☐ Você está interessado em integrar suas próprias ferramentas de aprendizado de máquina?

13. Gerenciamento de e-mails e vulnerabilidades

- ☐ Você precisa de melhor proteção contra ameaças avançadas por e-mail?
- ☐ Você tem dificuldades com atrasos e priorização de vulnerabilidades?
- ☐ Você se beneficiaria da correção automatizada de vulnerabilidades críticas?

Se você respondeu "**sim**" à maioria dessas perguntas, especialmente em áreas que se alinham aos desafios e objetivos específicos de segurança da sua organização, o Cortex XSIAM seria uma solução adequada para o seu SOC.

Comece hoje mesmo

Descubra como o Cortex XSIAM pode ajudar você e sua organização a simplificar as operações, unificar a segurança proativa e reativa, impedir ameaças em grande escala e acelerar a remediação de incidentes — hoje e no futuro.

ENTRE EM CONTATO CONOSCO →

Sobre o Cortex XSIAM

O Cortex XSIAM é a plataforma de operações de segurança orientada por IA para o SOC moderno, aproveitando o poder da IA para simplificar as operações de segurança, interromper ameaças em grande escala e acelerar a correção de incidentes. Reduza o risco e a complexidade operacional centralizando vários produtos em uma única plataforma convergente desenvolvida especificamente para operações de segurança.

O Cortex XSIAM unifica as melhores funções de operações de segurança, incluindo EDR, XDR, SOAR, ASM, UEBA, TIP e SIEM. O XSIAM centraliza todos os seus dados de segurança e usa modelos de dados de aprendizado de máquina projetados especificamente para segurança. Com o XSIAM, automatize a integração de dados, a análise e as ações de resposta, com o XSIAM permitindo que os analistas se concentrem nos incidentes que importam. Para saber mais sobre o Cortex, acesse www.paloaltonetworks.com/cortex/cortex-xsiam.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Principal	+1.408.753.4000
Vendas	+1.866.320.4788
Suporte	+1.866.898.9087

cortex_ebook_cortex-xsiam-buyers-guide_102125