10 melhores soluções NDR (Detecção e Resposta da Rede) em 2025 - Agai

Data: 2025-08-15 21:24:09

Autor: Inteligência Against Invaders

A rede continua sendo o sistema nervoso central de todas as organizações. Embora os pontos de extremidade e os ambientes de nuvem sejam cruciais, toda a atividade digital atravessa a rede. A implementação das melhores soluções NDR é essencial para monitorar e proteger essa infraestrutura crítica.

As defesas tradicionais do perímetro, como firewalls e sistemas de detecção de intrusões (IDs), não são mais suficientes para combater a furtividade e a sofisticação dos ataques cibernéticos modernos, que geralmente ignoram esses controles ou exploram vulnerabilidades internas.

É aqui que as soluções de detecção e resposta de rede (NDR) se tornam indispensáveis.

O NDR opera monitorando continuamente o tráfego de rede-norte-sul (dentro e fora da rede) e, crucialmente, leste-oeste (comunicação interna da rede). Muitos fornecedores da NDR oferecem soluções que analisam esse tráfego para detectar ameaças.

Ao contrário dos sistemas tradicionais baseados em assinatura, o NDR aproveita a análise avançada, o aprendizado de máquina (ML) e a inteligência artificial (AI) para estabelecer uma linha de base do comportamento da rede “normal”.

Em seguida, identifica anomalias, padrões suspeitos e indicadores de compromisso (IOCs) que significam um ataque contínuo, mesmo que não exista assinatura conhecida.

Essa abordagem proativa permite que as organizações detectem ameaças sofisticadas, como ataques internos, movimento lateral, Exfiltração de dadose malware polimórfico que de outra forma poderia passar despercebido.

Para uma compreensão mais profunda de como o NDR se encaixa no cenário mais amplo de segurança, explore os recursos sobre o que é detecção e resposta de rede (NDR)?.

Este artigo mergulha profundamente nos 10 melhores fornecedores de detecção e resposta de rede (NDR) para 2025, escolhidos meticulosamente por suas capacidades inovadoras, eficácia comprovada de detecção de ameaças, recursos de resposta robustos e comprometimento de fornecer visibilidade incomparável à rede.

O imperativo da NDR em 2025: por que a visibilidade da rede importa mais do que nunca

O cenário de segurança cibernética em 2025 exige uma abordagem proativa e abrangente para a segurança da rede. As soluções NDR são cruciais por vários motivos atraentes:

Detecção de ameaças evasivas: Os atacantes modernos empregam técnicas sofisticadas (por exemplo, malware sem arquivo, variantes polimórficas, canais C2 criptografados) que ignoram as defesas tradicionais baseadas em assinatura.

A análise comportamental da NDR e a AI se destacam em identificar essas anomalias sutis.

Visibilidade no tráfego interno (leste-oeste): Muitos ataques, especialmente após o compromisso inicial, envolvem movimento lateral dentro da rede.

O NDR fornece visibilidade crítica nesse tráfego leste-oeste, permitindo a detecção precoce de acesso não autorizado, escalada de privilégios e reconhecimento interno.

Implantação não agente: Diferentemente da detecção e resposta do endpoint (EDR), que requer agentes em dispositivos, o NDR opera analisando o tráfego de rede em pontos estratégicos, tornando -o ideal para monitorar dispositivos não gerenciados (IoT, OT), BYOD e dispositivos onde os agentes não podem ser instalados.

Caça proativa de ameaças: As ferramentas da NDR capacitam analistas de segurança a buscar ativamente ameaças ocultas e atividades suspeitas em toda a rede, usando dados históricos ricos e consultas avançadas para descobrir até mesmo os adversários mais furtivos.

Resposta e contexto automatizados: Além da detecção, as principais soluções da NDR oferecem recursos de resposta automatizados para conter rapidamente ameaças, como isolar dispositivos comprometidos ou bloquear a comunicação maliciosa, geralmente fornecendo um contexto profundo para uma remediação manual mais rápida.

Análise de tráfego criptografado (ETA): Com mais de 90% do tráfego de rede agora criptografado, a detecção de ameaças dentro desses fluxos é fundamental. As principais soluções NDR alavancam técnicas como análise de tráfego criptografado (ETA) para identificar padrões suspeitos sem descriptografia, preservando a privacidade, mantendo a segurança.

Fundação para XDR: O NDR é um pilar fundamental das plataformas estendidas de detecção e resposta (XDR), fornecendo telemetria de rede crítica que, quando correlacionada com dados de extremidade, nuvem e identidade, oferece uma visão verdadeiramente holística de um ataque.

Essa integração é vital para os centros de operações de segurança modernos (SOCs).

O mercado da NDR é projetado para um crescimento significativo até 2032, impulsionado pela crescente sofisticação de ameaças cibernéticas, a mudança para ambientes em nuvem e híbridos e a necessidade crítica de visibilidade mais profunda nas atividades da rede.

Isso apresenta uma oportunidade crescente para os fornecedores da NDR inovarem e expandirem suas ofertas para atender a essas demandas de segurança em evolução.

Nossa metodologia de seleção para os principais fornecedores de NDR (2025 Focus)

Nosso rigoroso processo de avaliação para os principais fornecedores de NDR em 2025 focou nos seguintes critérios críticos:

Eficácia e precisão da detecção: A capacidade comprovada de detectar uma ampla gama de ameaças (conhecidas e desconhecidas, internas e externas) com alta fidelidade e baixos falsos positivos, geralmente demonstrados através de avaliações independentes.

Recursos de AI/Machine Learning: A sofisticação e eficácia dos algoritmos AI/ML em comportamento normal de base, identificando anomalias e reduzindo a fadiga de alerta.

Visibilidade e cobertura: A amplitude da visibilidade da rede (norte-sul, leste-oeste, nuvem, OT/ICS) e a profundidade dos dados capturados (captura completa de pacotes, dados de fluxo, metadados).

Análise de tráfego criptografado (ETA): A capacidade de detectar ameaças no tráfego criptografado sem exigir descriptografia.

Resposta e automação: A velocidade e a eficácia das ações de resposta automatizadas e as ferramentas fornecidas para contenção manual e remediação.

Caça de ameaças e forense: O poder das ferramentas para caça proativa de ameaças, análise de dados históricos e investigações forenses detalhadas.

Integração e abertura: Capacidade de integrar -se perfeitamente ao SIEM, SOAR, EDR e outras ferramentas de segurança para contribuir para uma estratégia XDR mais ampla.

Escalabilidade e desempenho: A capacidade de lidar com altos volumes de tráfego de rede sem degradação e implantar em diversas arquiteturas de rede.

Usabilidade e gerenciamento: Console de gerenciamento intuitivo, facilidade de implantação e relatórios claros para equipes de segurança.

Satisfação e reputação do cliente: Forte reconhecimento da indústria e feedback positivo das implantações do mundo real.

Tabela de comparação: os 10 melhores fornecedores de detecção e resposta de rede (NDR) 2025

1. Darktrace

Por que escolhemos:

O Darktrace Detect ™ é pioneiro e líder no espaço da NDR, conhecido por seu aprendizado de máquina não supervisionado e abordagem de AI “auto-aprendizagem”.

Ele se destaca em estabelecer uma linha de base dinâmica de comportamento “normal” para cada usuário, dispositivo e segmento de redepermitindo identificar e contextualizar instantaneamente anomalias sutis que sinalizam ameaças emergentes, mesmo aquelas nunca vistas antes, inclusive em ambientes de OT/ICS e nuvem.

Especificações:

Darktrace é um dos principais fornecedores de NDR no mercado. Sua plataforma Detect ™ usa aprendizado de máquina não supervisionado para criar um entendimento único do ambiente digital de uma organização.

Ele monitora todo o tráfego de rede, incluindo fluxos criptografados (sem descriptografia), IoT, OT e ambientes em nuvem.

As principais especificações incluem detecção de anomalia em tempo real, visualização de ameaças, um profundo entendimento do comportamento interno da rede (tráfego leste-oeste) e um “sistema imunológico corporativo” que aprende e adapta autonomamente as ameaças em evolução.

Ele pode se integrar à resposta de Darktrace para a contenção automatizada de ameaças.

Motivo para comprar:

O Darktrace Detect ™ é ideal para organizações que buscam uma solução de NDR altamente inteligente e auto-aprendizado que pode detectar as ameaças mais sofisticadas e novas em ambientes complexos e diversos de TI, OT e nuvem.

Se você priorizar a detecção de ameaças autônomas e uma solução que se adapta à sua pegada digital em evolução, o Darktrace é uma escolha líder.

Características:

- IA não supervisionada para detecção de anomalia em tempo real.
- Visibilidade abrangente, OT/ICS, Cloud e SaaS.
- Análise de tráfego criptografada (ETA) sem descriptografia.
- Identificação proativa de ameaças internas e movimento lateral.
- Visualização de ameaças e painel intuitivo.
- Auto-aprendizagem e postura de segurança adaptativa.
- Pode se integrar ao Darktrace Responder para resposta autônoma.

Prós:

- Excepcional ao detectar ameaças desconhecidas e zero dias.
- Forte visibilidade no tráfego leste-oeste.
- Eficaz para a segurança da IoT/OT.
- Configuração mínima necessária devido à IA de auto-aprendizado.
- Reduz a fadiga de alerta, concentrando -se em verdadeiras anomalias.

Contras:

- Pode ser uma solução de preço premium.
- Requer uma curva de aprendizado para utilizar completamente seus recursos avançados.
- A natureza da “caixa preta” da IA não supervisionada às vezes pode ser percebida como a falta de transparência por alguns.

? Melhor para: empresas e organizações críticas de infraestrutura que exigem detecção avançada de anomalia orientada por IA para ameaças desconhecidas, ameaças privilegiadas e visibilidade abrangente, OT/ICS e ambientes de várias nuvens.

? Try Darktrace DETECT™ here ? Darktrace Official Website

2. Vectra ai

Por que escolhemos:

A plataforma Vectra AI se destaca em sua “detecção, investigação e resposta de ataques híbridos acionados por IA”, concentrando-se em comportamentos de invasors, em vez de apenas assinaturas.

Ele fornece detecções de alta fidelidade de ameaças sofisticadas, como movimento lateral, escalada de privilégios e atividade de comando e controle nas redes de identidade, nuvem pública, SaaS e data center.

Seus recursos de detecção como código permitem uma rápida adaptação a novas ameaças.

Especificações:

A plataforma Vectra AI aproveita a IA patenteada e o aprendizado de máquina para detectar comportamentos de invasor em tempo real em toda a rede, nuvemSaaS e camadas de identidade.

Ele analisa os metadados da rede e os logs de identidade para identificar reconhecimento de reconhecimento, movimento lateral, escalada de privilégios e exfiltração de dados.

As principais especificações incluem detecções-código para atualizações rápidas, triagem automatizada de alertas, integração com as capacidades EDR e SIEM para XDR e informações de ameaça de alta fidelidade.

Motivo para comprar:

A plataforma Vectra AI é um destaque entre os fornecedores da NDR, atendendo a empresas e Centros de Operações de Segurança (SOCs) que requerem detecção avançada e acionada por IA de comportamentos sofisticados de atacantes em toda a sua superfície de ataque híbrido, incluindo nuvem e saas.

Se você deseja uma solução que reduz significativamente o ruído de alerta e fornece informações acionáveis para a rápida resposta a incidentes, o Vectra AI é um dos principais candidatos.

Características:

- Detecção acionada por IA de comportamentos de invasor (reconhecimento, movimento lateral).
- Cobertura em rede, nuvem, SaaS e identidade.

- Detecções como código de ameaça ágil.
- Triagem automatizada e priorização de ameaças.
- Dados contextuais ricos para investigações.
- Capacidades proativas de caça de ameaças.
- Integra -se ao SIEM, Soar e EDR para segurança unificada.

Prós:

- Excepcional ao detectar comportamentos pós-compromissão.
- Os alertas de alta fidelidade reduzem os falsos positivos.
- Foco forte em ambientes híbridos e de várias nuvens.
- Simplifica investigações com contexto rico.
- Adaptativo a novas ameaças com detecções como código.

Contras:

- Pode exigir uma equipe de segurança mais madura para aproveitar completamente seus recursos avançados.
- A implantação e ajuste inicial podem ser complexos para ambientes muito grandes.
- Os preços podem ser um investimento significativo.

? Melhor para: grandes empresas e SoCs avançados se concentraram na detecção de comportamentos sofisticados do atacante, movimento lateral e ameaças em nuvem/saas com alta fidelidade e visibilidade abrangente.

`? Try Vectra AI here ?` Vectra AI Official Website

Por que escolhemos:

Extrahop é um dos principais fornecedores de NDR do mercado. Sua plataforma de revelação (x) se destaca por sua capacidade incomparável de fornecer uma visibilidade profunda à atividade da rede por meio de análise de dados de arame e aprendizado de máquina, mesmo para tráfego criptografado.

Ele oferece detecção em tempo real, recursos forenses robustos e monitoramento de desempenho de rede (NPM) em uma única plataforma, tornando-o inestimável para equipes de operações de segurança e de rede que buscam uma única fonte de verdade para todas as comunicações de rede.

Especificações:

Extrahop Revel (x) analisa todo o tráfego de rede no nível do pacote, alavancando o aprendizado de máquina para detecção de ameaças em tempo real e Monitoramento de desempenho da rede.

Ele fornece visibilidade sem agente, incluindo análise de tráfego criptografada (ETA) sem descriptografia, e oferece detecções de espectro total alimentadas pela IA.

As principais especificações incluem descoberta automatizada e classificação de ativos, visibilidade no nível da transação e integrações robustas com plataformas SIEM, SOAR e EDR.

Motivo para comprar:

O Extrahop Revel (x) é ideal para organizações que precisam de visibilidade incomparável em seu tráfego de rede, incluindo comunicações criptografadas, e desejam uma única plataforma para insights de segurança e desempenho de rede.

Se você priorizar recursos forenses profundos, implantação sem agente e detecção eficaz de ameaças escondidas nos fluxos de rede, o Extrahop é uma escolha de primeira linha.

Características:

- Análise de dados de arame em tempo real para uma profunda visibilidade da rede.
- Implantação e monitoramento sem agente.
- Análise de tráfego criptografada (ETA) para detecção de ameaças em fluxos criptografados.
- Detecção de anomalia comportamental movida a IA.
- Descoberta e classificação automatizadas de dispositivos e ativos.
- Recursos de monitoramento de desempenho da rede (NPM).
- Capacidades forenses abrangentes com dados históricos.

Prós:

- Visibilidade mais profunda no tráfego de rede, incluindo a camada 7.
- Excelente para detectar ameaças no tráfego criptografado.
- Combina informações de segurança e operações de rede.
- Impacto mínimo no desempenho da rede.
- Altamente eficaz para investigação de incidentes e forense.

Contras:

- Pode ser um investimento significativo, principalmente para opções completas de captura de pacotes.
- Requer alguma experiência em rede para aproveitar totalmente todos os recursos.
- A implantação pode envolver uma colocação cuidadosa do sensor para uma cobertura ideal.

? Melhor para: Enterprises e equipes de operações de segurança/rede que exigem visibilidade profunda e em tempo real em todo o tráfego de rede (incluindo criptografado), recursos forenses robustos e monitoramento combinado de segurança e desempenho.

`? Try ExtraHop here ?` [ExtraHop Official Website]

4. CoreLight

Por que escolhemos:

A CoreLight Open NDR se destaca por sua base em tecnologias de código aberto como Zeek (anteriormente Bro) e Suricata, que são confiáveis por pesquisadores de segurança e governos globalmente para uma análise profunda da rede.

O CoreLight transforma os dados de rede bruta em insights ricos e acionáveis, proporcionando visibilidade incomparável para a caça de ameaças, resposta a incidentes e investigações forenses, tornando -a uma ferramenta poderosa para organizações que exigem inteligência granular de rede.

Especificações:

O CoreLight Open NDR aproveita Zeek e Suricata para realizar a inspeção profunda de pacotes (DPI) e gerar metadados de rede abrangentes.

Ele fornece detecções de alta fidelidade, extração extensa e integração com várias ferramentas de segurança.

As principais especificações incluem flexibilidade de implantação (sensores físicos, virtuais e de nuvem), cobertura para ambientes de TI/OT/ICS e a capacidade de exportar dados ricos para análise SIEM, XDR e Data Lake.

Motivo para comprar:

A CoreLight é um dos principais fornecedores de NDR que fornece uma plataforma ideal para organizações maduras de segurança, SoCs e equipes de resposta a incidentes que exigem a mais profunda visibilidade possível da atividade da rede e a flexibilidade para realizar uma análise de ameaças altamente detalhada e análise forense.

Se sua equipe tiver a experiência e precisar de dados de rede ricos e personalizáveis para operações de segurança avançadas, o CoreLight é uma excelente opção.

Características:

- Baseado em Zeek e Suricata para análise profunda da rede.
- Gera metadados de rede ricos e acionáveis.
- Visibilidade abrangente, OT/ICS e nuvem.
- Detecções e alertas de alta fidelidade.
- Caça poderosa de ameaças e capacidades forenses.
- Arquitetura aberta para extensas integrações.
- Suporte para captura completa de pacotes.

Prós:

- Profundidade incomparável de dados de rede para investigações.
- Altamente personalizável para necessidades específicas de caça de ameaças.
- Aproveita a tecnologia de código aberto confiável.
- Forte para conformidade e auditoria.
- Excelente para detecção complexa e avançada de ameaças.

Contras:

- Requer analistas de segurança com experiência em rede forense e Zeek.
- Pode gerar um grande volume de dados, exigindo armazenamento e processamento robustos.

- Pode ter uma curva de aprendizado mais acentuada para as equipes novas para monitoramento de rede nesse nível.

? Melhor para: Centros de Operações de Segurança (SOCs) e equipes de resposta a incidentes que exigem visibilidade da rede granular profunda, caça de ameaças poderosas e capacidades forenses, particularmente aqueles que aproveitam as ferramentas de segurança de rede de código aberto.

`? Try Corelight here ?` `Corelight Official Website`

5. Arista

Por que escolhemos:

A Arista NDR, anteriormente acordada, se destaca por sua abordagem orientada a IA que identifica e perfana todas as entidades da rede, de dispositivos tradicionais à IoT e pontos de extremidade não gerenciados.

Essa visibilidade abrangente centrada na entidade, combinada com a detecção de anomalia comportamental, permite detectar ameaças, especialmente ameaças internas e ataques direcionadose fornece triagem e resposta autônomas em diversos ambientes.

Especificações:

A Arista é um dos principais fornecedores de NDR que utiliza a IA para criar uma impressão digital digital abrangente de todas as entidades da rede, monitorando seu comportamento em tempo real.

Ele fornece diagnóstico contínuo, detecta comportamentos de invasor (por exemplo, reconhecimento, C2) e oferece triagem e resposta autônomas.

As principais especificações incluem implantação sem agente, cobertura para redes tradicionais, IoT e nuvem e integração com a infraestrutura de rede da Arista para segurança unificada.

Motivo para comprar:

O Arista NDR é ideal para organizações que buscam uma solução avançada de NDR orientada a IA que fornece visibilidade centrada na entidade profunda e se destaque na detecção de ameaças privilegiadas e anomalias comportamentais sutis em diversas redes, incluindo a IoT.

Se você deseja uma solução que automatiza a triagem e forneça forense abrangente, o Arista NDR é uma escolha forte.

Características:

- Perfil de entidade orientada a IA para todos os dispositivos de rede.
- Detecção de anomalia comportamental para ameaças internas e ataques furtivos.
- Capacidades de triagem e resposta autônomas.
- Visibilidade abrangente em redes tradicionais de TI, IoT e nuvem.

- Suporte total forense e investigação de incidentes.
- Implantação sem agente.
- Pode se integrar ao portfólio de rede mais amplo da Arista.

Prós:

- Excelente em identificar e rastrear todas as entidades de rede.
- Forte detecção de ameaças internas e movimento lateral.
- Automatiza a triagem de incidentes, reduzindo a carga de trabalho manual.
- Boa visibilidade em dispositivos não gerenciados e IoT.
- Fornece contexto rico para investigações.

Contras:

- Os preços podem ser uma consideração para organizações menores.
- Os benefícios completos são realizados com um compromisso com sua abordagem orientada a IA.
- Pode exigir algum aprendizado inicial para entender seu modelo centrado na entidade.

? Melhor para: organizações que precisam de visibilidade abrangente da entidade e detecção comportamental orientada pela IA para ameaças privilegiadas, movimento lateral e segurança de dispositivos não gerenciados/IoT em ambientes de rede complexos.

`? Try Arista NDR here ?` Arista Official Website

6. Cisco Secure Network Analytics

Por que escolhemos:

A Cisco Secure Network Analytics, anteriormente Stealthwatch, aproveita o NetFlow e outras telemetria de rede para fornecer análises abrangentes de visibilidade e segurança em ambientes locais e no local.

Sua profunda integração com o portfólio mais amplo de segurança da Cisco permite uma abordagem unificada para detecção e resposta de ameaças, tornando -a uma escolha atraente para organizações já investidas em Infraestrutura da Cisco.

Especificações:

A Cisco Secure Network Analytics fornece visibilidade da rede e análise comportamental, coletando e analisando o NetFlow, o IPFIX e outros dados de telemetria de dispositivos de rede.

Ele usa o aprendizado de máquina para detectar anomalias, identificar ameaças internas, ameaças persistentes avançadas (APTs) e exfiltração de dados.

As principais especificações incluem análise de tráfego criptografada (ETA), monitoramento de segurança em nuvem e integração com os produtos de segurança da Cisco (por exemplo, Cisco

SecureX, ISE) para resposta automatizada.

Motivo para comprar:

A Cisco é um dos principais fornecedores de NDR do mercado. A Cisco Secure Network Analytics é ideal para grandes empresas e organizações investidas fortemente na infraestrutura de rede e segurança da Cisco.

Se você deseja aproveitar seus investimentos existentes na Cisco para uma visibilidade abrangente da rede, a detecção de ameaças orientada pela IA (inclusive dentro do tráfego criptografado) e resposta automatizada, a Cisco Secure Network Analytics oferece uma solução robusta.

Características:

- Visibilidade da rede abrangente usando NetFlow/IPFIX.
- Analítica comportamental e aprendizado de máquina para detecção de ameaças.
- Analítica de tráfego criptografada (ETA) para visibilidade da ameaça em fluxos criptografados.
- Monitoramento de segurança em nuvem para AWS, Azure e Google Cloud.
- Resposta de incidentes automatizados e integração com ferramentas de segurança.
- Detecção de ameaças e monitoramento de exfiltração de dados.
- Gerenciamento e relatórios centralizados.

Prós:

- Integração profunda com a extensa portfólio de networking e segurança da Cisco.
- Analítica de tráfego eficaz (ETA).
- Forte para ambientes de rede grandes e complexos.
- Bom para detecção de ameaças privilegiada e prevenção de perda de dados.
- Aproveita a vasta inteligência de ameaças da Cisco.

Contras:

- Mais adequado para organizações com infraestrutura significativa da Cisco.
- Pode ser complexo para implantar e gerenciar em ambientes não Cisco.
- Os preços podem ser um fator para organizações menores.

? Melhor para: grandes empresas e organizações com extensa infraestrutura de rede da Cisco que buscam visibilidade de rede integrada e orientada pela IA e detecção de ameaças, inclusive para ambientes criptografados de tráfego e nuvem.

? Try Cisco Secure Network Analytics here ? Cisco Official Website

7. Trend Micro

Por que escolhemos:

O Trend Micro é um dos notáveis fornecedores de NDR no mercado. Sua plataforma Vision One oferece uma plataforma XDR abrangente que integra recursos de NDR com segurança, email, nuvem e segurança do servidor.

Sua força está em fornecer uma visão unificada da postura de segurança e ataques em diversas camadas, simplificar a detecção e a resposta de ameaças para as equipes de segurança e alavancar a extensa inteligência global de ameaças da Trend Micro.

Especificações:

Trend Micro Vision One (com NDR) coleta e correlaciona a telemetria de sensores de rede, pontos de extremidade (Apex One), email, cargas de trabalho em nuvem e servidores.

Ele usa análises avançadas, aprendizado de máquina e inteligência global de ameaças (Trend Micro Research) para detecção e resposta de camadas cruzadas.

As principais especificações incluem análise de tráfego de rede, análise de tráfego criptografado (ETA), detecção automatizada, orquestração de resposta e insights de gerenciamento de riscos de superfície de ataque.

Motivo para comprar:

O Trend Micro Vision One (com NDR) é uma excelente opção para organizações que buscam uma plataforma XDR unificada que reúna rede, endpoint, e -mail e segurança em nuvem para detecção e resposta abrangentes de ameaças.

Se você deseja consolidar operações de segurança e se beneficiar da visibilidade de camadas cruzadas de um fornecedor confiável, a Trend Micro oferece uma solução forte.

Características:

- Plataforma XDR abrangente com NDR integrado.
- Visibilidade da camada cruzada (rede, endpoint, email, nuvem).
- A IA e a detecção de ameaças orientadas por aprendizado de máquina.
- Análise de tráfego criptografada (ETA).
- Orquestração de resposta automatizada.
- Atacar o gerenciamento de riscos superficiais e insights de postura.
- Aproveita a inteligência global de ameaças.

Prós:

- Fornece uma visão holística e unificada da segurança em várias camadas.
- Simplifica operações de segurança com visibilidade centralizada.
- Forte inteligência de ameaças de micro pesquisa de tendência.
- Eficaz para ambientes híbridos e de várias nuvens.
- Reduz a fadiga de alerta com detecções correlacionadas.

Contras:

- Os benefícios completos exigem a adoção da plataforma mais ampla da visão.
- Pode não ter a mesma profundidade da rede forense de rede pura que alguns nicho NDRs.
- A integração com micro ferramentas não tendências, embora suportada, pode ser menos nativa.

? Melhor para: organizações que buscam uma plataforma XDR unificada que integra o NDR ao endpoint, email e segurança em nuvem para detecção abrangente de ameaças de camadas cruzadas e operações de segurança simplificadas.

? Try Trend Micro here ? Trend Micro Official Website

8. Fidelis

Por que escolhemos:

A Fidelis Elevate Network fornece uma solução forte de detecção e resposta de rede (NDR) como parte de sua plataforma “XDR ativa” mais ampla.

Sua força está em combinar profundamente visibilidade da rede Com os recursos de tecnologia de decepção e prevenção de perda de dados (DLP), oferecendo uma mistura única de detecção de ameaças, defesa proativa e proteção de dados, tornando -a eficaz contra ameaças sofisticadas e tentativas de exfiltração de dados.

Especificações:

Fidelis é um dos principais fornecedores de NDR no mercado. Sua plataforma de rede elevada monitora todo o tráfego de rede em alta velocidade, usando aprendizado de máquina, análise comportamental e inteligência de ameaças para detectar ameaças conhecidas e desconhecidas.

Oferece captura de sessão total, triagem de alerta automatizada e integração com sua tecnologia de engano e segurança de endpoint.

As principais especificações incluem análise abrangente do protocolo, análise de tráfego criptografada (ETA) e a capacidade de detectar ameaças e exfiltração de dados.

Motivo para comprar:

A Fidelis Elevate Network é uma excelente opção para empresas que requerem uma visibilidade profunda da rede, detecção avançada de ameaças e uma combinação única de tecnologia de decepção e prevenção de perda de dados.

Se você está procurando uma plataforma abrangente para não apenas detectar ameaças, mas também enganar ativamente os atacantes e proteger dados sensíveis, a Fidelis oferece uma solução poderosa.

Características:

- Visibilidade da rede profunda com captura de sessão total.
- Aprendizado de máquina e análise comportamental para detecção de ameaças.
- Análise de tráfego criptografada (ETA).
- Integração com tecnologia de decepção para o envolvimento precoce da ameaça.
- Recursos de prevenção de perda de dados (DLP).
- Triagem e resposta de alerta automatizado.
- Extensas ameaças de caça e ferramentas forenses.

Prós:

- Combinação única de NDR, engano e DLP.
- Fornece dados forenses ricos para investigações.
- Eficaz contra a exfiltração de dados e as ameaças internas.
- Bom para o engajamento proativo de ameaças usando decepção.
- Altamente escalável para grandes redes corporativas.

Contras:

- Pode ser uma solução complexa, exigindo analistas qualificados.
- Os benefícios completos são realizados ao utilizar a plataforma mais ampla da Fidelis Elevate.
- A implantação pode ser intensiva em recursos, dependendo do tamanho da rede.

? Melhor para: empresas que buscam uma solução avançada de NDR que integra profunda visibilidade da rede à tecnologia de decepção e prevenção de perda de dados para detecção abrangente de ameaças e proteção de dados.

`? Try Fidelis here ?` [Fidelis Security Official Website]

9. Netwitness

Por que escolhemos:

A NetWitness Network é conhecida por seus recursos forenses excepcionais e capacidade de fornecer visibilidade altamente granular ao tráfego de rede, incluindo captura completa de pacotes.

É uma solução madura preferida por grandes e complexas organizações globais e SoCs que precisam realizar investigações profundas, entender o contexto completo de um ataque e extrair evidências detalhadas de conformidade e remediação.

Especificações:

A NetWitness Network fornece uma visibilidade abrangente da rede por meio de captura completa de pacotes e análise de metadados.

Ele usa análise comportamental, aprendizado de máquina e inteligência de ameaças para detectar ameaças avançadas.

As principais especificações incluem detecção de ameaças em tempo real, poderosas ferramentas de investigação forense, reconstrução de sessões e integração perfeita com a plataforma mais ampla de rede (SIEM, UEBA, EDR) para operações de segurança unificadas.

Motivo para comprar:

A Rede de Netwitness é ideal para grandes empresas, agências governamentais e organizações com SoCs altamente maduros que exigem a mais profunda visibilidade da rede, captura completa de pacotes para análise forense e poderosas capacidades de caça de ameaças.

Se sua prioridade são dados granulares para investigações e conformidade abrangentes, a Netwitness é uma escolha de primeira linha.

Características:

- Captura completa de pacotes (FPC) para obter detalhes forenses incomparáveis.
- Detecção de ameaças de rede em tempo real e análise de anomalia.
- Protocolo profundo Parsing e visibilidade da aplicação.
- Reconstrução da sessão para um entendimento detalhado de incidentes.
- Avançando a caça de ameaças e os recursos de consulta personalizados.
- Integração com a plataforma de rede para XDR.
- Opções de implantação flexíveis (no local, nuvem).

Prós:

- Capacidades forenses líderes do setor.
- Profundidade incomparável de visibilidade da rede.
- Altamente personalizável para operações de segurança avançadas.
- Eficaz para investigação complexa de incidentes e análise de causa raiz.
- Escalável para redes corporativas muito grandes.

Contras:

- Requer armazenamento significativo para captura completa de pacotes.
- Curva de aprendizado mais acentuada, melhor para analistas de segurança experientes.
- Pode ser um investimento considerável em termos de custo e recursos.

? Melhor para: grandes empresas, organizações governamentais e SoCs maduros que exigem recursos forenses de rede incomparáveis, captura completa de pacotes e investigação de ameaças de mergulho profundo.

? Try NetWitness here ? NetWitness Official Website

10. Cyber estelar

Por que escolhemos:

A plataforma XDR Open Cyber Open fornece uma solução abrangente de operações de segurança que inclui inerentemente recursos de NDR.

Sua abordagem “Open XDR” permite ingerir dados das ferramentas de segurança existentes (incluindo EDRs de terceiros, firewalls e logs em nuvem) e correlacioná-los com seus próprios dados de sensor de rede.

Esta plataforma unificada simplifica operações de segurançaacelera a detecção e capacita as equipes de segurança enxuta com investigação e resposta automatizadas.

Especificações:

A plataforma estelar cibernética XDR ingere dados de várias fontes (NDR, EDR, SIEM, Cloud, Identity, SaaS) e os correlaciona em um lago de dados, aplicando AI/ml para detecção de anomalias e investigação automatizada.

Seu componente NDR fornece visibilidade da rede, análise comportamental e detecção de ameaças.

As principais especificações incluem ingestão de dados de várias fontes, correlação de ataque automatizado (mapeamento da cadeia de mortes), controle de acesso baseado em função e recursos de Soar integrados para resposta automatizada.

Motivo para comprar:

A plataforma XDR do Cyber Open Stellar (com NDR) é uma excelente opção para organizações que buscam simplificar suas operações de segurança, consolidar várias ferramentas de segurança e melhorar seus recursos gerais de detecção e resposta.

Se você possui uma equipe de segurança enxuta e deseja uma plataforma unificada que aproveite o NDR como um componente principal do XDR abrangente, a Stellar Cyber oferece uma solução atraente.

Características:

- Plataforma “Open XDR” unifica dados de várias ferramentas de segurança.
- Recursos NDR integrados para visibilidade da rede.
- Detecção e correlação de ameaças acionadas por IA/ML.
- Investigação automatizada e geração de enredo de ataque.
- Soar embutido para resposta automatizada.
- Visibilidade abrangente no ponto de extremidade, rede, nuvem e muito mais.
- Reduz o tempo médio para detectar (MTTD) e o tempo médio para responder (MTTR).

Prós:

- Simplifica as operações de segurança, unificando várias ferramentas.
- Acelera a detecção e a resposta com automação.
- Bom para as equipes de segurança enxuta que procuram cobertura abrangente.
- A abordagem agnóstica do fornecedor se integra aos investimentos existentes.

- Fornece um forte gerenciamento geral de postura de segurança.

Contras:

- A natureza “aberta” significa que a eficácia pode depender da qualidade dos dados ingeridos.
- Requer integração eficaz com outras ferramentas de segurança para maximizar os benefícios.
- Embora abrangentes, alguns recursos de nicho podem ser menos especializados que os NDRs de jogo puro.

? Melhor para: organizações com equipes de segurança enxuta que desejam unificar e simplificar suas operações de segurança por meio de uma plataforma XDR aberta que inclui recursos robustos de NDR e automatiza a detecção e resposta de ameaças.

`? Try Stellar Cyber here ?` [`Stellar Cyber Official Website`]

Conclusão

À medida que as ameaças cibernéticas continuam evoluindo em furtividade e sofisticação, confiar apenas nas defesas do perímetro não é mais uma estratégia viável.

As soluções de detecção e resposta de rede (NDR) tornaram -se uma pedra angular da segurança cibernética moderna, fornecendo a visibilidade e a inteligência críticas necessárias para detectar, investigar e responder a ameaças que ignoram os controles de segurança tradicionais.

Ao monitorar continuamente todo o tráfego de rede, incluindo o Crucial Leste-Oeste de Comunicações NDR oferece uma defesa proativa contra ameaças privilegiadas, movimento lateral e ameaças persistentes avançadas.