



Inteligência



Visibilidade



Resposta a Ameaças na Rede

O **Blockbit NDR (Network Detection and Response)** é uma solução avançada que combina monitoramento contínuo da rede, análise comportamental e resposta automatizada a incidentes. Desenvolvido na Plataforma Blockbit, proporciona visibilidade completa do tráfego de rede, permitindo identificar ameaças conhecidas e desconhecidas antes que causem danos.

A integração nativa com o Blockbit CTI (Cyber Threat Intelligence) eleva o nível de detecção e resposta, garantindo que o Blockbit NDR esteja sempre atualizado com as mais recentes ameaças emergentes, vulnerabilidades e táticas de ataque. Isso melhora significativamente a precisão na identificação de ameaças, reduzindo falsos positivos e acelerando respostas a incidentes, permitindo que sua empresa esteja sempre à frente dos cibercriminosos.

O Blockbit NDR é a peça-chave para um SOC eficiente, proporcionando visibilidade total da rede, detecção inteligente de ameaças e resposta automatizada em tempo real. Com inteligência integrada e análise avançada de tráfego, sua equipe de segurança ganha o poder de antecipar, neutralizar e mitigar ataques antes que causem impacto.

Conheça os destaques do **Blockbit NDR**:



Análise Contínua do Tráfego de Rede

Monitoramento em tempo real de pacotes e metadados.



Detecção Baseada em Comportamento

Identificação de ameaças sem assinaturas tradicionais.



Integração Nativa com o Blockbit CTI

Inteligência de ameaças em tempo real para detecção mais precisa.



Machine Learning e Threat Intelligence

Correlação avançada de dados para minimizar falsos positivos.



Resposta Automatizada a Incidentes

Contenção rápida e mitigação de ameaças.



Integração com SIEM, XDR e SOAR

Correlação de eventos para resposta coordenada.



Flexibilidade de Implantação

Disponível como hardware appliance, virtual appliance e em nuvem.

Sobre a Blockbit

A **Blockbit** é líder em produtos de cibersegurança, protegendo milhares de empresas e milhões de usuários de ataques e ameaças digitais.



+5M
clientes corporativos



+2MM
usuários protegidos

Principais Funcionalidades

Monitoramento e Análise de Tráfego

- **Deep Packet Inspection (DPI):**
Inspeção detalhada do tráfego de rede, incluindo pacotes criptografados.
- **Análise de Tráfego Criptografado sem Descriptografia**
(Encrypted Traffic Analysis - ETA)
- **Detecção e prevenção de intrusões (IPS):**
Inspeção detalhada do tráfego de rede, detecta e responde à ataques.
- **Threat Protection (ATP):**
Proteção avançada contra malware e ataques sofisticados.
- **Cloud Sandbox:**
Execução de arquivos suspeitos em ambiente isolado.
- **NetFlow e Análise de Metadados:**
Coleta e correlação de fluxos de tráfego para detectar anomalias.
- **Detecção de Movimentação Lateral:**
Identificação de comunicações suspeitas dentro da rede.
- **Análise de Tráfego Norte-Sul e Leste-Oeste:**
Visibilidade completa para detectar ameaças internas e externas.
- **Botnet Detection:**
Monitoramento para identificar comunicações maliciosas.

Integração com SIEM, XDR e SOAR

<p>Correlação de Eventos Avançada</p>	<p>Indicadores de Comprometimento (IoCs)</p>	<p>Orquestração de Resposta a Incidentes</p>
<p>Análise de múltiplas fontes para detectar padrões de ataque.</p>	<p>Identificação e resposta rápida a ameaças conhecidas.</p>	<p>Automatização de workflows de segurança.</p>

Blockbit CTI

Cyber Threat Intelligence

Correlação em Tempo Real

Acesso a informações sobre ameaças emergentes e vulnerabilidades.

Detecção Aprimorada

Redução de falsos positivos e maior precisão na análise de ameaças.

Prevenção Proativa

Neutralização de ataques antes que se concretizem.

Resiliência Cibernética

Adaptação contínua às novas táticas e estratégias dos cibercriminosos.

Forense e Retenção de Dados



Captura de Pacotes (PCAP):

Coleta de tráfego para análise forense.

Retenção e Armazenamento de Logs:

Registro detalhado para auditoria e conformidade.

Relatórios Personalizáveis:

Insights sobre ameaças e atividades suspeitas.

Implantação Flexível



Hardware Appliance

Modelos para diferentes volumes de tráfego.



Virtual Appliance

Compatível com VMware, Hyper-V, Proxmox e KVM.



Cloud Instance

Suporte para AWS, Azure, Google Cloud, Oracle Cloud e IBM.

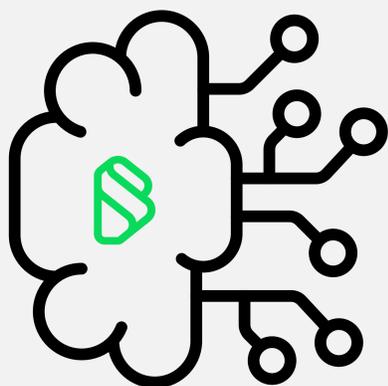
Desempenho e Especificações Técnicas

Modelo	Throughput de Análise (IMIX)	Análise SSL/TLS	Eventos Simultâneos
BBX40	200 Mbps	150 Mbps	4M conexões
BBX80	850 Mbps	700 Mbps	6M conexões
BBX140	1.5 Gbps	1.2 Gbps	7.5M conexões
BBX200	2.5 Gbps	1.3 Gbps	8.2M conexões
BBX700	3.6 Gbps	2.2 Gbps	20M conexões
BBX1500	6.5 Gbps	4.5 Gbps	22M conexões
BBX3000	13 Gbps	10 Gbps	30M conexões
BBX3600	20 Gbps	12 Gbps	45M conexões
BBX4200	26 Gbps	14 Gbps	55M conexões
BBX5000	40 Gbps	20 Gbps	70M conexões

Antecipe ameaças e automatize sua defesa com **inteligência avançada**

O Blockbit NDR vai além do monitoramento e resposta a ameaças – sua integração nativa ao Blockbit Cyber Threat Intelligence (CTI) permite acesso contínuo a uma rede global de inteligência sobre ameaças cibernéticas. Por meio da análise de milhões de eventos de segurança, machine learning e correlação avançada de dados, identifica padrões de ataque emergentes e antecipa riscos antes que comprometam sua infraestrutura.

Com monitoramento contínuo do tráfego de rede, detecção automatizada de ameaças e integração nativa com SIEM, XDR e SOAR, o Blockbit NDR fortalece a postura de segurança da sua organização, garantindo visibilidade total, análise preditiva e resposta automatizada contra ataques cibernéticos sofisticados.



Visibilidade Total e Análise Comportamental

Detecção Inteligente de Ameaças com Machine Learning

Resposta Automatizada para Mitigação Rápida

Correlação de Eventos e Integração com XDR/SIEM

Proteção Aprimorada com Inteligência Global do Blockbit CTI

Sobre a **Blockbit**

Com tecnologias de última geração e avançado laboratório de inteligência, a **Blockbit** desenvolve soluções proprietárias para proteção máxima de seus clientes, combinando alta qualidade e performance, sempre alinhada às principais tendências globais de cibersegurança.

Com a Blockbit, é fácil estar **seguro**

