A melhor resposta quando suas defesas falham

Detecte ameaças infiltradas na rede e responda a incidentes que ferramentas comuns não conseguem impedir.

Sumário executivo

O Zerum Lynx™ é uma solução completa de Detecção e Resposta a Incidentes em Rede (**Network Detection and Response - NDR**). Com ele, sua empresa identifica e reage rapidamente aos ataques mais avançados, evitando danos, facilitando a análise forense e reduzindo drasticamente o tempo de indisponibilidade.

Visibilidade sem igual

O Zerum Lynx provê informações cruciais para Resposta a Incidentes, coletando e analisando tudo que acontece na sua rede em tempo real.

- Monitore e analise o tráfego de rede, aplicações, bancos de dados e IOT;
- Acelere a investigação com interface intuitiva e flexível de Security Analytics;
- Customize visualizações e dashboards de acordo com cada caso de uso;
- Encontre informações e evidências rapidamente com busca instantânea;
- Resgate dados históricos para facilitar processos de auditoria.

Resposta inteligente

Com um sistema robusto de correlacionamento, o Zerum Lynx™ entende, enriquece e contextualiza os dados coletados, ajudando na detecção de ameaças em meio a milhões de transações e eventos.

- Conte com um conjunto embarcado de algoritmos de IA desenvolvidos para detectar as ameaças mais avançadas;
- Tenha integração nativa com fonte de Threat Intelligence líder de mercado;
- Receba alarmes contextualizados que reduzem ruídos e agilizam as análises.

Resultados imediatos

O Zerum Lynx™ entrega visibilidade e inteligência em uma solução de alta performance, que proporciona agilidade total da implementação à detecção e resposta a ataques.

- Plug & Play
- Integrável
- Escalável
- Suporte especializado

Funcionalidades

O Zerum Lynx™ é fornecido como appliance (físico ou virtual), integrando hardware, software e firmware em versões estáveis e constantemente atualizadas para perfeita execução de todas as suas funcionalidades com performance e confiabilidade.

Coleta, armazenamento e análise forense de dados de segurança

O Zerum Lynx™ unifica diversas funcionalidades avançadas de **coleta, armazenamento e análise de dados para cibersegurança**, proporcionando **visibilidade superior e rapidez para resposta a incidentes e análise forense**.

Coleta e armazenamento de dados

Tráfego de rede, logs, flows e metadados

Captura e armazenamento contínuo e não-intrusivos, com indexação automática de todos metadados e eventos. Coleta de tráfego via espelhamento passivo, ERSPAN e máquina virtual.

Análise de dados da camada de aplicação

Realiza a extração de metadados, em camada de aplicação *layer 7*, em tempo real, permitindo análises minuciosas de transações nos protocolos HTTP 1.0 e 1.1, LDAP, AJP, DNS, TNS, PostgreSQL, MySQL, TDS, DRDA, NFS, SMB/CIFS v1 e v2, TLS 1.0 a 1.3, SMTP, dentre outros. Para os protocolos HTTP e AJP até o conteúdo *body HTML* da transação pode ser coletado.

Granularidade máxima

No Lynx cada transação em rede é reconstruída de forma completa e intuitiva, juntando requisição e resposta no mesmo evento.

Agentes auxiliares

Possibilita a coleta de metadados de rede, métricas e eventos de máquinas Windows e Linux com auxílio de agentes.

Armazenamento inteligente de logs

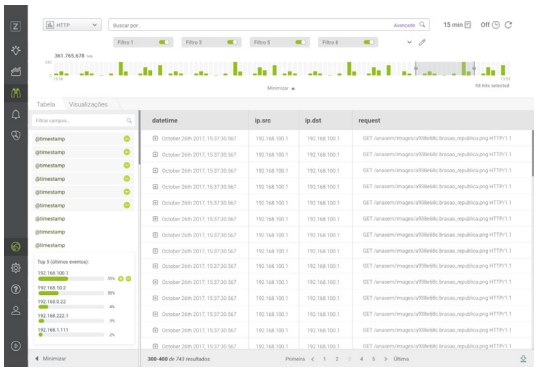
Suporte a eventos provenientes de SYSLOG, SNMP, MS Event Logging API, CEF e SNMP, dentre outros.

Deep Packet Inspection (DPI)

Realiza a reconstrução de sessões e o reconhecimento automático de aplicações, mesmo quando estas utilizam portas diferentes do padrão. Suporte a WhatsApp, Skype, YouTube, Netflix, Webmails, Telegram, Spotify, FTP, POP, SMTP, IMAP, DNS, HTTP, NFS, SMB, PostgreSQL, MySQL, Oracle (SGBD), MS SQL, RTSP, GRE, SSH, HTTPS, HTTP Proxy, SIP, VNC, Telnet, RDP, Websocket, Bittorrent, dentre outros protocolos e aplicações.

Monitoração remota (call home)

Emite alertas automaticamente caso a solução deixe de receber informações/eventos.



Resposta a Incidentes e Análise Forense

Coleta contínua de tráfego

Armazenamento em formato PCAP, realizando a correlação automática com todos os metadados de rede extraídos

Recuperação e reconstrução completa de arquivos

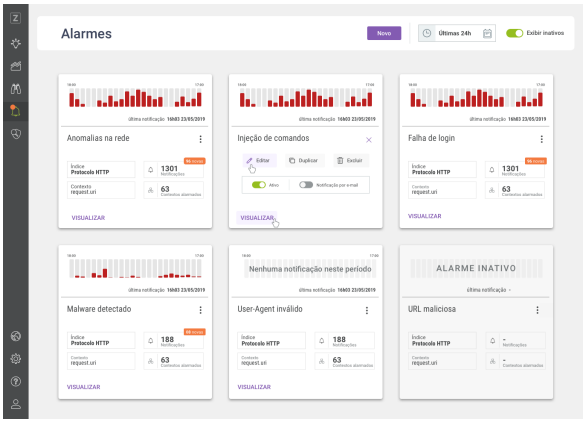
A partir do tráfego em protocolos HTTP, SMTP, SMB, FTP, POP3, IMAP, dentre outros.

Interface Web HTTP/S

O Zerum Lynx conta com interface web totalmente em HTML5, intuitiva e de fácil utilização, para execução de investigações de ataques e resposta a incidentes, fornecendo:

- Exploração rápida e fácil das informações, com correlação de eventos de diferentes origens e metadados extraídos em tempo real;
- Criação de dashboards totalmente customizados, com gráficos e tabelas definidos pelo usuário, usando informações de eventos, pacotes e flows presentes no sistema;
- Gráficos: o sistema permite a criação de gráficos de pizza, área, linha, barras, dispersão e grafos, dentre outros. O usuário pode definir a granularidade e o período a ser exibido, de forma totalmente intuitiva;
- Buscas com filtros textuais em todo o conteúdo armazenado, permitindo o uso de expressões regulares, palavras-chave e operadores lógicos. Todo o conteúdo do sistema é indexado automaticamente;
- Correlação, filtragem e download de arquivos PCAP de forma fácil e rápida, possibilitando a extração apenas dos dados necessários para investigação.

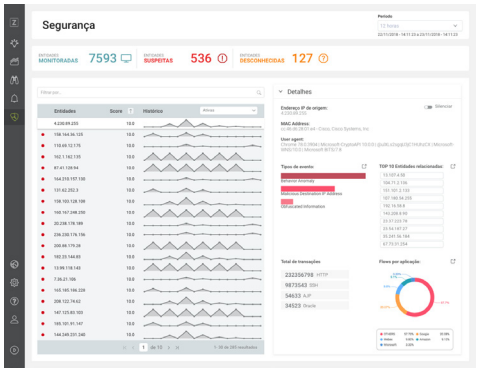
Criação de alarmes



Permite a criação de alarmes totalmente customizados, com verificação automática de regras e correlação de eventos e metadados em tempo real, oferecendo recursos avançados:

- **Aprendizado Inteligente**: realiza a análise de dados a partir de aprendizado dinâmico, em modelo treinado de acordo com parâmetros do usuário;
- **Contexto Automático**: identifica automaticamente contextos para os alarmes, de acordo com valores de campos apontados pelo cliente (ex.: IP, host, URL, etc);
- **Seleção de destinatários**: defina quem deve receber os alertas de cada alarme configurado. Cada alerta também é exibido em interface, de forma simples e intuitiva;
- **Integração**: todos os alarmes são exibidos na interface Security Analytics e enviados via CEF ou e-mail. O Zerum Lynx suporta ainda a integração com orquestradores de segurança (Security Orchestration Automation and Response), SIEM e bases de conhecimento diversas.

Análise de reputação



O Zerum Lynx calcula automaticamente a reputação de usuários e endpoints (computadores, servidores, IOT, etc) permitindo aos analistas de segurança identificar rapidamente quais são as maiores ameaças e vetores de ataques presentes na organização. O sistema monitora o status de risco de qualquer dispositivo que possua um endereço IP.

Inteligência Artificial e Threat Intelligence

Além de fornecer visibilidade superior, o Zerum Lynx™ combina **algoritmos de Inteligência Artificial, integração com Threat Intelligence e recursos avançados de enriquecimento** para correlacionar e contextualizar os dados e eventos coletados. Isso reduz a sobrecarga de notificações e acelera o processo de investigação com insights mais precisos e relevantes.

Inteligência Artificial

Algoritmos especializados de Cibersegurança ZML - Zerum Machine Learning®

O Zerum Lynx possui um conjunto de algoritmos de inteligência artificial, supervisionados e não-supervisionados, capazes de detectar anomalias de comportamento, insider threats e ataques de zero-day. Em caso de detecção de ataques alertas são gerados instantaneamente, correlacionando automaticamente diversas informações, inclusive de threat intelligence, geolocalização e demais informações para melhor entendimento do contexto do ataque. Entre os algoritmos da solução estão:

- **User & Entities Behavior Analytics (UEBA)**

  Realiza o aprendizado do comportamento de endpoints e usuários em rede através de algoritmo de Deep Learning e metadados do tráfego de rede, identificando anomalias e insider threats que sistemas convencionais não conseguem detectar;

- **DGA Detection**

  Detecta queries DNS e acessos HTTP a domínios criados dinamicamente, pelo Domain Generational Algorithm - DGA. Esse domínios são utilizados frequentemente por malwares diversos, como ransomware.

- **Beaconing Detection**

  Algoritmo especializado em detectar tráfego com comportamento de beaconing, técnica comumente utilizada por bots e malwares;

- **Command Injection Detection**

  Inspeciona o payload de aplicações e identifica anomalias em seu conteúdo automaticamente, a partir de treinamento customizado;

- **Streaming Malware Detection**

  Algoritmo especialmente treinado a partir de milhões de amostras de malwares. Detecta ataques de Zero-Day com extrema eficiência, 25 dias antes de antivírus convencionais, com excelente acurácia;

- **Network Scan Detection**

  Detecta varreduras em rede, quando atores maliciosos estão procurando brechas nos sistemas e buscando fazer movimento lateral;

- **Brute Force Detection**

  Identifica anomalias em transações de autenticação como tentativas de descobrir senha ou nome de usuário através de combinações aleatórias;

- **Dynamic Baseline**

  Algoritmos para detectar, por exemplo, desvios em volume de dados, inundação de pacotes, ataques de negação de serviços e comportamento de bots.

Threat Intelligence, enriquecimento e correlacionamento

Integração nativa com Threat Intelligence

Possui integração nativa com a base de inteligência de ameaças da OpenText/Webroot, líder mundial em informações de Threat Intelligence, para correlação dos dados.

Alertas automáticos

Em caso de transações com endereços IP, URLs, Hosts HTTP e Hashes MD5 de arquivos maliciosos e demais eventos detectados, com informações de contexto.

Integração com sistemas de enriquecimento

Conta com integração a sistemas diversos de enriquecimento das informações e auxílio nas investigações de ataques, como whois, nslookup e GeoIP. Permite ainda a integração sob demanda com outras fontes para o enriquecimento de dados.

Fingerprinting

Executa o fingerprinting de endpoints para identificação automática de Sistema operacional e Navegador a partir do tráfego de rede.

Correlação com nome de usuário

Correlaciona automaticamente o IP do endpoint com o nome e o grupo do usuário.

Identificação automática do formato e mime-type do arquivo, independente da extensão informada, permitindo o alerta em caso de suspeita de adulteração.

Garantia de segurança e sigilo dos dados

Conta com processos e mecanismos internos para assegurar a segurança e o sigilo dos dados capturados, indicando caso algum pacote capturado sofra violação de integridade. Todos os processos, incluindo análise e detecção de ameaças, são feitos pela solução localmente e de modo seguro, sem que os dados precisem ser transmitidos para ambientes externos.

Exportação de dados

Todos dados coletados são armazenados em formato JSON e podem ser exportados para outros sistemas utilizando API HTTP REST ou protocolo AMQP.

Análise de Performance

Cada transação em rede tem sua performance calculada, extraindo as seguintes métricas:

- **Server Connection Time (SCT)**: Performance para abrir a conexão TCP;
- **Client Time (CT)**: Performance de execução da requisição pelo cliente, após início da conexão TCP;
- **Server Processing Time (SPT)**: Performance para resposta da requisição pelo servidor;
- **Data Transfer Time (DTT)**: Performance para transmissão dos dados da resposta;
- **Transaction Time (TT)**: Tempo total para concluir requisição e resposta da transação;
- **Quantidade de pacotes Zero Window**
- **Quantidade de retransmissões TCP**

Webroot

Threat Intelligence

Os serviços de Threat Intelligence Webroot BrightCloud® utilizam sensores espalhados por todo o mundo para coleta contínua de informações de ameaças em serviços on-line. A plataforma contém mais de 25 bilhões de endereços de IP e URLs, categorizados e atualizados dinamicamente de acordo com a evolução de ataques que acontecem a todo momento, utilizando machine learning para classificar cada um de acordo com a ameaça que representam para seu negócio. O serviço ainda fornece o histórico de ameaça e reputação de endereços IP.

Streaming Malware Detection

O Streaming Malware Detection Webroot BrightCloud® inspeciona arquivos, pacote por pacote, enquanto são transmitidos através de dispositivos de rede. Realizando determinações sobre malware polimórfico, zero-day e outros tipos de arquivos maliciosos, o serviço consegue detectar um malware antes que se infiltre na rede, permitindo que dispositivos parceiros os bloqueiem ou redirecionem para investigação aprofundada.

- Fornece pontuações de risco para arquivos enquanto são transmitidos por dispositivos de rede;
- Realiza determinações onboard em milissegundos - acima de duas ordens de magnitude mais rápido que tecnologias convencionais de sandbox de rede;
- Melhora o desempenho da rede e reduz a latência minimizando a necessidade de reinspecionar arquivos considerados benignos;
- Faz proveito da escala massiva de machine learning avançado, aprimorando continuamente suas capacidades;
- Analisa o conteúdo de +5 mil arquivos por minuto, sem uso de sandbox.

File Reputation Service

O serviço de Reputação de Arquivos Webroot BrightCloud® fornece um serviço de lookup em tempo real para verificar rapidamente malware e arquivos, sejam maliciosos ou confiáveis, de forma que políticas possam ser estabelecidas para automatizar a permissão, bloqueio ou investigação dos mesmos.

- Reputações sempre atualizadas, baseadas em identificadores de arquivos maliciosos ou listados como confiáveis
- Detecção e prevenção desenvolvidas especificamente para infecções polimórficas singulares e outras ameaças emergentes de malware
- Um feed continuamente atualizado e mais de 36 bilhões de registros de comportamento de arquivos para descoberta de ameaças zero-day muito mais rápida que outros serviços

Hardware

O sistema do Zerum Lynx é altamente escalável, plug & play e de fácil gestão, além de contar com monitoração integrada de saúde e performance. A arquitetura em cluster horizontal com micro-serviços permite a adição de vários appliances para distribuição de carga, redundância dos dados e tolerância a falhas. O Zerum Lynx não possui limite de dispositivos monitorados, fazendo a análise de todos endpoints em rede, de acordo com a capacidade de recebimento de dados do(s) appliance(s).

Capacidade

Escalabilidade extrema, utilizando múltiplos appliances, permitindo armazenar meses ou anos de informações de pacotes (PCAPs) e eventos em estado bruto (raw).

Armazenamento de pacotes e eventos (logs e flows)	+100 Terabytes por appliance
Captura de pacotes	Até 100Gbps
Captura de eventos (logs e flows)	Até 100.000 eventos por segundo

Interface aceleradora para captura passiva de pacotes

- Suporte a IPv4 e IPv6;
- Marcação de timestamp em hardware;
- Recebimento de pacotes em túnel GRE;
- Buffer estendido para evitar perda de pacotes;
- Balanceamento de carga 5-tuple feito em hardware;
- Desduplicação de pacotes;
- Filtro para bloqueio de tráfego com informações de Protocolo, IP e porta;
- Sincronização de tempo com placas similares com precisão de nanosegundos.

Modelo	Velocidade	Portas	RAM Onboard
ZNT04	1Gbps	4 (SFP/SFP+)	4 GB
ZNT10	1/10 Gbps	2/4 (SFP/SFP+)	4 GB
ZNT40	40 Gbps	2 (QSFP28)	12 GB
ZNT100	100Gbps	1 (CFP4)	8 GB

Placa aceleradora para descriptografia

Descriptografia de sessões de rede, a partir do uso da chave-privada, com uso de Acelerador de Criptografia em hardware especializado para alta-performance.

ZAC10

Descriptografia de tráfego a 10Gbps
Até 100 mil operações por segundo (RSA 1024)

Arquitetura

O Zerum Lynx possui arquitetura para escalabilidade extrema. Todos os seus componentes permitem redundância e distribuição de carga, de forma automática. Os appliances Zerum Lynx são disponibilizados como máquinas virtuais ou físicas, podendo ainda ter todos os seus serviços distribuídos em múltiplos appliances.

Appliance virtual

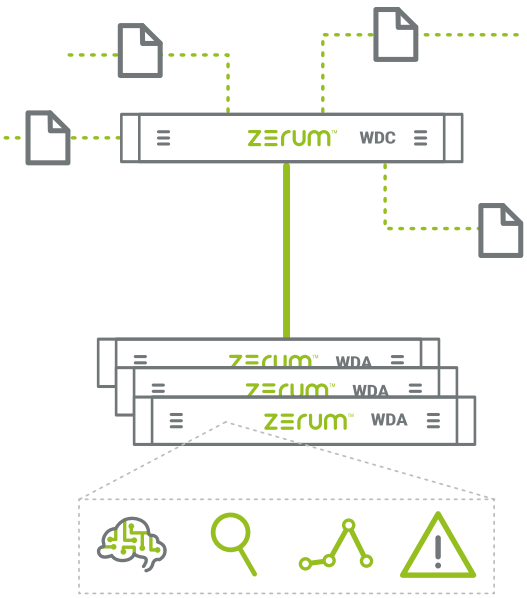
Pode ser implementado em nuvens VMWare e Amazon AWS, suportando throughput de +10Gbps.

Appliance all-in-one

Solução para demandas intermediárias onde todos os componentes são instalados em um único appliance, suportando throughput de até 4Gbps.

Cluster

Solução para demandas de grande porte. Prevê redundância de dados, tolerância a falhas e distribuição de carga. É implementada utilizando múltiplos appliances em formato físico e/ou virtual. Suporta throughput de +40Gbps.



Especificações Técnicas

Chassi	
Tamanho	1U montável em rack
Dimensões e peso	
Altura	1.7” (43mm)
Largura	17.2” (437mm)
Profundidade	27.82” (707mm)
Peso bruto	48lbs (21.8kg)
Baias de drive NVMe	
Hot-swap	10x 2.5” baias de drive NVMe Hot-swap
Drives NVMe	Até 10x drives NVMe
Refrigeração do sistema	
Exaustores	8 Exaustores com controle de velocidade otimizado
Fonte de alimentação	
Quantidade	2 Fontes de alimentação redundantes
Potência	1000W com PMBus
Voltagem	110/220V
Ambiente operacional / Conformidade	
RoHS	Em conformidade com RoHS
Especificações ambientais	
Temperatura operacional	De 10°C a 35°C (50°F a 95°F)
Temperatura de armazenamento	De -40°C a 60°C (-40°F a 140°F)
Umidade relativa operacional	De 8% a 90% (sem condensação)
Umidade relativa de armazenamento	De 5% a 95% (sem condensação)
Rede	
Interface de gerência	• 2 portas Ethernet 1/10GBASE-T RJ45 • 1 porta Ethernet Gigabit IPMI LAN dedicada RJ45
Part number	**Descrição**
ZRM-LNX	Zerum Lynx™ Appliance