NET SENSOR

CYBERSECURITY INTELLIGENCE

Identificação
e **bloqueio**
de ataques
cibernéticos.

O que é o NETSENSOR?

Composto por Hardware e Software, o NETSENSOR na borda da rede, à frente do Firewall tradicional e, até mesmo, à frente do roteador internet. Ele analisa o tráfego, identifica fontes maliciosas e, se assim estiver programado, **faz o bloqueio de ataques cibernéticos de maneira automática.**

A tecnologia do NETSENSOR utiliza conceitos de inteligência artificial (machine learning), de forma proativa e sem intervenção humana. Ele é capaz de **observar** de forma totalmente transparente todo o tráfego internet e **identificar padrões suspeitos** presentes na grande maioria dos ataques cibernéticos, **bloqueando-os já em suas fases iniciais**, antes que eles possam ser efetivados.

Através de uma interface WEB com **dashboard, gráficos e logs, o analista de segurança consegue acompanhar as tentativas de acesso maliciosas**, tipos dos tráfego, as aplicações mais atacadas e quais as origens desses ataques. Através de um mapa mundial o NETSENSOR destaca os países que originaram as tentativas de ataque, os colorindo conforme a quantidade (mapa de calor).

É uma incrível experiência de visibilidade das tentativas de ataques detectadas e bloqueadas, inclui estatísticas dos bloqueios realizados, quais os IPs e os Paises de origens, bem como quais as aplicações que mais sofreram tentativas de ataques.

Construído para promover uma proteção mais abrangente, inteligente e automática, é a ferramenta ideal para as corporações que estão em constante busca de soluções inteligentes para garantir a gerencia de eventos de segurança das informações.

Ao utilizar conceitos de inteligência artificial (machine learning) voltados à cibersegurança, o NETSENSOR, contribui de maneira consistente para oferecer soluções que possibilitam **aumentar a segurança do ambiente de TI da sua empresa.**

Como funciona
o NETSENSOR?

Para entender como funciona, é necessário entendermos como o NETSENSOR é instalado e quais são as suas funções.

Instalação do NETSENSOR:

O NETSENSOR é instalado na entrada do link de internet das corporações, para isso disponibiliza interfaces ethernet gigabit ou interfaces de fibra óptica.

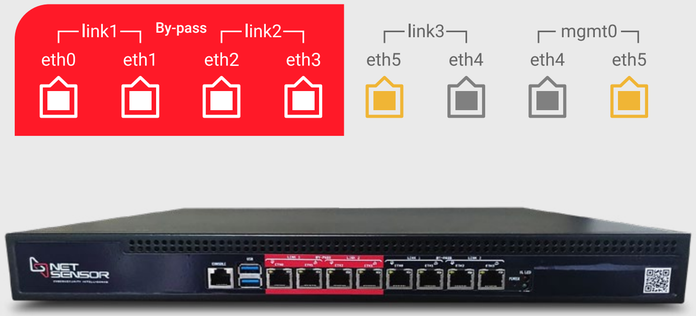
Para cada link a ser monitorado, o NETSENSOR disponibiliza 2(duas) Interfaces, sempre em pares. A 1º (primeira) interface está programada para receber o link e a 2º (segunda) interface está programada para repassar o link para a rede do cliente com total transparência, sem fazer nenhuma alteração.

O NETSENSOR trabalha de forma totalmente transparente do ponto de vista de topologia lógica, o que permite realizar sua instalação sem que seja necessário realizar qualquer alteração nas configurações de rede da estrutura existente, nem mesmo de alterar algum IP.

Para garantir ainda mais a qualidade de toda a instalação, foram homologados Hardware´s para cada tipo de projeto, o que garante robustez e alta qualidade com o melhor custo benefício. Opções como fontes redundantes e interfaces que utilizam a tecnologia by-pass também são disponibilizadas para os projetos com maior criticidade.

Basicamente a instalação consiste em conectar o cabo que vem da Operadora na 1º (primeira) interface do NETSENSOR e conectar a 2º (segunda) interface do NETSENSOR diretamente no Firewall ou roteador internet, ou seja, no mesmo local onde o cabo do link já estava conectado.

* Veja a linha de hardware que melhor atende o seu projeto.



Monitoramento do Link de Internet

Assim realizada a instalação do NETSENSOR, é iniciado o monitoramento de todo o trafego que por ali passa. Através do uso de sensores o NETSENSOR realiza o bloqueio e registro de todos os ataques detectados.
Para cada Link de Internet a ser monitorado, o NETSENSORdisponibiliza 1(um) par de interfaces elétricas (ethernet gigabit) ou interfaces ópticas (fibra óptica) com velocidades variadas. A 1º (primeira) interface recebe o Link da Operadora e a 2º (segunda) interface leva o Link até a rede onde o link estava conectado anteriormente.
*para cada link a ser monitorado o NETSENSOR necessita de 1(um) par de interfaces elétricas ou ópticas.

Configuração do NETSENSOR:
Antes de iniciar a configuração do NETSENSOR, é importante realizar uma análise criteriosa dos serviços válidos e reais do cliente, e isso poderá ser realizado de duas maneiras:

a) O cliente possui o controle de todas as informações dos serviços válidos e reais da rede, o que permite ativar os sensores que podem ser usados pelo NETSENSOR.

b) Para os projetos que o cliente possui dúvidas de quais os serviços podem ser bloqueados, sem que esse bloqueio traga algum transtorno, o NETSENSOR disponibiliza a opção ***"simulate"***, que permite analisar e simular quais seriam os resultados e quais seriam as origens bloqueadas caso esse sensor fosse habilitado para bloqueio.

Basicamente para configurar os sensores do NETSENSOR, é preciso saber quais serviços o cliente utiliza e quais portas não são usadas, permitindo a análise e ativação dos sensores mais eficientes para a carecterística daquela rede.
Nos projetos em que o cliente possui IPs válidos não usados, esses IPs podem ser habilitados e usados como iscas, pelo NETSENSOR, servindo como base de aprendizagem para a AI (Inteligência Artificial) do NETSENSOR.

Para acessar o sistema, o administrador receberá as credenciais para realizar a primeiro acesso.
O acesso ao NETSENSOR e às suas informações são realizadas através de uma **interface WEB amigável, intuitiva e rica em informações de fácil visualização e compreensão.**

Para realizar o acesso ao sistema, o NETSENSOR disponibiliza uma porta ethernet exclusiva, que possui configurado um IP padrão. (Informações como o IP, login e senha de acesso constam no manual de instalação). Todo o controle de quem irá fazer esse acesso é gerenciado pelo Administrador de Rede ou Analista de Segurança da empresa.

São disponibilizados dois tipos de usuários no NETSENSOR:

- **Administrador:** possui todas as permissões, inclusive de criar novos usuários. Tem administração total do NETSENSOR e das regras de bloqueio.

- **Operador:** possui permissões de acesso a todas as informações relevantes sobre o funcionamento do NETSENSOR e dos bloqueios, mas sem poder modificar regras de acesso, serviços e outros usuários.

Auditoria:
O sistema segue as mais rígidas normas de controle de acesso e segurança, todos os acessos são registrados incluindo quais foram as ações realizadas por cada usuário. Esses registros são armazenados e permanecem disponíveis para futuras consultas e auditorias.

Cada usuário terá acesso ao seu próprio cadastro onde poderá alterar seu perfil e personalizar as informações, bem como alterar a senha de acesso.

Configuração do Link:

Após realizadas as configurações de acesso, o próximo passo é identificar cada Link que será monitorado pelo NETSENSOR.

Para cada link a ser monitorado, podem ser identificadas informações sobre o link e a Operadora que o fornece.

Configuração de Rules Groups

É aqui que a mágica NETSENSOR começa, a configuração dos grupos de regras proporciona ao Analista de Segurança uma visão ampla e completa das tentativas de ataque detectadas e bloqueadas em seus links de Internet.

É disponibilizado nas configurações iniciais um grupo de regras de exemplo, “Default Rules Group”, que possui cadastrado diversos sensores que podem ser ativados e monitorados. Tem como objetivo demonstrar, auxiliar e facilitar a configuração inicial do sistema.

Configuração de Portas e Aplicações Monitoradas

Possibilita habilitar sensores em portas de serviços que não são disponibilizados através dos links internet (FTP, SSH, Telnet, SMTP, DNS, DHCP, VNC, MySQL, TFTP, NTP, RPC, NetBIOS-NS, IMAP, e qualquer outra porta não utilizada.
Através do monitoramento dos sensores do NETSENSOR, é possível ter uma visão completa e em tempo real das tentativas de invasões que estão acontecendo na rede monitorada.

Configuração de Origens confiáveis

Permite configurar que uma determinada origem jamais deve ser bloqueada por um sensor, assegurando que todas as solicitações que vierem de um determinado IP (uma origem confiável), consiga realizar o acesso sem nenhuma interferência.

É possível incluir nos Grupos de Regras, as regras de exceção para atender os Trusted Sources e o Real Services o que irá garantir que os serviços válidos não tenham nenhuma interferência ou bloqueio do sistema.

Configuração de Block or Simulate

A ativação da função Block deve ser feita nos sensores que deverão realizar bloqueio da origem. Assim que ativo, o NETSENSOR irá bloquear automaticamente todas as origens que disparem aquele sensor.

A configuração da função Simulate é indicada para aquelas portas onde há dúvidas do impacto causado se ela fosse bloqueada. Com isso, permite que o Administrador da Rede possa simular tal ação e ver quais IPs seriam bloqueados se essa regra estivesse ativa.
Na apresentação dos log’s de tentativas de ataque detectadas o NETSENSOR irá apresentar as informações da origem, destino, portas e a ação realizada.

Essa função permite que se tenha uma visão dos acessos destinados a uma determinada porta, possibilitando que antes que a regra seja configurada para bloqueio, o Administrador tenha uma simulação dos resultados que aconteceriam se tal regra fosse configurada para bloqueio.

Query Blocked IP

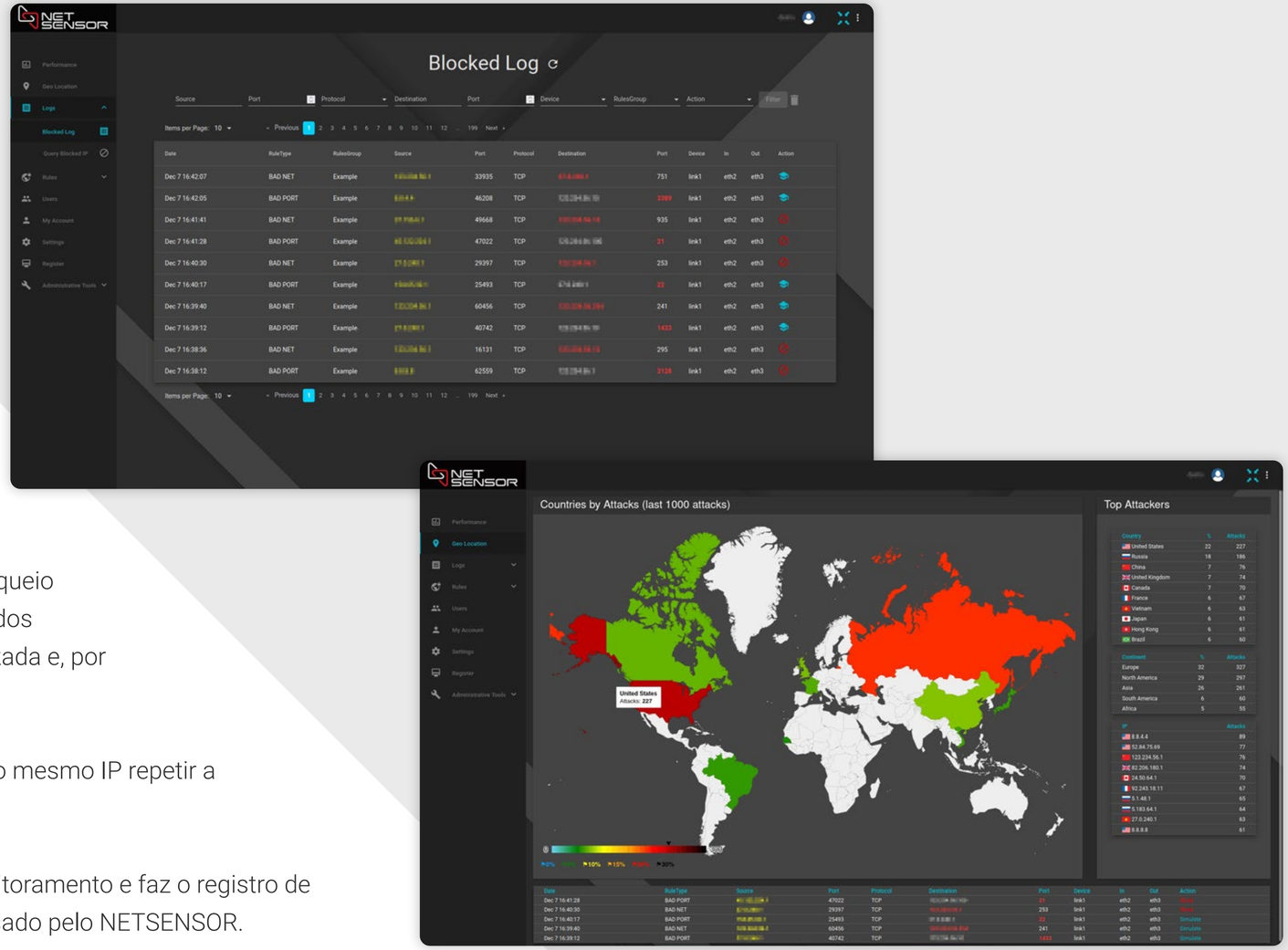
O NETSENSOR permite consultar se um determinado IP de origem foi bloqueado e qual foi o motivo do bloqueio. Na mesma tela da apresentação do resultado da pesquisa, o Administrador da rede tem a opção de remover o bloqueio desse IP.

O bloqueio de um IP ocorre quando ele tenta realizar acesso a um serviço e/ou alguma aplicação ou endereço indevido no qual foi configurado um sensor.

Essa funcionalidade facilita a gerencia na prática. Ela permite remover o bloqueio daquelas origens que, apesar de terem autorização para acessar determinados aplicativos, por “engano” tentaram fazer acesso a uma aplicação não autorizada e, por isso, tiveram o seu correto bloqueio.

*a ação de liberar o IP não irá alterar as regras configuradas no sistema, se o mesmo IP repetir a ação que o bloqueou, o NETSENSOR irá bloqueá-lo novamente.

Assim que instalado e configurado o NETSENSOR inicia o processo de monitoramento e faz o registro de informações que alimentam a base de dados da AI (Inteligência Artificial) usado pelo NETSENSOR.



Para que serve o NETSENSOR?

“O NETSENSOR foi construído para tornar a estrutura de rede de sua empresa invisível para os Hackers e visível para seus clientes”

O NETSENSOR foi construído para complementar a segurança do ambiente de TI. Combinado com as demais ferramentas de segurança, o NETSENSOR vem para agregar, agilizar e automatizar funções de bloqueios de tráfegos suspeitos, promovendo uma versatilidade e uma melhora significativa na segurança de acesso de sua empresa.

Com a implantação do NETSENSOR, todo o tráfego classificado como suspeito é bloqueado antes mesmo que possa iniciar um ataque, deixando a infraestrutura de rede de sua empresa invisível para os hackers, inclusive podendo desonerar de maneira significativa o processamento do Firewall durante períodos em que ele estaria sofrendo ataques.
Importante frisar que **o NETSENSOR não substitui a necessidade de outras ferramentas de segurança, como por exemplo um Firewall.**

O NETSENSOR, tem como proposta analisar informações relevantes do tráfego de Internet que chega na sua empresa e, de maneira automática, bloquear ataques em suas fases inicias antes que eles sejam efetivados.

O NETSENSOR irá te impressionar através da Dashboard e registros dos bloqueios de tráfegos maliciosos.

A instalação do NETSENSOR, irá otimizar a estratégia de defesa cibernética de sua empresa através da utilização da AI (Inteligência Artificial) e bloqueará de maneira automática tentativas de ataques, antes que eles sejam efetivados.

O dashboard do NETSENSOR proporciona uma visão completa e em tempo real de qual o trafego considerado maliciosos foi bloqueado e qual o trafego considerado malicioso seria bloqueado se a ação block estivesse sido habilitada

Com a constante atualização da base de conhecimento, através da AI (Inteligência Artificial), o NETSENSOR irá se aprimorar cada vez mais, terá respostas mais rápidas, mais atualizadas e mais eficazes.

Para quem serve
o NETSENSOR?

A cada dia que passa aumenta a quantidade de ataques cibernéticos e, cada vez mais, os criminosos tem sido bem-sucedidos na realização de seus crimes.

O roubo de informações com a cobrança de resgates já é uma realidade do nosso mercado e está cada vez mais perto.

Atualmente a frase; “se formos atacados... ” é substituída para “quando formos atacados! ”

Sem contar a perda e exposição dos dados e informações relevantes de uma empresa, o que isso pode representar ao mercado? Quais os verdadeiros prejuízos que essas invasões podem aferir diretamente na imagem da sua empresa?

O que realmente está em risco?

A paralisação de organizações de diversos tamanhos é cada vez mais comum no nosso dia a dia, o que só demonstra que a importância da segurança cibernética é cada vez maior.

O NETSENSOR foi construído para complementar a segurança de dados de uma empresa e, por utilizar a AI (Inteligência Artificial), consegue dar respostas mais rápidas e eficazes, e assim **permite dar um UP considerável na segurança da informação de sua empresa.**

O NETSENSOR, irá tornar a estrutura de segurança de sua empresa mais inteligente, forncendo uma camada extra que usa a AI (Inteligência Artificial) para tomar ações automáticas e possibilitar um controle muito mais abrangente e automático. Cada empresa terá seus próprios motivos para implantar o NETSENSOR, o que irá variar desde o tamanho da organização até o tipo de infraestrutura utilizada.

Temos a certeza que é possível melhorar em muito a segurança da informação de sua empresa com a instalação do NETSENSOR.

Se você está procurando uma ferramenta consistente, considere e deixe o NETSENSOR surpreender você. Tenha uma proteção mais eficiente, robusta e inteligente.

O que torna o NETSENSOR **diferente?**

Detecta atividades suspeitas e, de maneira rápida e eficaz, as bloqueia antes que elas efetivem um ataque.

Reduz as ameaças à segurança.
O NETSENSOR, através do uso de seu sistema de Inteligência Artificial, consegue detectar instantaneamente tráfegos maliciosos e faz o imediato bloqueio de sua origem.

Bloqueio automático, assim que é detectado, o tráfego suspeito é bloqueado pela origem e essa não consegue mais acessar a estrutura de rede, em outras palavras, a rede fica protegida, fica invisível para aquela origem classificada como maliciosa.

Desoneração do Firewall. Com a instalação do NETSENSOR, o tráfego suspeito é bloqueado pela sua origem. Com o bloqueio realizado pelo NETSENSOR, esse tráfego não chega mais ao Firewall, o que desonera o seu processamento.

Testes realizados em grandes corporações, constatou-se uma **redução no nível de processamento do Firewall**.

Todos os bloqueios realizados pelo NETSENSOR, sequer chegaram no Firewall.

“Sua estrutura de rede, invisível para os Hackers e visível para seus clientes”

NET SENSOR

CYBERSECURITY INTELLIGENCE

comercial@netsensor.com.br

(011) 3080 7900

(011) 3080 7900

www.netsensor.com.br