TREINAMENTO COMERCIAL

Claro empresas



Segurança
Soluções Digitais

Iniciar

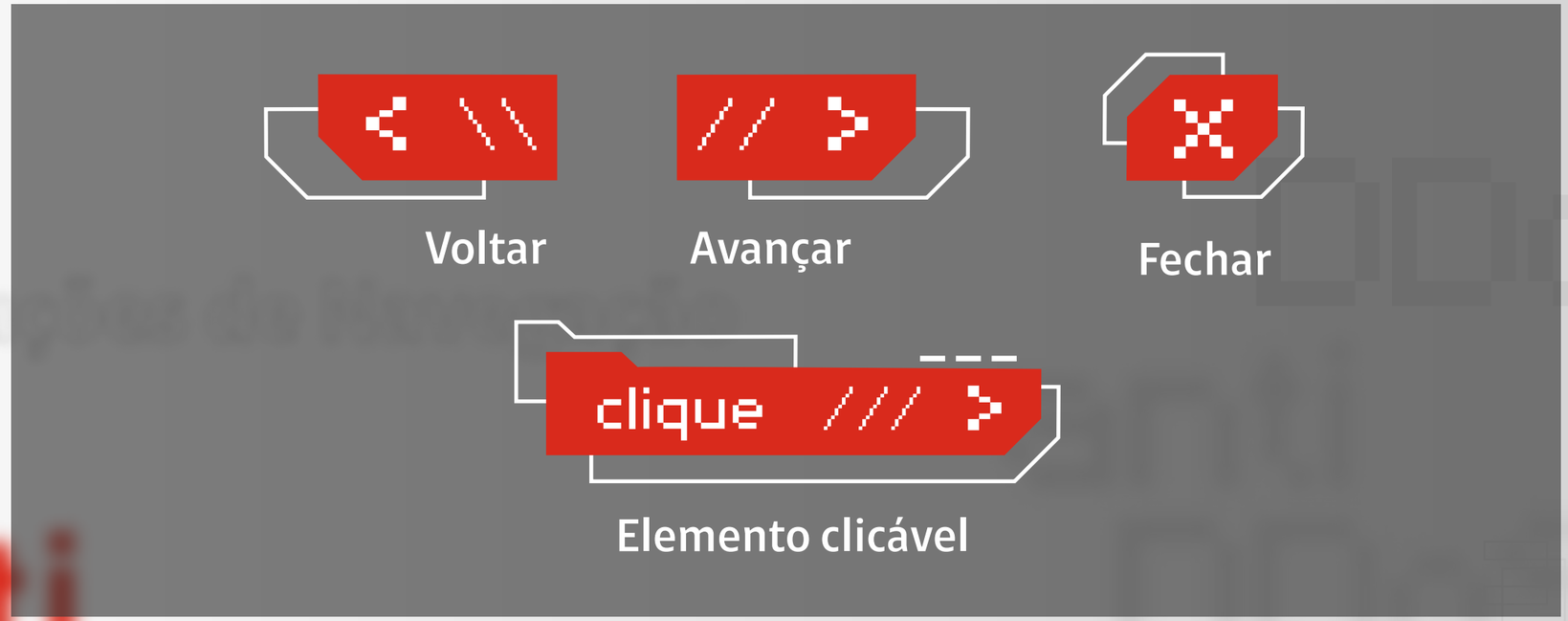
Clique para iniciar o treinamento

TREINAMENTO COMERCIAL

Claro empresas

Instruções de Navegação

Confira aqui como será a navegação e as interações do treinamento:



TREINAMENTO
COMERCIAL

Claro empresas



Seja bem-vindo

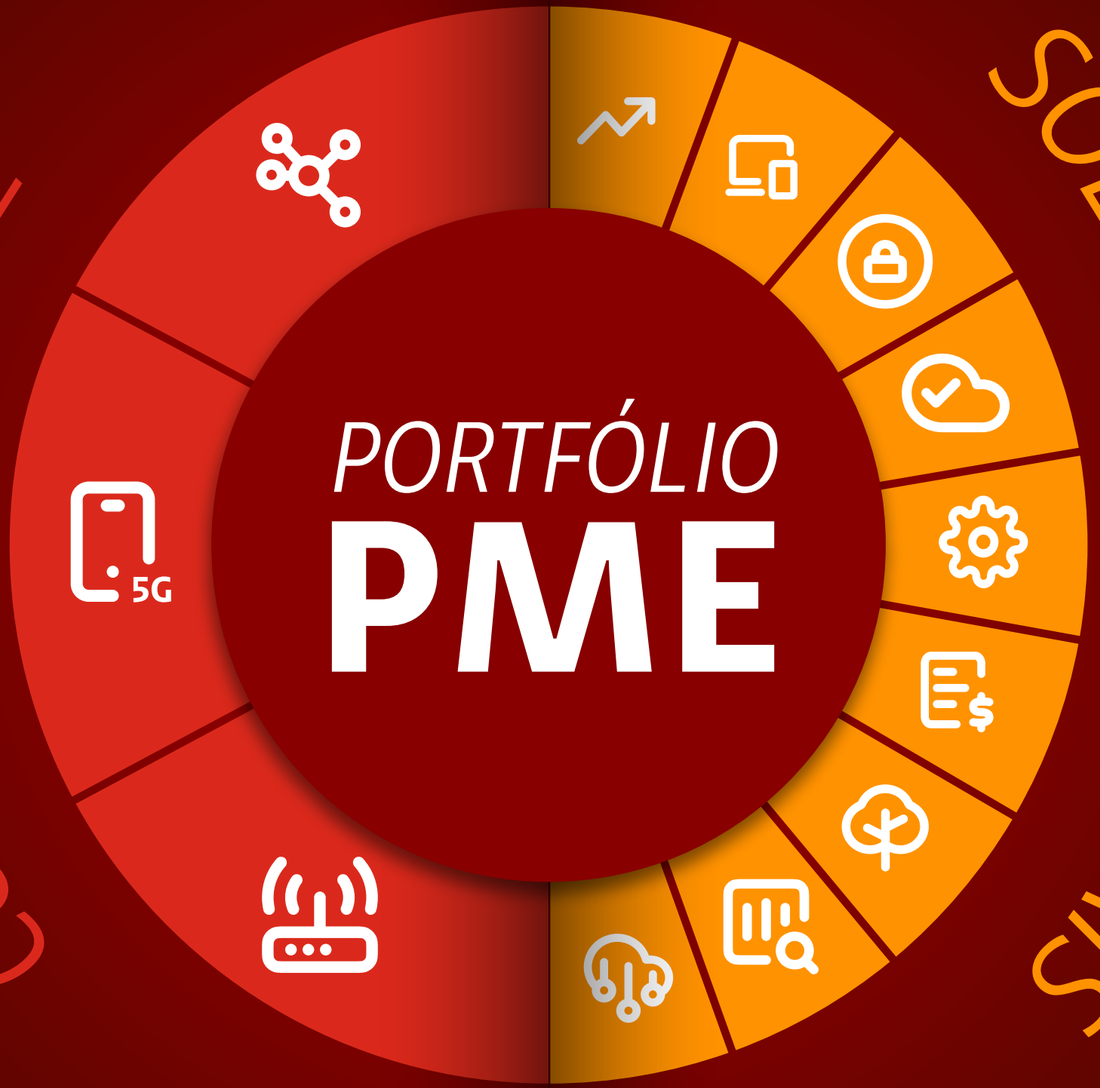
ao treinamento Anti-DDoS da Claro.

TREINAMENTO COMERCIAL

Claro empresas

CONECTIVIDADE

SOLUÇÕES DIGITAIS



PORTFÓLIO PME

TREINAMENTO COMERCIAL

Claro empresas



PORTFÓLIO PME

TREINAMENTO COMERCIAL

Claro empresas

PORTFÓLIO PME

Segurança

- Claro monitor (MDM)
- Proteção Digital (McAfee)
- Microsoft Defender
- Proteção de Dispositivos (EDR)
- Firewall gerenciado sem fio
- Firewall gerenciado
- WAF
- Anti-DDoS

TREINAMENTO COMERCIAL

Claro empresas

O mundo digital não para.

Empresas vendem, atendem e operam 24 horas por dia e, mesmo quando tudo parece normal, ameaças podem comprometer a operação.

Para garantir disponibilidade e continuidade dos negócios, é essencial contar com a proteção adequada.

Antes de entrar na solução tema deste treinamento, veja como as soluções de segurança da Claro empresas protegem a empresa do cliente.

Topologia dos Serviços

1

Empresas e colaboradores acessam a rede de diferentes lugares. Nesse contexto, **o SNOC da Claro** monitora e gerencia a segurança continuamente, garantindo mais proteção e disponibilidade para a operação dos clientes.



Topologia dos Serviços

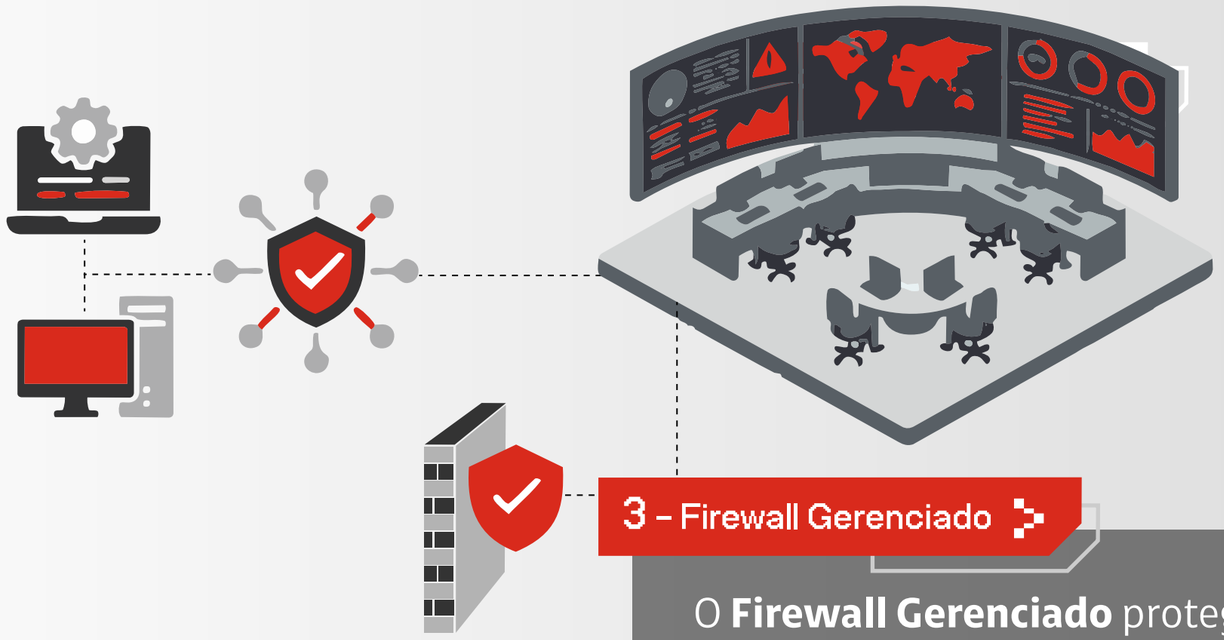
Iniciar



2 - EDR

EDR é a solução que pode ser instalada em cada dispositivo garantindo proteção independentemente de onde estejam conectados.

Topologia dos Serviços



3 – Firewall Gerenciado

O **Firewall Gerenciado** protege a rede, conecta matriz e filiais, permite acesso remoto e realiza balanceamento de link, garantindo mais estabilidade e segurança na conexão com o backbone da Claro.

Topologia dos Serviços



4 - Firewall Sem Fio

O **Firewall Sem Fio** é ideal para filiais pequenas: substitui o Wi-Fi comum por uma rede mais segura, com proteção suficiente para esse porte, mesmo sem todos os recursos de um firewall completo.

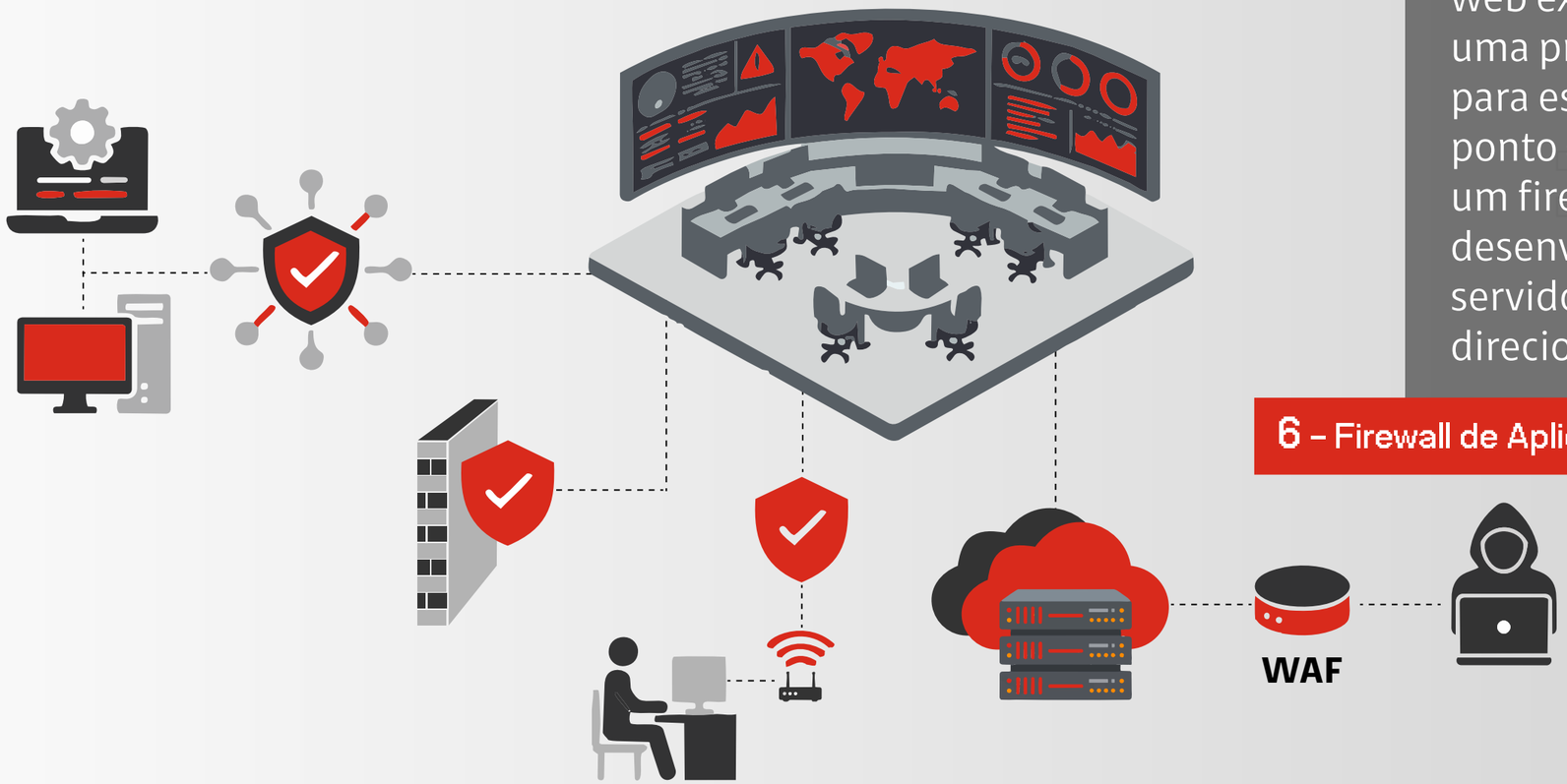
Topologia dos Serviços



5 – Servidor WEB

O **Servidor Web** oferece a infraestrutura para hospedar sites e outros serviços web que precisam ser acessados interna e externamente, podendo estar na nuvem ou na própria empresa.

Topologia dos Serviços



Sempre que há um serviço web exposto, é necessária uma proteção específica para esse ambiente. É nesse ponto que entra o **WAF**, um firewall de aplicação web desenvolvido para proteger servidores contra ataques direcionados às aplicações.

6 – Firewall de Aplicação Web

TREINAMENTO COMERCIAL

Claro empresas

Topologia dos Serviços



7 - Anti-DDoS

O **Anti-DDoS** detecta e filtra o ataque, enviando ao cliente apenas o tráfego legítimo. Seu funcionamento, diferenciais e benefícios serão detalhados ao longo deste treinamento.

TREINAMENTO COMERCIAL

Claro empresas

A partir dessa visão geral, começa sua jornada, com missões para aprofundar seu conhecimento sobre o Anti-DDoS da Claro.

TREINAMENTO COMERCIAL

Claro empresas

o que vamos ver

- O que é DDoS
- O anti-DDoS da Claro
- Como vender
- Como ativar

TREINAMENTO COMERCIAL

Claro empresas

o que vamos ver

- O que é DDoS
- O anti-DDoS da Claro
- Como vender
- Como ativar



Identificar a Ameaça

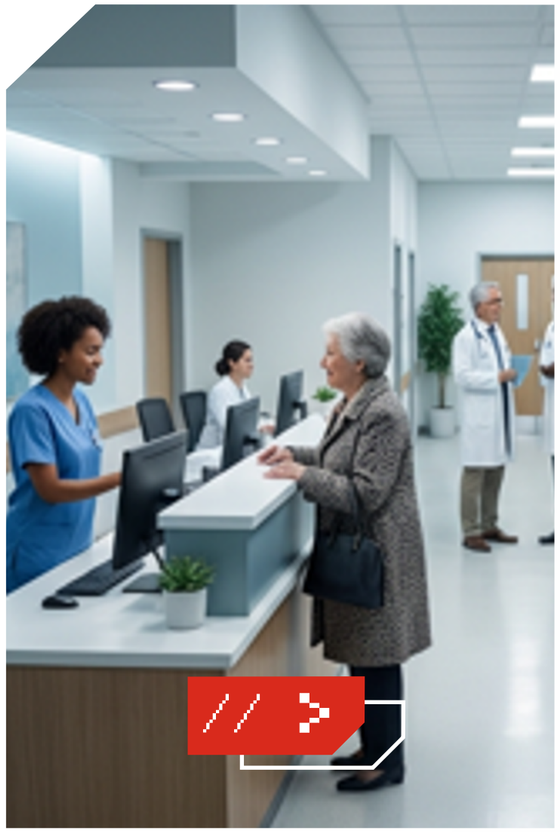
Neste momento, você assume o papel de **Protetor da Disponibilidade** — e sua primeira missão é conhecer o inimigo.

O vilão se chama **DDoS (Distributed Denial of Service)**. É um ataque cibernético que sobrecarrega servidores, redes ou aplicações, tornando os serviços indisponíveis.

TREINAMENTO COMERCIAL

Claro empresas

Clique para entender como o ataque DDoS acontece:







TREINAMENTO COMERCIAL

Claro empresas

Clique para entender como o ataque DDoS acontece:







TREINAMENTO COMERCIAL

Claro empresas

Clique para entender como o ataque DDoS acontece:







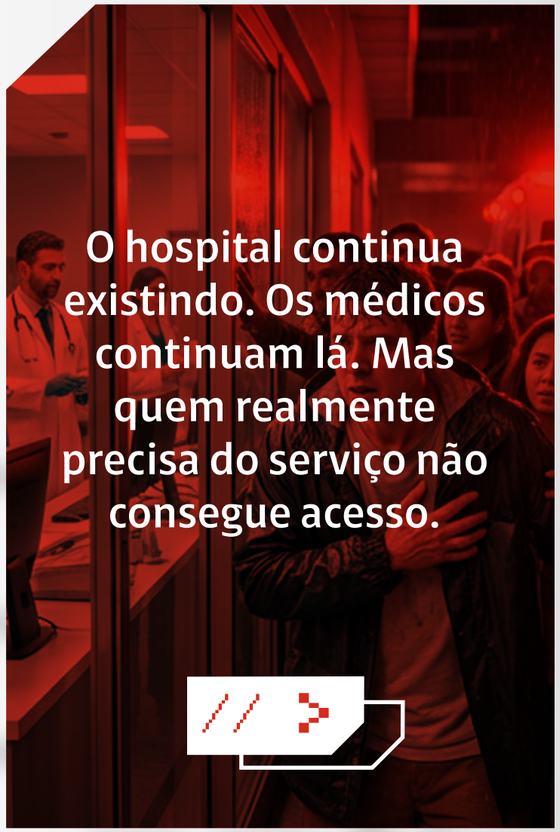
TREINAMENTO COMERCIAL

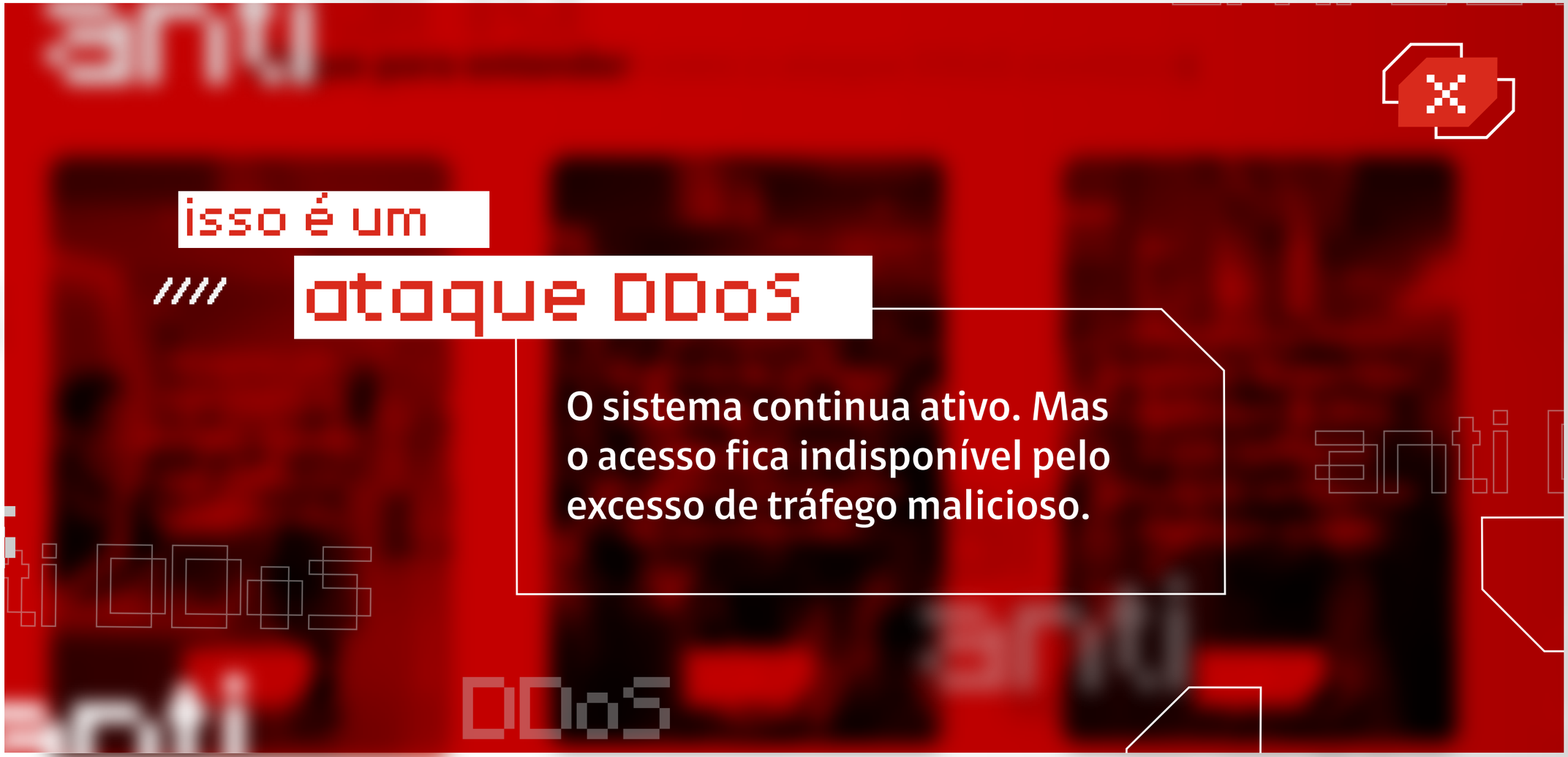
Claro empresas

Clique para entender como o ataque DDoS acontece:








isso é um
ataque DDoS
O sistema continua ativo. Mas o acesso fica indisponível pelo excesso de tráfego malicioso.

TREINAMENTO COMERCIAL

Claro empresas



- Qualquer dispositivo conectado à internet pode ser usado em ataques DDoS.
- Ataques DDoS **não** visam apenas grandes corporações.
- O ataque DDoS não é invasão ou roubo de dados, é indisponibilidade de acesso.

TREINAMENTO COMERCIAL

Claro empresas

Os ataques DDoS utilizam **diferentes métodos** para comprometer serviços online.

Ataques de Protocolo

Ataques na Camada de Aplicação

Ataques Volumétricos

É aqui que o Anti-DDoS Claro atua

Os ataques DDoS utilizam **diferentes métodos** para comprometer serviços online.

Os ataques de protocolo, exploram vulnerabilidades nos protocolos de comunicação, como TCP/IP e DNS, sobrecarregando recursos da infraestrutura ao manipular o próprio funcionamento da comunicação entre sistemas.



Ataques de Protocolo

Ataques na Camada de Aplicação

Ataques Volumétricos

É aqui que o Anti-DDoS Claro atua

Os ataques DDoS utilizam **diferentes métodos** para comprometer serviços online.

Os **ataques na camada de aplicação** tem como foco o servidor web ou a aplicação, por meio do envio massivo de requisições a páginas e APIs, simulando acessos legítimos até esgotar a capacidade de resposta do sistema.



Ataques de Protocolo

Ataques na Camada de Aplicação

Ataques Volumétricos

É aqui que o Anti-DDoS Claro atua

Os ataques DDoS são **diferentes métodos** para comprometer serviços online.

Os **ataques volumétricos** consistem no envio massivo de pacotes de dados com o objetivo de consumir toda a largura de banda disponível do alvo, impedindo o tráfego legítimo.

É exatamente nesse tipo de ataque que o Anti-DDoS da Claro atua, protegendo a rede antes que o impacto atinja o cliente.

Ataques de Protocolo

Ataques na Camada de Aplicação

Ataques Volumétricos

É aqui que o Anti-DDoS Claro atua

TREINAMENTO COMERCIAL

Claro empresas

Para finalizar sua primeira missão,
responda a questão a seguir.

TREINAMENTO COMERCIAL

Claro empresas

Assinale a alternativa correta

Os ataques volumétricos têm como principal objetivo:

A > Explorar falhas específicas no código de uma aplicação web.

B > Consumir toda a largura de banda disponível, impedindo o tráfego legítimo.

C > Roubar dados confidenciais armazenados no servidor.

D > Alterar informações exibidas em um site institucional.

TREINAMENTO COMERCIAL

Claro empresas

Assinale a alternativa correta

Os ataques volumétricos têm como principal objetivo:

A Explorar falhas em [illegible] de uma aplicação web.

B [illegible] tráfego legítimo.

C Roubar [illegible] servidor.

D Alterar informações exibidas em um site institucional.

Muito bem!

Você identificou corretamente o inimigo. Nos ataques volumétricos, o vilão tenta “entupir os portões” da rede com um volume massivo de tráfego, impedindo que clientes reais consigam entrar. É exatamente nesse cenário que o Anti-DDoS da Claro atua para manter a operação ativa.

TREINAMENTO COMERCIAL

Claro empresas

Assinale a alternativa correta

Os ataques volumétricos têm como principal objetivo:

A Explorar falhas específicas no código de uma aplicação web.

B Consumir toda a largura de banda disponível, impedindo o tráfego legítimo.

C Roubar dados confidenciais armazenados no servidor.

D Alterar informações exibidas em um site institucional.

Quase lá!

Retorne à pergunta e tente novamente.

TREINAMENTO COMERCIAL

Claro empresas

Assinale a alternativa correta

Os ataques volumétricos têm como principal objetivo:

A Explorar falhas específicas no código de uma aplicação web.

B Consumir toda a largura de banda disponível, impedindo o acesso legítimo.

C Roubar dados confidenciais armazenados no servidor.

D Alterar informações exibidas em um site institucional.

Essa não é a resposta correta.

O ataque volumétrico não tenta roubar dados nem explorar falhas específicas. Ele age como uma multidão bloqueando a entrada da empresa: envia tráfego em excesso para consumir toda a largura de banda e impedir o acesso legítimo.

TREINAMENTO COMERCIAL

Claro empresas

Missão 1

Primeira missão **concluída com sucesso!**
Siga para a próxima.

anti DDoS

TREINAMENTO COMERCIAL

Claro empresas

o que vamos ver

- O que é DDoS
- O anti-DDoS da Claro
- Como vender
- Como ativar

TREINAMENTO COMERCIAL

Claro empresas



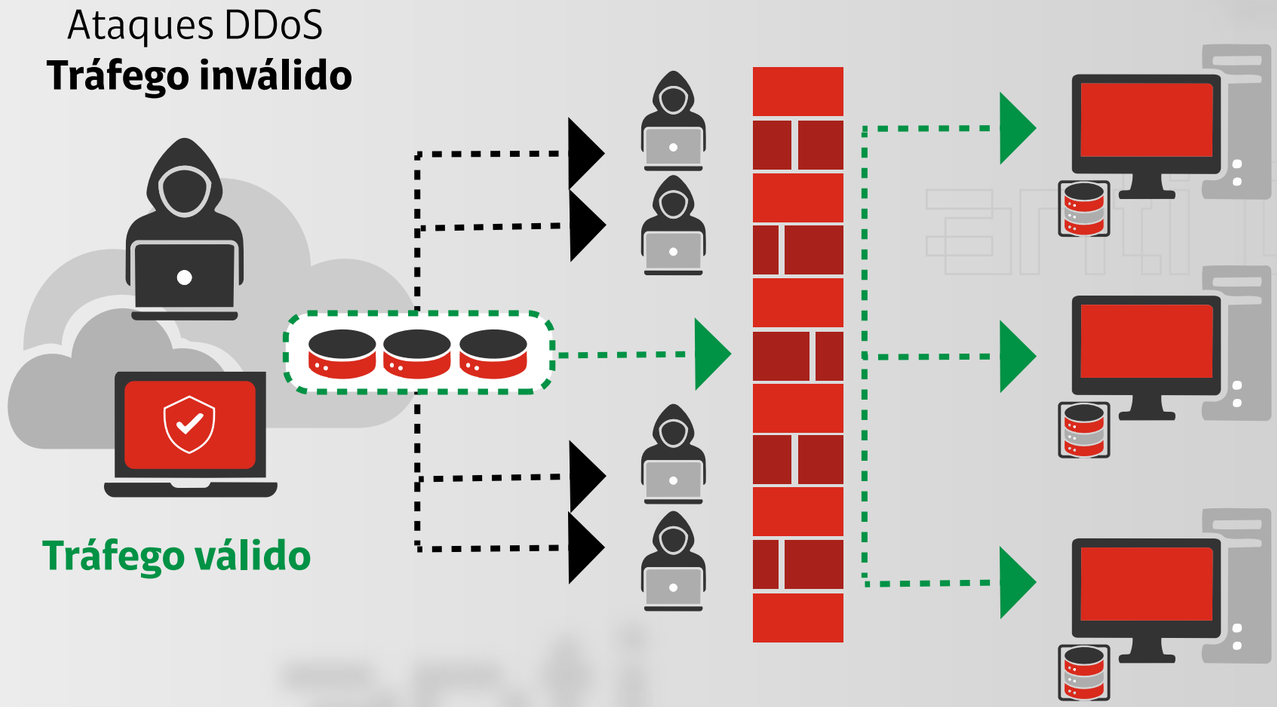
Dominar o Anti-DDoS da Claro

Todo **herói** precisa de habilidades especiais.

O **Anti-DDoS da Claro** é o conjunto de “superpoderes” que protege a operação dos clientes.

Anti-DDos da Claro

Identifica padrões anormais de tráfego que indicam um ataque e filtra o que é malicioso antes que chegue à infraestrutura do cliente, garantindo que os serviços continuem disponíveis.



TREINAMENTO COMERCIAL

Claro empresas



O Anti-DDoS está disponível somente para os links ativos **BLD Claro.**

TREINAMENTO COMERCIAL

Claro empresas

Processo de Defesa

Clique e veja como ocorre o processo de defesa do Anti-DDoS da Claro.

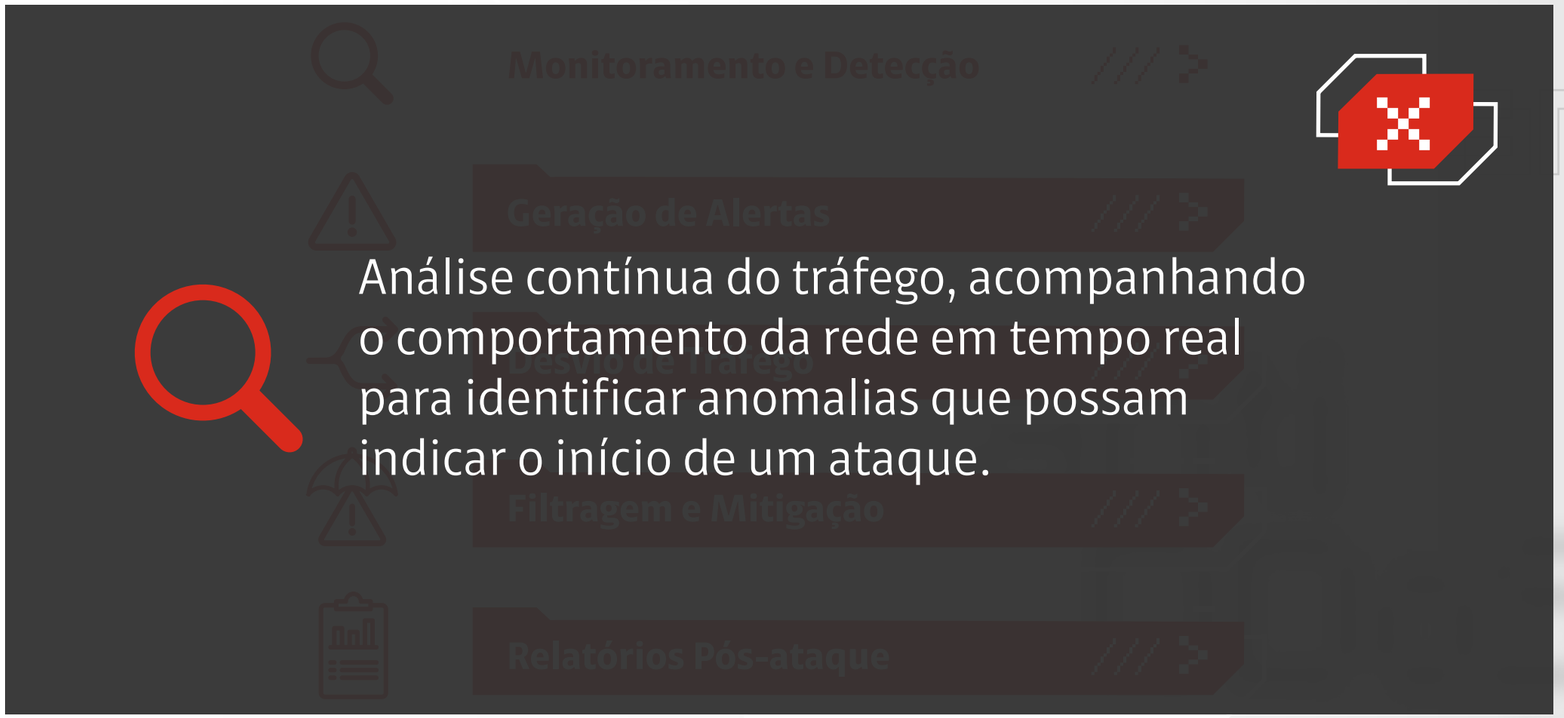
- Monitoramento e Detecção
- Geração de Alertas
- Desvio de Tráfego
- Filtragem e Mitigação
- Relatórios Pós-ataque

TREINAMENTO COMERCIAL

Claro empresas

Processo de Defesa

Clique e veja como ocorre o processo de defesa do Anti-DDoS da Claro.

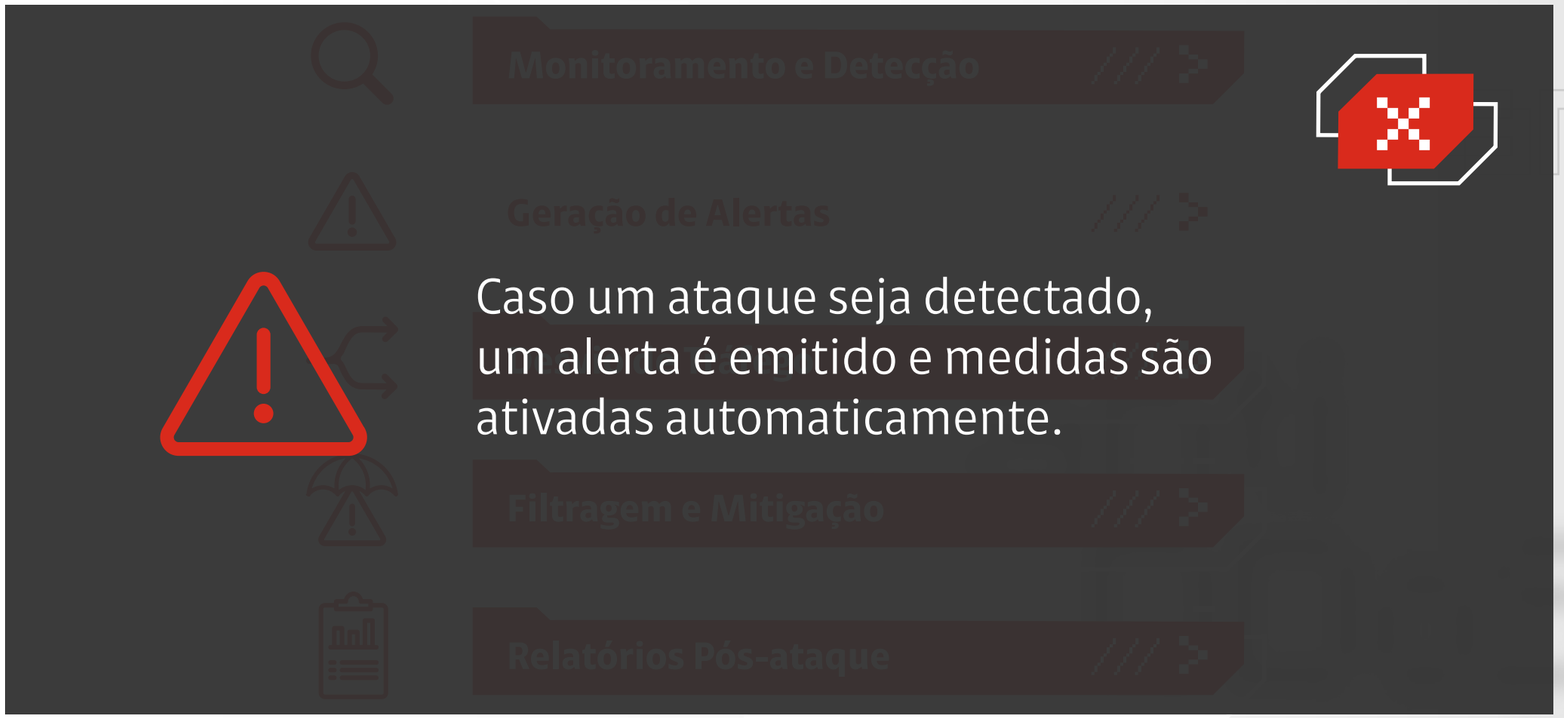


TREINAMENTO COMERCIAL

Claro empresas

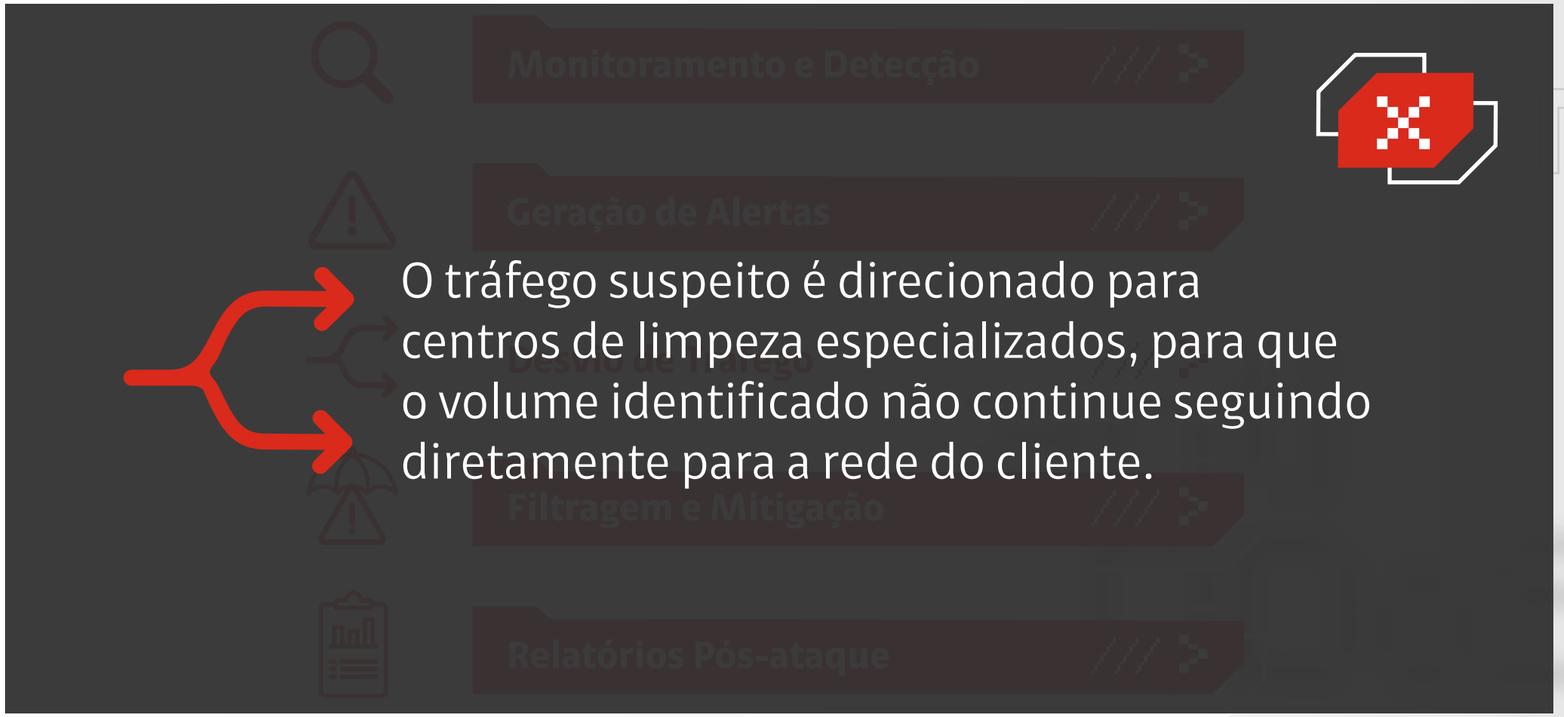
Processo de Defesa

Clique e veja como ocorre o processo de defesa do Anti-DDoS da Claro.



Processo de Defesa

Clique e veja como ocorre o processo de defesa do Anti-DDoS da Claro.

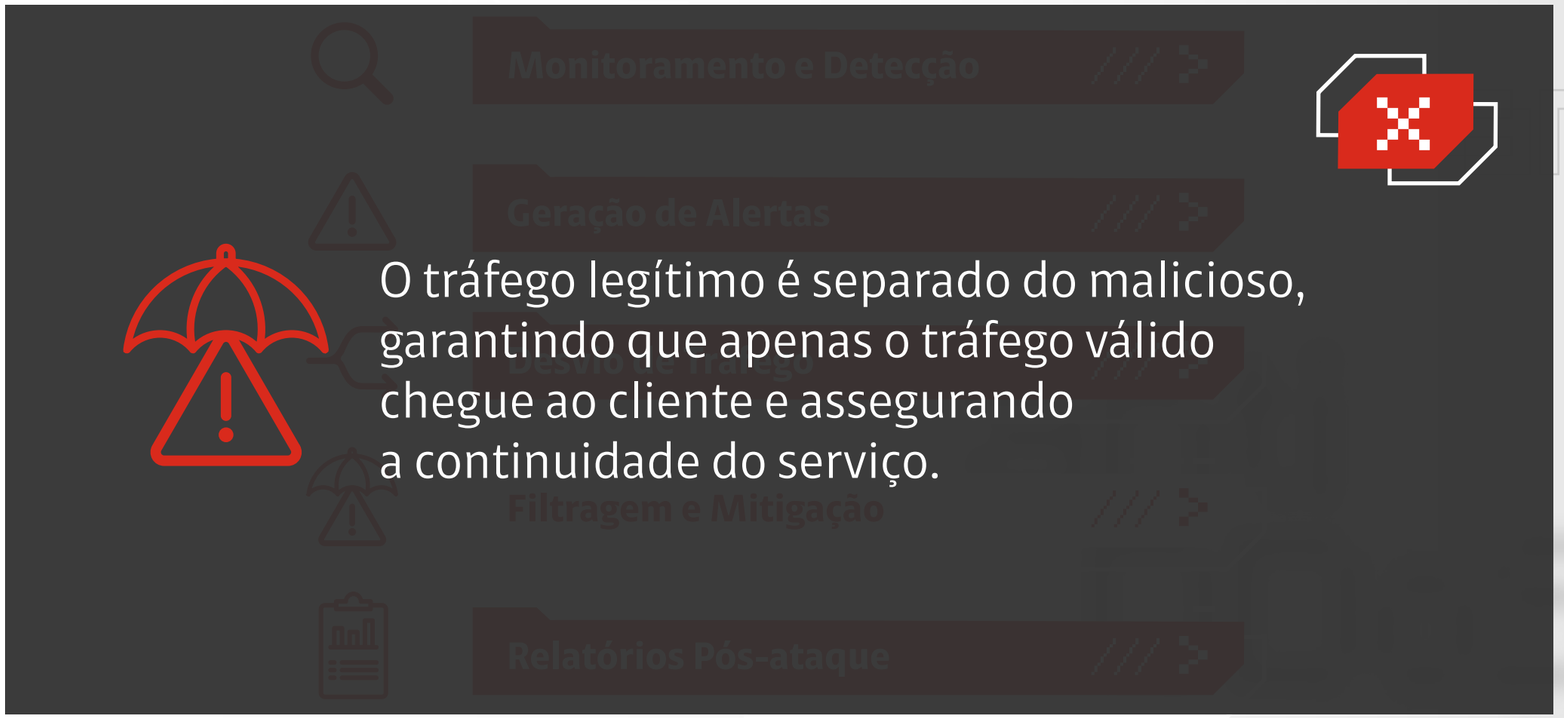


TREINAMENTO COMERCIAL

Claro empresas

Processo de Defesa

Clique e veja como ocorre o processo de defesa do Anti-DDoS da Claro.

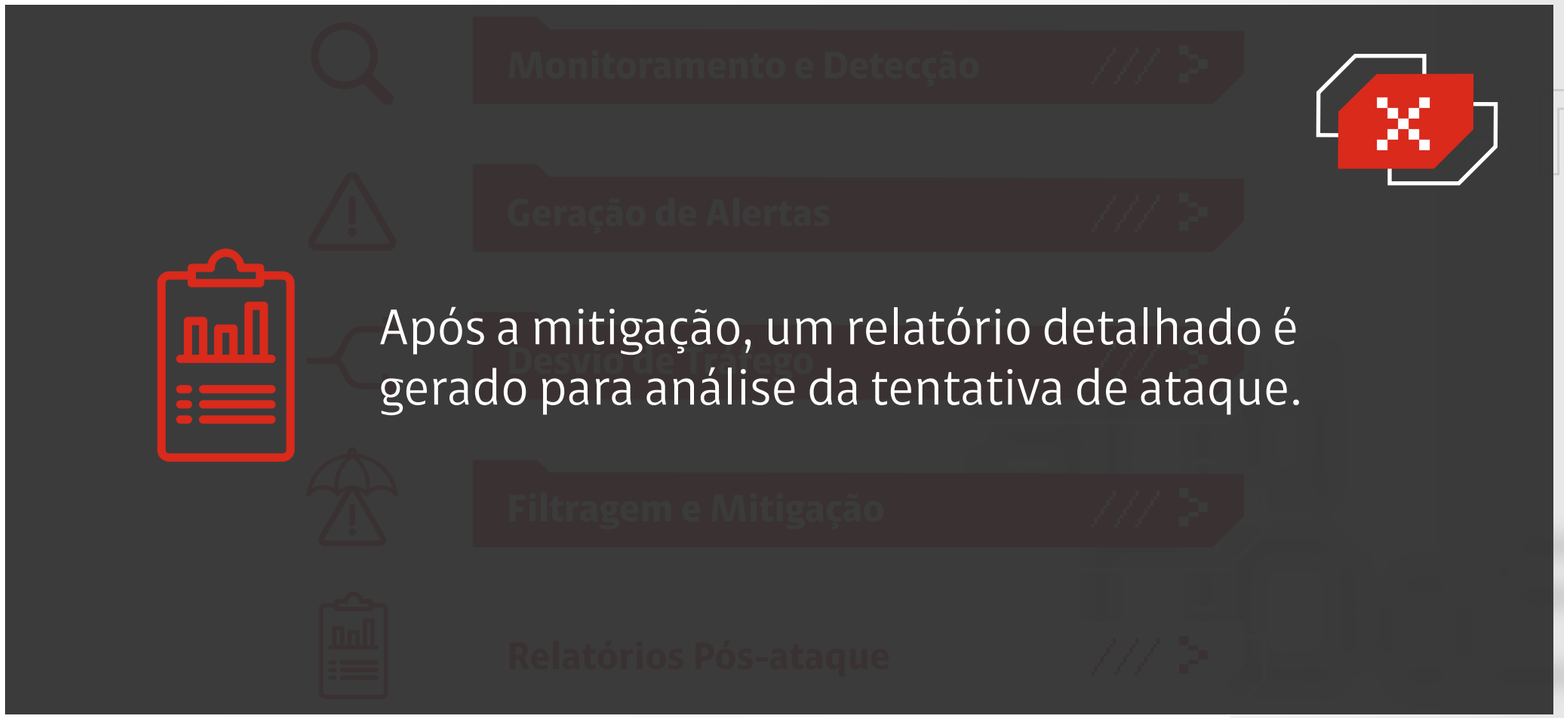


TREINAMENTO COMERCIAL

Claro empresas

Processo de Defesa

Clique e veja como ocorre o processo de defesa do Anti-DDoS da Claro.



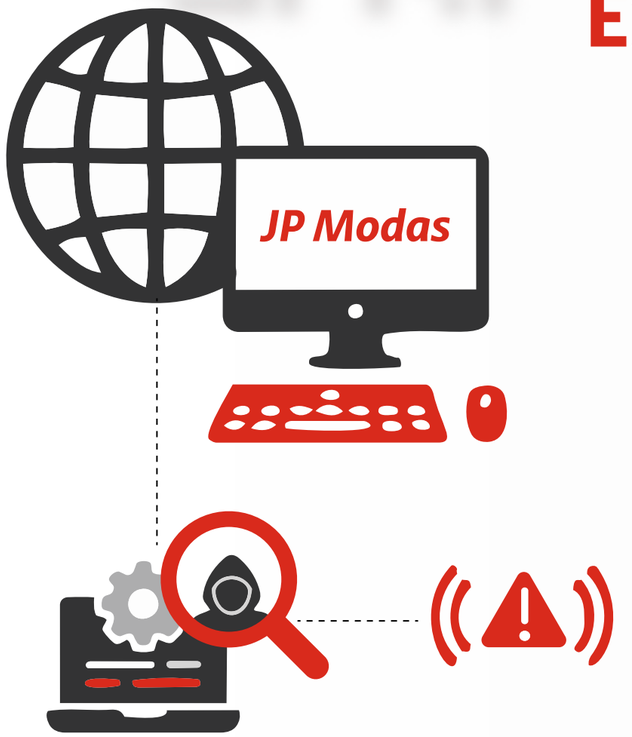
Exemplo



A empresa JP Moda depende do site para vender e começa a receber um volume anormal de acessos em poucos minutos. O tráfego dispara, mas não são clientes — é um ataque.

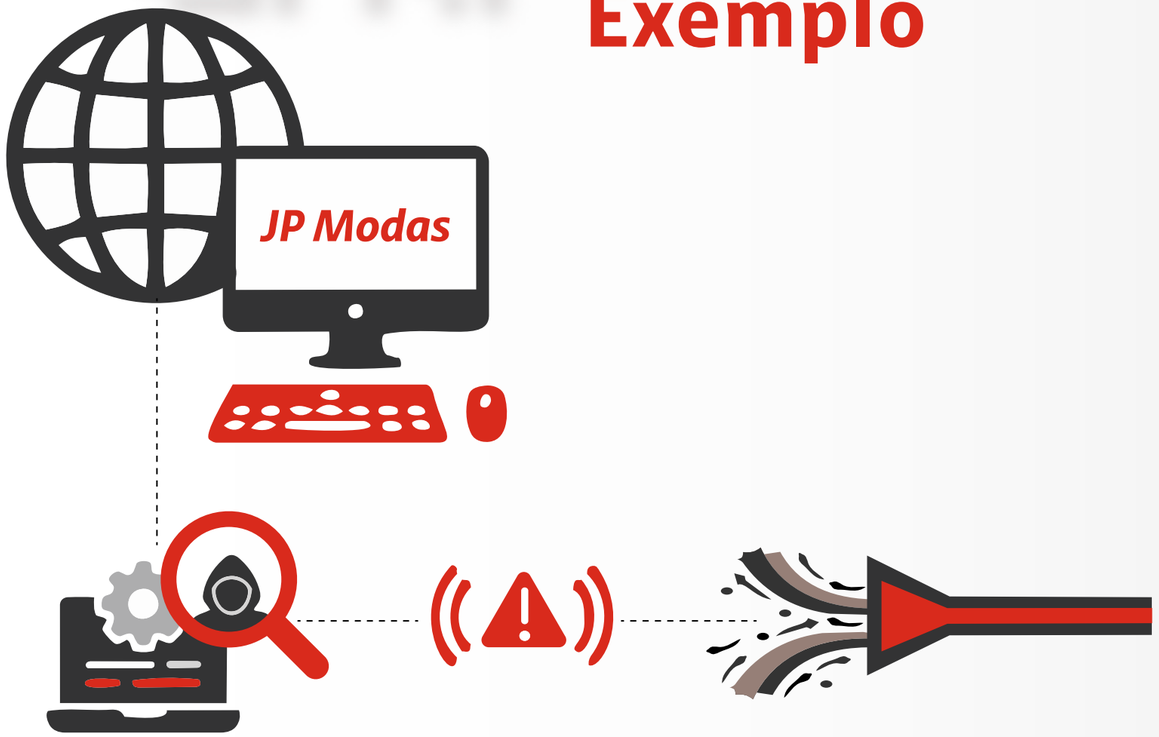
Como o Anti-DDoS atua?

Exemplo



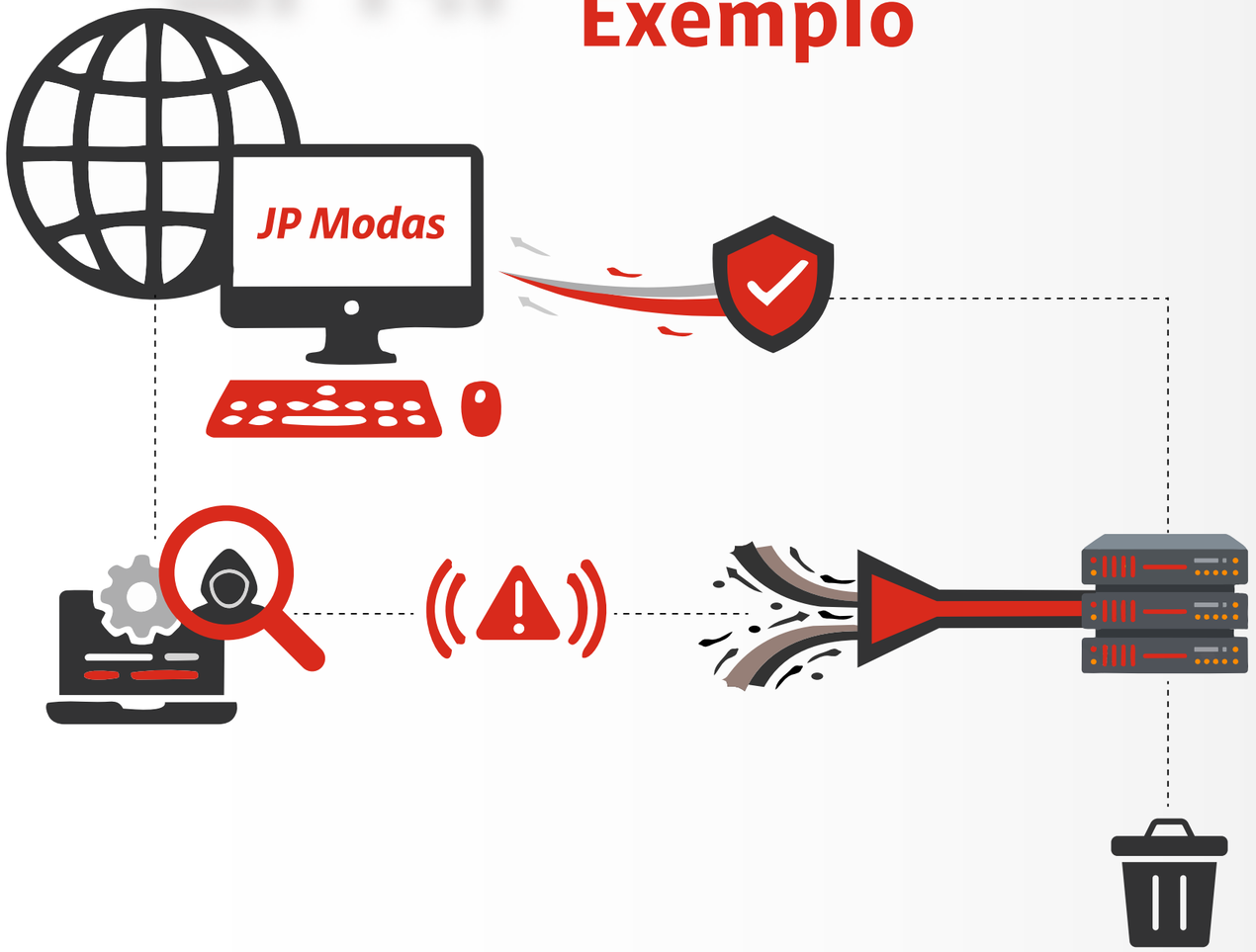
Com a **monitoração**,
o Anti-DDoS, **detecta** o
ataque e **gera um alerta**.

Exemplo



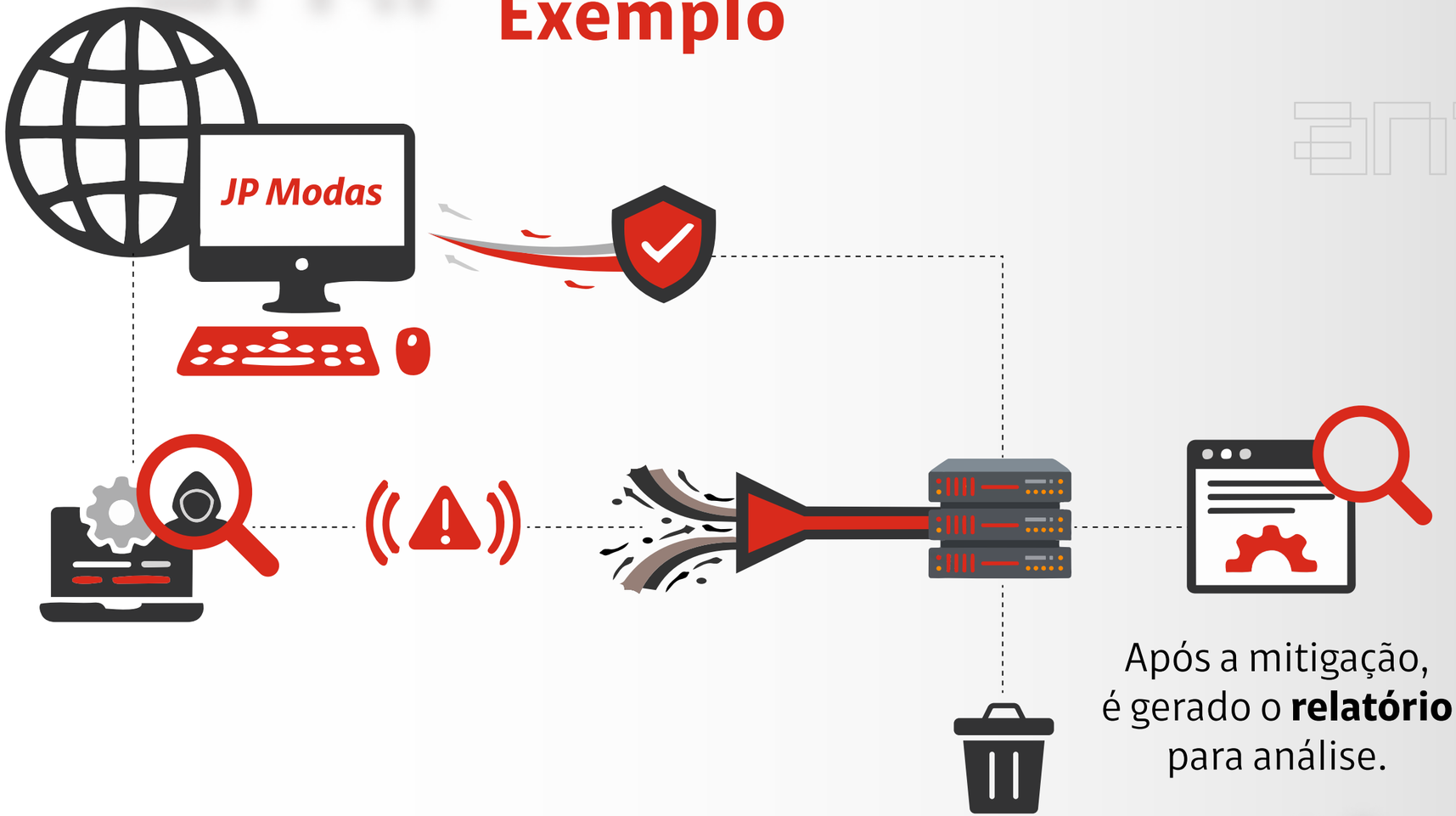
O **tráfego é desviado** antes que o volume suspeito atinja a rede da loja.

Exemplo



Nos centros especializados a **filtragem e mitigação**, separa o tráfego limpo do malicioso e descarta os acessos falsos.

Exemplo



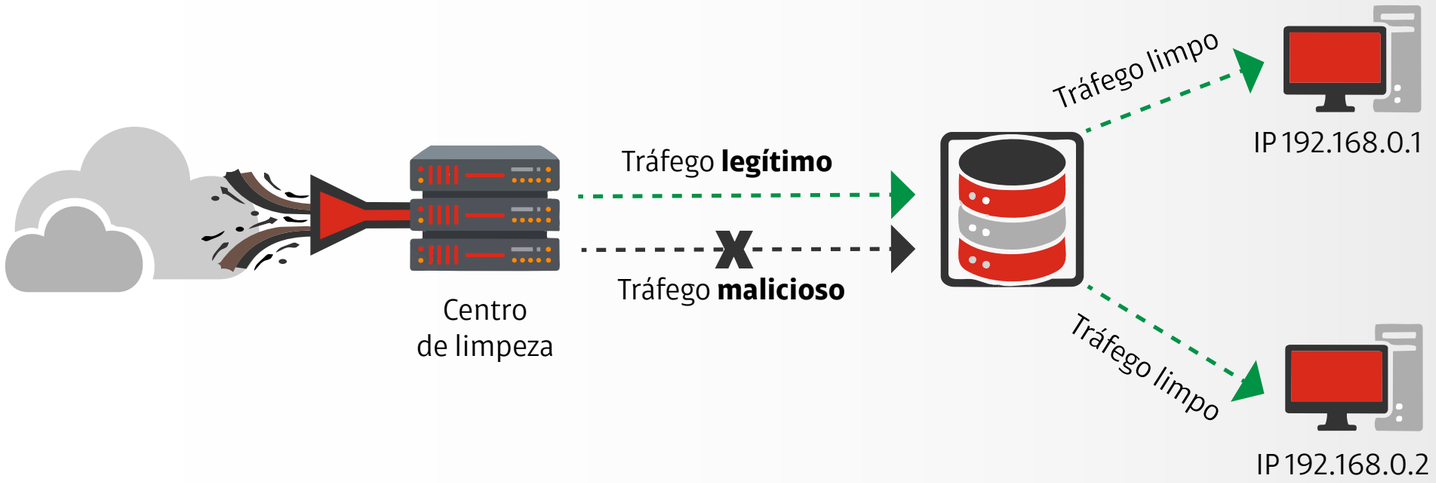
Após a mitigação,
é gerado o **relatório**
para análise.

Exemplo

Essa proteção é gerenciada, não depende da equipe de TI do cliente!

Planos com mitigação automática

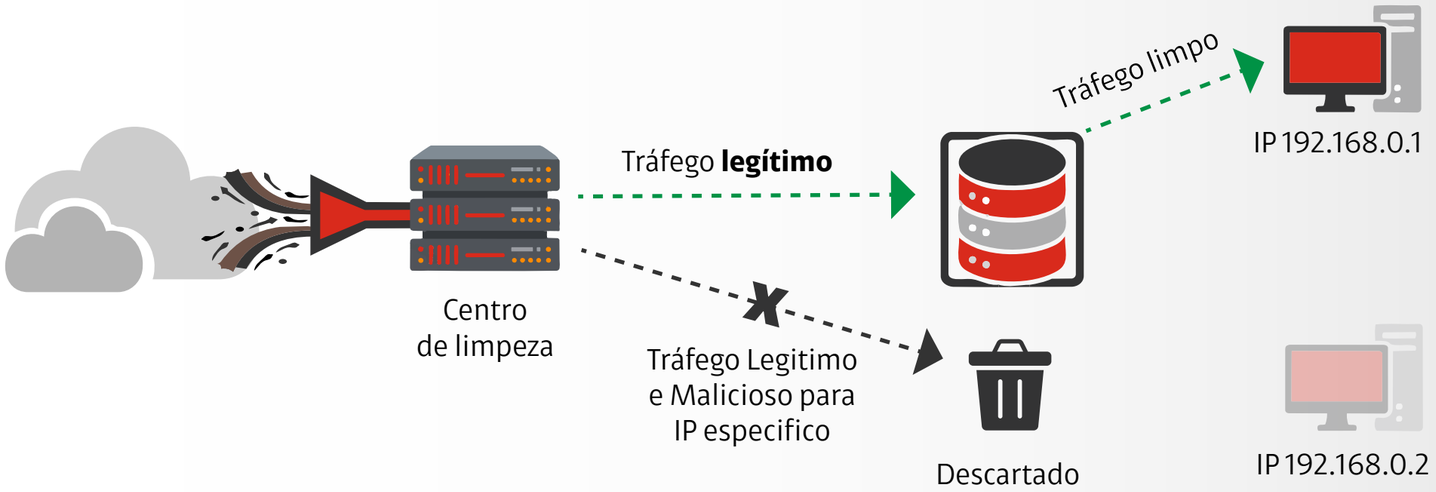
Mitigação automática até a capacidade contratada.



A monitoração automática, sem interação do SOC, garante detecção e resposta imediatas ao ataque, sem necessidade de acionamento manual. Uma vez identificado um ataque DDoS, a mitigação ocorre até o limite da capacidade contratada.

Planos com mitigação automática

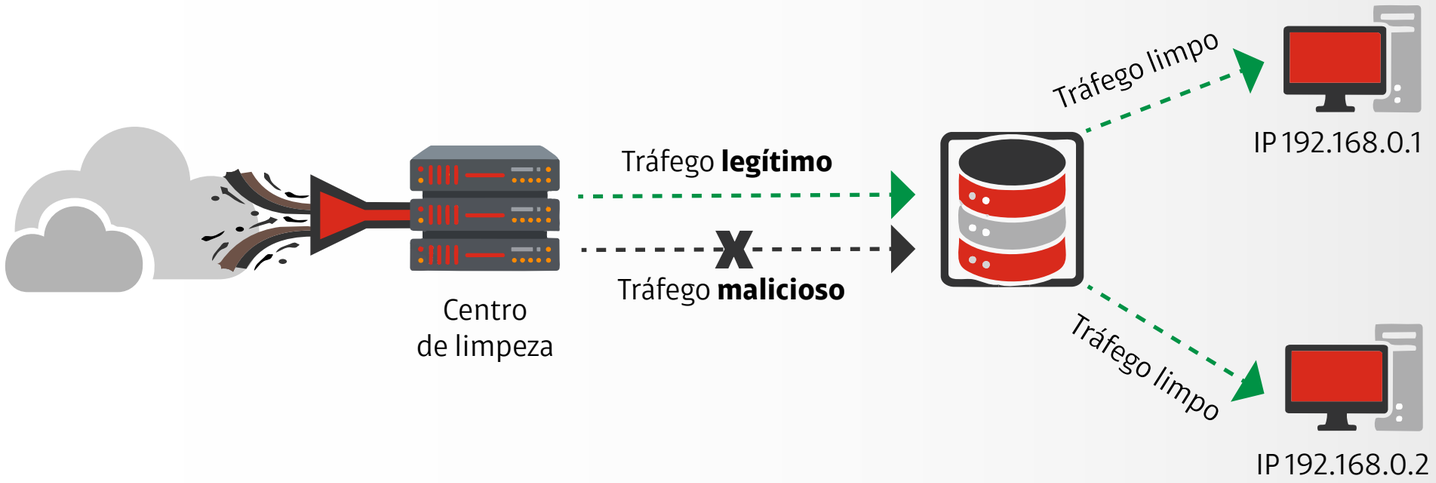
Mitigação automática até a capacidade contratada.



Quando a capacidade contratada é excedida, o IP entra em black hole (Offline), descartando todo o tráfego destinado ao IP ou range atacado e protegendo os BLDs e a rede contra sobrecarga.

Planos com mitigação automática

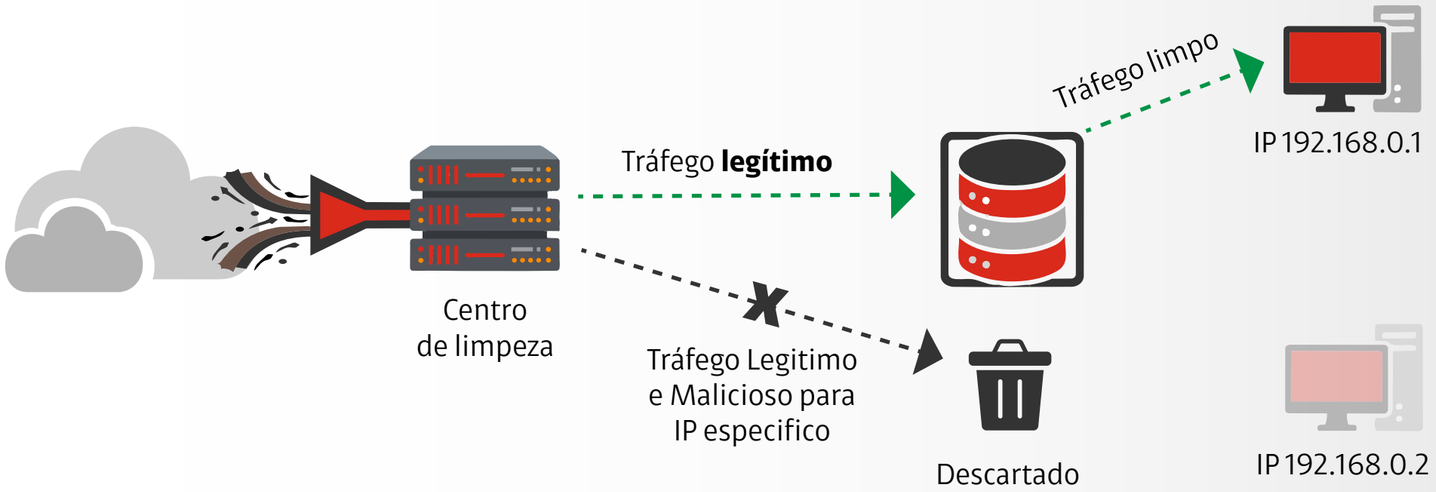
Mitigação automática até a capacidade contratada.



Nos planos com mitigação manual, o cliente conta com maior capacidade de proteção. Ao identificar o ataque, o SNOC redireciona o tráfego para um centro de limpeza, garantindo tratamento especializado.

Planos com mitigação automática

Mitigação automática até a capacidade contratada.



Caso o volume do ataque ultrapasse a capacidade contratada, o cliente é consultado sobre a continuidade do serviço, podendo haver cobrança adicional. Se não houver aceite, o tráfego é direcionado para black hole, protegendo os serviços e a rede contra sobrecarga.

Planos Anti-DDoD Claro

	Capacidade de Mitigação	Banda do BLD
1	0,1Gbps (Nac) + 0,25Gbps (Int)	Até 100 Mbps (Mitigação Automática)
2	0,2Gbps (Nac) + 0,5Gbps (Int)	Até 200 Mbps (Mitigação Automática)
3	0,4Gbps (Nac) + 1Gbps (Int)	Até 400 Mbps (Mitigação Automática)
4	0,5Gbps (Nac) + 10Gbps (Int)	Até 500 Mbps (Mitigação pelo SOC)
5	1,0Gbps (Nac) + 10Gbps (Int)	Até 1 Gbps (Mitigação pelo SOC)
6	2,0Gbps (Nac) + 15Gbps (Int)	Até 2 Gbps (Mitigação pelo SOC)
7	5,0Gbps (Nac) + 20Gbps (Int)	Até 5 Gbps (Mitigação pelo SOC)
8	10,0Gbps (Nac) + 30Gbps (Int)	Até 10 Gbps (Mitigação pelo SOC)
9	10,0Gbps (Nac) + 50Gbps (Int)	Até 10 Gbps (Mitigação pelo SOC)
10	10,0Gbps (Nac) + 100Gbps (Int)	Até 10 Gbps (Mitigação pelo SOC)

Características do Anti-DDoS da Claro

Suporte Especializado com equipes de segurança disponíveis 24/7.

Escalabilidade para lidar com ataques de diferentes tamanhos e complexidades.

Proteção Volumétrica que protege redes e servidores.

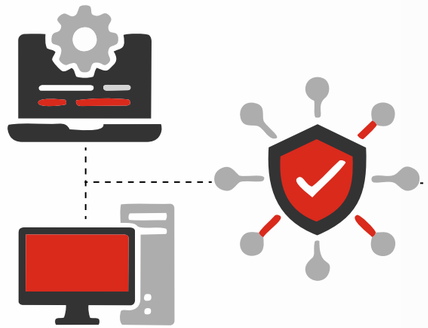
Monitoramento Contínuo que detecta anomalias no tráfego em tempo real.

Respostas Rápidas com mitigação de ataques em até 15 minutos, diretamente no backbone, reduzindo impactos na operação.

Centros de Limpeza Distribuídos, sendo 2 nacionais (SP e RJ) e 3 internacionais.

Benefícios do Anti-DDoS da Claro

Clique para saber mais sobre os benefícios do Anti-DDoS da Claro.



- Redução de Perdas Financeiras
- Proteção da Reputação
- Relatórios Detalhados
- Redução de Custos Operacionais
- Cumprimento de Normas e Regulamentos

Benefícios do Anti-DDoS da Claro

Clique para saber mais sobre os benefícios do Anti-DDoS da Claro.

Evita interrupções que poderiam resultar em prejuízos milionários.

- Redução de Perdas Financeiras
- Proteção da R
- Relatórios Detalhados
- Redução de Custos Operacionais
- Cumprimento de Normas e Regulamentos

TREINAMENTO COMERCIAL

Claro empresas

Benefícios do Anti-DDoS da Claro

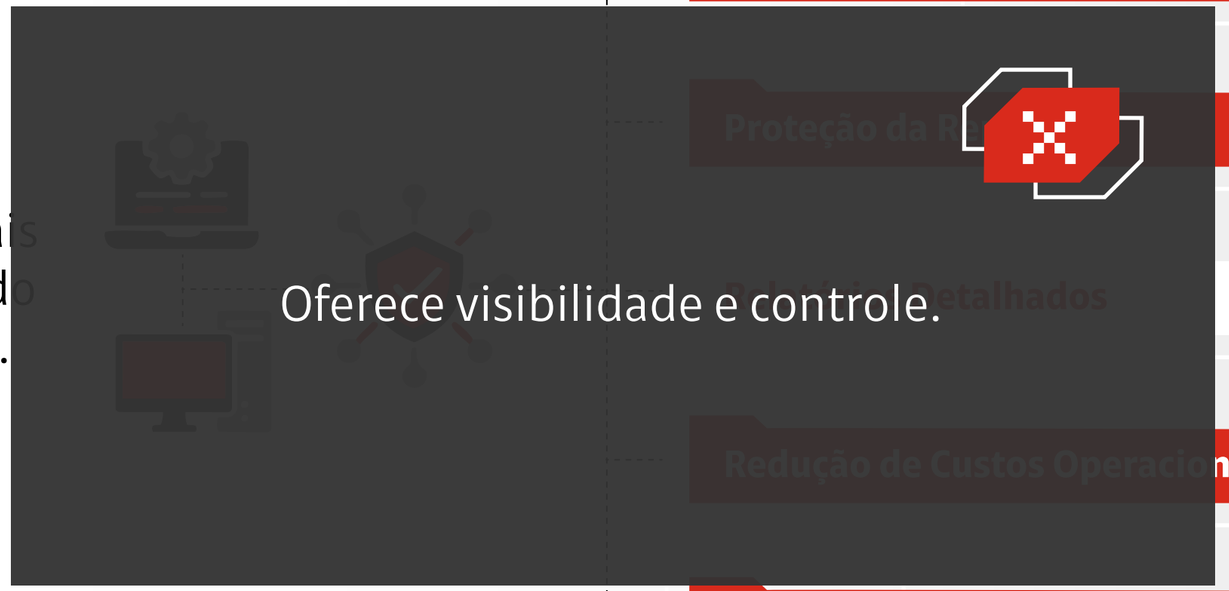
Clique para saber mais sobre os benefícios do Anti-DDoS da Claro.

Garante que clientes e parceiros confiem na segurança da empresa.

- Redução de Perdas Financeiras
- Proteção da R
- Detalhados
- Redução de Custos Operacionais
- Cumprimento de Normas e Regulamentos

Benefícios do Anti-DDoS da Claro

Clique para saber mais sobre os benefícios do Anti-DDoS da Claro.



- Redução de Perdas Financeiras
- Proteção da R
- Relatórios Detalhados
- Redução de Custos Operacionais
- Cumprimento de Normas e Regulamentos

Benefícios do Anti-DDoS da Claro

Clique para saber mais sobre os benefícios do Anti-DDoS da Claro.

Minimiza o impacto de falhas na infraestrutura de TI.

- Redução de Perdas Financeiras
- Proteção da R
- Relatórios Detalhados
- Redução de Custos Operacionais
- Cumprimento de Normas e Regulamentos

TREINAMENTO COMERCIAL

Claro empresas

Benefícios do Anti-DDoS da Claro

Clique para saber mais sobre os benefícios do Anti-DDoS da Claro.

Ajuda empresas que seguem padrões como ISO 27001 e LGPD.

- Redução de Perdas Financeiras
- Proteção da R
- Detalhados
- Redução de Custos Operacionais
- Cumprimento de Normas e Regulamentos

TREINAMENTO COMERCIAL

Claro empresas

Para finalizar sua segunda missão,
realize a atividade a seguir.

Organize o processo de defesa

A defesa começa com a **Monitoração e Detecção**, etapa responsável por identificar comportamentos anormais na rede. A partir dessa identificação, arraste cada etapa para a descrição correspondente.

Geração de Alertas

Desvio de Tráfego

Filtragem e Mitigação

O tráfego suspeito é direcionado para centros especializados, evitando que siga diretamente para a rede do cliente.

O tráfego legítimo é separado do malicioso, garantindo que apenas acessos válidos cheguem ao destino.

Um aviso é emitido automaticamente quando o sistema identifica um possível ataque.

TREINAMENTO COMERCIAL

Claro empresas

Organize o processo de defesa

A defesa começa com a **Monitoração e Detecção**, etapa responsável por identificar comportamentos anormais na rede. A partir dessa identificação, arraste cada etapa para a descrição correspondente.

Desvio de Tráfego

O tráfego suspeito é direcionado para centros especializados, evitando que siga diretamente para a rede do cliente.

Filtragem e Mitigação

O tráfego legítimo é separado do malicioso, garantindo que apenas acessos válidos cheguem ao destino.

Geração de Alertas

Um aviso é emitido automaticamente quando o sistema identifica um possível ataque.

Organize o processo de defesa

A defesa começa com a **Monitoração e Detecção**, etapa responsável por identificar comportamentos anormais na rede. A partir dessa identificação, arraste cada etapa para a descrição correspondente.

Geração de Alertas

Desvio de Tráfego

Filtragem e Mitigação

O tráfego suspeito é direcionado para centros especializados, evitando que siga diretamente para a rede do cliente.

O tráfego legítimo é separado do malicioso, mantendo apenas acessos válidos.

Um aviso é emitido automaticamente quando o sistema identifica um possível ataque.

Muito bem!

Após a Monitoração e Detecção, o sistema gera alertas, desvia o tráfego suspeito e realiza a filtragem e mitigação para proteger a operação. E não se esqueça: ao final de todo o processo, é emitido o **Relatório Pós-Ataque**, garantindo visibilidade e análise estratégica.

Organize o processo de defesa

A defesa começa com a **Monitoração e Detecção**, etapa responsável por identificar comportamentos anormais na rede. A partir dessa identificação, arraste cada etapa para a descrição correspondente.

Geração de Alertas

Desvio de Tráfego

Filtragem e Mitigação

O tráfego suspeito é direcionado para centros especializados, evitando que siga diretamente para a rede do cliente.

O tráfego legítimo é separado do malicioso, garantindo que apenas acessos válidos

Um aviso é emitido automaticamente quando o sistema identifica um possível ataque.

Essa não é a resposta correta.

Depois da Monitoração e Detecção, o fluxo correto é: gerar o alerta, desviar o tráfego suspeito e então realizar a filtragem e mitigação. Revise a sequência estratégica da defesa — e lembre-se de que o processo se encerra com o **Relatório Pós-Ataque**.

TREINAMENTO COMERCIAL

Claro empresas

Missão 2

Segunda missão **concluída com sucesso**!
Avance para o próximo aprendizado.

anti DDoS

TREINAMENTO COMERCIAL

Claro empresas

o que vamos ver

- O que é DDoS
- O anti-DDoS da Claro
- Como vender
- Como ativar



Transformar poder técnico em valor percebido

Como **Protetor da Disponibilidade**, seu papel é transformar os “superpoderes” do Anti-DDoS da Claro em valor real para a empresa do cliente.

Isso significa atuar como consultor, entender o impacto da indisponibilidade e mostrar como a solução protege o negócio.

Para começar, é essencial saber para quais empresas ela é indicada — afinal, **venda não é sobre produto, é sobre impacto no negócio**.

TREINAMENTO COMERCIAL

Claro empresas

Público do Anti-DDoS

Clique e veja como o Anti-DDoS da Claro é importante para essas empresas.

- E-commerce
- Instituições financeiras
- Setor Público
- Provedores de Serviçosde TI
- Setor de Entretenimento e Jogos Online

TREINAMENTO COMERCIAL

Claro empresas

Público do Anti-DDoS

Clique e veja como o Anti-DDoS da Claro é importante para essas empresas.

E-commerce

Instituições financeiras

Provedores de Serviçosde TI

Setor de Entretenimento e Jogos Online

Lojas online precisam garantir que seus clientes consigam acessar seus sites sempre.

TREINAMENTO COMERCIAL

Claro empresas

Público do Anti-DDoS

Clique e veja como o Anti-DDoS da Claro é importante para essas empresas.

E-commerce

Instituições financeiras

Setor Público

Provedores de Serviçosde TI

Setor de Entretenimento e Jogos Online



Bancos e seguradoras dependem de sistemas sempre disponíveis para transações seguras.

Público do Anti-DDoS

Clique e veja como o Anti-DDoS da Claro é importante para essas empresas.

E-commerce

Instituições financeiras

Setor Público

Provedores de Serviçosde TI

Setor de Entretenimento e Jogos Online



Órgãos governamentais precisam proteger informações e manter serviços acessíveis.

TREINAMENTO COMERCIAL

Claro empresas

Público do Anti-DDoS

Clique e veja como o Anti-DDoS da Claro é importante para essas empresas.

E-commerce

Instituições financeiras

Setor Público

Provedores de Serviçosde TI

Setor de Entretenimento e Jogos Online

Empresas de hospedagem, cloud computing e data centers são alvos frequentes de ataques.

TREINAMENTO COMERCIAL

Claro empresas

Público do Anti-DDoS

Clique e veja como o Anti-DDoS da Claro é importante para essas empresas.

E-commerce

Instituições financeiras

Setor Público

Provedores de Serviçosde TI

Setor de Entretenimento e Jogos Online

Plataformas de jogos online sofrem ataques frequentes para prejudicar a experiência do usuário.

TREINAMENTO COMERCIAL

Claro empresas

As empresas compram para evitar prejuízos, proteger a reputação, manter a operação sem sobrecarregar a TI e bloquear picos de tráfego malicioso.

TREINAMENTO COMERCIAL

Claro empresas

no momento da venda:

//// Argumento-chave

Para posicionar o Anti-DDoS da Claro como uma solução de continuidade do negócio.

Argumente

“Se a sua empresa depende de presença online para vender e atender, o Anti-DDoS trabalha para que você continue operando mesmo quando alguém tentar te derrubar.”

TREINAMENTO COMERCIAL

Claro empresas

no momento da venda:

//// Pergunta-chave

Para provocar reflexão, gerar senso de urgência e ajudar o cliente a perceber o risco real de indisponibilidade.

Pergunte

“Se o seu site ou sua VPN ficar fora do ar por 1 hora, qual é o impacto direto nas suas vendas e na sua operação?”

TREINAMENTO COMERCIAL

Claro empresas

Política Comercial Anti-DDoS da Claro

É importante conhecer as políticas comerciais para que o atendimento seja eficaz. Clique e saiba mais.

Rescisão de Contrato

Pagamento

TREINAMENTO COMERCIAL

Claro empresas

Política Comercial Anti-DDoS da Claro

É importante conhecer as políticas comerciais para que o atendimento seja eficaz. Clique e saiba mais.

Rescisão de Contrato

Caso o **cliente rescinda o contrato**, total ou parcialmente, ou caso a rescisão ocorra por motivo a ele imputável, será devida uma **multa compensatória**.

Pagamento

TREINAMENTO COMERCIAL

Claro empresas

Política Comercial Anti-DDoS da Claro

É importante conhecer as políticas comerciais para que o atendimento seja eficaz. Clique e saiba mais.

Rescisão de Contrato

Pagamento

A multa compensatória é equivalente a **30%** do valor das parcelas vincendas, calculada com base no valor da parcela vigente no mês da rescisão, a ser paga em parcela única.

TREINAMENTO COMERCIAL

Claro empresas

Política Comercial Anti-DDoS da Claro

É importante conhecer as políticas comerciais para que o atendimento seja eficaz. Clique e saiba mais.

Rescisão de Contrato

Pagamento

O contrato contará com opções de permanência de 12, 24 ou 36 meses (canais diretos).

TREINAMENTO COMERCIAL

Claro empresas

Para finalizar sua terceira missão,
responda a questão a seguir.

TREINAMENTO COMERCIAL

Claro empresas

//// Assinale a alternativa correta

Durante uma atendimento, o cliente afirma:
“Já temos firewall e antivírus. Não vejo necessidade de investir em mais uma solução de segurança.” Como Protetor da Disponibilidade, seu objetivo não é só discutir tecnologia, mas gerar percepção de risco e valor de negócio utilizando o argumento-chave e a pergunta-chave do Anti-DDoS.

Qual abordagem demonstra o uso mais estratégico desses dois recursos?

A >

“Entendo. O Anti-DDoS possui monitoramento constante, detecta tráfego anormal e conta com centros de limpeza especializados. Ele complementa o firewall tradicional com uma camada adicional de proteção contra ataques.”

B >

“Entendo. Mas se o seu site ou sua VPN ficar fora do ar por uma hora, qual seria o impacto direto nas suas vendas e na sua operação? O Anti-DDoS da Claro trabalha justamente para que sua empresa continue operando, mesmo quando alguém tentar derrubar o seu ambiente.”

TREINAMENTO COMERCIAL

Claro empresas

Assinale a alternativa correta

Durante uma atendimento, o cliente afirma:

“Já temos firewall e antivírus. Não vejo necessidade de investir em mais uma solução de segurança.” Como Protetor da Disponibilidade, seu objetivo não é só discutir tecnologia, mas gerar percepção de risco e valor de negócio utilizando o argumento-chave e a pergunta-chave do Anti-DDoS.

Qual abordagem demonstra o uso mais estratégico desses dois recursos?

A

“Entendo. O Anti-DDoS possui monitoramento constante, detecta tráfego anormal e conta com a camada

B

“Entendo. Mas se o seu site ou sua VPN ficar fora do ar por uma hora, qual seria o impacto direto nas suas vendas e na sua operação? O Anti-DDoS da Claro trabalha justamente para que sua empresa continue operando, mesmo quando alguém tentar derrubar o seu ambiente.”

Muito bem!

Você escolheu a abordagem que eleva a conversa para o impacto no negócio. Ao usar a pergunta-chave, você provoca reflexão e senso de urgência. Ao aplicar o argumento-chave, posiciona o Anti-DDoS da Claro como solução de continuidade operacional, não apenas como mais um recurso técnico.

Assinale a alternativa correta

Durante uma atendimento, o cliente afirma:

“Já temos firewall e antivírus. Não vejo necessidade de investir em mais uma solução de segurança.” Como Protetor da Disponibilidade, seu objetivo não é só discutir tecnologia, mas gerar percepção de risco e valor de negócio utilizando o argumento-chave e a pergunta-chave do Anti-DDoS.

Qual abordagem [illegible] os?

A

“Entendo. O Anti-DDoS possui monitoramento constante, detecta tráfego anormal e conta com centros de limpeza especializados. Ele complementa o firewall tradicional com uma camada adicional de proteção contra ataques.”

B

“Entendo. Mas se o seu site ou sua VPN ficar fora do ar por uma hora, qual seria o impacto direto nas suas vendas e na sua operação? O Anti-DDoS da Claro trabalha justamente para que sua empresa continue operando, mesmo quando alguém tentar derrubar o seu ambiente.”

Esta não é a resposta correta.

Embora a explicação técnica agregue informação, ela mantém a conversa centrada no produto. O uso estratégico do argumento-chave e da pergunta-chave direciona o cliente para o impacto financeiro e operacional da indisponibilidade, conduzindo-o à percepção real de risco.

TREINAMENTO COMERCIAL

Claro empresas

Missão 3

Terceira missão concluída com sucesso!
Siga em frente para a próxima etapa da jornada.

TREINAMENTO COMERCIAL

Claro empresas

o que vamos ver

- O que é DDoS
- O anti-DDoS da Claro
- Como vender
- Como ativar



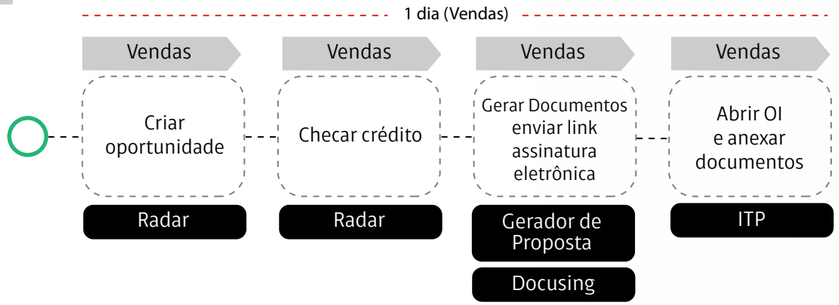
Garantir que a proteção saia do discurso e vire realidade

Como **Protetor da Disponibilidade**, além de saber como vender, você precisa conhecer o processo de ativação como um todo.

Entender a **jornada de ativação** assegura que o que foi vendido se transforme em defesa ativa.

Macro Fluxo Anti-DDoS

Etapa 1: Pré-Venda

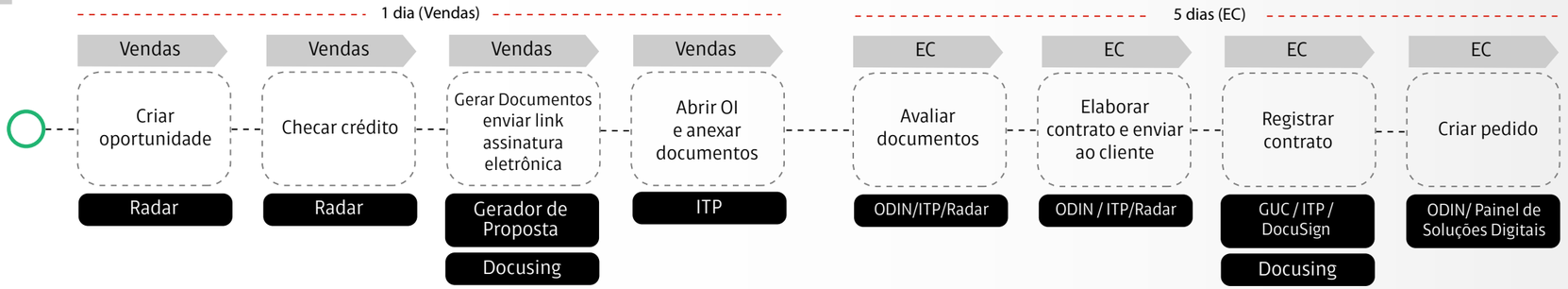


Sob responsabilidade de Vendas e com SLA de 1 dia, nesta etapa são cadastrados os dados da empresa, criada a oportunidade no Radar e solicitada a análise de crédito.

Em seguida, é elaborada a proposta, aberta a OI e anexados os documentos obrigatórios no ITP. Informações completas e corretas evitam cancelamentos futuros.

Macro Fluxo Anti-DDoS

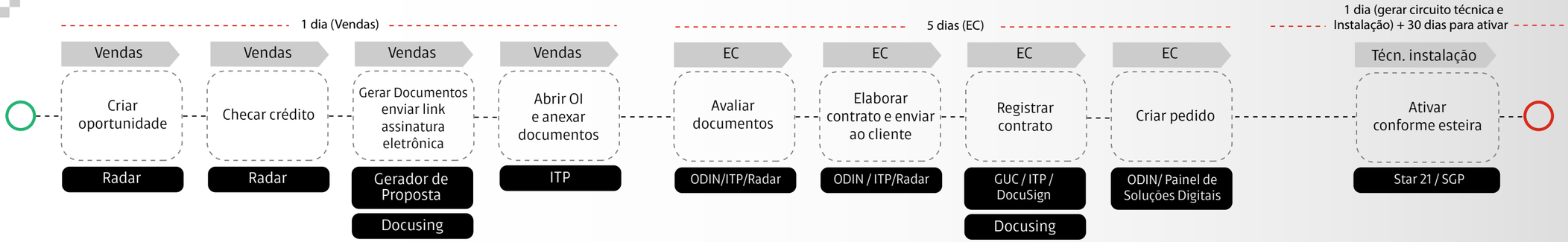
Etapa 2:
Análise de Documentação e Input



Com SLA de 5 dias. A equipe recebe a OI, valida a documentação , elabora e envia o contrato ao cliente, registra no GUC e associa ao serviço. Em seguida, cria o pedido no Painel de Soluções Digitais. Essa etapa formaliza o contrato nos sistemas corporativos.

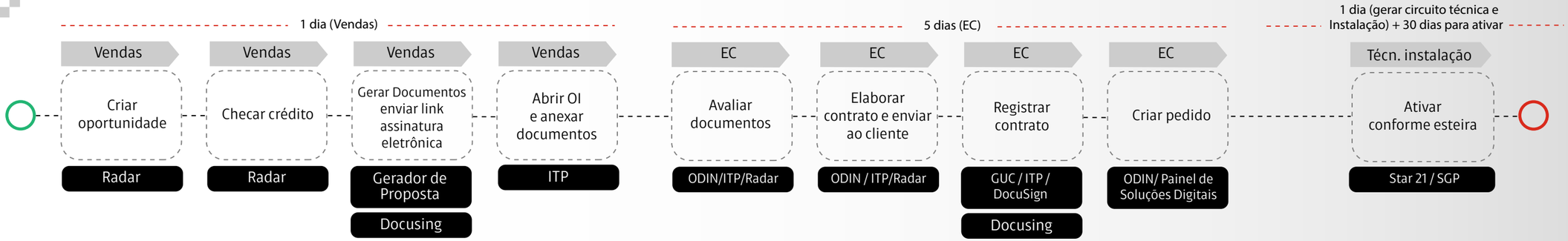
Macro Fluxo Anti-DDoS

Etapa 3: Técnica e Instalação



A área técnica é responsável pelo processo. Após o registro do pedido, o time gera o circuito nos sistemas Star 21 e SGP. O SLA é de 1 dia para geração do circuito e até 30 dias para ativação, seguindo a esteira até a entrega final.

Macro Fluxo Anti-DDoS



O macrofluxo mostra quem executa cada etapa, em qual sistema e em qual prazo, garantindo padronização, integração entre áreas e cumprimento do SLA até a ativação do Anti-DDoS.

TREINAMENTO COMERCIAL

Claro empresas



O SLA total do processo é de 7 dias
+ 30 dias de SLA para a Ativação.

TREINAMENTO COMERCIAL

Claro empresas

Para finalizar sua quarta missão,
responda a pergunta a seguir.

Assinale a alternativa correta

O macro fluxo do Anti-DDoS é importante apenas para a área técnica, pois trata da instalação da solução.

Certo

Errado

TREINAMENTO COMERCIAL

Claro empresas

//// Assinale a alternativa correta

O macro fluxo do Anti-DDoS é importante apenas para a área técnica, pois trata da instalação da solução.

Muito bem!

O macro fluxo não é importante apenas para a área técnica. Ele envolve Vendas, análise de documentação, input em sistemas e ativação. Compreender todo o processo garante alinhamento entre áreas, cumprimento de SLA e uma entrega eficiente ao cliente.

TREINAMENTO COMERCIAL

Claro empresas

//// Assinale a alternativa correta

O macro fluxo do Anti-DDoS é importante apenas para a área técnica, pois trata da instalação da solução.

Esta não é a resposta correta.

O macro fluxo vai além da instalação técnica. Ele começa na pré-venda, passa por validações e registros sistêmicos e só então chega à ativação. Entender essa jornada completa é essencial para garantir que o que foi vendido se transforme em proteção ativa.

TREINAMENTO COMERCIAL

Claro empresas

Missão 4

Quarta missão concluída com sucesso!
Antes de encerrar sua jornada, revise
os principais pontos deste treinamento.

anti DDoS



Ao longo deste treinamento, vimos que o **Anti-DDoS**:

- É uma solução que protege a disponibilidade dos serviços contra ataques volumétricos;
- Detecta e filtra o tráfego malicioso antes de atingir a rede do cliente, garantindo a continuidade do negócio e funcionando como um “seguro de disponibilidade”;
- É indicado para empresas de qualquer porte que dependam de disponibilidade online;
- Exige BLD Claro ativo;
- Tem SLA de 7 dias, mais 30 dias para ativação.

TREINAMENTO COMERCIAL

Claro empresas

Parabéns por finalizar sua jornada neste treinamento!

Agora você está pronto para agir como um verdadeiro **Protetor da Disponibilidade**, que vende segurança, continuidade e confiança para cada cliente.

Boas Vendas!

anti DDoS

TREINAMENTO COMERCIAL

Claro empresas



Segurança
Soluções Digitais

Finalizar

Clique para finalizar o treinamento