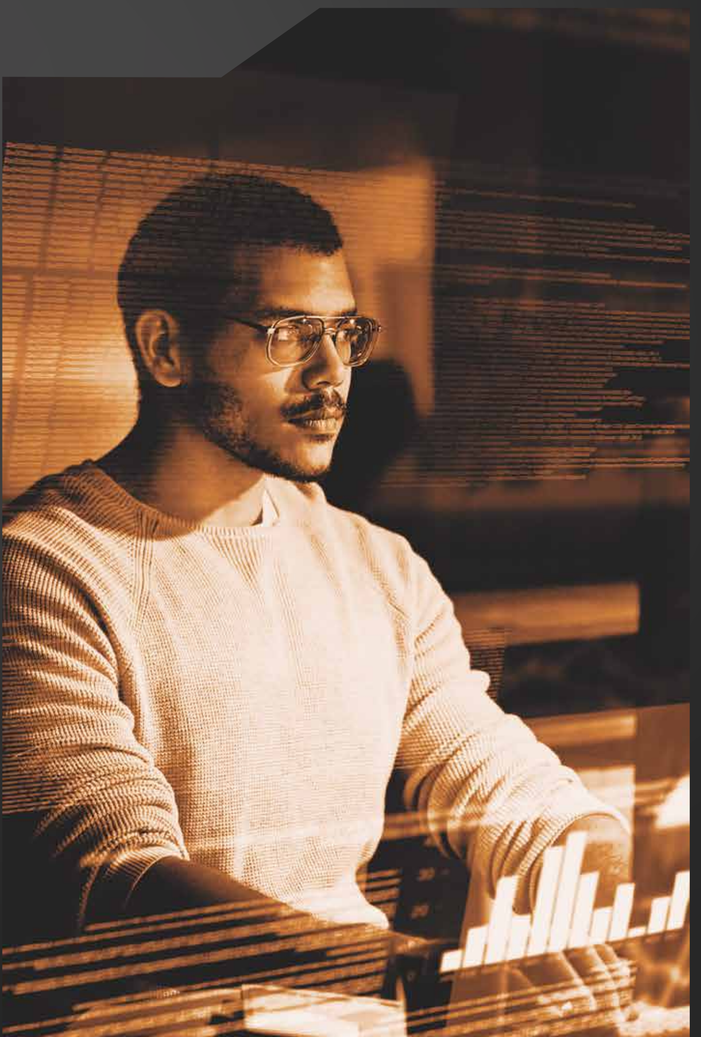
BASE4
SECURITY

Seu aliado cibernético



OFFENSIVE

Um investimento seguro com metodologias avançadas e abordagens criativas

DIFERENCIAIS

OSCP OSCE OSWP

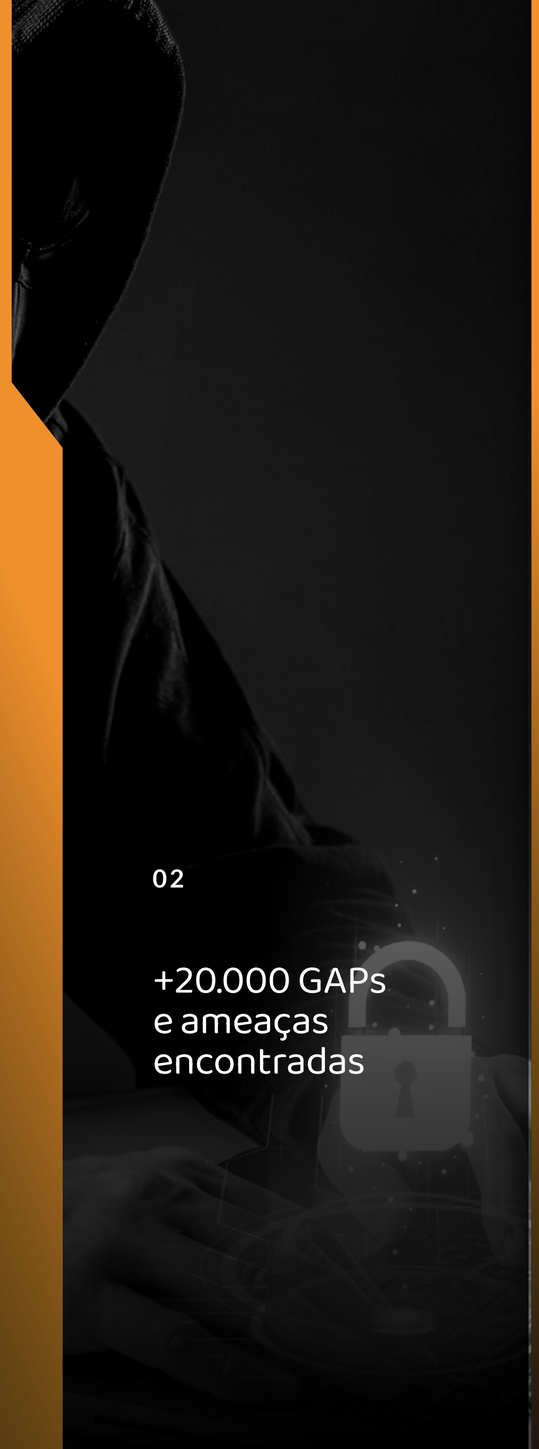
OSWE OSED

eCPPT V2 eWPTX V2 eMAPT

C|EH Certified Ethical Hacker

01

+1.000 projetos implementados manualmente



02

+20.000 GAPs e ameaças encontradas

03

+500 clientes satisfeitos

04

Conhecimento de redes e estruturas industriais e de IoT - MITRE/OWASP

Purple Team

Defesa e ataque em perfeita sincronia. O Purple Team é um serviço colaborativo que simula ataques cibernéticos em um ambiente controlado, combinando técnicas ofensivas e defensivas para avaliar a preparação e a capacidade de resposta da sua organização em tempo real

PROCESSO

- Planejamento do exercício: definimos o escopo e os objetivos das simulações
- Ataques controlados: a Red Team imita os adversários, enquanto a Blue Team responde
- Retroalimentación estratégica: Se comparten los resultados y se ajustan procesos de forma colaborativa

CARATERÍSTICAS NOTÁVEIS

Simulações controladas conduzidas por nossa Red Team, imitando ataques cibernéticos reais

Resposta ativa da Blue Team, identificando e atenuando ataques em tempo real.

Análise pós-exercício, na qual são compartilhados os resultados, as lições aprendidas e as estratégias de aprimoramento

Por que escolhê-la?

- Identificação de falhas de segurança: detectamos os pontos fracos e as melhorias necessárias em suas defesas
- Avaliação realista: simulamos táticas e procedimentos reais (TTP) para um diagnóstico prático
- Melhoria contínua e aprendizado mútuo: promovemos uma cultura de segurança proativa em cada exercício

Entre em contato conosco em

Continuous Pentesting

Segurança constante, adaptação contínua. Implementamos uma abordagem dinâmica e proativa que difere do pentesting tradicional. Esse serviço testa de forma contínua e sistemática, adaptando-se rapidamente às mudanças no ambiente e às ameaças emergentes

PROCESSO

- Avaliação inicial e configuração: definimos o escopo e os objetivos
- Testes automatizados e manuais: testes contínuos de aplicativos e sistemas
- Relatórios regulares: status de segurança, riscos e planos de ação.

CARATERÍSTICAS NOTÁVEIS

- Monitoramento constante por meio de tecnologias avançadas e técnicas automatizadas
- Experiência combinada: análise aprofundada e estratégica feita por especialistas em segurança
- Relatórios regulares e em tempo real, com vulnerabilidades detectadas e recomendações de atenuação

Por que escolhê-la?

- Identificação e correção em tempo real: detectamos vulnerabilidades antes que elas sejam exploradas pelos invasores
- Integração contínua no ciclo de desenvolvimento: aprimoramos a segurança em todo o desenvolvimento de software e infraestrutura
- Conformidade com os regulamentos: Adaptação aos padrões e regulamentos mais exigentes

Entre em contato conosco em

Adversarial Emulation

Enfrente as ameaças como um atacante real faria. Nosso serviço Adversarial Emulation permite avaliar a capacidade da sua organização de resistir a ataques cibernéticos específicos e conhecidos. Por meio de operações ofensivas controladas, simulamos as técnicas, as táticas e os procedimentos (TTPs) usados por agentes de ameaças reais, ajudando a fortalecer sua postura de segurança e a prever possíveis riscos

PROCESSO

- Avaliação do ambiente: identificação dos adversários mais prováveis e relevantes
- Simulação de ataque: reprodução de TTPs usadas por atores reais para testar a defesa
- Relatório e recomendações: Relatório com vulnerabilidades detectadas e melhorias sugeridas.

CARATERÍSTICAS NOTÁVEIS

- Análise baseada nos agentes de ameaças mais relevantes para o seu setor
- Relatório detalhado com descobertas e recomendações específicas
- Operações ofensivas seguras e controladas, minimizando o impacto na produção

Por que escolhê-la?

- Detecção preventiva: identificamos e corrigimos as vulnerabilidades antes que elas sejam exploradas
- Simulação realista: recriamos os ataques mais prováveis para sua organização com base em ameaças específicas do setor
- Fortificação proativa: fornecemos recomendações acionáveis para melhorar a defesa contra possíveis adversários

Entre em contato conosco em

Digital Footprint

Mapeie e proteja sua pegada digital. Nosso serviço Digital Footprint oferece uma visão abrangente da presença digital de sua organização por meio de técnicas avançadas de OSINT (Open Source Intelligence). Essa solução de segurança ofensiva permite que você identifique riscos ocultos e possíveis vetores de ataque, avaliando a exposição de informações confidenciais e o impacto sobre a reputação

PROCESSO

- Coleta e análise: exploração da Web pública, da Deep e Dark Web e de outras fontes relevantes
- Identificação de riscos: detecção de vetores de ataque e informações vazadas
- Relatório de resultados: entrega de um relatório com os riscos encontrados e as medidas de mitigação.

CARATERÍSTICAS NOTÁVEIS

- Pesquisa avançada conduzida por especialistas experientes em OSINT
- Detecção antecipada de informações expostas para evitar ataques
- Relatórios detalhados com as principais descobertas e recomendações acionáveis

Por que escolhê-la?

- Análise exaustiva de fontes abertas (web, fóruns, redes sociais, repositórios, Deep e Dark Web)
- Identificação de vetores de ataque e dados confidenciais expostos
- Avaliação de riscos à reputação e detecção de oportunidades para mitigar ameaças

Entre em contato conosco em

Malware Emulation

Simulação avançada de ameaças. A emulação de malware é um serviço especializado que permite avaliar a capacidade dos seus sistemas de resistir a ataques avançados de malware, como ransomware e spyware, em um ambiente controlado e seguro

PROCESSO

- Design de malware personalizado: adaptado às ameaças mais relevantes para sua organização
- Simulações em ambientes seguros: avaliamos como seus sistemas respondem a ataques reais
- Relatório de resultados: inclui análise detalhada e recomendações para fortalecer sua segurança

CARATERÍSTICAS NOTÁVEIS

Simulação controlada de malware: emulamos ataques reais para avaliar os níveis de proteção

Análise detalhada da eficácia dos controles de segurança implementados

Relatório técnico abrangente, incluindo resultados, técnicas utilizadas e sugestões de aprimoramento

Por que escolhê-la?

- Identificação de vulnerabilidades críticas: descobrimos pontos fracos que podem ser explorados por malware real
- Avaliação abrangente da defesa: testamos a eficácia de soluções como antivírus, firewalls, EDRs e sistemas de detecção de intrusão
- Melhoria contínua da segurança: fornecemos recomendações personalizadas para otimizar controles e processos

Entre em contato conosco em

Application Pentesting Manual

Protegendo seus aplicativos críticos. Avaliamos minuciosamente a segurança de seus aplicativos da Web, móveis e de API, usando técnicas avançadas de teste de penetração. Simulamos ataques reais em ambientes controlados para detectar vulnerabilidades e erros críticos que podem comprometer seus negócios

PROCESSO

- Planejamento e escopo: identificação de aplicativos críticos
- Execução do teste: Simulação de ataques cibernéticos controlados
- Relatório e recomendações: Análise de risco e plano de mitigação detalhado.

CARATERÍSTICAS NOTÁVEIS

- Cobertura completa: Avaliações manuais de aplicativos da Web, APIs e aplicativos móveis
- Simulação de ataques controlados para entender o comportamento de ameaças reais
- Relatório com um roteiro de mitigação priorizado, facilitando as decisões estratégicas

Por que escolhê-la?

- Descoberta de vulnerabilidades ocultas: detectamos falhas que podem não ser detectadas em avaliações tradicionais
- Análise detalhada e priorizada: fornecemos relatórios com descobertas críticas e recomendações práticas
- Proteção abrangente: testamos tudo, desde o código e as configurações até as práticas de segurança, para proteger todas as camadas do seu aplicativo

Entre em contato conosco em

Red Team Exercise

Teste sua resiliência com simulações realistas. Nosso serviço Red Team Exercise concentra-se na infiltração estratégica da infraestrutura da sua organização para simular ataques avançados. Por meio de uma combinação de técnicas de ataque, engenharia social e emulação de adversários, avaliamos a capacidade dos seus sistemas de resistir a ataques cibernéticos reais

PROCESSO

- Planejamento: definição de cenários e objetivos estratégicos
- Execução do ataque: infiltração controlada de sistemas e ativos críticos
- Relatório de resultados: análise de vulnerabilidade e recomendações claras para mitigação

CARATERÍSTICAS NOTÁVEIS

- Simulações realistas alinhadas com as táticas de adversários reais
- Análise abrangente dos controles técnicos e operacionais
- Relatório detalhado com descobertas críticas e um roteiro de aprimoramento priorizado

Por que escolhê-la?

- Identificação de lacunas críticas: descobrimos vulnerabilidades e falhas que podem ser exploradas
- Recomendações acionáveis: fornecemos sugestões priorizadas para fortalecer seu plano de segurança
- Testes de controles abrangentes: avaliamos a prevenção, a detecção, a recuperação e a resposta da sua organização

Entre em contato conosco em

Social Engineering

Fortalecendo sua primeira linha de defesa. Avaliamos o preparo de sua organização para ataques de Phishing, Smishing e Vishing por meio da simulação controlada desses cenários. Nosso objetivo é identificar as vulnerabilidades humanas e melhorar a conscientização da equipe sobre segurança cibernética por meio de testes realistas que refletem as táticas atuais usadas pelos criminosos cibernéticos

PROCESSO

- Projeto de cenários: criação de ataques simulados alinhados com as ameaças atuais
- Execução do ataque: lançamento de campanhas controladas para avaliar a resposta
- Relatório e treinamento: Recomendações personalizadas e, opcionalmente, palestras para eliminar as lacunas identificadas

CARATERÍSTICAS NOTÁVEIS

- Análise do comportamento da equipe com indicadores de maturidade
- Relatórios detalhados com pontos fortes, pontos fracos e recomendações específicas
- Simulações realistas de Phishing, Smishing e Vishing.

Por que escolhê-la?

- Detecção de vulnerabilidades culturais: identificamos áreas de melhoria na resposta dos funcionários
- Cenários personalizados: adaptamos os ataques simulados de acordo com as ameaças mais relevantes para o seu setor
- Conscientização ativa: acompanhamento opcional na estratégia de treinamento por meio de palestras virtuais e presenciais

Entre em contato conosco em

Pentest Cloud | IT OT Infrastructure

Avaliação abrangente de vulnerabilidades. Identifica e avalia vulnerabilidades na infraestrutura tecnológica de sua organização, abrangendo ambientes de tecnologia da informação (TI), tecnologia operacional (TO) e nuvem, com uma abordagem proativa e abrangente

PROCESSO

- Simulação de ataques reais: emulação de táticas que os invasores usariam em ambientes de TI, OT e nuvem
- Análise de infraestrutura crítica: avaliamos os principais componentes, como servidores, redes e aplicativos
- Relatório abrangente e priorizado: descobertas detalhadas e recomendações de mitigação

CARATERÍSTICAS NOTÁVEIS

- Coleta de dados e planejamento: identificamos o escopo e definimos os objetivos do teste
- Teste de penetração avançado: simulamos ataques reais aos diferentes componentes
- Análise de risco: Avaliamos o impacto e a probabilidade de cada vulnerabilidade encontrada
- Relatório e recomendações: geramos uma análise detalhada com etapas prioritárias para melhorar a segurança

Por que escolhê-la?

- Descoberta de falhas de segurança: identificamos e avaliamos configurações incorretas e vulnerabilidades exploráveis
- Visão abrangente da postura de segurança: fornecemos uma avaliação completa da infraestrutura
- Prevenção proativa de ameaças: ajudamos a reduzir os riscos antes que eles se tornem incidentes

Entre em contato conosco em

Por que escolher a BASE4 Security?

> **Garantia de serviço**
Oferecemos uma medida de garantia e confiança na qualidade dos nossos serviços de segurança cibernética.

> **Com o apoio de talentos reconhecidos mundialmente**
Nossa cultura empresarial certificada e premiada é escolhida por pessoas de alto calibre e renome técnico.

> **Serviço consultivo**
Oferecemos soluções personalizadas aos clientes para atender a desafios ou necessidades específicas de segurança cibernética.

BASE4
SECURITY

www.base4sec.com