BASE4 SECURITY

Ajudando a construir um ecossistema digital mais seguro.

Red team

DATA SHEET

Digital Footprint

Através das técnicas avançadas da OSINT, protegemos sua organização contra riscos ocultos na Internet, realizamos pesquisas, análises e identificação de possíveis vetores de ataque e reduzimos os riscos cibernéticos.

Nosso serviço de Pegada Ecológica Digital oferece uma análise abrangente e detalhada da pesquisa de informações de código aberto para ajudar sua organização a identificar riscos e oportunidades potenciais, usando técnicas e ferramentas avançadas. Nossa dedicada equipe OSINT tem ampla experiência na pesquisa e análise de informações de uma variedade de fontes, incluindo websites, fóruns, mídia social, repositórios de código, Deep and Dark Web. Com estas informações, podemos ajudar sua organização a identificar vetores de ataque potenciais, detectar informações sensíveis expostas e avaliar o risco de reputação, bem como detectar atividade maliciosa na Internet.

Com nosso serviço de pegada digital você pode melhorar a segurança cibernética de sua organização e proteger seu ecossistema digital, enquanto melhora sua capacidade de responder a incidentes e ameaças, a fim de assegurar a proteção de seus ativos digitais e minimizar riscos cibernéticos, não hesite em nos contatar, ficaremos felizes em ajudá-lo.

Adversarial Emulation

Conduzimos uma avaliação abrangente dos riscos cibernéticos de sua organização usando técnicas avançadas como a Emulação de Ataques e a Pesquisa de Informação de Código Aberto (OSINT). Identificamos e emulamos vetores de ataque potenciais, ajudando sua organização a detectar e mitigar vulnerabilidades críticas em seus sistemas.

Nosso Adversary Emulation é um serviço abrangente de segurança cibernética que combina técnicas avançadas de ataque como Adversary Simulation e OSINT para avaliar o risco cibernético de sua organização. Nós imitamos um ataque realista e profundo contra sua infra-estrutura tecnológica, identificando vetores de ataque potenciais específicos para sua organização. Além disso, indicamos as Táticas, Técnicas e Procedimentos Mitre ATT&CK (TTPs) que funcionaram e escaparam dos controles durante a análise, fornecendo uma compreensão detalhada dos riscos cibernéticos e ajudando a melhorar a detecção e resposta a incidentes em seu serviço SOC. Os benefícios de nossa emulação adversária incluem avaliar o risco cibernético de sua organização, identificar seus principais vetores de ataque e avaliar a resiliência de sua organização a ataques reais potenciais.

Red Team

Nosso serviço Red Team é um serviço especializado de segurança cibernética que combina técnicas avançadas de ataque como OSINT, Engenharia Social e Emulação Adversary para avaliar a preparação de sua organização para ataques cibernéticos realistas.

Nosso serviço da Red Team é um serviço de segurança cibernética altamente especializado que se concentra no planejamento e execução de projetos estratégicos de infiltração na infra-estrutura de uma organização com o objetivo de obter e extrair informações valiosas e acessar sistemas críticos. Nossos especialistas em segurança utilizam e combinam técnicas avançadas de ataque e simulações de comportamento de atacantes potenciais para avaliar minuciosamente a prevenção, detecção, recuperação, resposta e controle de resiliência de sua organização.

O objetivo é encontrar possíveis violações, falhas de segurança e vulnerabilidades críticas, e fornecer recomendações para melhorar seu plano de segurança existente. Com nosso serviço da Red Team, sua organização pode estar melhor preparada para lidar com incidentes e ameaças reais no mundo digital.

Advanced Penetration Testing

Identifique potenciais fraquezas e vulnerabilidades em sua Web, API e sistemas móveis, bem como sua Infra-estrutura Cibernética através de testes abrangentes e aprofundados e técnicas de forma controlada e segura.

Nossos projetos Pentest são compostos de técnicas avançadas de ataque, 70-80% dos quais são realizados manualmente, controlados e em profundidade, os testes são exaustivos, tentando explorar as vulnerabilidades identificadas com o objetivo de reproduzir um cenário de ataque real realizado por um atacante potencial.

Realizamos testes avançados de intrusão em todos os tipos de sistemas, redes e plataformas:

- Pentest Web
- Pentest API
- Pentest Android / iOs
- Pentest Wireless
- Pentest Cloud / Kubernetes
- Pentest ATM
- Pentest SCADA / OT / ICS

A metodologia adotada pela BASE4 Security divide o Teste de Pentest ou Intrusão em fases e estágios, que seguem um padrão industrial e as melhores práticas como OSSTMM, OWASP, PCI-DSS, NIST SP 800-115, que acompanham as necessidades e expectativas do Cliente. Por sua vez, as tarefas realizadas e as ações específicas tomadas e exploradas são escolhidas com base na oportunidade

percebida e muitas vezes são aumentadas com abordagens adicionais à medida que os vários testes são executados seguindo os padrões acima mencionados.

Este alinhamento metodológico permitirá uma administração eficaz e um gerenciamento assertivo dos resultados, planos de ação e estratégias de gerenciamento de risco associados a vulnerabilidades que podem ser descobertas nos sistemas, plataformas e aplicações do cliente.

Meta:

Com base nos resultados obtidos através dos projetos Pentest, nossos clientes terão um ambiente tecnológico mais seguro e controlado diante de possíveis ataques cibernéticos, evitando assim vazamentos de informação e a indisponibilidade de seus serviços, além de mitigar riscos, fraudes, danos econômicos e exposição da marca e imagem da empresa.

Ingenieria Social

Nosso serviço de Engenharia Social consiste em simular ataques de Phishing, Smishing e Vishing para avaliar a preparação e resposta de sua organização a essas ameaças e melhorar a conscientização de segurança de seus funcionários.

A **BASE4 Security** oferece apoio anual para fornecer indicadores sobre o grau de maturidade interna do usuário e campanhas de conscientização através de técnicas de engenharia social, como a engenharia social:

- Phishing & Spear Phishing
- Smishing
- Vishing
- Tailgating
- Bating
- Dumpster Diving
- Hacking WiFi

Também oferecemos apoio na estratégia de Conscientização e Comunicação através de palestras e treinamentos presenciais e virtuais.

Meta:

Aumentar o nível de maturidade da segurança cibernética dos funcionários da empresa para reduzir a superfície de ataque em larga escala em um curto período de tempo.

BASE4
SECURITY

www.base4sec.com