BASE4 SECURITY

Ajudando a construir um ecossistema digital mais seguro.

Blue Team

DATA SHEET

Diagnóstico de Segurança

Adquira um diagnóstico preciso de segurança cibernética de sua empresa a fim de medir e priorizar os riscos em um plano de curto, médio e longo prazo.

Através de uma equipe de trabalho formada por diferentes perfis (Auditoria, Networking, Ethical Hacking, Cloud Architects, entre outros), é realizado um Diagnóstico Integral de Segurança com o objetivo de proporcionar visibilidade e priorização dos vetores de ataque e riscos da empresa. Estes estão alinhados com o negócio a fim de elaborar um Plano de Ação de Curto e Médio Prazo, priorizando os riscos, os investimentos e os tempos de remediação para cada vetor.

- O diagnóstico de segurança é baseado em estruturas internacionais, como CIS e NIST.
- O diagnóstico visa obter os riscos dos principais vetores de ataque da empresa, tais como equipamentos perimetrais (FW, WAF, VPN), IPs internos, pessoas, processos e a arquitetura da empresa.
- Os resultados do Diagnóstico buscam obter um quadro atual do estado de maturidade da empresa em questões de cibersegurança e fornecer um roteiro para futuros projetos e investimentos a serem priorizados na área.

Digitalização de vulnerabilidades

Obtenha um instantâneo das principais vulnerabilidades da infra-estrutura interna e externa do cliente em um exercício curto e econômico.

Usando ferramentas de terceiros, a BASE4 Security realiza um exercício de Vulnerability Scanning, tentando obter vulnerabilidades de redes internas e serviços públicos.

As vulnerabilidades descobertas são entregues nestes serviços em ordem de prioridade, assim como uma recomendação de remediação.

A **BASE4 Security** pode fornecer um Plano de Remediação além destes serviços de um tiro e também fornecer uma plataforma de nuvem online para que os clientes gerenciem as vulnerabilidades. Comercializamos o serviço One Shot, o serviço contínuo de nosso CyberSOC e a gestão das plataformas de escaneamento do cliente.

Avaliação tecnológica

Realizar uma avaliação de configuração de tecnologias de cibersegurança, tais como Firewalls, WAF's, Ddos, EDR's, SIEM's, DLP's, entre muitas outras, a fim de encontrar melhorias nelas, bem como para amortizar tal investimento.

O principal objetivo é pesquisar os diferentes componentes da arquitetura de tecnologia de segurança dentro da rede para determinar o grau de separação dos ambientes de produção, desenvolvimento e teste em cada componente, assim como suas respectivas configurações e melhores práticas.

Uma vez concluída a avaliação inicial e documentada a situação atual, é determinado o GAP entre a situação atual e as melhores práticas com base nas recomendações da indústria e da tecnologia. As licenças e capacidades não utilizadas da plataforma também serão detectadas no trabalho para que possam ser exploradas pelo cliente no futuro e possam amortizar melhor seu investimento.

O cliente é fornecido com um documento de endurecimento da plataforma e a BASE4 Security pode realizar o ajuste fino da plataforma, se solicitado pelo cliente.

Hardening

Execute o endurecimento das plataformas tecnológicas de segurança cibernética através do ajuste fino das mesmas, em busca de uma proteção mais profunda de sua organização.

O endurecimento das tecnologias ajuda a amortizar o investimento e a proteger a empresa contra os atacantes. O serviço reduz erros humanos e riscos para a organização, pois estas plataformas são freqüentemente estratégicas para a organização, tais como plataformas Perimeter Firewalls, Antimalware ou Information Leakage.

A experiência na implementação e suporte destas tecnologias, bem como a capacidade técnica da equipe de Segurança da BASE4, garantem seu correto endurecimento e o correto aproveitamento do licenciamento contratado.

A BASE4 Security tem experiência em mais de 40 marcas no mercado, bem como em todas as plataformas tecnológicas de ciber-segurança.

BASE4
SECURITY

www.base4sec.com