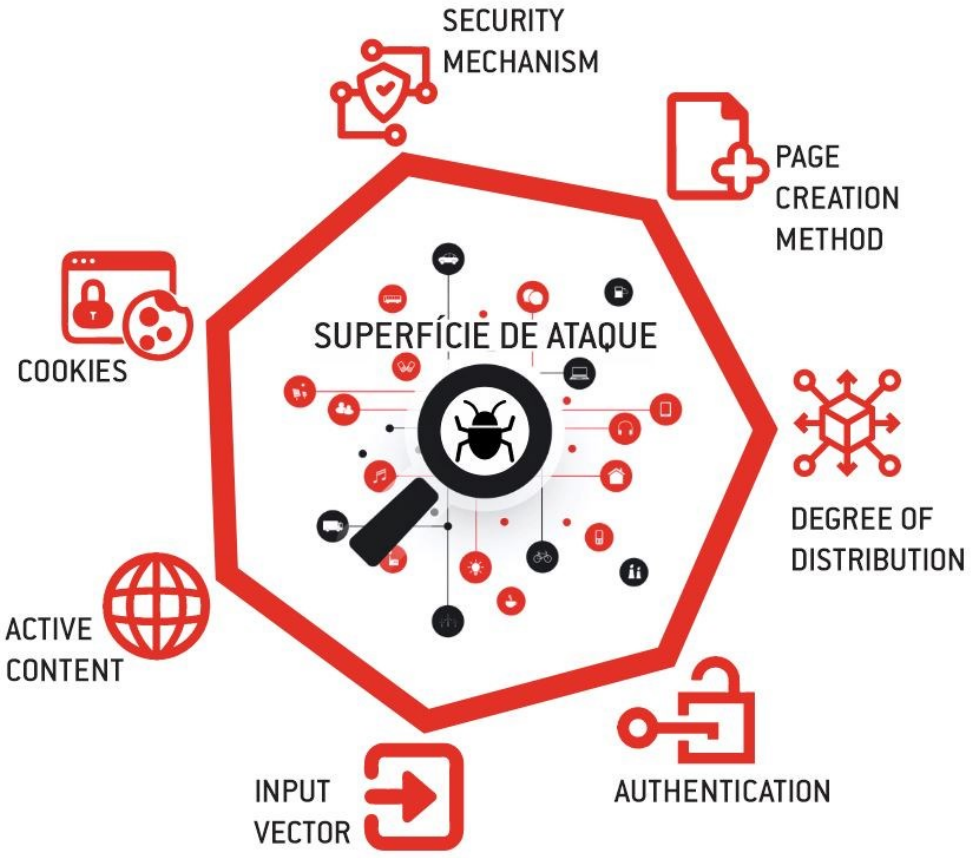
SCUNNA EASM

SCUNNA Consulting Services

O Gerenciamento da Superfície de Ataque Externa (External Attack Surface Management) é um conjunto de práticas e estratégias utilizadas para identificar, avaliar e mitigar as vulnerabilidades e pontos de exposição que podem ser facilmente explorados. Em outras palavras, trata-se do monitoramento e controle dos pontos de entrada que podem ser alvo de ataques cibernéticos vindos de fora da organização, minimizando as oportunidades para que os invasores explorem vulnerabilidades e acessem sistemas ou informações sensíveis.

Isso inclui servidores web, aplicativos da web, APIs, dispositivos IoT, sistemas de e-mail, sistemas, aplicativos e serviços que estão expostos à Internet ou que podem ser acessados remotamente, entre outros. Cada um desses pontos de entrada representa uma possível vulnerabilidade que pode ser explorada por atacantes para comprometer a segurança da organização.

Vetores de Ataque



Solução EASM

MONITORAMENTO
Verificação contínua de uma variedade de ambientes externos (como serviços em nuvem e infraestruturas locais voltadas para o exterior) e superfícies de ataque distribuídas.

DESCOBERTA
Mapeamento de assets externos desconhecidos e suas conexões com sistemas dentro da organização.

ANÁLISE
Avaliação e análise dos atributos para determinar se um ativo é arriscado, vulnerável ou se comporta de maneira anômala.

PRIORIZAÇÃO
Utilização de um sistema de pontuação em várias camadas para reduzir o ruído e priorizar riscos e vulnerabilidades com base na criticidade.

REMEDIAÇÃO
Apresentação de planos de ação para a mitigação de ameaças priorizadas, bem como o fluxo de trabalho de remediação.

scunna

Benefícios

Identificação de Pontos de Entrada
O processo de gerenciamento começa com o Discovery no domínio principal da organização, onde poderemos identificar todos os sistemas e recursos que estão expostos externamente, incluindo servidores, serviços, aplicativos e dispositivos.

Avaliação de Risco
Cada ponto de entrada é avaliado de acordo com seu grau de exposição, criticidade do negócio e update de frequência, analisando indicadores de higiene como portas abertas, páginas de login, certificado inválido, cookies de consentimento e até mesmo política de privacidade de dados.

Redução de Superfície de Ataque
Com base na identificação dos pontos de entrada e avaliação de riscos, medidas são tomadas para minimizar a superfície de ataque. Isso pode incluir a desativação de serviços desnecessários, a implementação de firewalls, o fortalecimento da segurança dos aplicativos da web e a aplicação regular de patches de segurança.

Monitoramento Contínuo
A superfície de ataque externa é monitorada de forma contínua para detectar atividades suspeitas ou anormais que possam indicar tentativas de invasão.

Resposta a Incidentes
Caso uma atividade maliciosa seja detectada, a organização deve estar preparada para responder rapidamente, mitigando o impacto e restaurando a segurança.

Conformidade com Regulamentos
O gerenciamento da superfície de ataque externa ajuda as organizações a atender aos requisitos regulatórios de segurança cibernética, como a Lei Geral de Proteção de Dados (LGPD) ou o Regulamento Geral de Proteção de Dados (GDPR).

Entregáveis

Mapeamento completo
Visão abrangente dos pontos de entrada para a sua organização, identificando vulnerabilidades antes que sejam exploradas.

Varreduras profundas
Varreduras minuciosas para descobrir vulnerabilidades e avaliar seus riscos, fornecendo insights claros sobre os próximos passos.

Mitigação customizada
Indicação de correções e medidas proativas para neutralizar vulnerabilidades e fechar portas de entrada indesejadas.

Relatórios impactantes
Receba relatórios detalhados que comunicam os progressos feitos, métricas de segurança, indicação de redução de riscos, correção e proteção.

Delta
Receba o comparativo mês a mês e fique a par de todos os ativos que foram adicionados e removidos.

SCUNNA Consulting Services

Com o SCUNNA Consulting Services independentemente do porte e do nível de maturidades de segurança da Organização, podemos apoiar no avanço da jornada de postura de segurança para seu negócio, reduzindo riscos e auxiliando a sua conformidade. Oferecemos serviços consultivos personalizados de acordo com suas necessidades.

Gestão de Projetos Scunna

A metodologia Gestão de Projetos Scunna oferece:

Um projeto entregue corretamente e dentro dos prazos e especificações, reduzindo custos e recursos;

Rápida migração, reduzindo o tempo desperdiçado com soluções de legado;

Identificação clara da aplicabilidade dos produtos ofertados;

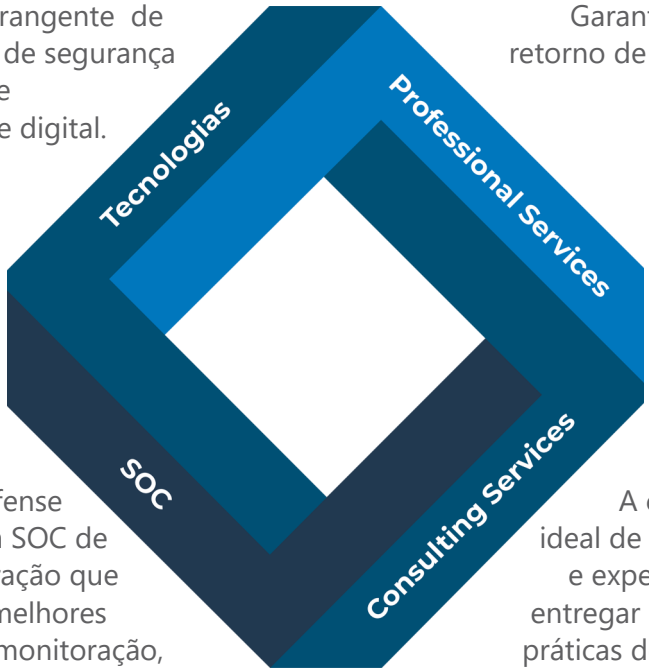
Avaliação constante da entrega de resultados;

Comunicação constante com as partes interessadas sobre o andamento do projeto.

O que fazemos

Portfolio abrangente de tecnologias de segurança cibernética e performance digital.

Garantia do melhor retorno de investimento das soluções contratadas.



O Cyber Defense Center é um SOC de próxima geração que entrega as melhores práticas de monitoração, detecção e resposta a incidentes.

A combinação ideal de qualificação e experiência para entregar as melhores práticas de segurança agnóstica.

A Scunna

Mais de 30 anos no mercado de Tecnologia da Informação.

Integradora de produtos e serviços com **foco em Segurança da Informação e Performance de Aplicações.**

Abordagem **técnica e consultiva,** priorizando a **qualidade de entrega.**

Portfólio completo de **soluções de mitigação de riscos digitais,** abrangendo do **EndPoint ao Cloud Computing.**

Líder em soluções de Application Performance Management, Cloud Infrastructure Monitoring, AIOps e Digital Experience Management.

Expertise consultiva em Cyber Security Strategy, Data Privacy Assessment (LGPD/GDPR), Post Incident Review, External Attack Surface Management, Business Continuity Management, entre outros.

Customização de soluções consultivas de acordo com as necessidades do cliente.

Oferece o **Cyber Defense Center** (Security as a Service) com enfoque em **orquestração, automação e resposta a incidentes cibernéticos** (Next-Generation SOC).

scunna