MEMORIAL DESCRITIVO BLINDAGEM DE SITES

A Blindagem de Sites é o nome comercial dado para o agrupamento de softwares cuja principal função é auditar e proteger aplicações web e servidores de tentativas de ataques de hackers.

Cada nível de blindagem de sites contém um grupo de módulos, resumidos na tabela abaixo:

Características	**Nível I**	**Nível II**	**Nível III**
Scan de Malware para Aplicações Web - Scan automatizado diário online que simula um usuário navegando pelo site e avalia se o mesmo está infectado, contaminando o computador dos visitantes. O relatório da análise mostra qual página do site possui o código malicioso do malware.	Sim	Não	Sim (50 páginas)
Scan de Vulnerabilidade em IP´s Públicos – Análise de vulnerabilidade semanal automatizadas para IP´s públicos visando encontrar brechas de segurança na infraestrutura dos sites	Não	Sim	Sim
Scan de Vulnerabilidades para Aplicações Web – Scan semanal busca falhas de segurança em aplicações web que permitam que hackers acessem dados confidenciais, mostrando qual a solução adequada para as vulnerabilidades apresentadas	Não	Sim	Não
Pen Test Automatizado em Aplicações Web – O teste de penetração automatizado é mais abrangente e profundo que o scan de vulnerabilidade comum. Visa explorar todos os atributos de uma aplicação web, incluindo: preenchimento de formulários, testes de autenticação, entre outros; simulando um ataque de hacker.	Não	Não	Sim
Certificado Digital SSL Blindado – É um protocolo que provê a privacidade e a integridade de todos os dados transmitidos pela internet prevenindo o roubo de informações de ***sniffing***. As informações são codificadas através de um processo de criptografia, impossibilitando que hackers possam decifrá-las	Não	Sim	Não
Certificado SSL Blindado - EV – Combate ***phishing,*** fraude eletrônica caracterizada por tentativas de roubo de informações sigilosas na web. Diferentemente dos certificados comuns, o SSL EV traz aspectos que chamam mais a atenção do usuário e facilitam o reconhecimento de páginas seguras, oferecendo um nível de confiança e segurança muito maior reconhecido pelos usuários devido a BARRA VERDE	Nào	Não	Sim

Mini Pen Test – Testes manuais de segurança e de lógica de aplicação. Analisa 7 itens de segurança	Não	Não	Sim

Todos os módulos são acessíveis via web, através da URL: https://portal2.siteblindado.com denominado PORTAL SITE BLINDADO que contempla as seguintes funções e características:

1) Minha Conta

a. Cadastro de até 5 usuários, com diferentes perfis de acesso
b. Alteração de dados cadastrais da empresa contratante
c. Definição das regras de notificação por e-mail de cada usuário

2) Dashboard

Tela com os principais indicadores de segurança, status da conta e notificações das ações realizadas nos dispositivos, esta seção tem por objetivo dar uma visão geral da conta.

3)Dispositivos

Os dispositivos são qualquer ativo de rede onde possa ser atribuído um IP ou uma aplicação web acessível via internet.

a. Cadastro / remoção de dispositivos (URL, IP)
b. Criação de álias (apelido) para cada dispositivo
c. Atribuição de descrição para todos os dispositivos URL para que sejam listados no diretório de clientes do Site Blindado.

4) Scans de Vulnerabilidade

a. Scan executado semanalmente de forma automatizada, com escolha de período pelo usuário (manhã, tarde e noite) e dia da semana.
b. Agendamento de scans de vulnerabilidade para dispositivos IP ou URL, para realização entre os scans automatizados
c. Relatório de vulnerabilidades que contém o título de cada vulnerabilidade, sua criticidade dividida em 5 níveis (1 a 5), descrição completa das ameaças e impactos das vulnerabilidades identificadas e uma sugestão de como corrigí-las, em PDF ou para navegação em HTML
d. Função de abertura de chamado para contestação de falso-positivo de vulnerabilidade apontada no relatório.

5) Scans de Malware em páginas web

a. Scans diários e automatizados até a quantidade de páginas permitida pelo plano contratado
b.Relatório de infecção por malware que demonstrar se as URLs analisadas estão listadas em blacklist (listas negras de empresas de internet como Google, Firefox e a maioria dos fabricantes de anti-virus) acusando como URLs infectadas por malware, se estão infectadas e em qual linha do código fonte está o link malicioso do malware e instruções de como removê-lo.

6) Exibição de Selos de Certificação SITE BLINDADO ou ANTI-MALWARE

a. Todos os serviços de blindagem de sites níveis I, II ou III, incluem a exibição de selos de certificação de segurança, sendo que cada serviço tem o seu selo específico. Mas existem algumas regras para os selos serem exibidos no seu site:
b. Pageviews: Verifique no Termo de Adesão o limite de pageviews permitida para o selo incluído no seu plano. Ao alcançar o limite de pageviews, a imagem do selo deixa de ser exibida (é trocada por uma imagem transparente) até o fim do mês em questão, quando ela volta a ser exibida. Para ter o selo exibido durante o mês todo, faça o upgrade de plano.
c. SELO SITE BLINDADO: Pode ser exibido após o término do primeiro scan de vulnerabilidades, desde que não haja vulnerabilidades de níveis críticos: 3, 4 ou 5 identificadas na sua aplicação web. Ao longo da vigência do contrato, quando o selo estiver sendo exibido normalmente e o scan semanal detectar uma vulnerabilidade de nível crítico, o sistema enviará um alerta por e-mail notificando todos os usuários da conta. E após 72 horas, o selo é automaticamente removido do seu site (troca por imagem transparente).
d. SELO ANTI-MALWARE. O selo anti-malware não tem limite de pageviews para os planos de BLOGS e SITES INSTITUCIONAIS, entretanto para o plano de E-COMMERCE o limite é de 100.000 pageviews por mês. Caso o site esteja infectado o selo é automaticamente removido.
e. O Site blindado fornece a TAG (código-fonte) do selo a ser exibido pela loja virtual. Esse código não pode ser customizado ou alterado. O selo Site Blindado do Nível de Blindagem III é servido por uma CDN (content delivery network) e possuem uma disponibilidade de 99,8% em base mensal. Os demais selos e para o plano de blindagem nível II, o selo tem uma disponibilidade de 98%.

7) Certificados Digitais SSL BLINDADO

Alguns planos de blindagem possuem certificado digital incluído. Os certificados digitais possuem memorial descritivo exclusivo.

8) Suporte

Todos os planos de blindagem de Sites tem direito a suporte técnico por telefone (011-3454-3310) e e-mail (suporte@siteblindado.com.br), em horário comercial nos dias úteis, exceto feriados nacionais e do município de São Paulo.

9) SLA – Nível de Serviço do Módulo de Blindagem de Sítes

O nível de serviço para o sistema “SLA” é de 95% do tempo de disponibilidade (*up-time*) calculados com base mensal, exceto quando especificado de forma diferente no memorial descritivo do módulo contratado.