

A Iniciativa

A proposta deste conteúdo é fornecer um roteiro de estudo estruturado sobre segurança, com foco em aplicações web (embora não se restrinja somente a isso), visando incentivar que novos profissionais se interessem pela área. O intuito desse conteúdo é criar uma rota de aprendizagem colaborativa.

Contexto

Em 2001, dado as sucessivas detecções, análises e alertas generalizados referente a um *worm* conhecido como [LiOn](#), criou-se o [Internet Storm Center \(ISC\)](#), uma central que provê análises e alertas para milhares de usuários e organizações na internet, contribuindo ativamente com os provedores de internet, no intuito de combater ataques maliciosos. Através de ferramentas como o [DShield Sensor](#), o ISC coleta diariamente milhões de detecções, cobrindo mais de 500.000 endereços IP em mais de 50 países, com o apoio e suporte do instituto [SANS](#), além de voluntários do setor denominados [Handlers](#).

Handlers

Handlers¹ são profissionais que doam seu valioso tempo na detecção e investigação de incidentes e anomalias, provenientes de ataques cibernéticos. Atualmente formado por [19 pessoas](#), os Handlers contribuem regularmente sobre o tema, seja elaborando ideias, pontuando observações ou apresentando casos reais de forma educativa.

A jornada para se tornar um Handler é longa, envolta de desafios e descobertas. O [roadmap oficial](#) contém detalhes minuciosos sobre o processo, bem como os requisitos a serem atendidos. Dentre eles, destacaremos aqui a:

1. [Certificação GIAC](#) ou uma significativa contribuição na área.

Primeiros passos

Se você não faz ideia do que trata o certificado GIAC e tem zero contribuição na comunidade, não desanime, pois todo objetivo precisa iniciar de algum lugar, e é esse o propósito dessa iniciativa.

Explicado, [vamos começar!](#)

Nota¹: o nome *Handlers* (Manipuladores, em tradução livre) é usado nesse contexto, pois no protocolo web, "Handlers" são pontos de passagem onde eventos ocorrem, podendo ser observados, capturados ou anulados.

Introdução

É fundamental adotar uma abordagem abrangente e estruturada para garantir a segurança das aplicações web. Por isso, este conteúdo é embasado em referências reconhecidas, como **CERT, ISC, CVE, NVD, NIST, ISO, OWASP** e nas melhores práticas de **Pentest**, com o objetivo de fortalecer a resiliência e robustez dos ambientes digitais.

Aqui, são apresentados **experimentos e casos reais** que exploram possíveis violações de diretrizes e melhores práticas, proporcionando uma análise crítica e aprofundada sobre segurança cibernética.

Info