Cursos do cert.br | SEI Partner Network

Curso Oficial do CERT® Division: *Foundations of Incident Management* (FIM)

Descrição

Este curso de 5 dias é destinado ao pessoal técnico de Grupos de Segurança e Resposta a Incidentes (CSIRTs), SOCs e outras áreas relacionadas com atividades de Gestão de Incidentes de Segurança Cibernética.

Este curso fornece conhecimentos fundamentais para profissionais que precisam entender as funções de um serviço de Gestão de Incidentes Cibernéticos e como prover este serviço com resiliência. Ele apresenta uma visão geral dos conceitos relacionados com gestão de incidentes, onde estas atividades se encaixam no ecossistema de segurança cibernética e gestão de risco, bem como aborda tópicos como ameaças atuais mais relevantes e a natureza das atividades de resposta a incidentes.

Durante o curso os alunos irão:

- aprender como obter as informações necessárias para tratar um incidente;
- compreender a importância de possuir e seguir políticas e procedimentos pré-definidos;
- entender os aspectos técnicos relacionados com tipos de ataques comumente reportados;
- realizar tarefas de análise e resposta em diversos cenários de incidentes;
- aplicar habilidades de pensamento crítico na resposta a incidentes;
- identificar potenciais problemas a serem evitados durante o trabalho de gestão de incidentes.

O curso incorpora atividades interativas, discussões em grupo e exercícios práticos. Os participantes terão a oportunidade de participar em cenários de resposta a incidentes que poderão encontrar no dia-a-dia do seu trabalho, em exercícios em formato *table top*.

Após completar este curso, os participantes são encorajados a fazer o curso complementar *Advanced Topics in Incident Handling*.

Objetivos

Este curso ajudará os participantes a:

- identificar o que deve ser implementado previamente para facilitar o tratamento de incidentes
- definir consciência situacional e os tipos de fontes de dados para coletar informações de interesse
- comparar os tipos de análise que podem ser realizados, como eles diferem e quando usá-los
- explorar os desafios no compartilhamento de informações e algumas iniciativas que procuram lidar com esses desafios
- reconhecer ameaças e alvos atuais
- reconhecer a importância de seguir processos, políticas e procedimentos bem definidos
- identificar as questões técnicas, de comunicação e coordenação envolvidas na execução bem-sucedida do tratamento de incidentes
- analisar criticamente e avaliar o impacto dos incidentes de segurança da informação
- construir e coordenar estratégias efetivas de resposta para vários tipos de incidentes de segurança da informação

Tópicos Abordados

- processos básicos de gestão de incidentes e possíveis serviços, de acordo com o *FIRST CSIRT Services Framework*
- compreensão do ambiente de ameaças atual
- código de ética de um CSIRT
- ferramentas e tecnologias de segurança usadas por um CSIRT
- identificação de informações críticas
- detecção e análise de incidentes
- processo de triagem
- identificação dos passos básicos da resposta

- ataques envolvendo DNS e uso de DNS no processo de tratamento de incidentes
- busca de informações de contato
- coordenação da resposta a incidentes e disseminação de informações
- tratamento de ataques comuns envolvendo *phishing*, *e-mails*, *ransomware* e outros códigos maliciosos
- visão geral de riscos envonvendo *insider threats*
- cooperação com as polícias e os operadores da justiça

Público Alvo

- integrantes de CSIRTs e analistas de SOC que tenham pouca ou nenhuma experiência (um a três meses de experiência), e que estejam envolvidos com atividades de gestão de incidentes, incluindo atividades detecção e resposta a ataques
- integrantes experientes de CSIRTs e SOCs que tenham interesse em validar seus processos ou em aumentar seus conhecimentos através de treinamento formal e boas práticas operacionais
- profissionais que potencialmente venham a atuar em grupos de resposta a incidentes (CSIRTs) ou áreas ligadas à gestão de incidentes
- administradores de redes e sistemas que sejam responsáveis por identificar e responder a incidentes de segurança ou outras atividades ligadas à proteção das redes

Pré-Requisitos

Para participar deste curso os candidatos devem preencher os seguintes pré-requisitos:

- **Inglês técnico** intermediário ou avançado (o material é em Inglês).
- Familiaridade com protocolos e serviços Internet (TCP/IP).
- Alguma experiência com administração de sistemas Unix ou Windows.

Obtenção do Certificado

Os certificados dos Cursos Oficiais do CERT® Division ministrados pelo CERT.br têm a mesma validade daqueles emitidos diretamente pela Carnegie Mellon® University.

Serão emitidos certificados para os alunos que obtiverem **90% de presença**.

O certificado de conclusão do curso é equivalente a 2.5 CEUs (*Continuing Education Units*), emitidos pela *Carnegie Mellon® University*.

O curso *Foundations of Incident Management* faz parte dos requisitos para obter diretamente no SEI/CMU a credencial CERT® Incident Response Process Professional Certificate.

Carga Horária

O curso possui carga horária equivalente a 40 horas.

O curso é ministrado de segunda a quinta-feira das 08h30 às 17h00, e na sexta-feira das 08h30 às 15h30.

Incluído na Inscrição

Estão incluídos no valor da inscrição:

- Apostila em formato impresso e PDF;
- Cópias impressas dos exercícios práticos e de documentos de apoio;
- Almoço e *coffee-breaks* pela manhã e à tarde.

SIGA O NIC.BR

SIGA O CERT.BR

CONTATO

Privacidade e Termos de Uso – NIC.br
Privacidade – Cursos do CERT.br

Última atualização: `$Date: 2025/01/22 18:29:55 $`

NIC.BR - Núcleo de Informação e Coordenação do Ponto BR
CNPJ:05.506.560/0001-36