CYBFND (TELECON FUNDAMENTOS EM CYBERSECURITY) 1.0

Objetivo

ApÃ³s a participaÃ§Ã£o nesse treinamento o aluno serÃi capaz de: â□¢ Explicar o funcionamento de um Centro de OperaÃ§Ãµes de SeguranÃ§a (SOC); â□¢ Descrever os diferentes tipos de serviÃ§os que sÃ£o executados na perspectiva de um analista de SOC; â□¢ Explicar as ferramentas para Monitoramento de SeguranÃ§a de Rede (NSM); â□¢ Explicar os dados necessÃirios para o analista de seguranÃ§a de rede; â□¢ Descrever os conceitos bÃisicos, utilizaÃ§Ã£o e emprego da criptografia; â□¢ Descrever as falhas de seguranÃ§a do protocolo TCP/IP que podem ser utilizadas em ataques; â□¢ Compreender as tecnologias comuns empregadas na seguranÃ§a de equipamentos de usuÃirios e servidores; â□¢ Compreender a cadeia de eliminaÃ§Ã£o (Kill Chain) e os modelos Diamante na conduÃ§Ã£o de investigaÃ§Ãµes de incidentes; â□¢ Identificar recursos necessÃirios para identificar as ameaÃ§as cibernÃ©ticas; â□¢ Explicar a necessidade da normalizaÃ§Ã£o de dados e da correlaÃ§Ã£o; â□¢ Identificar os vetores de ataque mais comuns; â□¢ Identificar atividades maliciosas; â□¢ Identificar padrÃµes de comportamentos suspeitos; â□¢ Conduzir investigaÃ§Ãµes em incidentes de seguranÃ§a; â□¢ Explicar a utilizaÃ§Ã£o de um Playbook tÃpico em SOC; â□¢ Explicar a utilizaÃ§Ã£o de mÃ©tricas em SOC para medir a sua eficÃicia; â□¢ Explicar a utilizaÃ§Ã£o de um sistema de gerenciamento de fluxo de trabalho e automaÃ§Ã£o para melhorar a eficÃicia de um SOC; â□¢ Descrever um plano tÃpico de resposta a incidentes; â□¢ Descrever as funÃ§Ãµes de uma Equipe de Resposta a Incidentes de SeguranÃ§a(CSIRT); â□¢ Explicar a utilizaÃ§Ã£o do VERIS (Vocabulary for Event Recording and Incident Sharing) para documentar os incidentes de seguranÃ§a para um formato padronizado.

PÃºblico Alvo

Este curso foi desenvolvido para: â□¢ Profissionais que buscam se preparar a exercer a funÃ§Ã£o de Analista de SeguranÃ§a CibernÃ©tica; â□¢ Profissionais de TI que buscam conhecimentos e a capacitaÃ§Ã£o em operaÃ§Ãµes de seguranÃ§a cibernÃ©tica; â□¢ Profissionais que desejam se preparar ao exame de certificaÃ§Ã£o Cisco Certified CyberOps Associate(200-201 CBROPS); â□¢ Profissionais que desejam se preparar ao exame de certificaÃ§Ã£o CompTIA Cybersecurity Analyst Certification (CS0-002 CySA+).

PrÃ©-Requisitos

Ã□ desejÃivel possuir os seguintes conhecimentos e habilidades: â□¢ Familiaridade com redes Ethernet e TCP/IP; â□¢ Conhecimento prÃitico dos sistemas operacionais Windows e Linux; â□¢ Familiaridade com conceitos bÃisicos de seguranÃ§a de rede.

Carga HorÃiria

40 horas (5 dias).

ConteÃºdo ProgramÃitico

Centro de Operações de Segurança
Tipos de Áreas SOC
Ferramentas do Analista de SOC
Introdução a Análise de Dados (Data Analytics)
Relatórios Automatizados
Alertas de Anomalias
Equipe de Resposta à Incidentes
Papéis Exercidos em um SOC Típico
Integração do SOC com a Organização

Infraestrutura de Rede e Monitoramento da Segurança
Revisão: Fundamentos de NAT
Revisão: Filtragem de Pacotes com ACLs
Métodos Empregados Para Controle de Acesso
Revisão: Conceito AAA
Revisão: Balanceamento de Carga
Proteção Contra Malware Baseada em Rede
Ferramentas de Monitoramento de Rede

Categorias dos Tipos de Dados
Dados para Monitoramento da Segurança de Rede
Dados de Segurança e Sistemas de Gerenciamento
Orquestração, Automação e Resposta em Segurança
Conceito: Segurança em Camadas
Dados pela Captura de Pacotes
Dados de Sessão: Conversação entre Partes
Dados da Transação: Requisições e Respostas
Dados de Alertas de IPS e IDS
Outros Tipos de Dados
Correlação de Dados e Eventos
Conceito: CID
Dados e Proteção das Conformidades Externas

Entendendo os Conceitos Básicos de Criptografia
Impacto da Criptografia nas Investigações de Segurança
Visão Geral em Criptografia
Algoritmos de Hash
O Que é Criptanálise
Algoritmos de Criptografia Simétrica
Algoritmos de Criptografia Assimétrica
Protocolo Diffie-Hellman
Assinaturas Digitais e Certificados
Visão Geral em PKI
Operações de Uma PKI
Gerenciamento de Chaves e Algoritmos

Noções básicas sobre ataques TCP/IP comuns
Protocolo de Resolução de Endereço DNS
Vulnerabilidades Herdadas do Modelo TCP/IP
Vulnerabilidades do IP
Vulnerabilidades do ICMP
Vulnerabilidades do TCP
Vulnerabilidades do UDP
Ataques e seus Vetores
Ataques de Reconhecimento
Ataques de Acesso
Ataques Man-in-the-Middle
Negação de Serviço e Negação Distribuída de Serviço
Ataques por Reflexão e Ampliação
Ataques de falsificação (Spoofing)
Ataques so Serviço DHCP

Tecnologias de Segurança Para Dispositivos de Usuários
Firewall Pessoal Baseado em Dispositivo
Antivírus Baseado em Dispositivo
Sistema de Prevenção de Intrusão para Dispositivos Usuários
Listas de Aplicativos Permitidos e Bloqueados
Proteção Contra Malware Baseada em Dispositivos
Concietos de Sandboxing
Verificação da Integridade de Arquivos

Análise de Incidentes em SOC
Visão Geral do Modelo Kill Chain
Fase 1: Reconhecimento
Fase 2: Armamento
Fase 3: Entrega
Fase 4: Exploração
Fase 5: Instalação
Fase 6: Comando e Controle
Fase 7: Ações Nos Objetivos
Aplicando o Modelo Descrito
Visão Geral do Modelo Diamante
Aplicando o Modelo Diamante
Estrutura MITRE ATTACK™
Investigação & Metodologia

Identificando Recursos na Busca Às Ameaças Cibernéticas
Conceitos de Busca Às Ameaças Cibernéticas
Modelo de Maturidade
Ciclo da Busca
Sistema de Pontuação da Vulnerabilidade
Pontuação CVSS v3.0
Painel de Ameaças "Quentes"
Recursos para Conscientização Sobre Ameaças

Outras Fontes de Inteligência de Ameaças Externas
Inteligência de Segurança
Sistemas Analíticos de Ameaças
Ferramentas de Segurança
Análise e Busca de Tráfego Malicioso

Correlação e Normalização de Eventos
Fontes de Eventos
Busca de Evidência
Cadeia de Custódia
Normalização de Dados em Segurança
Correlação de Eventos

Identificando Vetores de Ataque Comuns
Operações de DNS
Operações HTTP e HTTPS
Operações SQL e Injeção de SQL
Operações SMTP
Script da Web
JavaScript ofuscado
Shellcode e Exploits
Cargas de Metasploit Comuns
Percurso de Diretório
Script Entre Sites
Código Puny
Tunelamento de DNS
Obtendo acesso por meio de ataques baseados na Web
Exemplos de Kits de Exploração

Identificando Atividades Maliciosas
Entendendo o Design de Rede
Modelo de Confiança Zero
Identificando Atores de Ameaças
Registros do Sistema
Registro do Firewall & NGFW
Registro DNS
Registro de Proxy da Web
Registro de Proxy de e-mail
Registro do Servidor AAA
Registro de aplicativos
NetFlow Como Ferramenta de Segurança
Detecção de Anomalias de Comportamento da Rede
Técnicas Para Evasão de IPS
Obtendo Acesso e Controle
Redes do Tipo Peer-To-Peer
Encapsulamento de Tráfego

Identificando Padrões de Comportamento Suspeito

Linha de Base da Rede (Baseline)
Identificando Anomalias e Comportamentos Suspeitos
Análise PCAP
Investigar Atividade Suspeita com Security Onion

Investigações em Incidentes de Segurança
Procedimentos de Investigação em Incidentes de Segurança
Exemplo: Trojan de Acesso Remoto
Investigação Avançada de Ameaças Persistentes

Modelo de Manual & Monitoramento de Segurança
Análise de Segurança
Definição do Manual
Sistema de Gerenciamento por "Playbook"

Noções básicas sobre métricas de SOC
Agregação de Dados de Segurança
Tempo Para Detecção
Eficácia da Detecção dos Controles de Segurança
Métricas SOC

Entendendo o fluxo de trabalho e a automação SOC
Conceitos SOC & WMS
Fluxo de Trabalho de Resposta a Incidentes
Integração SOC & WMS
Exemplo de Automação do Fluxo de Trabalho SOC

Descrevendo a Resposta a Incidentes
Planejamento de Resposta a Incidentes
Ciclo de Vida de Resposta a Incidentes
Elementos da Política de Resposta a Incidentes
Categorias de Ataques Incidentes
Requisitos de Resposta a Incidentes
Categorias CSIRT
Estrutura CSIRT
Serviços de Tratamento de Incidentes CSIRT

Entendendo o VERIS
Visão geral do VERIS
Estrutura de Incidentes VERIS
VERIS 4 A's
Registros VERIS
Banco de Dados da Comunidade VERIS

Sistema Operacional Windows
Histórico do Sistema Windows
Arquitetura do Sistema Windows
Espaço de Endereço de Memória Virtual do Windows

Serviços do Windows
Sistema de Arquivos do Windows
Estrutura do Sistema de Arquivos do Windows
Domínios do Windows e Usuários Locais
A interface GUI do Windows
Executar Tarefas Como Administrador
A interface CLI do Windows
O Windows PowerShell
Comando Net do Windows
Controlando Serviços de Inicialização
Executando o Desligamento do Sistema
Serviços e Processos de Controle
Recursos do Sistema de Monitoramento
Processo de Inicialização do Windows
A Rede Windows
Uso do Comando netstat do Windows
Registro do Windows
Instrumentação de Gerenciamento do Windows
Funções comuns do Windows Server
Ferramentas de Terceiros

Sistema Operacional Linux
História do Linux
Arquitetura Linux
Visão Geral do Sistema de Arquivos Linux
Comandos Básicos de Navegação
Gerenciamento do Sistema de Arquivos
Propriedades e Permissões de Arquivo
Discos e Sistemas de Arquivos
Inicialização do Sistema
Opções de Inicialização de Emergência/Alternativa
Desligando o Sistema
Processos do Sistema
Interagindo com Linux
Conceitos do Shell de Comando do Linux
Ferramentas Úteis CLI do Linux
Rede do Linux
Visualizando Serviços de Rede em Execução
Visualizando o Tráfego de Rede
Configurando o Syslog Remoto
Executando Software no Linux
Gerenciadores de Pacotes & Linux
Aplicativos do Sistema

laboratório
Lab 1R: Descobrindo o ambiente de laboratório
Lab 2L: Tecnologias Criptográfica
Lab 3R: Ferramentas de Monitoramento de Segurança de Rede

LAB 4L: Ataques em TCP/IP
LAB 5L: Explorando as Ferramentas de Dispositivo Usuário
Lab 6R: Ferramentas de Monitoramento de Segurança de Dispositivo Usuário
Lab 7R: Analisando a saída da topologia e ferramentas de enumeração de host
Lab 8R: Testando a segurança de credenciais
Lab 9R: Configurando a segmentação e a segurança da rede
Lab 10R: Avaliando o impacto das vulnerabilidades de aplicativos da Web
LAB 11L: Explorar o sistema operacional Windows
LAB 12L: Explorar o sistema operacional Linux