DSO 120 | ANÁLISE DE PACOTES EM REDES E APLICAÇÕES

ANTEBELLUM

psi Testing Excellence · iapp · CompTIA · EXIN · Pearson VUE Authorized Test Center

Com 25 anos de experiência em Capacitação de recursos em Segurança da Informação, **a Antebellum foi fundada em 1997**, a partir da observação de um grupo de instrutores e professores de Tecnologia e Segurança da Informação, sobre as mudanças nos cenários nacional e internacional e as dificuldades encontradas pelos profissionais destas áreas para a contratação de treinamentos que se encaixassem em suas agendas e orçamentos.

Diante deste contexto os primeiros cursos foram criados, apresentando seus conteúdos de forma aprofundada e objetiva, sendo claramente notados pelo material do aluno, transformando-o em uma fonte de referências futuras e apoio ao estudo para os exames de certificação.

O pioneirismo do fundado, a qualidade dos instrutores e o extenso número de certificações de reconhecimento internacional, resultou em aproximação e parceria com as maiores autoridades no segmento de Tecnologia e Segurança da informação mundial, entregando ao mercado brasileiro, conteúdo de qualidade diferenciada, com constantes atualizações.

Algumas das conquistas realizadas pela Antebellum:

- Foi a primeira empresa no mundo a ministrar os treinamentos oficiais da PCI Council, além de ser a única empresa ter seus treinamentos ministrados em Português Brasileiro;
- Foi primeira empresa nas Américas a ministrar os treinamentos oficiais da EXIN, para a formação e certificação DPO (Data Protection Officer), baseada na GDPR da Europa;
- Em 2019 oficializou a parceria com a IAPP (international Association of Privacy Professionals), podendo ministrar treinamentos para as certificações CDPO-BR, CIPM, CIPP/E, além de ser a única parceira a oferecer o treinamento CIPT no Brasil.

Assim, ao longo desta jornada, a Antebellum acumulou experiência em capacitação de recursos em segurança da informação, tendo treinado milhares de profissionais em todo o país.

"Porque antes de tudo mais, preparar-se é o segredo do sucesso."

Henry Ford

Missão

Preparar os Profissionais com as habilidades e competências necessárias para enfrentar os desafios da tecnologia da informação, proteção e privacidade de dados

Visão

Inovar, Engajar, Transformar!

A Antebellum é movida pela paixão pelas pessoas, ajudando a transformar a carreira de cada um de seus estudantes, inovando a cada dia para engajá-los em um ciclo vitorioso de aprendizado.

Assim, nós da Antebellum trabalhamos com pessoas, com seus sonhos profissionais e suas realizações, ao longo destes 25 anos, inúmeros sonhos realizados, novos caminhos se abriram e diversas foram as conquistas, pois buscamos sempre potencializar pessoas e valorizar negócios.

Então... Qual é seu sonho profissional???

A Antebellum tem a filosofia de associar-se a empresas no exterior para trazer os melhores treinamentos em Tecnologia da Informação e Segurança da Informação para a América Latina.

A Antebellum foi a única empresa no mundo a receber a autorização para ministrar os treinamentos oficiais do PCI Council.

October 02, 2012 10:15 AM Eastern Daylight Time

PCI Security Standards Council anuncia disponibilidade de treinamento em português no Brasil. Nova organização sócia brasileira oferecerá treinamento de alta qualidade em PCI com instrutor na língua local.

O PCI Security Standards Council se associará à Antebellum, uma empresa brasileira líder em treinamento em TI, para oferecer cursos orientados por instrutores para o programa de Internal Security Assessor (ISA) e classe de Conscientização de PCI.

Todos os materiais e discussões na sala de aula serão fornecidos em português.

Fonte: http://www.businesswire.com/news/home/20121002006183/pt

DEPOIMENTO

"Temos o prazer de anunciar nossa primeira parceria internacional de treinamento e estamos muito satisfeitos em associar-nos à Antebellum, uma organização com conhecimento profundo dos padrões da PCI"

"A educação é um elemento imprescindível na segurança de pagamentos, e o Conselho da PCI está comprometido com a expansão de oportunidades de treinamento da PCI globalmente"

Bob Russo,
General Manager, PCI SSC

DEVSECOPS

O DevSecOps incorpora automaticamente a segurança em todas as fases do ciclo de vida de desenvolvimento de software, permitindo o desenvolvimento de software seguro na velocidade do Agile e do DevOps.

A Análise de Pacotes em Redes e Aplicações aumenta sua capacidade de entender os pacotes e os protocolos e é uma habilidade crítica para administradores de rede e de sistemas, engenheiros de rede, desenvolvedores, investigadores forenses, analistas de SOC, engenheiros de segurança, profissionais de suporte e programadores.

Os pacotes apresentam a radiografia de todos os componentes operando junto, como aplicações, dispositivos de rede, servidores e protocolos. Você precisa aprender como identificar os pacotes desses componentes e suas principais características.

Por que fazer este curso?

Este curso apresentará os conceitos fundamentais, as metodologias e ferramentas necessárias para análise de redes e aplicações, tráfego de rede e protocolos em ambientes de TI e TA de qualquer tamanho. Além disso, você poderá :

- Conhecer os 04 pilares da Análise de Redes, Protocolos e Aplicações
- Calcular a latência, a utilização de banda e o Throughut da rede
- Analisar e entender redes WLan (Wi-Fi)
- Entender o Tráfego de virtualização de armazenamento

Objetivos deste curso

Capacitar profissionais para analisar aplicações nas redes de trabalho baseados na ferramenta de análise de protocolos, determinar pontos de falha e implementar segurança de infraestrutura. Elaborar VPN e garantir sua segurança.

Metodologia de ensino

- Modalidade online, ao vivo: O aluno assiste as aulas quando elas acontecem, estando sempre em sincronismo com a turma e matéria, possibilitando a interação direta com o instrutor.
- Metodologia ativa de ensino: O conteúdo é desenvolvido de forma contextualizada, pautada na prática problematizadora, a partir de casos práticos, na qual a discussão entre os alunos e instrutor, amplia e facilita o processo de ensino e aprendizagem.
- Laboratórios práticos: Laboratórios práticos para desenvolver e testar suas habilidades examinando centenas de capturas que irão fortalecer os conceitos que você aprendeu.

Carga-horária

- 40 horas de treinamento (online, ao vivo)

Pré-requisitos

- É recomendável ter conhecimento básicos de rede

Público-alvo

- Profissionais de suporte em TI
- Desenvolvedores
- Administradores de sistema
- Engenheiros de rede
- Investigadores forenses
- Analistas de SOC
- Engenheiros de software
- Programadores em geral

Instrutores

PAULO COELHO

INSTRUTOR

AWS | CCDA | CCNA | CCNP | CNE | CNI | CWNA | MCSA | VMware

Certificações do curso

Não há certificações disponíveis para este curso

Programa do curso

MÓDULO 01 | Introdução à Análise de Redes

- As 10 verdades sobre análise de rede
- Entendendo análise de rede
- Por que as redes ficam lentas?
- Metodologia de troubleshooting
- Modelo OSI e seus elementos
- Pilhas de protocolos comerciais
- Tráfegos Windows e Linux
- Identificando os problemas pelas camadas
- Laboratório prático

MÓDULO 02 | Entendendo os analisadores de protocolos

- O que são os analisadores de protocolo
- Tipos de analisadores
- Posicionamento de um analisador
- TAP X SPAN
- Analisadores por software
- Analisadores por hardware
- Laboratório prático

MÓDULO 03 | Entendendo o Wireshark

- O que é o Wireshark
- Interface básica do Wireshark
- Opções de captura
- Filtros
- Analisando TCP e UDP streams
- Estatísticas
- Analisando telefonia
- Como construir uma probe ou appliance para análise de redes
- Laboratório prático

MÓDULO 03 | Filtros Wireshark

- Componentes do Wireshark
- Função dos filtros
- Filtro de captura
- Filtro de display
- Criando filtros com a interface gráfica
- Aplicando os filtros na análise de redes e aplicações
- Laboratório prático

MÓDULO 05 | Linhas de comando Wireshark

- Comandos de linha Wireshark
- Funções dos comandos de linha
- Configurar o path
- Descrição de cada comando
- Aplicações dos comandos de linha na análise de redes e aplicações
- Laboratório prático

MÓDULO 06 | Entendendo a tecnologia Ethernet

- Camada física
- A influência da certificação do cabeamento no tráfego de rede
- Frames empregados na tecnologia Ethernet
- Tecnologias de 10Mbps a 40Mbps
- O CSMA/CD
- Tráfego half e full-duplex
- Erros na camada 2
- Tráfegos Unicast, Multicast e Broadcast
- Indicadores de desempenho em uma rede Ethernet
- Laboratório prático

MÓDULO 07 | Entendendo o tráfego de Vlan

- Conceitos de uma rede hierárquica
- Switches Blocking x Non-Blocking
- Métodos de Switching
- Fundamentos de VLAN
- VLAN Tagging
- Q-in-Q VLANs
- Laboratório prático

MÓDULO 08 | Entendendo o tráfego de Spanning Tree

- Exigências da camada core
- Principais impactos causados pela redundância
- Protocolo Spanning-Tree
- Como o Spanning-tree opera
- Terminologia Spanning-tree
- Procolo Rapid Spanning-tree
- Laboratório prático

MÓDULO 09 | Entendendo os protocolos IPV4

- A pilha de protocolos IPv4
- Protocolo ARP
    - Por que o ARP é necessário
    - Principais características do ARP
    - Descrever o tráfego de ARP
    - Identificação de IPs duplicados
    - Entender o RARP
    - Tráfego ARP que deve ser observado
    - Principais assinaturas
    - Laboratório prático

- Protocolo IP
    - Entendendo o Best Efford
    - Datagrama IP
    - Type of service
    - Fragmentação IP
    - IP Options
    - Principais assinaturas
    - Laboratório prático

- Protocolo ICMP
    - Entender a função do protocolo ICMP
    - Descrever as principais mensagens do protocolo ICMP
    - Descrever a estrutura de um pacote ICMP
    - Utilitários que empregam o ICMP
    - Principais mensagens ICMP
    - Principais assinaturas
    - Laboratório prático

- Protocolo TCP/UDP
    - O que faz a camada de transporte?
    - Portas TCP/UDP
    - Socket e Winsock
    - Protocolo TCP
    - Estrutura do segmento TCP
    - Flags TCP
    - Como os hosts se comunicam com TCP
    - Processo de estabelecimento de sessão
    - State Machine do protocoloTCP
    - Protocolo UDP
    - Principais assinaturas
    - Laboratório prático

MÓDULO 10 | Entendendo o tráfego IPV6

- Introdução ao IPv6
- Características e benefícios do IPv6
- Diferenças entre IPv4 e IPv6
- Terminologia IPv6
- Endereçamento IPv6
- Datagrama IPv6
- ICMPv6
- Principais Serviços IPv6
- Principais assinaturas
- Laboratório prático

MÓDULO 11 | Entendendo as aplicações IPV4/IPV6

- Serviço DHCP
- Serviço HTTP – Web Server
- Resolução de nomes com DNS
- Servidor FTP
- Servidor de correio SMTP
- Protocolo POP3
- Protocolo IMAP4
- Telnet
- Servidor TFTP
- Laboratórios práticos

MÓDULO 12 | Protocolo TCP Avançado

- As características avançadas do protocolo TCP
- Entendendo as retransmissões
- Timeouts de redes
- Controle de fluxo e janelamento
- Entendendo os Acks
- Zero Window
- Entendendo o congestionamento da rede
- Laboratório prático

MÓDULO 13 | Protocolos Windows

- Entendendo a pilha de protocolos Windows
- Protocolos Kerberos e AD
- Protocolo SSDP
- Protocolo LLNM
- Tráfego netbios
- SMB/CIFS
- RDP
- Principais assinaturas
- Laboratório prático

MÓDULO 14 | Entendendo o tráfego de Banco de Dados

MÓDULO 15 | Entendendo o tráfego de virtualização e armazenamento
- Cluster virtualizado
- Vxlan
- Tráfego de armazenamento
- Principais assinaturas
- Laboratório prático

MÓDULO 16 | Caracterizando o tráfego de rede
- Padrões do tráfego de rede
- Por que a rede fica lenta?
- Entendendo a latência
- Dissecando os tempos da LAN
- Caracterização de serviços
- Tarefas que devem ser realizadas
- Caracterizar o tráfego
- Padrões de tráfego das aplicações
- Ferramentas do Wireshark
- Entendendo os temporizadores
- Laboratório prático

MÓDULO 17 | Analisando o tráfego de segurança
- Scan SYN
- NMAP
- Fingerprinting
- Manipulação de tráfego
- Malware
- Principais assinaturas
- Laboratório prático

MÓDULO 18 | Construindo um relatório
- Porque fazer um relatório de análise
- Dez dicas sobre relatórios
- Ferramentas
- Usando WireShark
- Modelo de Relatório

MÓDULO 19 | Outras soluções de Análise de Tráfego e Aplicações
- Monitoramento SNMP
- APM
- Análise de logs
- Laboratório prático

“Jamais destrua seus sonhos
Destrua seus limites”

(autor desconhecido)

/cursosantebellum

/cursos.antebellum

@cursosantebellum

cursos@antebellum.com.br