ISUTC
INSTITUTO SUPERIOR DE TRANSPORTES E COMUNICAÇÕES

paloalto NETWORKS

ACADEMIA PALO ALTO NETWORKS DO ISUTC

CERTIFICAÇÕES EM CYBERSECURITY DA PALO ALTO NETWORKS

PCCSA (*Certified Security Associate*) – Associado Certificado pela *Cybersecurity* da Palo Alto *Networks*

Associado certificado de segurança cibernética da Palo Alto Networks (**PCCSA**) possui conhecimentos da tecnologia de ponta disponível actualmente para gerir as ameaças cibernéticas futuras. Para possuir o nível de **PCCSA**, os participantes deverão ter concluído com êxito os módulos :

CYBERSECURITY FOUNDATION

Visão geral do curso:

Este curso, permitirá aos participantes aprender os fundamentos da segurança cibernética e identificar os conceitos necessários para reconhecer e potencialmente mitigar ataques contra redes organizacionais, bem como para infraestrutura de missão crítica.

Objectivos do Curso:

Após a conclusão deste curso, os alunos serão capazes de realizar o seguinte:

- Identificar o cenário de segurança cibernética e como as vulnerabilidades afectam os sistemas de infra-estrutura de TI em nível organizacional.
- Definir os papéis desempenhados pelos principais actores de ameaças nos ciberataques modernos e suas principais motivações.
- Avaliar os vários tipos de ataques cibernéticos e técnicas de ataque perpectuadas por actores.
- Explicar como *DDOS*, explorações de *WiFi* e acções de ameaças avançadas são usadas para realizar ataques cibernéticos.
- Fazer a distinção entre conformidade e segurança.
- Descrever os fundamentos básicos dos modelos de segurança de rede baseados em perímetro e *Zero Trust*.
- Explicar como a segurança do *Data center* virtualizado difere da segurança do *Data center* físico.
- Conhecer o conceito de segurança da computação em nuvem e como ela afecta as redes organizacionais.
- Comparar os vários dispositivos de segurança de rede, incluindo *firewalls*, *VPNs* e muito mais.

ISUTC
INSTITUTO SUPERIOR DE TRANSPORTES E COMUNICAÇÕES

paloalto NETWORKS

CYBERSECURITY GATEWAY

Pré-requisitos do curso: Cybersecurity Foundation

Visão geral do curso:

Este curso visa ensinar aos alunos a entender os conceitos fundamentais da rede e os conceitos gerais envolvidos na manutenção de um ambiente seguro de utilização na rede.

Após a conclusão bem-sucedida deste curso, os participantes podem examinar, descrever os fundamentos gerais da rede e implementar técnicas básicas de configuração da rede.

Objectivos do curso:

- Demonstrar conhecimento da tecnologia interconectada na comunicação diária e no estilo de vida e entender os sistemas que precisam de protecção.
- Examinar os ambientes de cenário de segurança cibernética, vectores de ameaças de ataque, exposição, vulnerabilidades e factores de risco.
- Demonstrar conhecimento de endereçamento físico, lógico e virtual que acomoda redes de vários tamanhos por meio do uso de esquemas de máscara de sub-rede.
- Explicar o modelo TCP / IP e identificar correctamente as funções das camadas específicas, incluindo o encapsulamento de pacotes e o ciclo de vida.
- Explicar com precisão ou uso comum dos procedimentos de nuvem, virtualização, armazenamento, backup e recuperação.
- Aplicar o conhecimento e as habilidades necessárias para planeiar, projectar, implementar, solucionar problemas e manter ambientes de infraestrutura de rede.

CYBERSECURITY ESSENTIALS

Pré-requisitos do curso: Cybersecurity Gateway

Visão geral do curso:

Este curso avalia os princípios de segurança cibernética e demonstra como proteger um ambiente de computação em rede através da aplicação de controles de segurança.

Os participantes aprenderão a natureza e o escopo dos desafios actuais de segurança cibernética, estratégias para defesa de rede, além de informações detalhadas sobre as soluções de próxima geração de segurança cibernética. Os alunos também implantarão uma variedade de metodologias de segurança, além de tecnologias e conceitos usados para implementar um ambiente de rede seguro.

Objectivos de aprendizagem:

Após a conclusão deste curso, os participantes serão capazes de:

- Formular um projecto padrão do sector para proteger a infraestrutura contra ameaças de segurança cibernética.
- Aplicar metodologias avançadas de filtragem, como usuário, aplicativo e ID do conteúdo, para proteger contra todos os vectores de ataque conhecidos e desconhecidos.
- Descrever o básico da criptografia, incluindo criptografia síncrona / assíncrona, PKI, e certificados.
- Demonstrar capacidade de avaliar e fortalecer *endpoints* com base em políticas de segurança.
- Descrever os usos de pesquisas e análises avançadas de *malware* para fornecer protecção aprimorada para redes empresariais.
- Examinar tecnologias de conexão móveis e baseadas na nuvem.