Implementing and Configuring Cisco Trustsec 2.0

Course Objective:

This Training covers topics relevant to TrustSec and will also include references to some new features recently made available on devices like the Cisco ASA. This Training helps in understanding how Cisco TrustSec differs from traditional methods for securing network access and also to understanding the benefits this brings to an organization from both a cost-effectiveness standpoint as well as meeting ease of use, centralized policy management, and compliance goals.

Major topics Covered in the Training are as follows:

- Understanding and Positioning Cisco TrustSec
- Cisco TrustSec Functions: Classification, Propagation, and Enforcement
- Implementing TrustSec using In-Line Tagging.
- Implementing TrustSec on Cisco ISE
- Implementing TrustSec on Wired and Wireless Devices
- Implementing Cisco TrustSec on Cisco Firewalls
- Implementing Cisco TrustSec with Cisco VPN Solutions
- TrustSec Deployment Considerations

Course Delivery and Duration

Delivery method can be Classroom and Online
Duration of Training: **5 Days**

Course Outline

1. **Understanding and Positioning Cisco TrustSec**

   - TrustSec Problem Space
   - TrustSec Versus Legacy Network Access
   - TrustSec Domains
   - TrustSec Functions

2. **Understanding TrustSec Functions – Classification**

   - Classification Fundamentals
   - Dynamic Classification
   - Static Classification Types and Methods
   - Static Classification Implementation

3. **Understanding TrustSec Functions – Propagation**

   - Inline Propagation
   - SXP Propagation
   - Propagation Using SGT Caching

4. **Understanding TrustSec Functions - Enforcement**

- Enforcement Characteristics and Security Group Tags
- Enforcement with Security Group ACLs
- IOS Switch Configuration for Enforcement
- Enforcement on Firewalls
- Enforcement Verification

5. **Implementing TrustSec on Cisco ISE**

- Creating TrustSec Domains using Switches and Routers
- Security Group Tags
- Building a policy matrix using SGACLS and Egress Policies

6. **Implementing TrustSec on Cisco Wired and Wireless Devices**

- Design Considerations for TrustSec on Cisco Wired/Wireless Devices
- Wired Classification
- Wired Propagation and Enforcement
- Extending TrustSec
- Wireless Networks
- Verifying Deployment

7. **Implementing Cisco TrustSec on Cisco Firewalls ASA and Firepower Services**

- Design Considerations
- Cisco Adaptive Security Appliance
- Cisco Zone-Based Firewall
- Configuring In-Line SGT using Firepower services

8. **Cisco ISE Integrated Solutions with Cisco Firepower Solutions**

- Introducing Cisco ISE 2.x pxGrid
- Configuring PxGrid with ISE and Firepower to propagate SGT 's and Context Data
- Create Access Control Policy on Firepower to filter traffic using SGT's.

9. **Implementing TrustSec with Cisco VPN Solutions**

- IKEv2 and IPsec VPNs
- DMVPN
- GETVPN
- AnyConnect VPNs

10. **TrustSec Deployment Considerations**

- Platform Guidelines
- SXP Design Guidelines
- Incorporating Non-TrustSec Devices
- User-to-Data Center Use Case