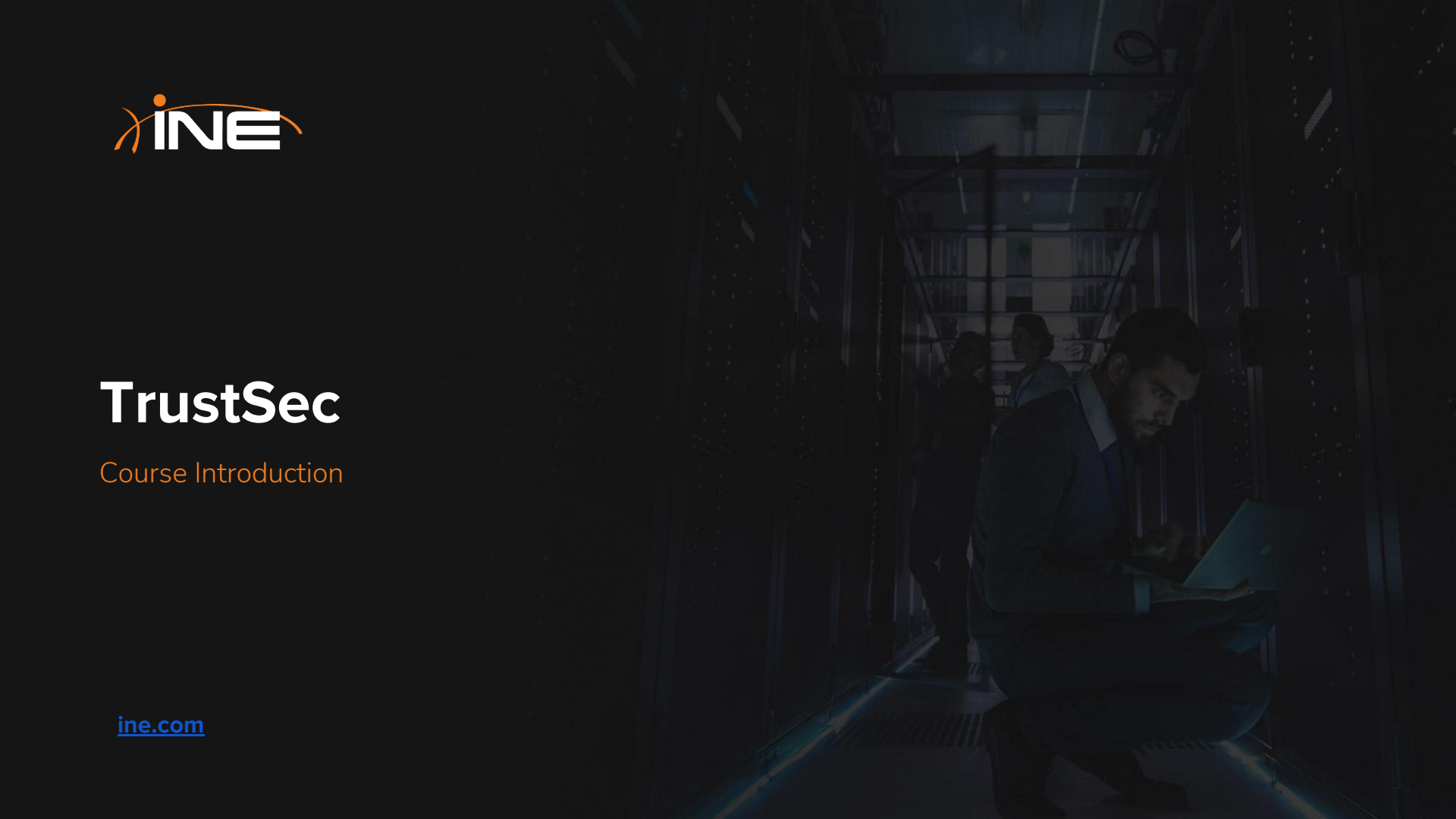


TrustSec

Course Introduction

ine.com

Piotr Kaluzny

CCIE #25665

pkaluzny@ine.com
linkedin.com/in/piotrkaluzny

CCIE Security

+ ISE GUI
+ Basic wireless concepts

Course Prerequisites

Course Overview

- Module 1 Introduction to TrustSec
- Module 2 Classification & SGT
- Module 3 Propagation & SXP
- Module 4 Enforcement & SGACL
- Module 5 TrustSec on IOS
- Module 6 TrustSec on ASA
- Module 7 TrustSec for Wireless Networks


INE

Introduction to TrustSec

Module Overview

- Traditional network segmentation
- Cisco TrustSec
- TrustSec operations

Traditional Network Segmentation

- Traditional access control relies on VLANs & ACLs
  - VLANs
    - Context-based allocation
      - User department/role, device function/type, etc.
    - Traffic filtering performed at the L3 edge
      - The more ACEs (sources x destinations x permissions), the more problems
  - Downloadable ACLs (dACLs)
    - Ingress enforcement after successful authentication
      - Single source, but possibly multiple destinations & permissions
      - May be problematic due to limited TCAM space
- Not scalable, increased complexity

Cisco TrustSec

- Next-generation segmentation for simplified access control
  - Controls are defined based on roles/context rather than IP addresses
    - Security Groups
      - E.g. Contractors, Employees-tablets or PCI-servers
  - Each Security Group is assigned a tag (label) for identification & filtering
    - Security Group Tag (SGT)
  - Filtering policy is defined through Security Group ACLs (SGACLs)
    - Source SGT, destination SGT, action & protocol
      - Contractors (10) -> PCI-servers (90) : deny ip log
    - The policy is scalable, “follows a user” and does not depend on the network topology
- Domain authentication (NDAC) & encryption (MACsec) is optional

TrustSec Operations

- Classification
  - Assignment of a SGT to a session or resource
    - Usually performed ingress
- Propagation
  - Distribution of IP-SGT mappings to enforcement points
- Enforcement
  - Application of configured (downloaded) policies
    - Usually performed egress

Campus LAN Use Case

- Classification
  - User connects to an access-layer switch & authenticates
    - 802.1x, MAB or WebAuth
  - Authorized session becomes associated with a SGT (ISE)
- Propagation
  - The SGT is propagated from the access layer up to the DC
- Enforcement
  - Egress DC switch enforces policy via SGACL downloaded from ISE
    - Destination servers are SGT-mapped statically

Classification & SGT

Module Overview

- TrustSec classification
- SGT

Security Group Tag (SGT)

- A 16-bit numerical value representing a Security Group
  - Session, device or session context

- SGT Considerations
  - The “Unknown” SGT corresponds to a numerical tag value 0
    - Represents untagged traffic
  - Traffic originated by a network device can be tagged as well
    - **Work Centers -> TrustSec -> TrustSec Policy -> Network Device Authorization**

- ISE comes with a bunch of preexisting SGTs

Classification

- A process of associating SGTs with sessions or devices
  - Dynamic or Static
- Dynamic Classification
  - A result of 802.1x/MAB/Web authentication (AuthZ Profile)
    - Users and/or endpoints
  - Via pxGrid or API calls
- Static Classification
  - IP address, subnet, VLAN or Port
    - IT infrastructure
  - Performed on ISE and/or NAD

Static Classification

- ISE
  - **Work Centers -> TrustSec -> Components -> IP SGT Static Mapping**
- IOS/ASA
  - **cts role-based sgt-map**
  - **show cts role-based sgt-map**

Propagation & SXP

Module Overview

- TrustSec propagation
- Inline Tagging
- SXP

Propagation

- A process of sharing SGT mappings with enforcement points
  - Inline (Native) Tagging
  - SGT Exchange Protocol (SXP)
  - pxGrid
    - FTD, WSA or ecosystem vendor product

- Most deployments combine Inline Tagging with SXP

Inline Tagging

- Allows to carry SGT information in modified data frames
  - On Ethernet, Cisco Meta Data (CMD) header follows Src MAC (or 802.1q) field
    - EtherType is set to 0x8909
  - The tag is maintained hop-by-hop allowing to enforce policies at any point
    - If packet is to be allowed the last-hop device removes the tag
  - Similar logic is used in supported Virtual Private Network environments
    - IKEv2 IPsec, DMVPN, GETVPN & VXLAN

- Pros & Cons
  - No performance degradation
  - Requires hardware support
    - TrustSec Platform Capability Matrix

Configuring Inline Tagging

- IOS/ASA
- Enable the manual CTS mode on an interface
  - **cts manual**
- Configure inline tagging
  - Make sure **propagate sgt** is on
  - **policy static sgt [trusted]**
- Verify
  - **show cts interface**

SGT Exchange Protocol (SXP)

- A Control Plane peering protocol used for SGT mapping propagation
  - Used for devices with no CTS hardware support
  - Runs over TCP port 64999
    - No need for hop-hop peerings
    - Uses MD5 for authentication & integrity checks (TCP Option 19)
      - BGP authentication considerations apply for cross-firewall peerings
  - A SXP peer can act as a Speaker (tx), Listener (rx), or both
  - Supported on network devices, ISE & OpenDaylight
    - Centralized peerings with ISE are common
      - Using a standalone node is recommended

Configuring SXP

- IOS/ASA
  - Enable SXP
    - **cts sxp enable**
  - Create password (optional)
    - **cts sxp default password**
  - Configure peering
    - **cts sxp connection peer**
  - Verify
    - **show cts sxp**

Configuring SXP

- ISE
  - Enable SXP on a node
    - **Administration -> System -> Deployment**
  - Configure SXP settings
    - **Work Centers -> TrustSec -> Settings -> SXP**
  - Add a peer
    - **Work Centers -> TrustSec -> SXP -> SXP Devices**

Enforcement & SGACL

Module Overview

- TrustSec enforcement
- SGACLs

Enforcement

- Cisco TrustSec (CTS) policies can be enforced using two methods
  - Security Group ACL (SGACL)
    - Centralized definition (ISE)
    - Stateless
  - Security Group Firewall (SGFW)
    - Supported on ASA, FTD & IOS ZFW
    - Local tag-based rules
      - Regular syntax
    - Stateful

Security Group ACL (SGACL)

- Stateless tag-based access control mechanism
  - CTS policy enforcement is represented as a spreadsheet (ISE Matrix View)
    - Source SGT to Destination SGT
  - Each SGT pair (“cell”) points to SGACL
    - Action, protocol, port, “log”
      - E.g. “permit icmp log” or “deny udp dst eq 3389”

- SGACLs are normally configured on ISE
  - The policy must be downloaded by NADs
  - Local configuration (e.g. ASR 1k) is less common
  - Monitor mode allows to test the deployment without blocking traffic

Configuring SGACLs

- ISE
  - **Work Centers -> TrustSec -> Components -> Security Group ACLs**
- ASR1k (only for your reference)
  - **ip access-list role-based**
  - **cts role-based permissions**

TrustSec on IOS

Module Overview

- CTS integration
- Configuration syntax

IOS CTS Integration

- CTS policy download requires NAD to enroll with ISE or a peer
- Relies on EAP-FAST
  - Phase 0 distributes a PAC (Protected Access Credential) after authentication
    Catalysts 3750X support automatic PAC provisioning

TrustSec IOS Configuration

- Switch
  - Start with regular 802.1x configuration (global)

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
radius server ISE
 address ipv4 10.1.1.100 auth-port 1812 acct-port 1813
aaa server radius dynamic-author
 client 10.1.1.100 server-key cisco
radius-server vsa send authentication
radius-server vsa send accounting
dot1x system-auth-control
```

TrustSec IOS Configuration

- Switch
  - Start with regular 802.1x configuration (interface)

```
interface GigabitEthernet1/0/1
 switchport mode access
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication host-mode multi-auth
 mab
 dot1x pae authenticator
```

TrustSec IOS Configuration

- Switch
  - Configure CTS settings
    - Specify which server stores the CTS policy
      - **aaa authorization network *name* group [radius | *gname*]**
      - **cts authorization list *name***
    - Configure CTS device-ID & password
      - **cts credentials id**
    - Add Radius PAC key
      - **pac key**
    - Enforce downloaded policies
      - **cts role-based enforcement**, **cts role-based enforcement vlan-list**
    - Verify
      - **show cts pac**, **show cts environment-data**, **show cts role-based**

TrustSec IOS Configuration

- Switch (3750-X)
  - Enable Device Tracking globally AND at the interface level
    - **ip device tracking** (global), **ip device tracking maximum** (interface)
      - For the policy to be enforced, entries must exist for sources & destinations
- ISE
  - Configure TrustSec settings on NADs
    - **Advanced TrustSec Settings**
  - Other TrustSec configuration, such as SXP, may be needed
- TrustSec Troubleshooting Guide
  - https://community.cisco.com/t5/security-documents/trustsec-troubleshooting-guide/ta-p/3647576#toc-hId-1418373399

TrustSec on ASA

Module Overview

- CTS integration
- Configuration syntax

ASA CTS Integration

- ASA requires manual PAC provisioning
  - PAC is generated on ISE and downloaded OOB
    - **cts import-pac**

- ASA cannot use or download SGACLs
  - Only part of environment data is downloaded
    - SGTs & Security Group names

TrustSec ASA Configuration

- ISE
  - Configure TrustSec settings on NADs (**Advanced TrustSec Settings**)
- ASA
  - Configure ISE server
    - **aaa-server *name* protocol radius**
    - **aaa-server *name (interface)* host *ISE_IP***
      - **key *password***
  - Import PAC & designate server for CTS
    - **cts import-pac, cts server-group *name***
    - Verify with **show cts environment-data sg-table**
  - Configure SXP & security policy

TrustSec for Wireless Networks

Module Overview

- GUI configuration

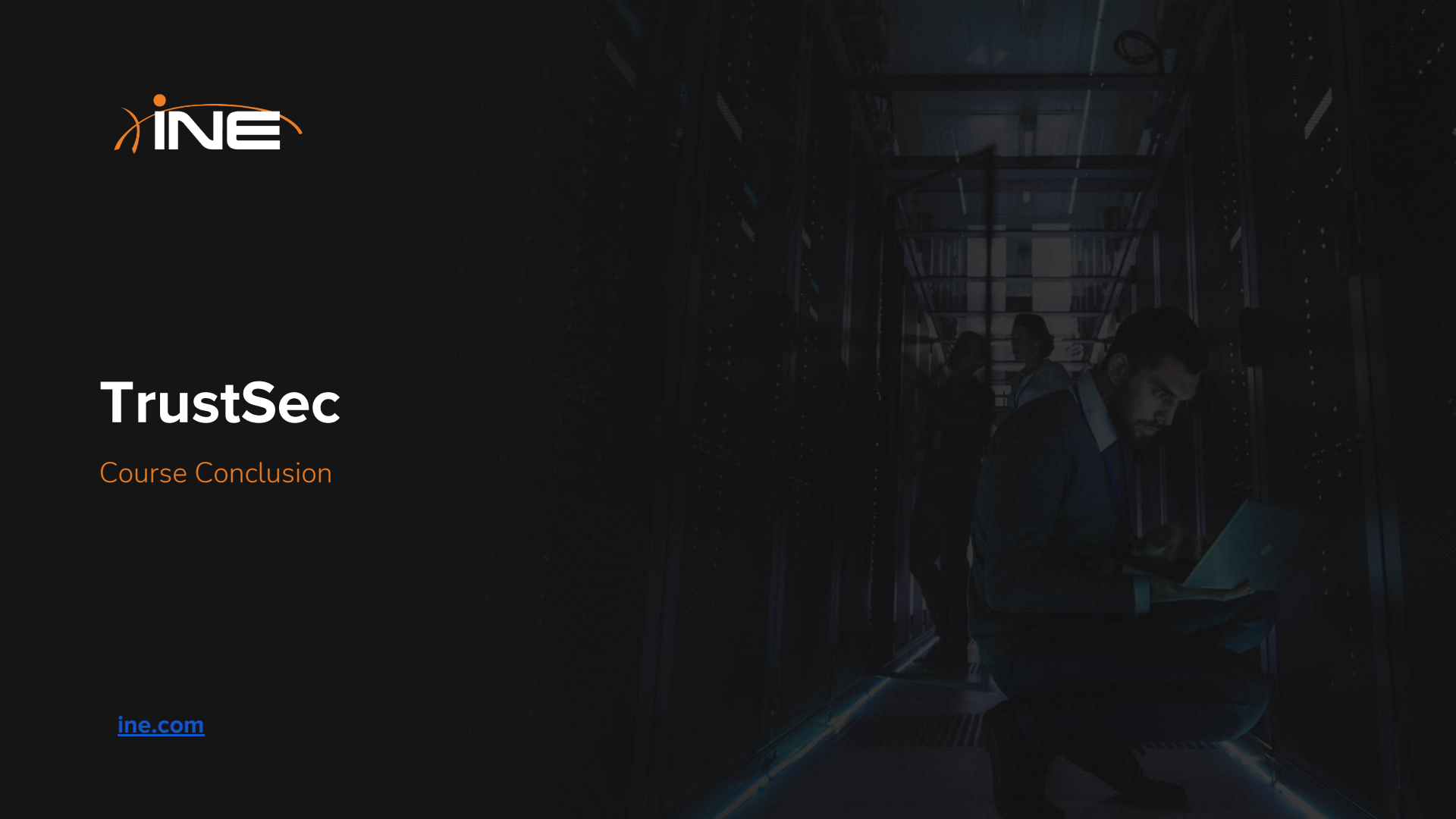
TrustSec WLC Configuration

- WLC
  - Enable PAC provisioning for the RADIUS server
    - **Security -> AAA -> RADIUS -> Authentication**
  - Integrate with ISE for CTS
    - **Security -> TrustSec -> General**
      - **Refresh Env Data**
  - Configure WLAN AAA settings
    - **Advanced -> Allow AAA Override**
    - **Advanced -> NAC State -> ISE NAC**
  - Verify the CTS policy
    - **Security -> TrustSec -> Policy**

TrustSec WLC Configuration

- WLC
  - SXP Configuration
    - **Security -> TrustSec -> SXP Config**
    - FlexConnect Mode
      - **Wireless -> Access Points -> All APs -> Trusted Security**

- ISE
  - Configure TrustSec settings on NADs
    - **Advanced TrustSec Settings**



TrustSec

Course Conclusion

ine.com

Course Conclusion

- Traditional network segmentation might not be scalable
- Classification associates a SGT with a resource
- Propagation distributes IP-SGT mappings to policy nodes
- Enforcement is typically performed with the aid of SGACLs
- Implementation details depend on the underlying platform

Thank You


INE