Splunk4Admins

Encryption of Data in Transit
(DIT)

splunk>
a CISCO company

Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words “will,” “believes,” “plans,” “anticipates,” “expects,” “estimates,” “strives,” “goal,” “intends,” “may,” “endeavors,” “continues,” “projects,” “seeks,” or “targets,” or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management’s beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management’s control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk’s and Cisco’s complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco’s current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk’s market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco’s ability to implement its plans, forecasts and other expectations with respect to Splunk’s business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk>

REGISTRATION 5 MINS

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet: https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event: https://show.splunk.com/event/<eventID>
3. Download the hands-on lab guide: https://splk.it/S4A-DIT-Lab-Guide

   Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck: https://splk.it/S4A-DIT-Attendee

Goal

Enroll in today's event

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

Workshop Agenda

- Discuss Who?|What?|Why?
- Install Splunk Securely on Linux - Lab 1
- Obtain Certificates - Lab 2
- Prepare TLS certificates for use with the Splunk platform - Lab 3
- Configuring Splunk Indexing and forwarding using TLS certificates - Lab 4
- Configuring Splunk web to use TLS - Lab 5
- Configuring Splunkd to use TLS - Lab 6
- Appendix

Audience

Who is this Workshop for?

- Those who are interested in how to observe and detect issues within Splunk …
  - Splunk Admins
  - “Required”: Power User Certified
  - “Preferred”: Splunk Admin enabled (at least started …), Certified
- To be successful you should have knowledge of the following concepts
  - OpenSSL
  - Certificate Management
  - CLI, VI, Linux OS
  - Principle of Least Privilege
  - Zero Trust Architecture

Expectations for Workshop

- Last roughly 75-90 minutes
- Securely install Splunk Enterprise on Linux
- Experience creating self-signed certificates and prepping them for use with Splunk Enterprise
- Configure Splunk to use TLS for:
  - Forwarder to Indexer
  - SplunkWeb
  - Splunkd

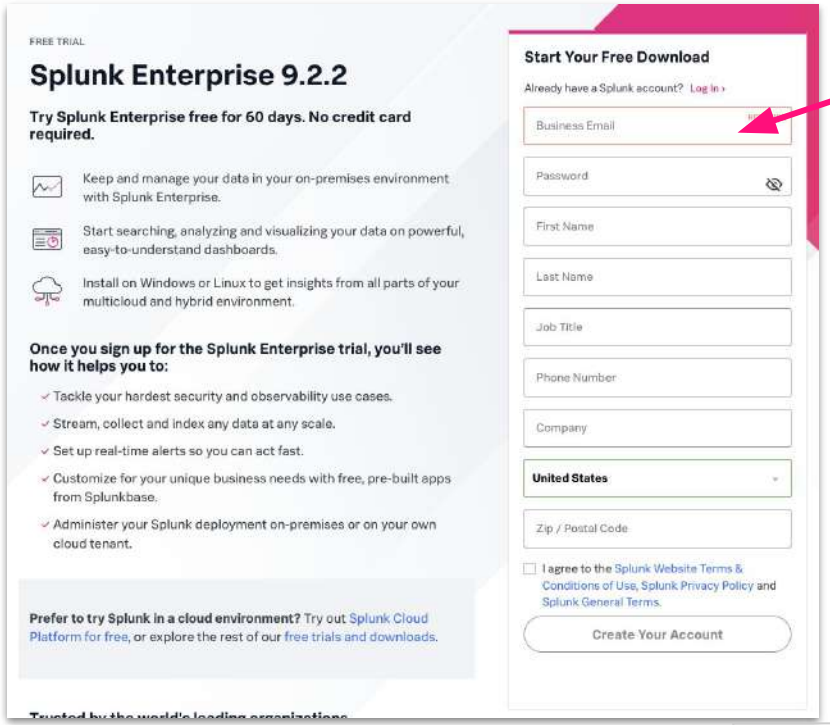
Workshop Agenda

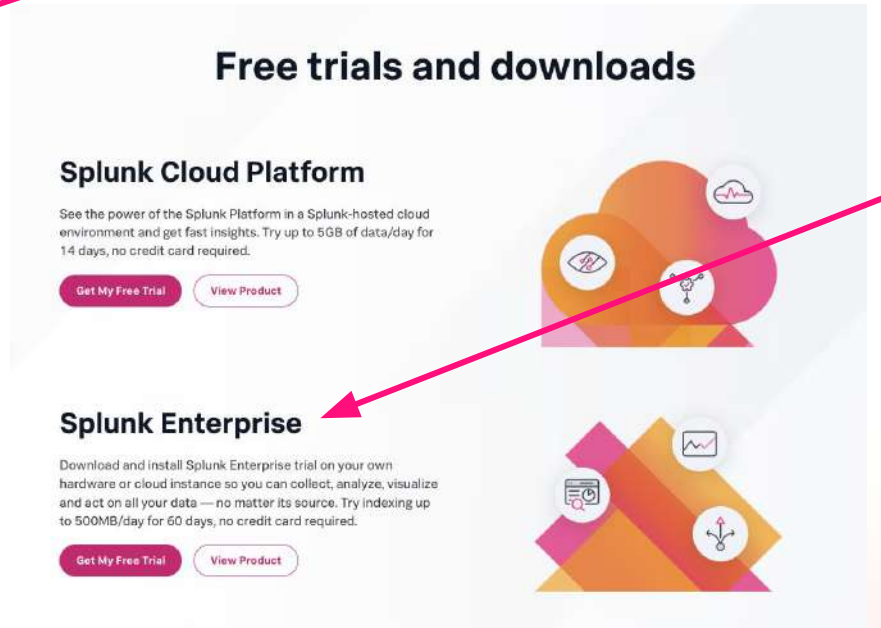
- Discuss Who?|What?|Why?
- Install Splunk Securely on Linux - Lab 1
- Obtain Certificates - Lab 2
- Prepare TLS certificates for use with the Splunk platform - Lab 3
- Configuring Splunk Indexing and forwarding using TLS certificates - Lab 4
- Configuring Splunk web to use TLS - Lab 5
- Configuring Splunkd to use TLS - Lab 6
- Appendix

Install Splunk Securely on Linux

Navigate to the downloads page

From here, you will either want to create a new account on login using your existing account



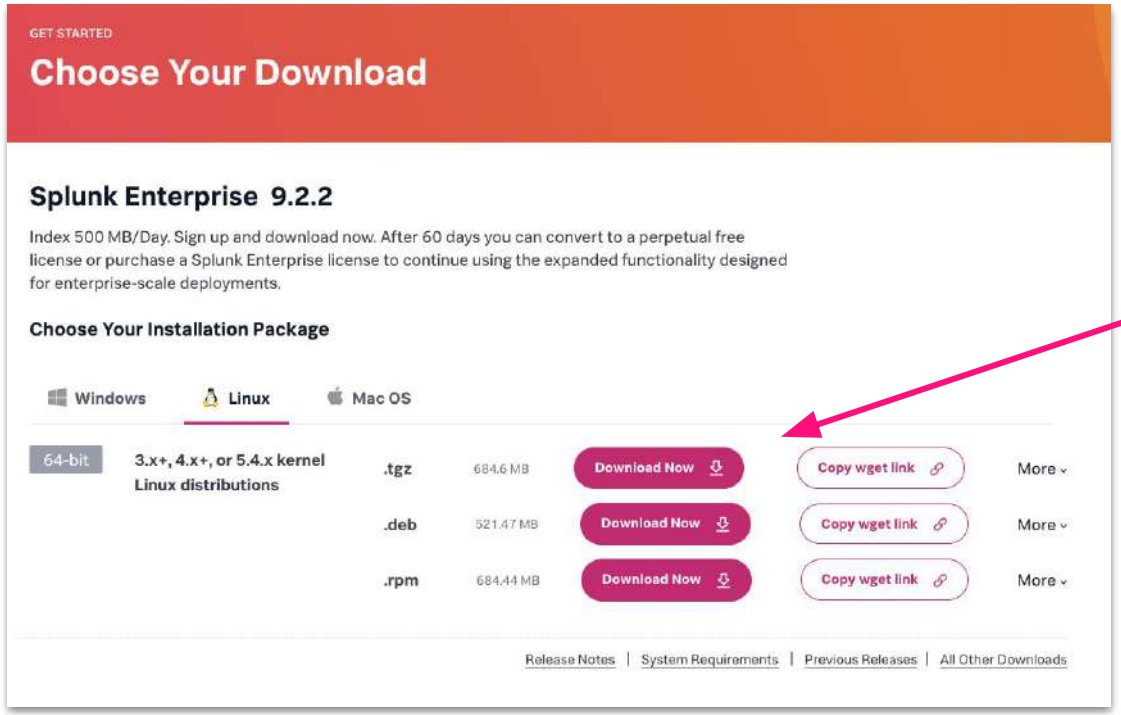


Downloads	Choose Your Download

Install Splunk Securely on Linux

Choose your download

For the purpose of this course, choose the most recent release of the tgz for Linux



Downloads	Choose Your Download

Install Splunk Securely on Linux

Download and Verify Checksum

Select the link to download the MD5 to verify your bits


```
root@ip-172-31-67-43:/tmp# md5sum splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
da10ab0199358aa96b3a29420a9d5f4b  splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz
root@ip-172-31-67-43:/tmp# cat splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz.md5
MD5(splunk-9.2.2-d76edf6f0a15-Linux-x86_64.tgz)= da10ab0199358aa96b3a29420a9d5f4
```

Securing Splunk	https://docs.splunk.com/Documentation/Splunk/latest/Security/InstallSplunksecurely

Install Splunk Securely on Linux

Install Splunk Enterprise

- Please see the Installation instructions in the Installation Manual, for the purposes of this workshop, use the /opt/showlab directory to install Splunk.
- **DO NOT START SPLUNK**

Installation Manual	https://docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform

Install Splunk Securely on Linux

Create Secure Admin Credentials

- Use user-seed.conf to create secure administrative credentials
  - Create the /opt/showlab/s4a-aio/splunk/etc/system/local/user-seed.conf file
  - Start Splunk Enterprise

```
[user_info]
USERNAME = admin
PASSWORD = <your password>
```

Create secure credentials	https://docs.splunk.com/Documentation/Splunk/latest/Security/Secureyouradminaccount

Workshop Agenda

- Discuss Who?|What?|Why?
- Install Splunk Securely on Linux - Lab 1
- Obtain Certificates - Lab 2
- Prepare TLS certificates for use with the Splunk platform - Lab 3
- Configuring Splunk Indexing and forwarding using TLS certificates - Lab 4
- Configuring Splunk web to use TLS - Lab 5
- Configuring Splunkd to use TLS - Lab 6
- Appendix

Obtain Certificates

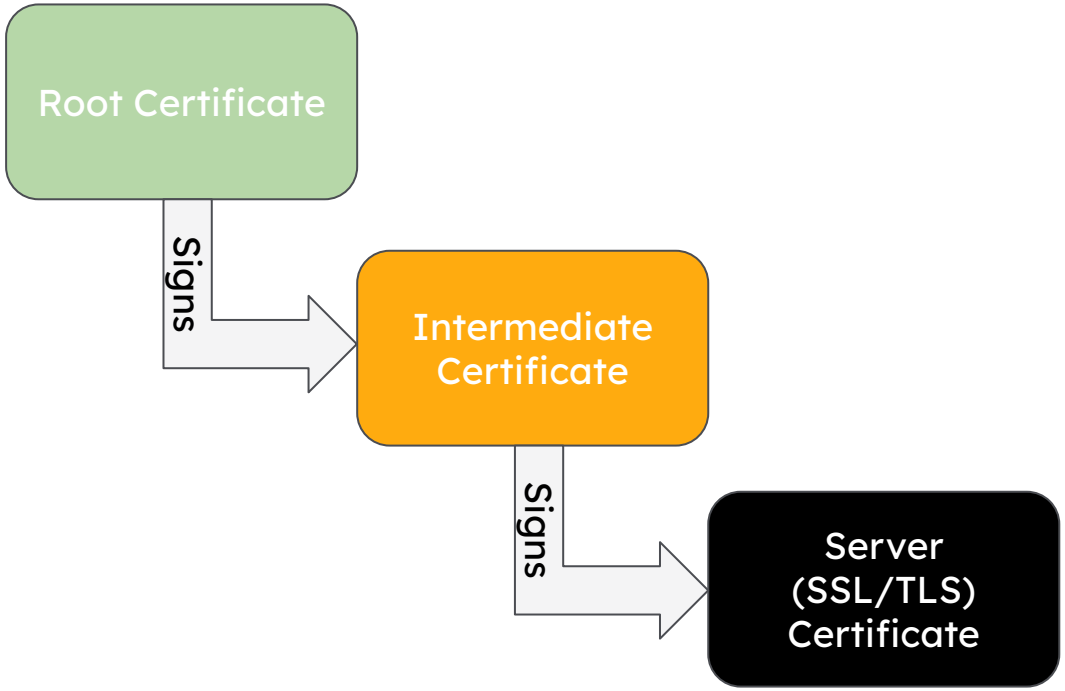
Decide how you want to secure your Splunk platform deployment

- You will secure the following ports using self-signed certs:
  - Web port
  - Splunk2splunk port
  - Management port

Installation Manual	https://docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform

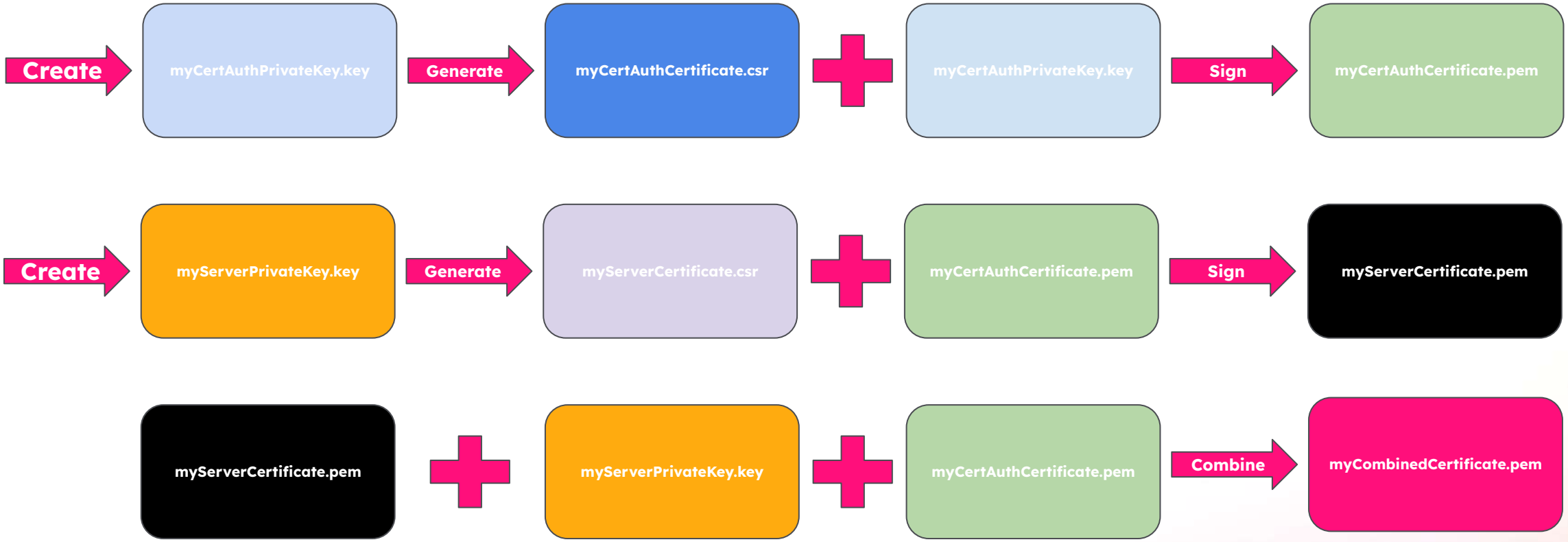
Certificate Chain

What is a certificate chain and how does it work?



Certificate Chain

Understanding the parts of the Certificate Chain



Obtain Certificates

Obtain the TLS certificates you need to secure the deployment

- Create the root certificate authority certificate
  - Open a command line interface, such as shell prompt or Terminal
  - Connect to the Splunk lab instance where you will generate the certificate signing request (CSR)
  - Create a new directory within the Splunk platform instance installation for the certificates
  - Create a private key for your root certificate authority certificate

Secure Splunk with TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/StepstosecuringSplunkwithTLS
Create and self-sign a TLS certificate	https://docs.splunk.com/Documentation/Splunk/latest/Security/Howtoself-signcertificates#Create_and_self-sign_a_TLS_certificate

Obtain Certificates

Create the root certificate authority certificate

- When the OpenSSL program prompts you, enter a password for the key.
- Use the private key to generate a CSR for your certificate.
- Enter the password you created for your private key.
- You will be prompted to fill in values for the new CSR file:
  - Country Name
  - State or Province Name (full name)
  - Locality Name (eg, city)
  - Organization Name (eg, company)
  - Organizational Unit Name (eg, section)
  - Common Name (e.g. server FQDN or YOUR name)
  - Email Address

Secure Splunk with TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/StepstosecuringSplunkwithTLS
Create and self-sign a TLS certificate	https://docs.splunk.com/Documentation/Splunk/latest/Security/Howtoself-signcertificates#Create_and_self-sign_a_TLS_certificate

Obtain Certificates

Create the root certificate authority certificate cont.

- After you enter the information the OpenSSL program creates a new CSR file
- Use the CSR file you created and sign it with the private key you created previously to create the root certificate authority certificate
- When prompted, enter the password you created for your private key
  - A root certificate authority certificate file will then be created

Secure Splunk with TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/StepstosecuringSplunkwithTLS
Create and self-sign a TLS certificate	https://docs.splunk.com/Documentation/Splunk/latest/Security/Howtoself-signcertificates#Create_and_self-sign_a_TLS_certificate

Obtain Certificates

Create server certificates and sign them with the root certificate authority certificate

- Create a private key for the server certificate
- When prompted, enter a password for the key
  - The OpenSSL program then creates a private key file
- Use the private key to generate a CSR for your certificate
- When the OpenSSL program prompts you, enter the password you created for the private key
- Provide the requested information for your certificate
  - The OpenSSL program creates a new CSR file
- Use the CSR file you created and sign it with the private key you created previously, the certificate authority certificate, and its private key to create the server certificate
- When prompted, enter the password you created for the private key
  - The OpenSSL program creates the server certificate file

Secure Splunk with TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/StepstosecuringSplunkwithTLS
Create a server cert	https://docs.splunk.com/Documentation/Splunk/latest/Security/Howtoself-signcertificates#Create_server_certificates_and_sign_them_with_the_root_certificate_authority_certificate

Obtain Certificates

Next Steps...

Now that you have the certificate authority certificate and at least one server certificate, we will prepare the certificate(s) for use on the Splunk platform, including concatenating any intermediate certificates in the next lab.

Secure Splunk with TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/StepstosecuringSplunkwithTLS
Create a server cert	https://docs.splunk.com/Documentation/Splunk/latest/Security/Howtoself-signcertificates#Create_server_certificates_and_sign_them_with_the_root_certificate_authority_certificate

Workshop Agenda

- Discuss Who?|What?|Why?
- Install Splunk Securely on Linux - Lab 1
- Obtain Certificates - Lab 2
- Prepare TLS certificates for use with the Splunk platform - Lab 3
- Configuring Splunk Indexing and forwarding using TLS certificates - Lab 4
- Configuring Splunk web to use TLS - Lab 5
- Configuring Splunkd to use TLS - Lab 6
- Appendix

Prepare TLS certificates for use with the Splunk platform

Create a single combined certificate file

- Create a combined certificate file in pem format in the following order:
  - The server certificate
  - The private key
  - The certificate authority certificate

```
cat myServerCertificate.pem myServerPrivateKey.key myCertAuthCertificate.pem >
myCombinedCertificate.pem
```

Prepare TLS Certificates	https://docs.splunk.com/Documentation/Splunk/latest/Security/HowtoprepareyoursignedcertificatesforSplunk

Workshop Agenda

- Discuss Who?|What?|Why?
- Install Splunk Securely on Linux - Lab 1
- Obtain Certificates - Lab 2
- Prepare TLS certificates for use with the Splunk platform - Lab 3
- Configuring Splunk Indexing and forwarding using TLS certificates - Lab 4
- Configuring Splunk web to use TLS - Lab 5
- Configuring Splunkd to use TLS - Lab 6
- Appendix

Configuring Splunk indexing and forwarding using TLS certificates

Create a base app

- Create a new base app named all_indexer_base with all relevant configs and directories as indicated in the lab manual
  - Ensure that inputs.conf and server.conf are configured correctly to enable S2S SSL

inputs.conf

```
# BASE SETTINGS
[splunktcp-ssl://9997]

# SSL SETTINGS
[SSL]
serverCert = /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCombinedCertificate.pem
sslPassword = myCertificatePassword
# requireClientCert = true
sslVersions = *,-ssl2
# sslCommonNameToCheck = aio.mydomain.com
```

server.conf

```
[sslConfig]
sslRootCAPath = /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCertAuthCertificate.pem
```

Configure Splunk indexing and forwarding	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureSplunkforwardingtousesignedcertificates

Configuring Splunk indexing and forwarding using TLS certificates

Configure Universal Forwarder

- Navigate to the UF installation under the showlab directory and copy the indicated certificates to the newly created mycerts directory

```
cp /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCertAuthCertificate.pem
/opt/showlab/s4a-s-aio/splunkforwarder/etc/auth/mycerts/
cp /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCombinedCertificate.pem
/opt/showlab/s4a-s-aio/splunkforwarder/etc/auth/mycerts/
mv myCombinedCertificate.pem myClientCertificate.pem
```

- Create all_forwarder_outputs base app and all relevant configs and directories as indicated in the lab manual
  - Ensure that outputs.conf and server.conf are configured correctly to enable S2S SSL

Configure Splunk indexing and forwarding	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureSplunkforwardingtousesignedcertificates
Troubleshooting TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/Validateyourconfiguration

Configuring Splunk indexing and forwarding using TLS certificates

Configure Universal Forwarder cont.

outputs.conf

```
# BASE SETTINGS

[tcpout]
defaultGroup = primary_indexer
forceTimebasedAutoLB = true
forwardedindex.0.whitelist = (_audit|_introspection|_internal)

[tcpout:primary_indexer]
server = localhost:9997
disabled = 0
clientCert =
/opt/showlab/s4a-s-aio/splunkforwarder/etc/auth/mycerts/myClientCertificate.pem
useClientSSLCompression = true
sslPassword = myCertificatePassword
# sslCommonNameToCheck = aio.mycompany.com
# sslVerifyServerCert = true
```

server.conf

```
[sslConfig]
sslRootCAPath =
/opt/showlab/s4a-s-aio/splunkforwarder/etc/auth/mycerts/myCertAuthCertificate.pem
```

Configure Splunk indexing and forwarding	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureSplunkforwardingtousesignedcertificates
Troubleshooting TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/Validateyourconfiguration

Workshop Agenda

- Discuss Who?|What?|Why?
- Install Splunk Securely on Linux - Lab 1
- Obtain Certificates - Lab 2
- Prepare TLS certificates for use with the Splunk platform - Lab 3
- Configuring Splunk Indexing and forwarding using TLS certificates - Lab 4
- Configuring Splunk web to use TLS - Lab 5
- Configuring Splunkd to use TLS - Lab 6
- Appendix

Configuring Splunk Web to use TLS

Create web certificates

- Use openssl command to remove the password from the server private key and save it as the web certificate
- Make a copy of the combined certificates we have already created and update the name

```
cp myServerPrivateKey.key mySplunkWebPrivateKey.key
openssl rsa -in myServerPrivateKey.key -out mySplunkWebPrivateKey.key
```

Configure Splunk Web SSL	https://docs.splunk.com/Documentation/Splunk/latest/Security/SecureSplunkWebusingasignedcertificate

Configuring Splunk Web to use TLS

Create a web base app

- Create a new base app named all_search_base with all relevant configs and directories as indicated in the lab manual
  - Ensure that web.conf is configured correctly to enable Web SSL

web.conf

```
[settings]
httpport = 8443
enableSplunkWebSSL = true
privKeyPath = /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/mySplunkWebPrivateKey.key
serverCert = /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/mySplunkWebCertificate.pem
```

Configure Splunk Web SSL	https://docs.splunk.com/Documentation/Splunk/latest/Security/SecureSplunkWebusingasignedcertificate
Troubleshooting TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/Validateyourconfiguration

Workshop Agenda

- Discuss Who?|What?|Why?
- Install Splunk Securely on Linux - Lab 1
- Obtain Certificates - Lab 2
- Prepare TLS certificates for use with the Splunk platform - Lab 3
- Configuring Splunk Indexing and forwarding using TLS certificates - Lab 4
- Configuring Splunk web to use TLS - Lab 5
- Configuring Splunkd to use TLS - Lab 6
- Appendix

Configuring Splunkd to use TLS

Update server.conf on AIO instance

- Update the existing server.conf file in the all_indexer_base app
- Remove entry for sslConfig stanza in $SPLUNK_HOME/etc/system/local
- Restart Splunk

…/all_indexer_base/local/server.conf

```
[sslConfig]
enableSplunkdSSL = true
sslRootCAPath = /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCertAuthCertificate.pem
serverCert = /opt/showlab/s4a-s-aio/splunk/etc/auth/mycerts/myCombinedCertificate.pem
sslPassword = myCertificatePassword
# requireClientCert = true
sslVersions = *,-ssl2
# sslCommonNameToCheck = aio.mydomain.com
```

$SPLUNK_HOME/etc/system/local/server.conf

```
#[sslConfig]
#sslPassword = $7$oE9ikOJjA9cnEaOfw+NaLbzufl3TqLyigBHfwWYpYgm8hhziWqx9fg==
```

Configuring Splunkd to use TLS

Connect the UF to the AIO

- Copy the required certificates to a new directory on the UF deployment
- Copy the all_deploymentclient app from the UF apps directory to the deployment-apps directory on the AIO instance
- Create a server.conf file for the UF in the all_deploymentclient app's local directory
- Remove entry for sslConfig stanza in /system/local of UF directory
- Restart splunk

$SPLUNK_HOME/etc/deployment-apps.all_deploymentclient/local/server.conf

```
[sslConfig]
enableSplunkdSSL = true
sslRootCAPath =
/opt/showlab/s4a-s-uf/splunkforwarder/etc/auth/mycerts/myCertAuthCertificate.pem
serverCert =
/opt/showlab/s4a-s-uf/splunkforwarder/etc/auth/mycerts/myCombinedCertificate.pem
sslPassword = myCertificatePassword
# requireClientCert = true
sslVersions = *,-ssl2
# sslCommonNameToCheck = aio.mydomain.com
```

$SPLUNK_HOME/etc/system/local/server.conf

```
#[sslConfig]
#sslPassword = $7$oE9ikOJjA9cnEaOfw+NaLbzuf13TqLyigBHfwWYpYgm8hhziWqx9fg==
```

Configure Splunk inter-splunk TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigTLSCertsS2S
Troubleshooting TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/Validateyourconfiguration

Summary

Splunk Encryption of Data in Transit

- Installed Splunk Securely
- Obtained and Managed Certificates
- Prepared Certificates for Deployment
- Configured Secure Indexing & Forwarding
- Secured Splunk Web
- Enabled SSL for Splunkd

Workshop Agenda

- Discuss Who?|What?|Why?
- Install Splunk Securely on Linux - Lab 1
- Obtain Certificates - Lab 2
- Prepare TLS certificates for use with the Splunk platform - Lab 3
- Configuring Splunk Indexing and forwarding using TLS certificates - Lab 4
- Configuring Splunk web to use TLS - Lab 5
- Configuring Splunkd to use TLS - Lab 6
- Appendix

Certificates and Configs

What services need certificates for secure communication?

Service	Default Port(s)	Certificate(s) Needed	Configuration File	Configuration Stanza
Splunk Web	8000	web_privkey.key web_cert.pem cacert.pem	web.conf	[settings] httpport = enableSplunkWebSSL = true privKeyPath = serverCert =
Splunkd	8089	cacert.pem + server.pem + privkey.key ->
CombinedCert.pem	server.conf	[sslConfig] enableSplunkdSSL = true sslRootCAPath = serverCert = sslPassword = sslVersions =
Replication	8191 (SHC) 9887 (IDXC)	cacert.pem server.pem	server.conf	[replication_port-ssl://9887] rootCA = serverCert = sslPassword =

Certificates and Configs

What services need certificates for secure communication?

Service	Default Port	Certificate(s) Needed	Configuration File	Configuration Stanza
KV Store	8191	cacert.pem server.pem	server.conf	[kvstore] caCertFile = serverCert = sslPassword =
HTTP Event Collector (HEC)	8088	server.pem privkey.key cacert.pem	inputs.conf	[http] enableSSL = true serverCert = privKeyPath = caCertFile =

Certificates and Configs

What services need certificates for secure communication?

Service	Default Port	Certificate(s) Needed	Configuration File	Configuration Stanza
Forwarding (Forwarder)	9997	server.pem	outputs.conf	[tcpout:<output_group>] server = disabled = 0 clientCert = useClientSSLCompression = true sslPassword =
Forwarding (Forwarder & Data Receivers)	9997	cacert.pem	server.conf	[sslConfig] sslRootCAPath =
Forwarding (Data Receivers)	9997	cacert.pem + server.pem + privkey.key -> CombinedCert.pem	inputs.conf	[splunktcp-ssl://9997] [SSL] serverCert = sslPassword =

Certificate Management

Are there apps out there that can help?

App	Link	Description
SSL Certificate expiry collection	https://apps.splunk.com/app/6475/	This Certificates Expiry Add-on for Splunk allows a Splunk® Enterprise or Splunk Cloud administrator to collect data from hostnames or FQDN. The add-on collects the certificate and records details from the certificate to a splunk index.
SSL Certificate Checker	https://splunkbase.splunk.com/app/3172	The SSL Certificate Checker Technology Add-on contains scripts and inputs designed to index the expiration date and name of the SSL certificates you want to monitor. From there you can setup a dashboard/report/alert to monitor when your SSL certificates are about to expire.
SSL Certificate Lookup	https://splunkbase.splunk.com/app/4580	Provides sslcert_lookup, an external lookup that when given an IP or domain (works with SNI) and optionally port from an existing search, can give enrich the search by finding values from an SSL certificate like CN , SAN (Subject Alternative Names), and expiration.

Links (In order of appearance)

Install Splunk Enterprise securely	https://docs.splunk.com/Documentation/Splunk/latest/Security/InstallSplunksecurely
Create secure administrator credentials	https://docs.splunk.com/Documentation/Splunk/latest/Security/Secureyouradminaccount
About TLS encryption and cipher suites	https://docs.splunk.com/Documentation/Splunk/latest/Security/AboutTLSencryptionandciphersuites
Secure Splunk Enterprise with FIPS	https://docs.splunk.com/Documentation/Splunk/latest/Security/SecuringSplunkEnterprisewithFIPS
Harden the Splunk Enterprise installation directory on Windows	https://docs.splunk.com/Documentation/Splunk/latest/Security/HardenyourWindowsinstallation
Secure Splunk Enterprise on your network	https://docs.splunk.com/Documentation/Splunk/latest/Security/SecureSplunkonyournetwork
Disable unnecessary Splunk Enterprise components	https://docs.splunk.com/Documentation/Splunk/latest/Security/DisableunnecessarySplunkcomponents
Secure Splunk Enterprise service accounts	https://docs.splunk.com/Documentation/Splunk/latest/Security/Secureyourserviceaccounts
Deploy secure passwords across multiple servers	https://docs.splunk.com/Documentation/Splunk/latest/Security/Deploysecurepasswordsacrossmultipleservers
Introduction to securing the Splunk platform with TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/AboutsecuringyourSplunkconfigurationwithSSL
Steps for securing your Splunk Enterprise deployment with TLS	https://docs.splunk.com/Documentation/Splunk/latest/Security/StepstosecuringSplunkwithTLS
How to obtain certificates from a third-party for inter-Splunk communication	https://docs.splunk.com/Documentation/Splunk/latest/Security/Howtogetthird-partycertificates
How to obtain certificates from a third-party for Splunk Web	https://docs.splunk.com/Documentation/Splunk/latest/Security/Getthird-partycertificatesforSplunkWeb
How to create and sign your own TLS certificates	https://docs.splunk.com/Documentation/Splunk/latest/Security/Howtoself-signcertificates
How to prepare TLS certificates for use with the Splunk platform	https://docs.splunk.com/Documentation/Splunk/latest/Security/HowtoprepareyoursignedcertificatesforSplunk
Configure Splunk indexing and forwarding to use TLS certificates	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureSplunkforwardingtousesignedcertificates
Configure TLS certificates for inter-Splunk communication	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigTLSCertsS2S
Configure Splunk Web to use TLS certificates	https://docs.splunk.com/Documentation/Splunk/latest/Security/SecureSplunkWebusingasignedcertificate
Test and troubleshoot TLS connections	https://docs.splunk.com/Documentation/Splunk/latest/Security/Validateyourconfiguration

Thank you

splunk> a CISCO company