



# Hackers Uninvited Guests

James Johnson - Tridium



#### Objectives

- Why should you care about security?
- Best practices for hardening a Niagara application

- Security Service and Dashboard
- PKI certificates
- Code signing



#### Why Should You Care?

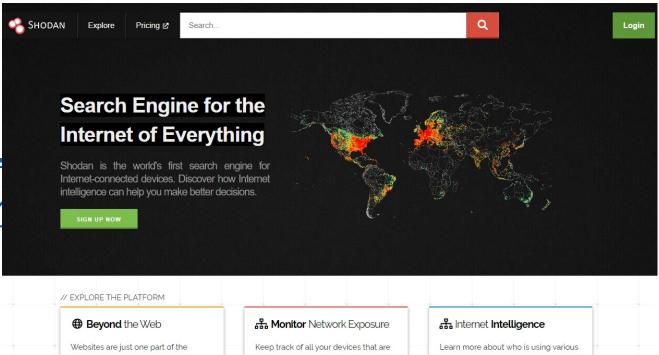






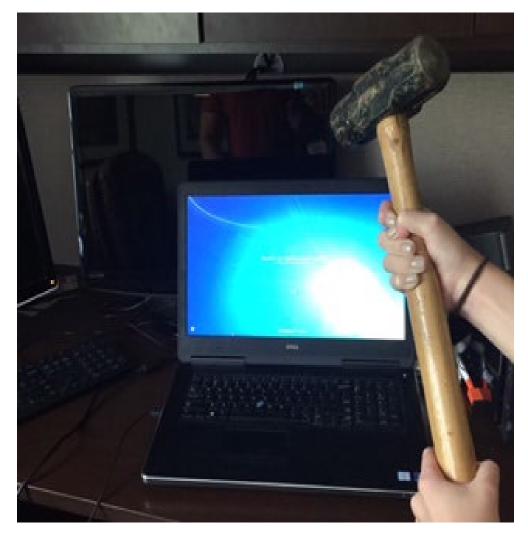
# IoT Search Engines

- <u>https://www.shodan.io</u>
- <u>https://censys.io</u>
- <u>https://www.punkspider.</u>
- <u>https://www.zoomeye.or</u>
- <u>https://ivre.rocks</u>





#### **People Forget Physical Security**



- Many successful cyber attacks begin with a physical attack.
- Malware can be introduced through USB devices.





#### Protect Against Ransomware

- Use anti-virus software.
- Perform periodic scheduled backups.
- Treat systems as missioncritical infrastructure, which means it shouldn't be used for surfing the web or checking email.





#### Patch Management is Critical

- Many organizations provide services internationally, reporting vulnerabilities in hardware and software.
- Advisories may affect millions of devices.
- Vendors release security patches and updates.
- An unpatched system on your network may be an attacker's avenue https://www.cisa.gov/



CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/

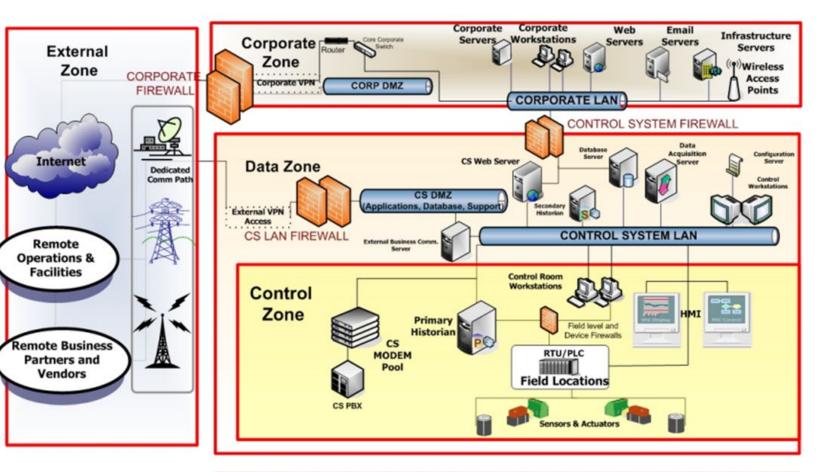
https://www.cisa.gov/uscert/ics



# Network Defense In Depth

Recommended Practice: Improving Industrial Control Cybersecurity with Defense-In-Depth Strategies

DHS, ICS-CERT 2009



Safety Zone





## Good Behavior Through Technology

- Secure by Default
  - Forcing default credential changes upon commissioning
  - Strongest authentication mechanisms
  - Enforcement of strong passwords
  - Encrypted communications
- Encryption of sensitive information at rest
- Digitally signed code validated for integrity at run time
- Secure Boot





#### Flexible Authentication Schemes

- Lightweight Directory Access Protocol (LDAP) and Active Directory (AD) – integrates to existing directory information services.
- Security Assertion Markup Language (SAML) works with popular on premise and cloud Identity Providers
- Client Certificate utilizes PKI certificate authentication
- Google provides two factor authentication using the Google Authenticator app



#### IEEE 802.1X

- Port-based Network Access Control (PNAC)
- Provides authentication mechanism to devices wishing to attach to a network
- Available for JACE-8 and Niagara Edge controllers with Niagara 4.8 or newer version.





#### What are your assets and risks?

 Understand your organization's appetite for risk and determine a risk threshold using a CVSS score.

- Identify electronic assets to protect and document security requirements.
- Engage an independent team to a threats and potential vulnerabilities you network and assets.
- Perform a periodic assessment becassets and requirements change over time.



#### Security Service and Dashboard

- Security Service provides a dashboard view to help assess the security posture of a Niagara application.
- Available in Niagara 4.8 for Supervisor, JACE and Edge controller stations.

🕛 nss

Ŧ

TRIDIUN

 $\odot$ 

Q

🝷 🧐 Palette Optional certificate expiry alarm D





#### Security Dashboard – System View

(i) Info 11

- Scores the station and all Niagara network devices.
- Tiles show details for individual devices.
- Hyperlink to more detailed information.

r	256 TOTAL FEATURES	⊘ C Hide	)K 192	i Info Hide	64	
	Bldg1F1	Only validly signed program objects can be executed.	$\odot$	<u>Bldg1F2</u>	$\oslash$	Only validly signed program objects can be executed.
•	C Refreshed a few seconds ago	<ul> <li>I55 modules are validly signed.</li> <li>No modules have additional permissions.</li> <li>Lock Out feature is enabled in the User</li> </ul>	$\sim$	efreshed a few econds ago	0	155 modules are validly signed. No modules have additional permissions. Lock Out feature is enabled in the User
	43	<ul> <li>Service.</li> <li>All password-based authentication schemes are configured with strong</li> <li>All log levels are acceptable.</li> <li>Fox is disabled, while Foxs is set to true.</li> </ul>		43	0 0 0	Service. All password-based authentication schemes are configured with strong All log levels are acceptable. Fox is disabled, while Foxs is set to true.
	⊘ OK 32	Foxs Min Protocol is TLSv1.2+.		⊘OK 32	$\oslash$	True. Foxs Min Protocol is TLSv1.2+.

(i) Info 11



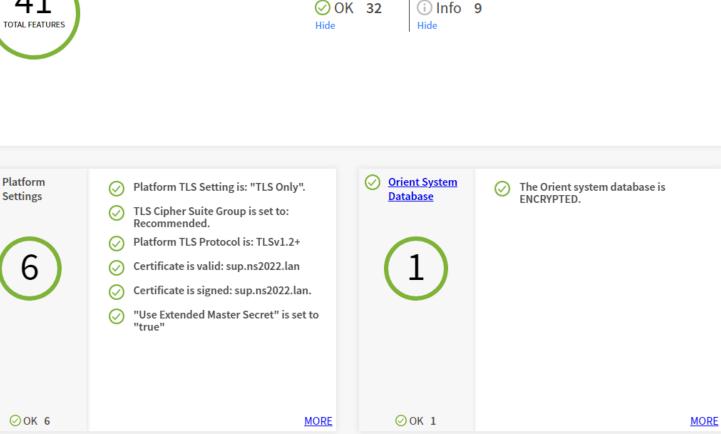
MORE

#### Security Dashboard – Station View

- Scores the station.
- Tiles show details for individual networks, services and configuration option
- Hyperlink to more detailed information



Settings







#### Public Key Infrastructure (PKI)

- An infrastructure that supports the distribution of certificates containing public identification keys that are used to both securely identify entities and provide confidentiality of transmissions.
- A Certificate Authority (CA) is an organization which issues and signs digital certificates.
- A digital certificate is an electronic document used to identify an entity, digitally signed by a trusted CA.





# Public Key Cryptography

- Private Key Key
- Uses a private and public key pair, used together for encrypting and signing.
- Keys are asymmetric, meaning each key is unique but only two specific keys work together.
  - The public key is not a secret and is available to everyone.
  - Each participant keeps its private key a secret.
  - A sender encrypts data with a recipient's public key and only the recipient with the private key can decrypt the data.
  - A sender can sign data with their private key and

Selerating involvation ender's public key.

#### What Does a TLS Certificate Provide

#### Security overview

🗎 🛈 🔺

#### This page is secure (valid HTTPS).

#### Certificate - valid and trusted

The connection to this site is using a valid, trusted server certificate issued by NS2022 Intermiedate CA.

View certificate

Connection - secure connection settings

The connection to this site is encrypted and authenticated using TLS 1.3, X25519, and AES\_256\_GCM.

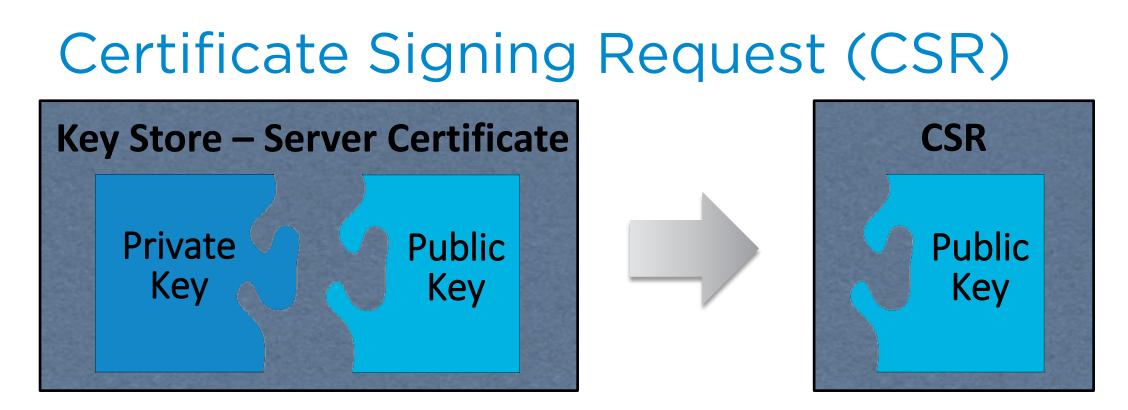
Resources - all served securely

All resources on this page are served securely.

- The client establishes an encrypted connection with the server.
- Verifies the identity of the server.
- Validates the authenticity of the server's certificate.
- A connection can be encrypted without verifying the server's identity or



validating the certificate

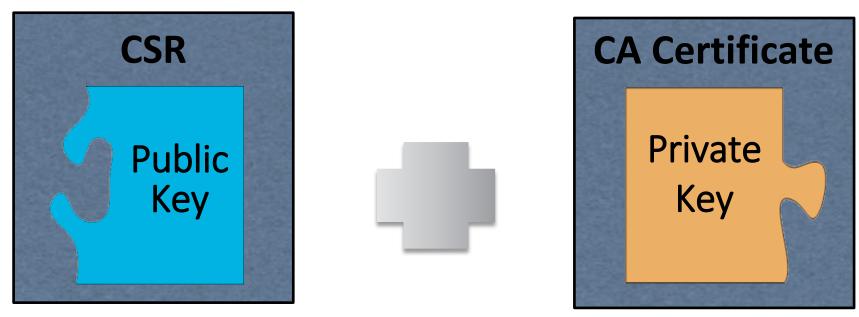


- Only includes the public key from the server's certificate.
- The original private key must remain in the server's key store.





## Signing a Certificate Signing Request



- Only includes the public key from the server's certificate.
- The original private key must remain in the server's key store.





#### Chain of Trust

- Shows the chain of certificates used to digitally sign the certificate.
- Typically includes at least an intermediate and root certificate.

Certificate	× Certificate	×
General Details Certification Path	General Details Certification Path	
Certificate Information	Certification path	
This certificate is intended for the following purpose(s):		
<ul> <li>Ensures the identity of a remote computer</li> <li>Proves your identity to a remote computer</li> </ul>		
Issued to: sup.ns2022.lan	-	
Issued by: NS2022 Intermiedate CA	View Certificate	
Valid from 3/1/2022 to 2/28/2023	Certificate status: This certificate is OK.	_



# Certificate Trust Stor

- Collection of root and intermediate certificates including their public keys.
- Typically populated by the C or application provider with well-known public CAs.

Certmgr - [Certificates - Current User\Trusted	Root Certification Authorities\Certificates]	- O X						
File Action View Help								
<ul> <li>Certificates - Current User</li> <li>Personal</li> <li>Trusted Root Certification Authorities</li> <li>Certificates</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authorities</li> <li>Active Directory User Object</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Third-Party Root Certification Authoritie</li> <li>Trusted People</li> <li>Other People</li> <li>Certificate Enrollment Requests</li> <li>Smart Card Trusted Roots</li> </ul>	Issued To AddTrust External CA Root AddTrust External CA Root Baltimore CyberTrust Root Certum CA Certum Trusted Network CA Calss 3 Public Primary Certification Authority COMODO RSA Certification Authority COMODO RSA Certification Authority COMODO RSA Certification Authority Copyright (c) 1997 Microsoft Corp. Deutsche Telekom Root CA 2 DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance EV Root CA	Issued By AddTrust Exte AffirmTrust C Baltimore Cyt Certum CA Certum Trust Class 3 Public COMODO RS, Copyright (c) Deutsche Tele DigiCert Assu DigiCert Glob DigiCert High						
< >	DST Root CA X3  Entrust Root Certification Authority	DST Root CA Entrust Root (						
Trusted Root Certification Authorities store contains 52 certificates.								

TRIDIUN

- Can import additional certificates from other CAs.
- Used by client to validate the digital signature in a certificate's chain of trust.



# Code Signing

- Code Signing Options

   Signing Cert
   ns2022 code signing

   Tsa Url
   http://timestamp.digicert.com
- Process of digitally signing executables and scripts to confirm the software author and guarantee the code has not been altered or corrupted since it was signed.
- Trusted timestamping is the process of securely tracking the creation and modification times of a document.
- Timestamping Authority (TSA) URL server which timestamps the code signature.





#### Code Signing – Verification Modes

- Low (4.8 default) modules that are not signed or are signed with an untrusted or expired certificate will cause warnings but still function normally. Errors occur if a signed module is modified and installation of such modules is not allowed.
- Medium (4.9 default) modules must be signed be a valid trusted certificate, but this certificate may be self-signed. Installation of unsigned or invalidly signed modules is not allowed.
- High modules must be signed by a valid trusted CA signed certificate. Installation of modules with a selfsigned certificate is not allowed.



# Code Signing – Jar Signer Tool

- Workbench menu select Tools
- Used to code sign an already compiled module.

Jar Signer	×					
Jar Signer Sign a jar with a selected certificate.						
Select a jar to sign:						
file:!modules/vykonPro-rt.jar						
Certificate Alias: ns2022 code signing 🔻						
Certificate Password: ••••••••						
TSA URL: http://timestamp.digicert.com						
OK Cancel						

# Code Signing – A Code Repository

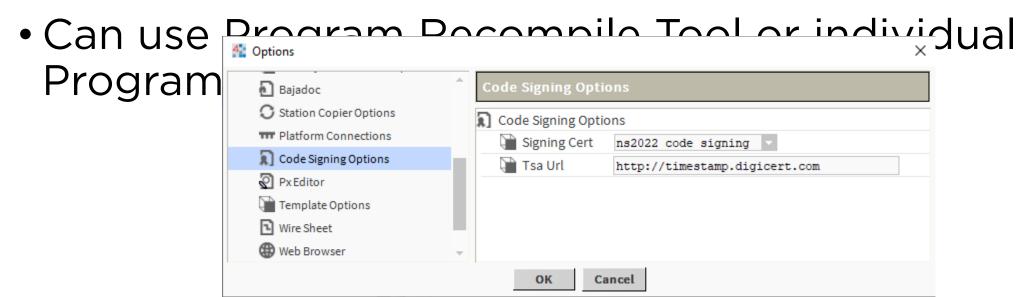
module://docDeveloper/doc/security/codeSigning.html





# Code Signing – Program Objects

- Workbench menu select Tools → Options → Code Signing Options.
- Used to code sign a program object when compiling.







# Provisioning – Security Related Job Steps

- Certificate
  - Generate Certificate in remote key store (4.6)
  - Import Signed Certificate in remote key store (4.6)
  - Install Certificate in remote user trust store (4.3)
  - Sign Certificate in remote key store (4.6)
  - Export Certificate Signing Request from remote key store (4.7)
  - Set Certificate Alias used by Fox, Web and Platform Services (4.6)
- Station Users
  - Add Station User (4.8)
  - Remove Station User (4.8)

Set Station User Password (4.7)



#### Provisioning – Security Related Job Steps • Platform

- Set Platform Credentials (4.6)
- Set System Passphrase (4.6)
- Remove Platform User (4.12)
- Set Platform User Password (4.12)
- Network Connection
  - Set Station Connection Credentials (4.8)
  - Setup Reciprocal Connection (4.6)
  - Set TLS Level for Platform, Fox, Web (4.6)
- General
  - Set Property (4.8) / Remove Property (4.12)
  - Configure Niagara IdP and SAML Scheme (4.9)



#### Summary

- Multiple layers of security provide defense in depth.
- Secure systems require active management including but not limited to managing certificates, installing software patches and conducting security audits.
- PKI certificates are used to establish trust between a client and server by verifying identities and encrypting data exchanged over the network.

TRIDIU

 Security Dashboard helps assess the security posture.

ACCELERATING JUNG AGE IN SIGNING CONFIRMS SOftware author and

#### Questions





