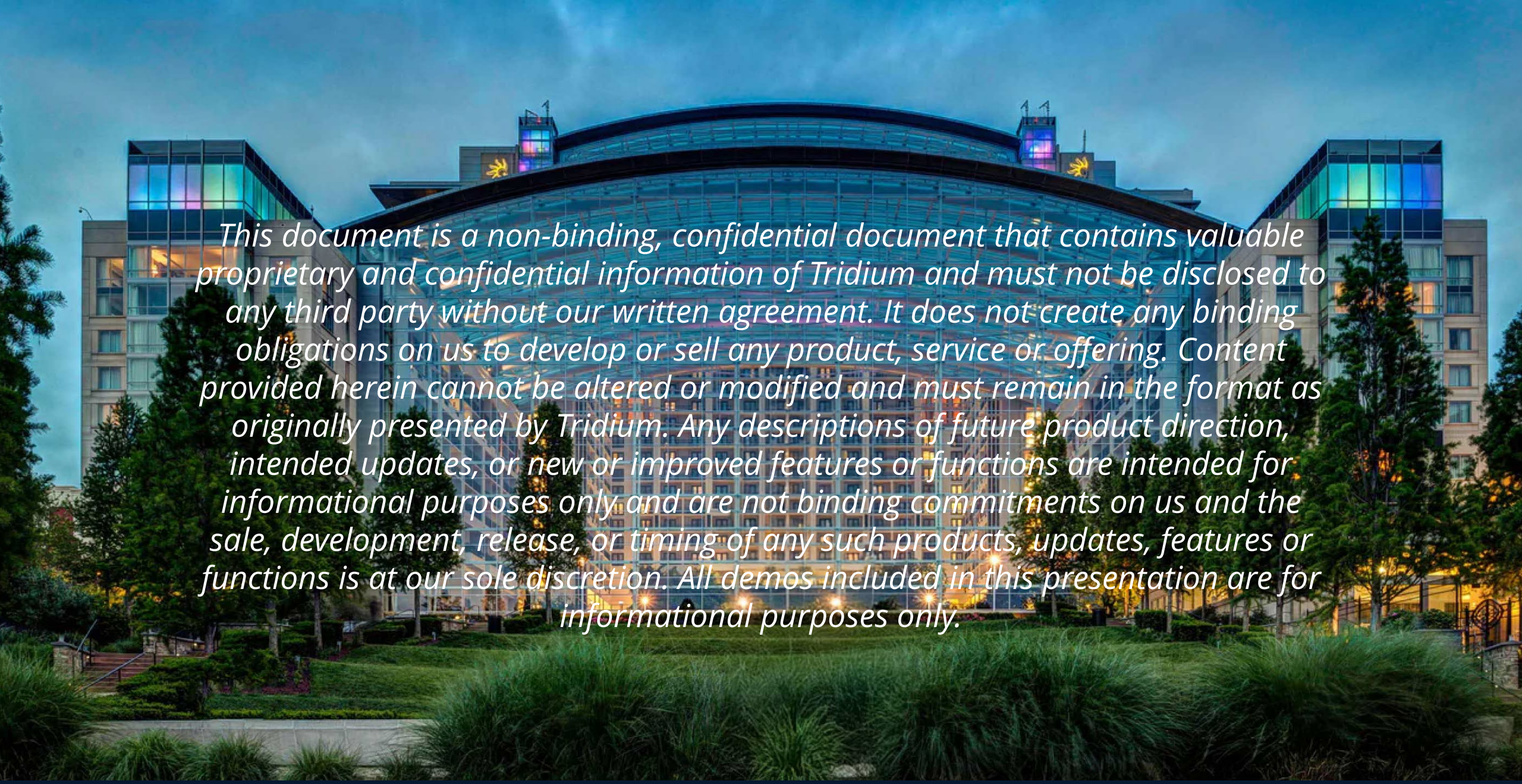

NIAGARA
SUMMIT
2026
SEAMLESS CONNECTIVITY,
POWERFUL INTELLIGENCE
TRIDIUM

Cybersecurity: Is Your Organization Next?

Michael McLaughlin
Sr. Sales Engineer

TRIDIUM


This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Tridium and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Tridium. Any descriptions of future product direction, intended updates, or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release, or timing of any such products, updates, features or functions is at our sole discretion. All demos included in this presentation are for informational purposes only.

Cybersecurity | Is Your Organization Next?

- IT + OT Reality Check
- Data Breaches & Headlines
- What We Can — and Are — DoingSecurity Dashboard
- Certificates | What They Are & Why They Matter
- Certificate Management in Niagara 4.15
- Syslog Integration
- Code Signing | What It Is & Why It Matters
- Provisioning | Secure by Default at Scale
- The Secure-by-Default Workflow

IT + OT Reality Check

- **IT and OT used to be separate worlds.**
  - IT cared about data, apps, users, and networks
  - OT cared about HVAC, lighting, access control, and equipment

- **That separation is gone.**
  - BAS now rides on the same networks as corporate IT
  - talk over IP, Wi-Fi, cloud, APIs, and mobile apps
  - Attackers don't care if it's "IT" or "OT" — it's all an entry point

- **The result:**
- Buildings are now part of the cybersecurity attack surface
- And most BAS were never designed with modern cyber threats in mind

Data Breaches & Headlines

- Ransomware, supply-chain compromise, credential theft, and remote-access attacks continue to impact organizations across OT environments

- OT systems — including HVAC, access control, lighting, water, and manufacturing — are increasingly targeted by attackers

- Connected building systems are routinely scanned, indexed, and probed by automated tools and threat actors

- The next major breach could easily involve a BAS — this is the reality of connected OT

- The urgency is real — but Niagara gives us the tools to help manage it

Sources:
SecurityWeek – *Building Automation Protocols Increasingly Targeted in OT Attacks* (Forescout Threat Roundup data).
Waterfall Security – *2024 Threat Report: OT Cyberattacks with Physical Consequences* (ransomware + vendor compromise trends).
CyberSec Magazine – *Case Study: Real-World OT Cyberattacks and Lessons Learned* (HVAC/OT remote-access exploitation).
BitSight – *ICS/OT Exposure Report* (180,000+ exposed ICS/OT devices monthly).

NS26

TRIDIUM

What We *Can* and *Are* Doing

- **Secure by Default**: designing Niagara so the secure choice is the easy — and often only — choice
- **Stronger platform & station security** in Niagara 4.15: TLS improvements, encrypted bog files, better certificate workflows
- **Improved code signing & Syslog integration** for integrity and visibility
- **Secure Boot on JACE hardware** ensures only Tridium-signed software can run
- **End-to-end ecosystem hardening:** platform, station, certificates, TLS, code signing, Syslog, provisioning, and hardware
- **Deprecation of non-secure Web and Fox in future versions of N5** to enforce TLS-only communication

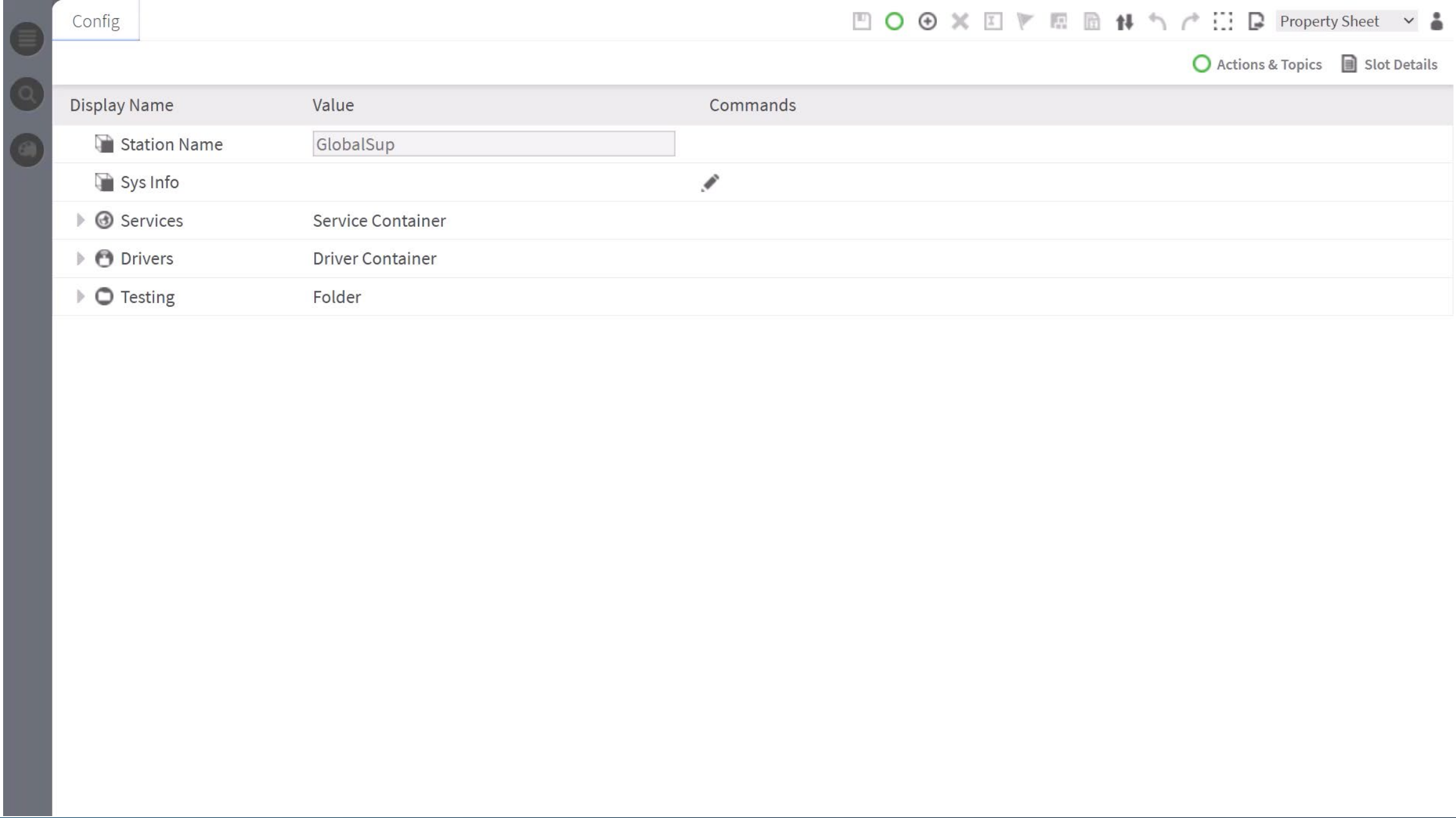
Security Dashboard

- Provides a unified view of a station’s overall security posture
- Surfaces certificate issues, weak credentials, and insecure configurations
- Breaks visibility into clear layers — Platform, Station, and Services — for faster diagnosis
- Highlights items that may need attention and offers guided remediation steps
- Helps operators validate trust chains, service settings, and secure-by-default configurations
- Scales from single stations to multi-site deployments with consistent posture reporting

Security Dashboard

Video Demo

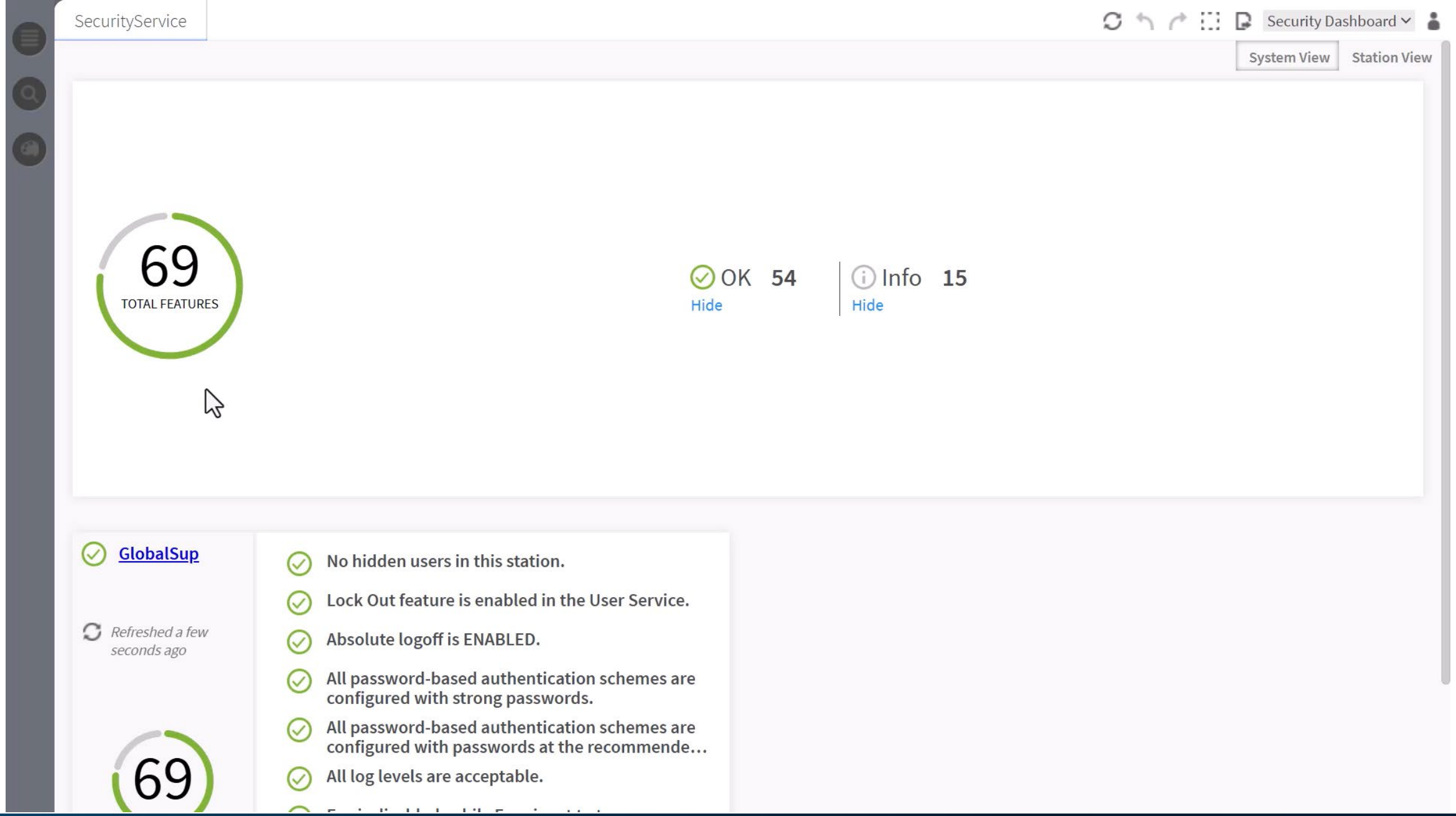
"All demos are for informational purposes only."


Config
Property Sheet
Actions & Topics
Slot Details
Display Name
Value
Commands
Station Name
GlobalSup
Sys Info
Services
Service Container
Drivers
Driver Container
Testing
Folder

Multi-Tiered Security Dashboard & Reachable Stations

Video Demo

"All demos are for informational purposes only."

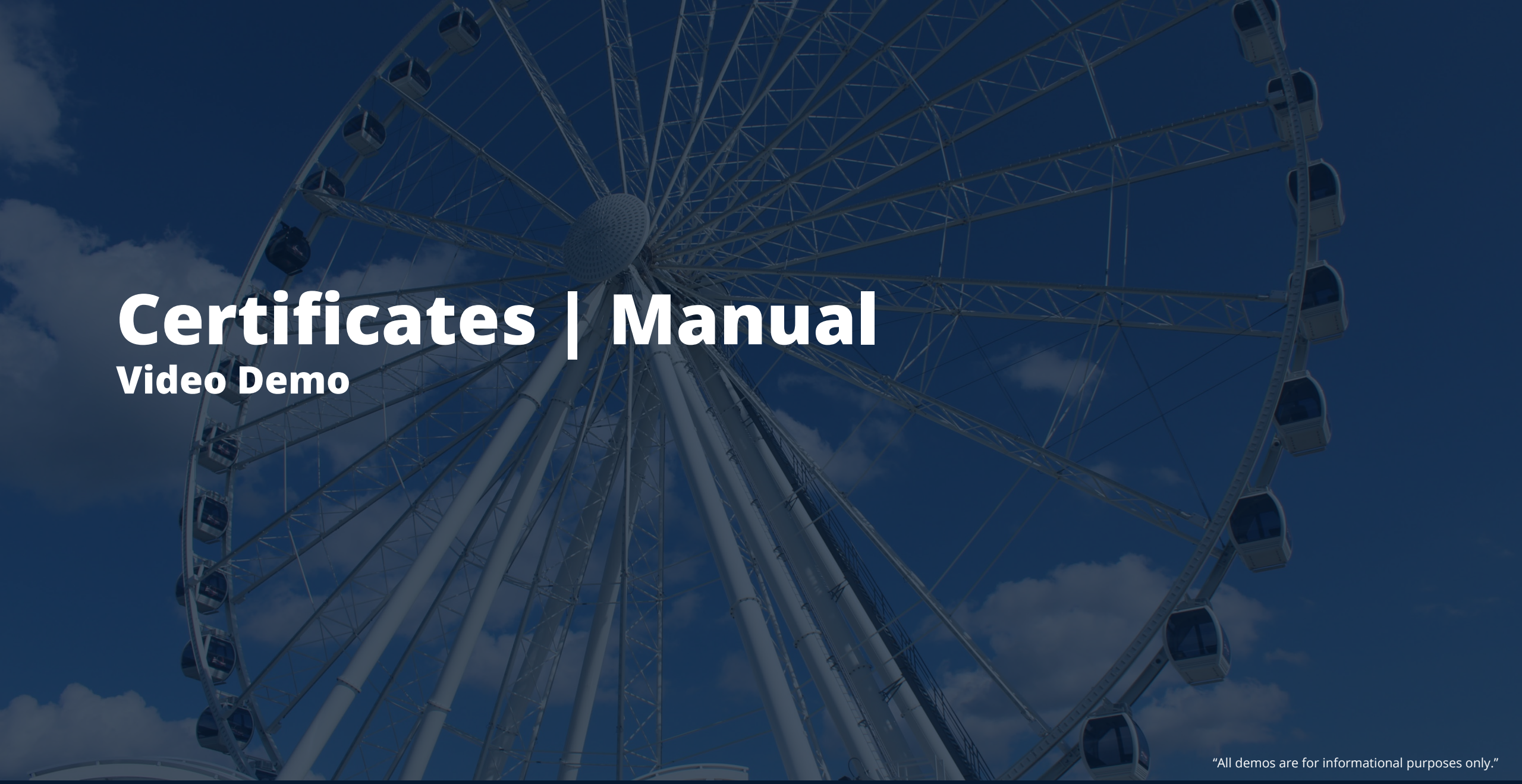

SecurityService
Security Dashboard
System View
Station View
69
TOTAL FEATURES
OK 54
Hide
Info 15
Hide
GlobalSup
Refreshed a few seconds ago
No hidden users in this station.
Lock Out feature is enabled in the User Service.
Absolute logoff is ENABLED.
All password-based authentication schemes are configured with strong passwords.
All password-based authentication schemes are configured with passwords at the recommende…
All log levels are acceptable.
69

Certificate Management in Niagara 4.15

- A certificate acts like a digital ID — it helps confirm a device's identity
- It supports creating an encrypted connection, so data is protected in transit
- It helps reduce impersonation risk — attackers have a harder time posing as trusted devices
- Every Niagara station benefits from having a valid certificate for secure communication
- TLS and certificates will be required going forward as non-secure Web and Fox are being deprecated in future versions of N5

Certificates | Manual

- Generate a CSR on the station for the Platform, WebService, FoxService, or combined
- Export the CSR and have it signed by your Certificate Authority
- Import the signed certificate back into Niagara
- Configure the Platform, WebService, and FoxService services to use the new certificate
- Validate the chain and confirm everything is healthy in the Security Dashboard
- Repeat the process for every station — consistent but time-intensive at scale



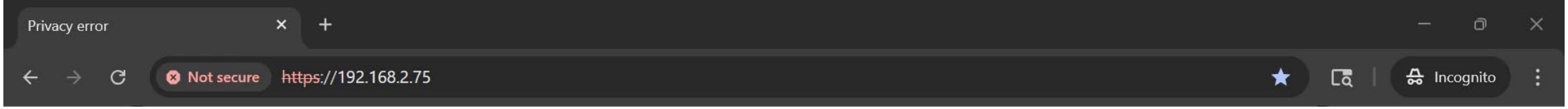
Certificates | Manual

Video Demo

"All demos are for informational purposes only."

NS26

TRIDIUM



Your connection is not private

Attackers might be trying to steal your information from **192.168.2.75** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

Advanced

Back to safety

Certificates | Signing Service

- Automatically generate CSRs for multiple stations in a single provisioning job
- Certificate Signing Service signs them centrally using your trusted CA
- Provisioning deploys the signed certs, aliases, and trust chains at scale
- Drives consistent, repeatable certificate management across fleets
- Ideal for multi-site, enterprise, and Secure-by-Default deployments

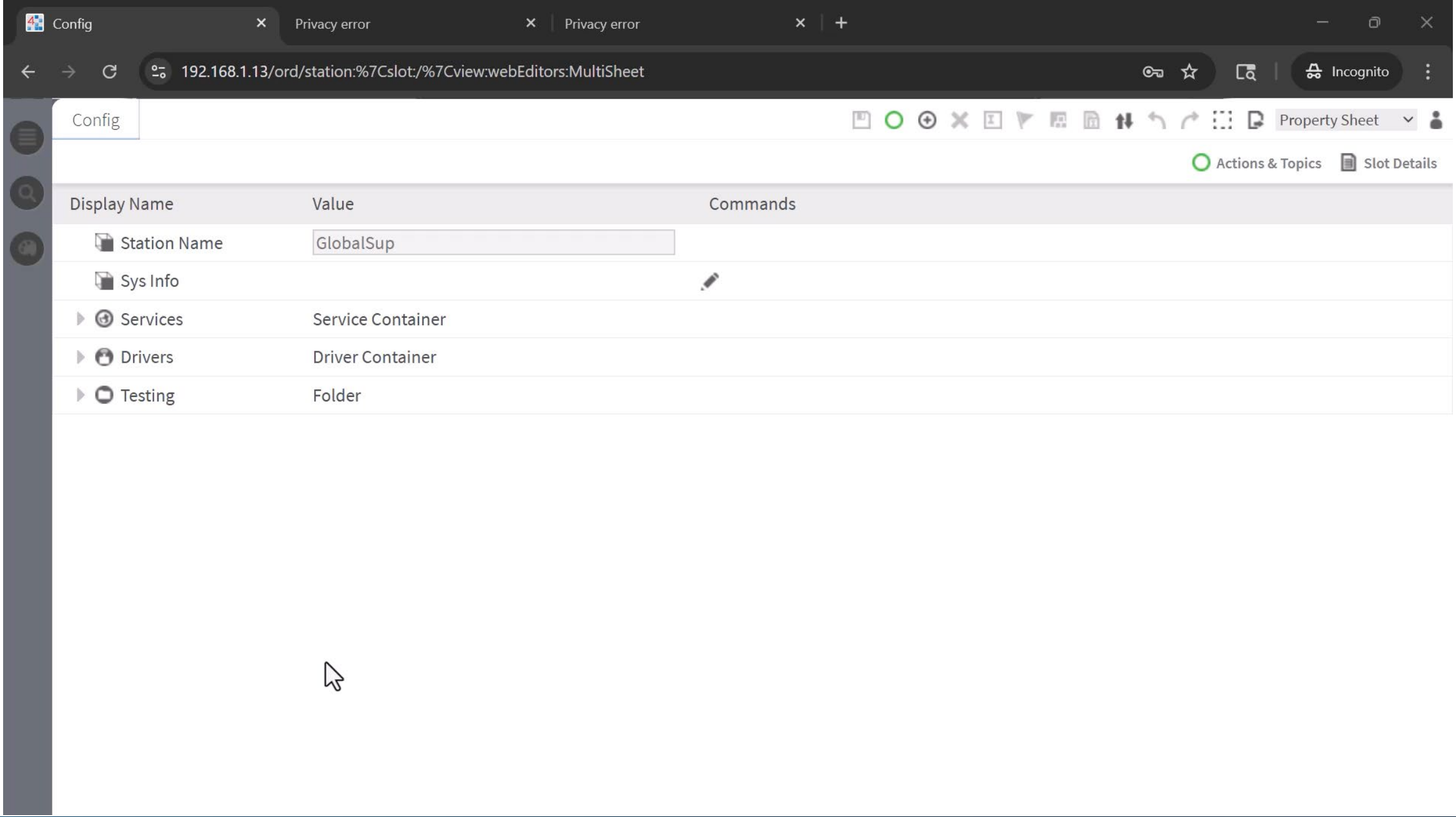
Certificates —Signing Service

Video Demo

"All demos are for informational purposes only."

NS26

TRIDIUM


Config
Privacy error
Privacy error
192.168.1.13/ord/station:%7Cslot:/%7Cview:webEditors:MultiSheet
Incognito
Config
Property Sheet
Actions & Topics
Slot Details
Display Name
Value
Commands
Station Name
GlobalSup
Sys Info
Services
Service Container
Drivers
Driver Container
Testing
Folder

Code Signing

Ensures integrity | signed code lets Niagara verify nothing has been altered

Blocks tampering | unsigned or modified logic won't run

Verifies authorship | signatures and trusted timestamps confirm who signed and when

Supports TSA | timestamping authority records allow validation of signature time

Protects modules | all Tridium modules are signed; third-party modules and program objects may also be signed

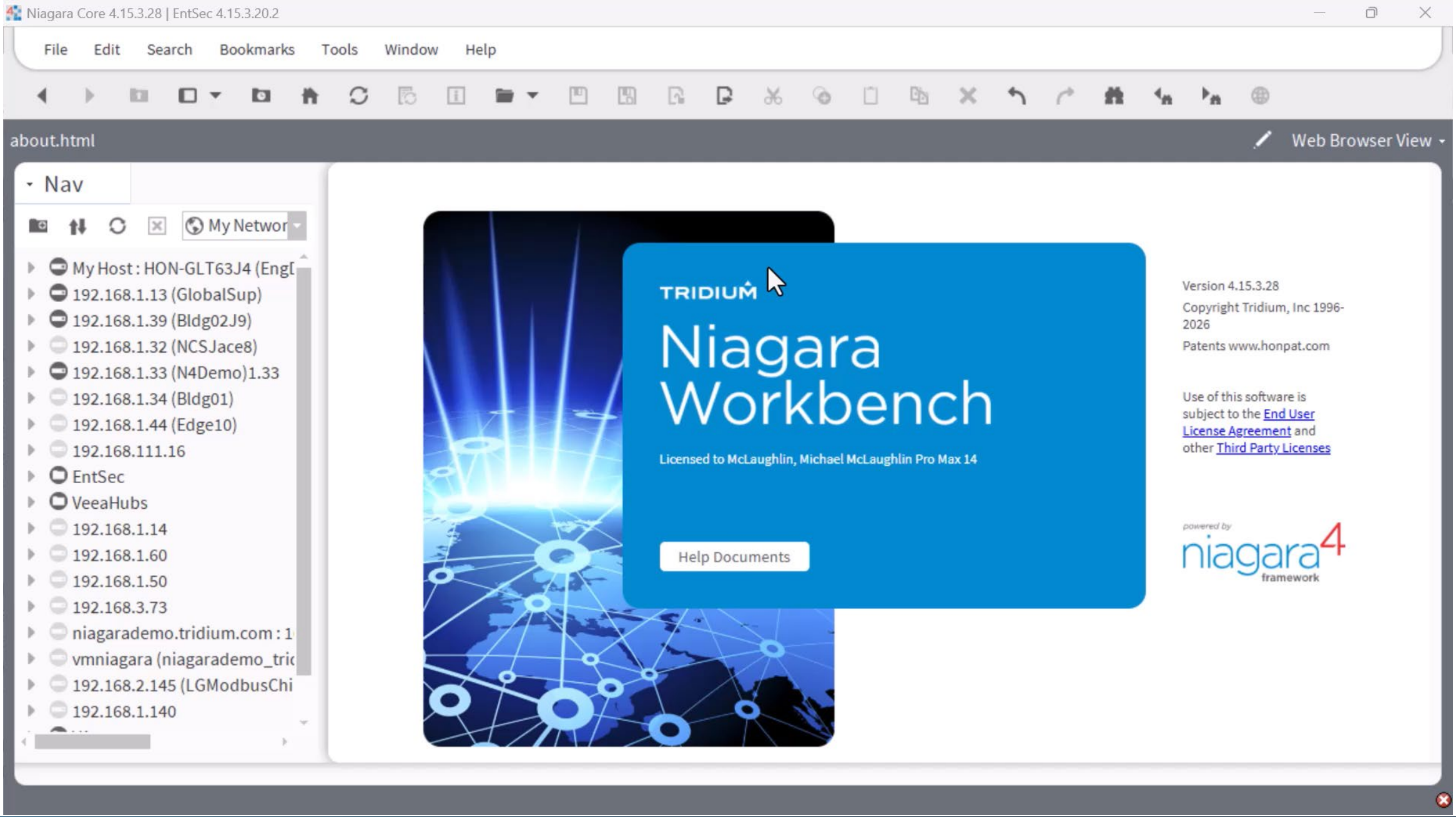
Secure Boot | JACE hardware loads only Tridium-signed firmware

N5-aligned | signed program objects become the expected model going forward

Code Signing

Video Demo

"All demos are for informational purposes only."


Niagara Core 4.15.3.28 | EntSec 4.15.3.20.2
File Edit Search Bookmarks Tools Window Help
about.html
Web Browser View
Nav
My Networ
My Host : HON-GLT63J4 (Engl
192.168.1.13 (GlobalSup)
192.168.1.39 (Bldg02J9)
192.168.1.32 (NCSJace8)
192.168.1.33 (N4Demo)1.33
192.168.1.34 (Bldg01)
192.168.1.44 (Edge10)
192.168.111.16
EntSec
VeeaHubs
192.168.1.14
192.168.1.60
192.168.1.50
192.168.3.73
niagarademo.tridium.com : 1
vmniagara (niagarademo_tric
192.168.2.145 (LGModbusChi
192.168.1.140
TRIDIUM
Niagara Workbench
Licensed to McLaughlin, Michael McLaughlin Pro Max 14
Help Documents
Version 4.15.3.28
Copyright Tridium, Inc 1996-2026
Patents www.honpat.com
Use of this software is subject to the End User License Agreement and other Third Party Licenses
powered by niagara4 framework

Encrypted Hashed Passwords

- Passwords are not stored in plain text — they’re hashed, salted, and encrypted
- Even if the file is accessed, the hashed password is not directly recoverable
- Salting ensures every password hash is unique, even if two users choose the same password
- Encryption adds a second layer of protection on top of hashing
- In 4.15, Bog files use modern hashing and encryption, providing stronger security

Encrypted Hashed Passwords

Live Demo

"All demos are for informational purposes only."

Syslog Integration

- Centralized monitoring = faster detection and response
- Security events shared outside of the Niagara environment
- It closes the IT/OT visibility gap
- Helps security teams identify patterns that may not be visible in OT alone
- Helps organizations meet audit and compliance expectations

Syslog Integration
Video Demo

"All demos are for informational purposes only."

NS26

TRIDIUM

Config

Property Sheet

Actions & Topics | Slot Details

Display Name	Value	Commands
Station Name	GlobalSup	
Sys Info		
Services	Service Container	
Drivers	Driver Container	
Testing	Folder	

Host Header Validation

- Validates approved hostnames and IP addresses
- Prevents spoofed or malicious web requests
- Enforces secure access
- Supports certificates, proxies, and cloud deployments
- Key component of Niagara’s modern security model

Securing Niagara

- TLS-only communication as non-secure Web and Fox are planned to be deprecated in future N5 versions
- Use the Niagara Hardening Guide for Platform and Station configuration expectations
- Apply role-based access with a least-permissions-necessary approach
- Use provisioning templates to support consistent secure deployments
- Maintain module integrity through signed modules and validated program objects
- Collaborate with IT teams to define responsibilities and align security practices

Niagara Cloud | Secure Remote Connectivity

- Supports secure remote access with two-factor authentication
- Uses mutual TLS (mTLS) for trusted, certificate-based connections
- Reduces reliance on VPNs that may require ongoing maintenance
- Provides centralized identity and device registration
- Native to the Niagara ecosystem
- Backups are encrypted with Niagara Recover
- N5-specific features coming in the future

Niagara Cloud | Secure Remote Connectivity

Live Demo

"All demos are for informational purposes only."

NS26

TRIDIUM

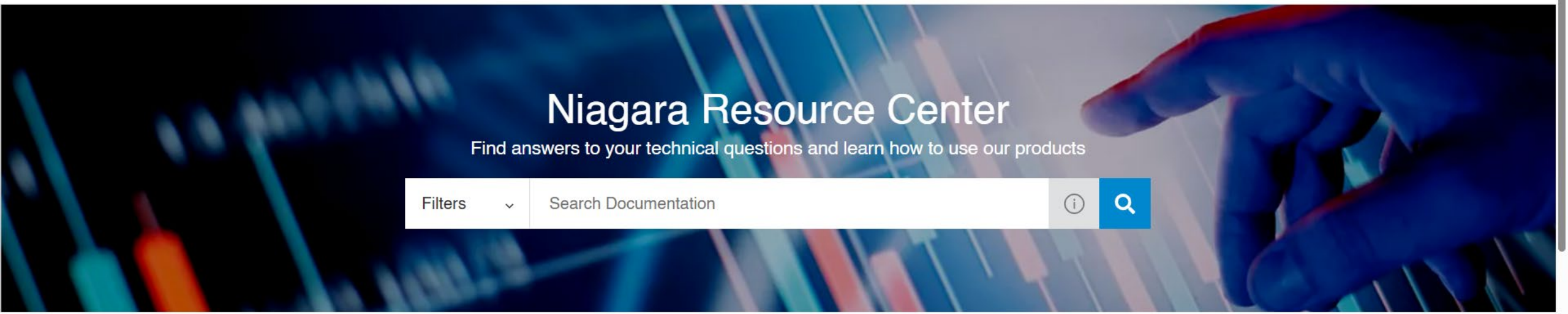
Niagara Cloud | FoxC

Live Demo

"All demos are for informational purposes only."

NS26

TRIDIUM



Niagara Resource Center

Find answers to your technical questions and learn how to use our products

Filters Search Documentation

Information Categories

Niagara

Niagara 5 - FAQ
Getting Started with Niagara
Installation Guide
Containerized Niagara Guide
Documentation Library

Features, Compatibility, and Releases

Niagara 4 Features Overview
Niagara Compatibility Statement (NiCS)
Niagara 4 Release Page

Niagara Security

Station Security Guide
Niagara Hardening Guide
Niagara 4 Security Page

Niagara Marketplace

Marcomm and Legal

Niagara Cloud

Thank You!

NS26

TRIDIUM