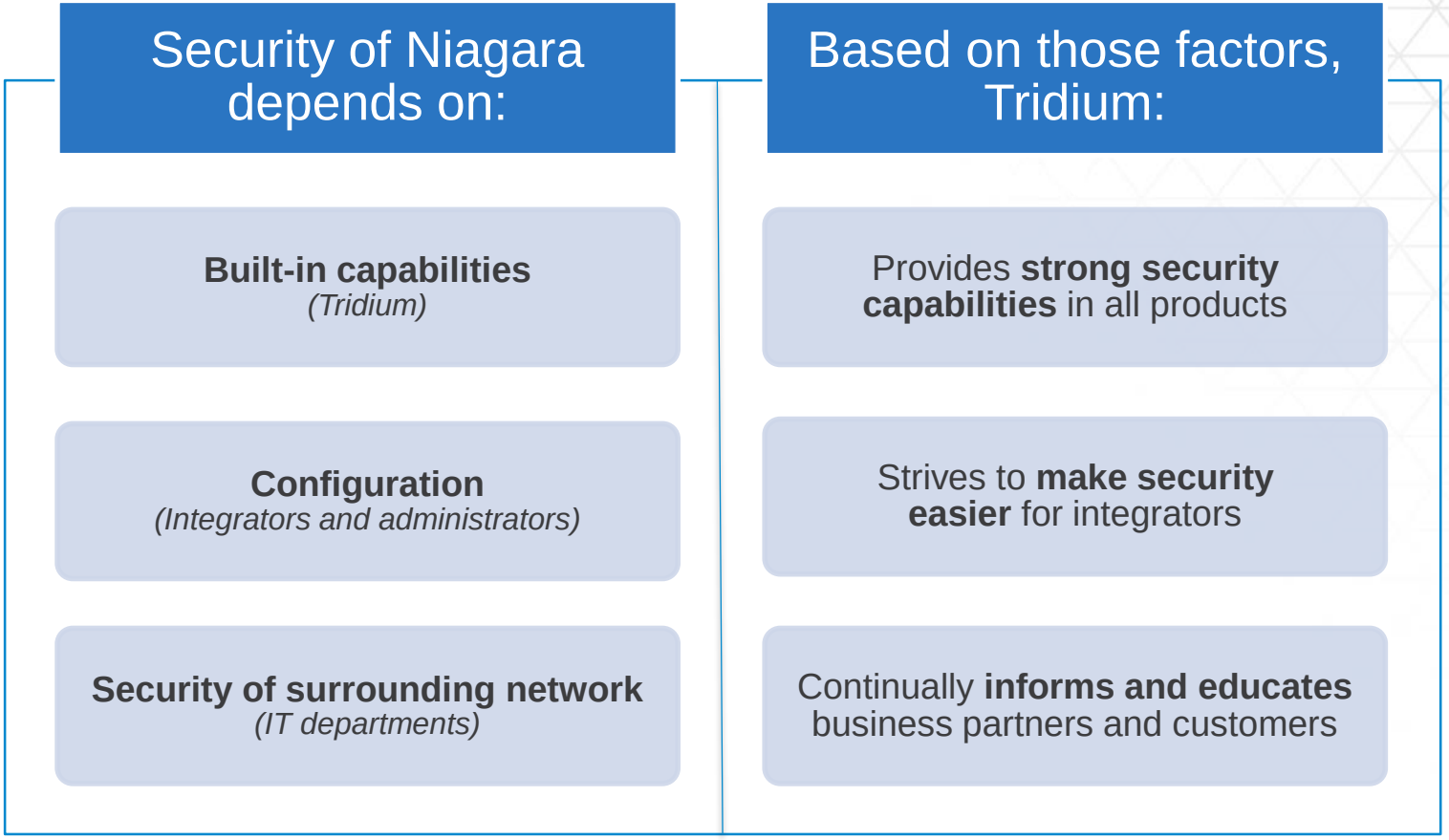
Cybersecurity approach and best practices

TRIDIUM

Cybersecurity is a priority



TRIDIUM

Security Processes

Tridium's Security Processes at a Glance	
Security Requirements	Based on ISA 62443-3-3 Security Level 4 for Critical Infrastructure - Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation
Internal Reviews by Tridium's Product Security Team	• Security Design Reviews, Security Code Reviews • Security Threat Modeling • Automated Security Tests for ISA 62443-3-3 Security Requirements • Reviews for vulnerabilities in third party libraries • Static Code Analysis and Binary Code Analysis • Risks managed in Risk Register according to CVSS Score
Reviews by External Teams	• Routine and Periodic Robust Security Testing by External Organizations on new and existing releases – partnering with commercial and government entities, throughout the year • Penetration Testing, Abuse Case Testing, Security Code Reviews
Reviews by Internal Security Auditor, CTO, and CCB approval	• 5 Phase Process, where all security artifacts from above are reviewed, and must have CTO signoff before Tridium CCB meets to vote on each phase
Risk Management Process with Deadlines on mitigating all found threats	• All known security vulnerabilities have visibility at the highest level, with 30-day, 60-day, 90-day, 120-day requirements for mitigation based on CVSS Score
Product Security Incident Response Team	• Robust process for investigating vulnerabilities, mitigating threats, and communication response. • Work closely with US-CERT and ICS-CERT
Support	• Routinely patch potential vulnerabilities, release security update builds, and send communications to the Niagara community

Security capabilities

Authentication	Pluggable schemes provide flexibility; defaults are the most secure; Multi-Factor Authentication (MFA) now an option with Google 2 Factor Authentication; Niagara 4.8 includes digital certificate authentication & 802.1x device network authentication
Identity infrastructure and PKI integration	Can integrate with any PKI infrastructure, LDAP directories, Kerberos, and SAML 2 Identity Providers for Single Sign-On; Niagara 4.8 also includes 802.1x device authentication to the network when available.
Role-Based Access Control	Provides access control for users by security role
Authorization at API level	Controls what individual software components can do
Encryption of all communications	All communications encrypted by default
Encryption at rest	Sensitive data is encrypted on disk
Digitally signed code, validated at run-time	Assures that core framework code can't be altered or manipulated
Hardware Security: JACE-8000 Secure Boot & HSM	Hardware root-of-trust; Only boots our digitally-signed trusted software, providing assurance against alteration; Also, Hardware Security Module provides hardware protection of private key for device authentication
Common-sense user account management	Configurable security mechanisms for attack prevention (lockouts, password strengths, etc.)
Auditing of all user activity	User access is logged to customized levels

niagara4 Security standards / protocols

Authentication	SCRAM-SHA (256/512 bit) DIGEST – default JACE-8000: WPA-PSK128, WPA2PSK256, Google 2 Factor Auth
Identity infrastructure integration	PKI, LDAP, Kerberos authentication, SAML 2 IDP SSO Integration
Encrypted communications* *(By default – only perfect forward secrecy ciphers are used)	TLS 1.2, 1.1, 1.0 (FOXS / HTTPS) • Issued with RSA 2048 bit certificate, SHA256withRSA
Encryption at rest	AES 256-CBC Symmetric Key Encryption PBKDF2-HMAC-SHA256
Digital signatures	SHA256withRSA (2048-bit RSA asymmetric key)
Compliance	4.6+ = FIPS 140-2 Compliance, using FIPS 140-2 cryptographic module; For Federal Government, DoD Risk Management Framework (RMF) Artifacts for Niagara 4 available in SAFE
User authorization	RBAC (Role-Based Access Control)
User account management	OWASP Recommendations
General Security Requirements	Security Requirements for Niagara derived from ISA 62443 Security Level 3 & 4

Bitter Details:
Ciphers Used & Available in TLS:

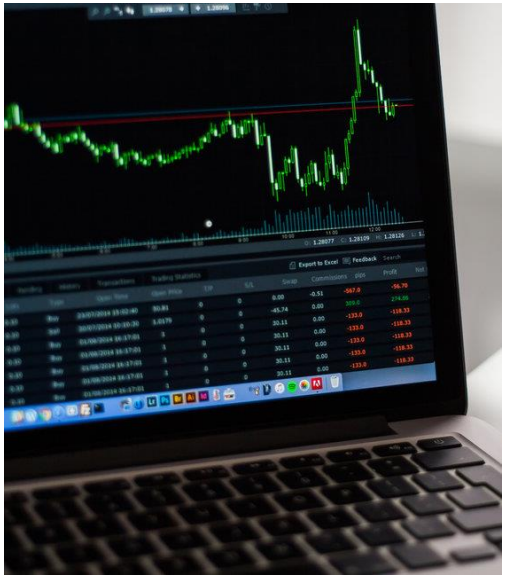
Recommended:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

Supported:

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA

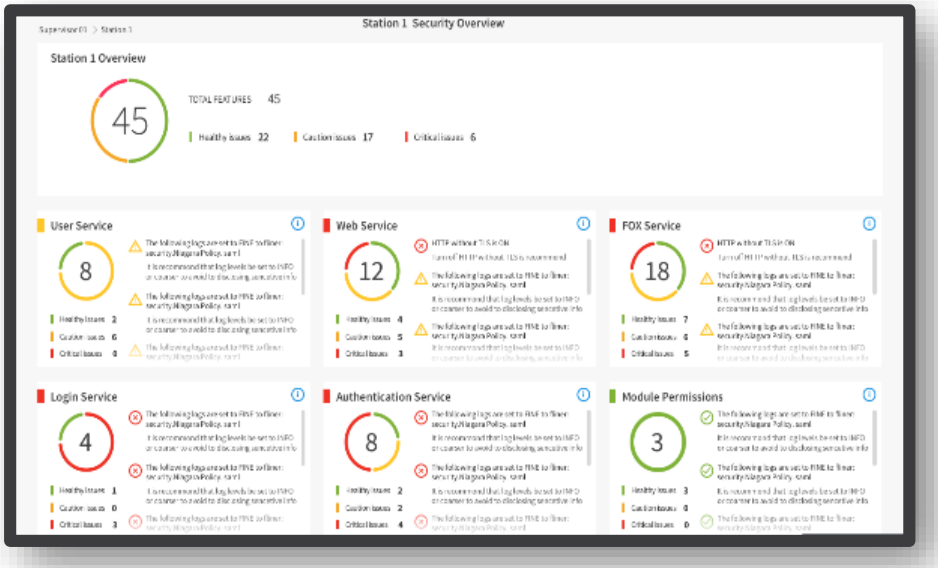
Our “Secure by Default” principle

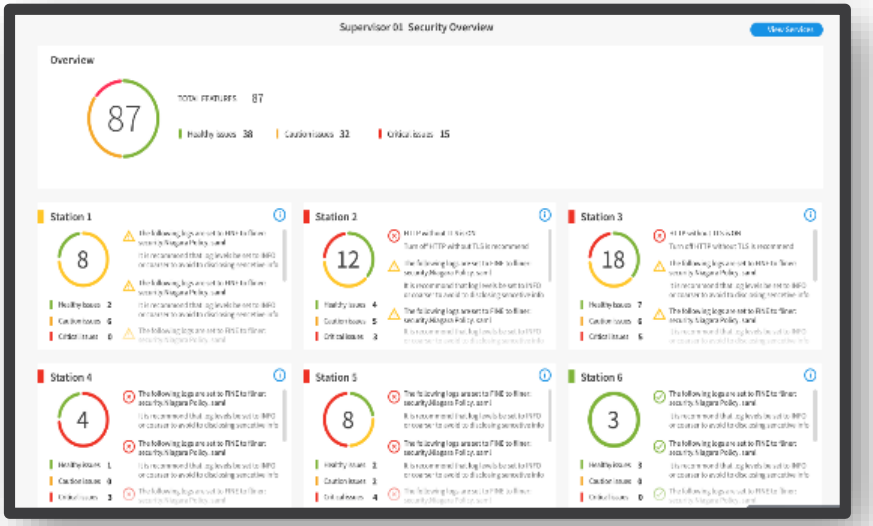


1. Make security easier: default to the most secure configurations
   - All transmissions encrypted
   - Users forced to have strong password strengths
   - Users set up with the strongest authentication mechanism
   - User lockouts upon consecutive bad log-ins
2. Force administrators to do the right thing
   - Factory default password must be changed after commissioning
3. Do the right thing, regardless of configuration
   - Encrypt sensitive information at rest
   - Digitally Signed Code: validated at run-time
   - JACE-8000 Secure Boot: trusted software validated at boot-time
4. Provide stronger configuration options based on best practices
   - Articles, documentation, TridiumTalks provide detailed guidance

We provide strong security capabilities – but it is important for our our partners and customers to configure and manage Niagara correctly!

Security Dashboard in Niagara 4.8





Providing an Instant View of the Security Posture of Your Stations

… so that you can adjust your settings for the best security.

Best practices: resources

- Recent White Paper:
  - “Cybersecurity and the IoT – Threats, Best Practices, and Lessons Learned”
- Technical bulletins
  http://www.tridium.com/en/resources/library
- White papers
  http://www.tridium.com/en/resources/library
  - Niagara 4 & AX Hardening Guides
- Niagara 4 documentation
  - Station Security Guide (ships with Niagara 4)
- Replay of Webex Webinars on Cybersecurity Best Practices, available on Tridium’s Web Site


white paper

Cybersecurity and the IoT—Threats, Best Practices and Lessons Learned

Kevin T. Smith, Chief Architect, Tridium

The market for the Internet of Things (IoT) is continuing to grow at a phenomenal pace. According to research from the International Data Corporation released early in 2017, the IoT market will reach $1.29 trillion by 2020.[1] IHS Markit forecasts that the IoT market will grow from what was an installed base of 15.4 billion devices in 2015 to 75.4 billion devices in 2025.[2] Other market research firms are releasing similar staggering statistics, and while estimates vary, all parties agree: network-connected devices and their capabilities are and will continue to be a disruptive force in the way that everyone does business.

Adding network connectivity to any “thing” can certainly provide great value, but it also brings along with this connectivity potential risks related to network security

But 15 years ago—long before anyone had ever heard of the IoT—Tridium developed the Niagara Framework, a general-purpose, open and extensible software framework built for the purpose of connecting, managing and controlling any device over computer networks. A general-purpose IoT framework that allows integrators to connect and control devices, regardless of protocol and manufacturer, Niagara has changed the way that organizations do business, putting the “smarts” in smart buildings and data centers, providing significant cost savings and capabilities. Over the years, this experience has given us much insight into the areas of device connectivity and control, automation, analytics and cybersecurity.

Cybersecurity should be a concern for any user or owner of connected devices. In our fast-paced world of ever-changing technology, the cyberthreat landscape continues to evolve at an alarming rate. With recent cybersecurity incidents showing unprecedented growth in the frequency, scale and sophistication of advanced cyberattacks, combined with the number of high-profile data breaches and hacks hitting the front pages of newspapers on an almost weekly basis, it should not be a surprise that most organizations are taking a newfound interest in protecting the systems on their networks.

Regarding the IoT, adding network connectivity to any “thing” can certainly provide great value, but it also brings along with this connectivity potential risks related to network security. In the past few years, we have seen web cameras, baby monitors, smart refrigerators and even cars electronically hacked. We have seen an alarming rise in data breaches costing organizations billions of dollars. We have seen the rise of security and privacy concerns related to smart devices. We have seen an alarming rise in malware threats infecting computers and smart devices. We have seen the increase of hacker-friendly tools and websites that allow

TRIDIUM

[1] http://www.idc.com/getdoc.jsp?containerId=prUS42209117.
[2] https://www.ihs.com/info/0416/internet-of-things.html.

Thank You!

Kevin T. Smith, CISSP, CSSLP
CTO

ksmith@tridium.com
www.linkedin.com/in/kevintsmith/

TRIDIUM