NHP ELECTRICAL ENGINEERING PRODUCTS

Safety through security

Protecting people, the environment and critical industrial infrastructure against security threats

➤ nhpnz.co.nz

☎ 0800 647 647

✉ sales@nhp-nz.com

Is your business protected?

Industrial cybersecurity is a critical consideration for modern manufacturers. With increasing reliance on data, information and technology, it is essential to safeguard these assets from cyberattacks which can result in disclosure of confidential information or threat thereof, modification, disruption, or other improper use.

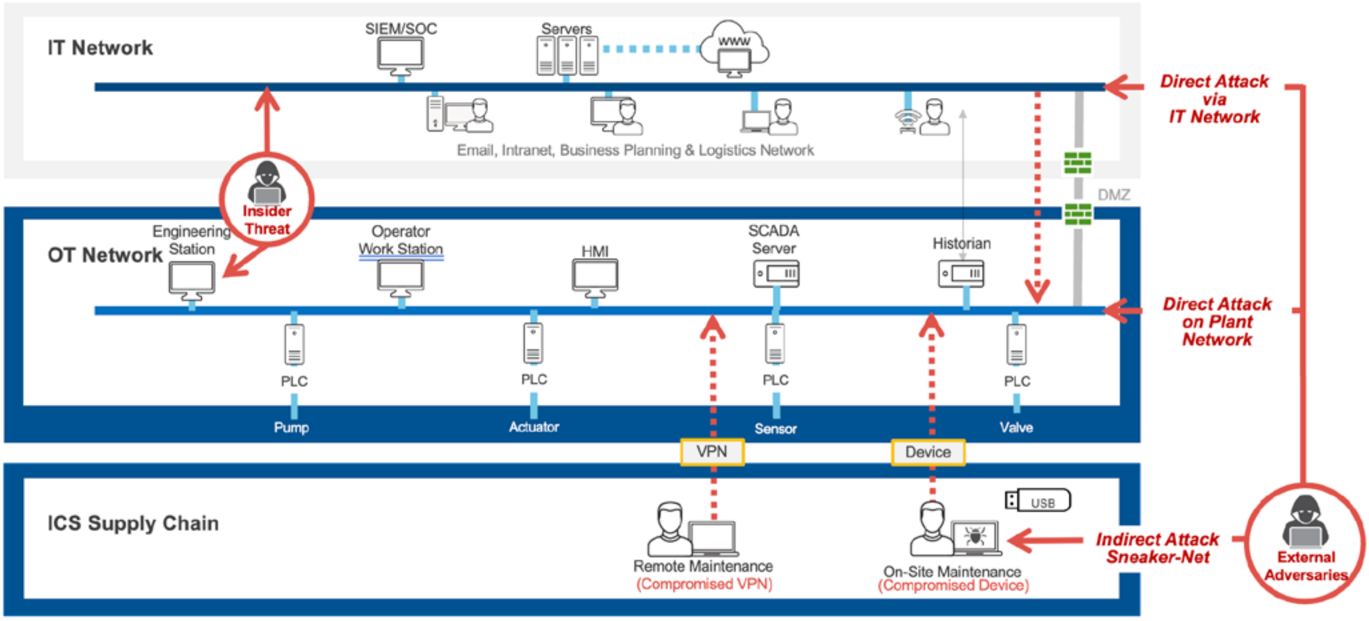
In New Zealand, cybersecurity has become a growing concern in recent years, with several high profile cases demonstrating that even the biggest and well-resourced organisations can be vulnerable. Organisations of all sizes across all industries must take a proactive approach to OT cybersecurity to protect their businesses, employees and customers.

Knowing where to start can be the biggest roadblock to implementing a successful cybersecurity strategy for your organisation. NHP and Rockwell Automation offer tailored, in-depth solutions in conjunction with world-class partners that can help manufacturers achieve their cybersecurity goals.

Understanding the threat vectors

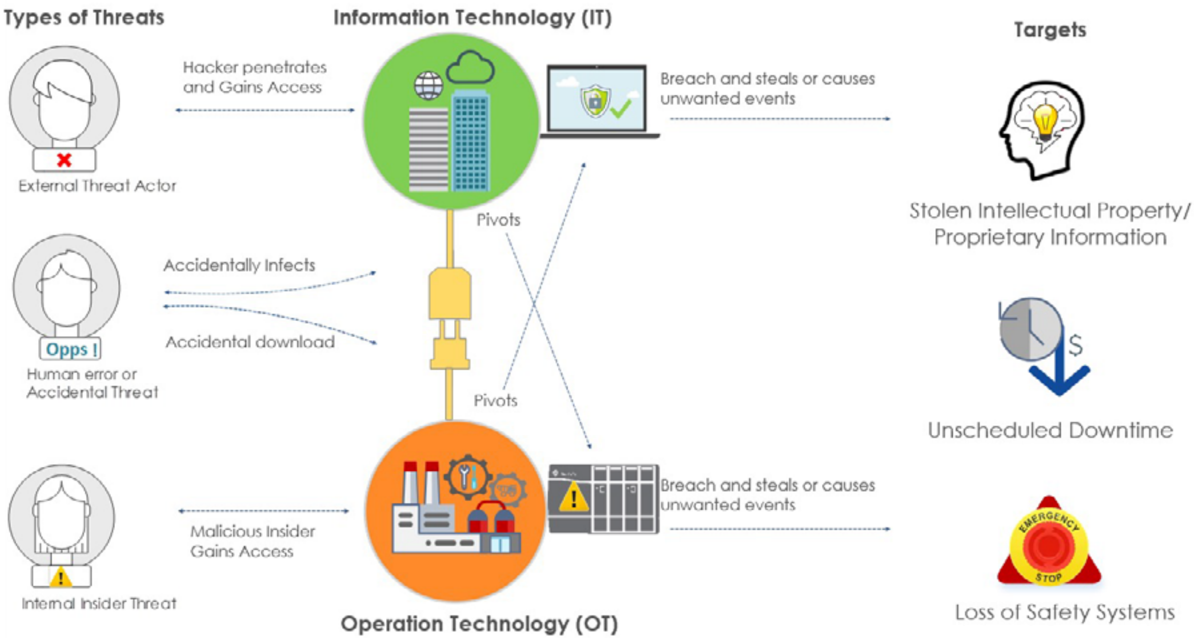
Threat vector is a term used to describe the method a cybercriminal uses to gain initial access to a victim network or infrastructure. Common threat vectors include digital attacks, physical attacks and social engineering attacks, which must be prevented whenever possible.

Common Threat Vectors



Types of threats

Internal cybersecurity risks can be just as devastating as external ones. While we enjoy the benefits of IT-OT convergence, it is important to understand and protect against both IT and OT devices and applications face continuous threats. Threats are undesirable events where anything might exploit a vulnerability to cause negative impacts on the operation or availability of equipment.


Types of Threats
Information Technology (IT)
Targets
Hacker penetrates and Gains Access
Breach and steals or causes unwanted events
External Threat Actor
Pivots
Stolen Intellectual Property/ Proprietary Information
Accidentally Infects
Accidental download
Opps !
Human error or Accidental Threat
Pivots
Unscheduled Downtime
Breach and steals or causes unwanted events
Malicious Insider Gains Access
Internal Insider Threat
Operation Technology (OT)
EMERGENCY
STOP
Loss of Safety Systems

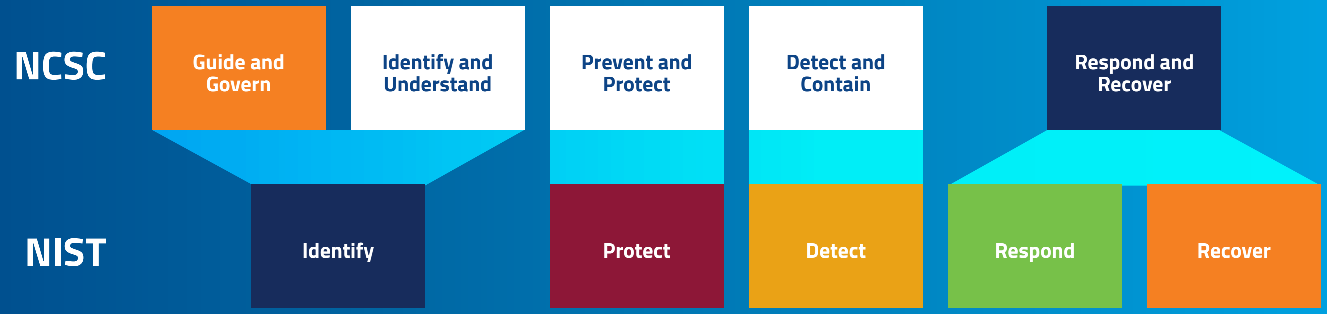
New Zealand's cybersecurity obligations

The National Cyber Security Centre (NCSC), part of the Government Communications Security Bureau (GCSB), supports nationally significant organisations to improve their cyber security posture and responds to national-level harm.

The National Cyber Security Centre's Cyber Security Framework is a way of organising thinking about cyber security activities, and it provides a common language to describe them. Organisations can refer to the framework to understand how the NCSC uses advice, guidance, standards, and security services to communicate consistently what being cyber secure and cyber resilient means. The National Cyber Security Centre (NCSC) has based its framework on the popular NIST Cyber Security Framework (CSF) and adapted this to the New Zealand context. The NCSC's framework content is freely available (under Creative Commons) for others to adopt or adapt to suit their own needs.

How does the NCSC framework compare to NIST's cyber security framework?

This framework is very similar to the NIST cyber security framework, and both contain five high-level functions. The main point of difference is that NCSC have chosen to place greater emphasis on security governance and culture by separating it from the Identify function. To reflect the interconnected nature of incident response and recovery, they have merged NIST's Respond and Recover functions (which are separated in NIST's framework).



For more information visit NCSC Cyber Security Framework | National Cyber Security Centre

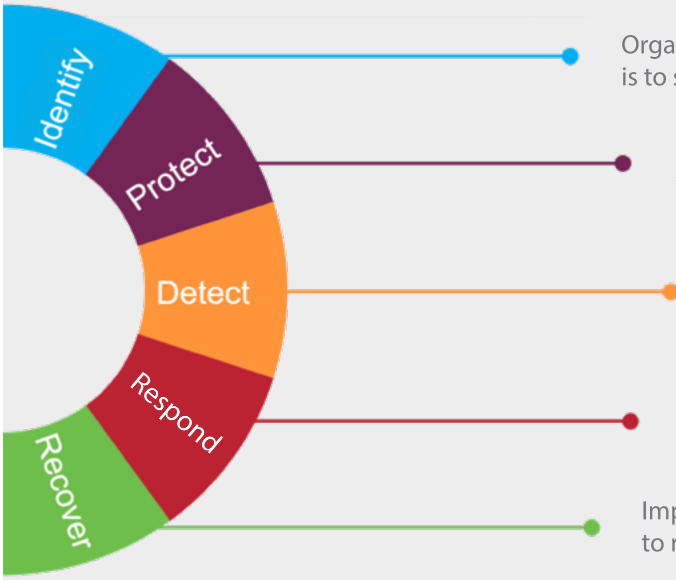
Cybersecurity standards and framework

The National Institute of Standards and Technology (NIST) framework of the United States of America provides a simple structure which helps businesses of all sizes better understand, manage and reduce their networks and data. The NIST framework is aligned with the ISA/IEC 62443 and ISO 27001 standard.

The ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). These standards set best practices for security and provide a way to assess the level of security performance. Their approach to the cybersecurity challenge is a holistic one, bridging the gap between operations and information technology as well as between safety and cybersecurity.

The ISA/IEC standards set cybersecurity benchmarks in all industry sectors that use IACS, including building automation, electric power generation and distribution, medical devices, transportation and process industries such as chemicals and oil and gas.

NIST cybersecurity framework



Organisation understands what the current state and risk is to systems, assets and data.

Implement safe guards to ensure delivery of critical infrastructure services.

Implement appropriate activities to identify a cyber security event.

Implement activities to take action regarding a detected cybersecurity event.

Implement activities to maintain plans for resiliance and to restore capabilities.

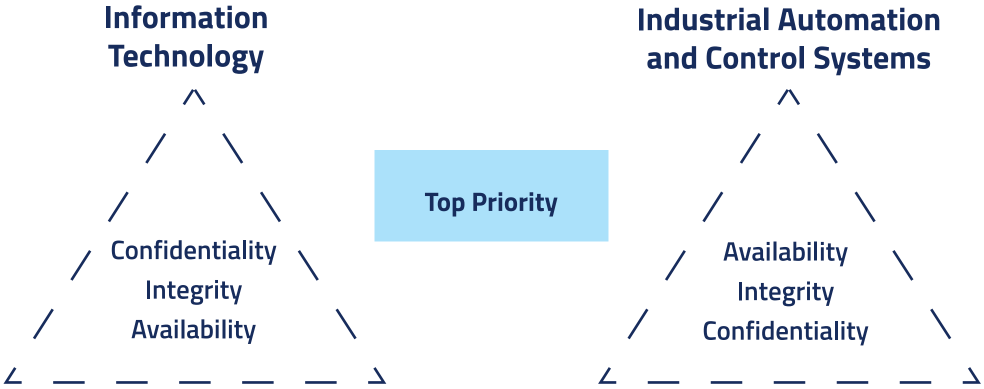
How IT and OT converge

Confidentiality, integrity, availability, authenticity and non-repudiation are the five core security properties that are used to ensure the security and reliability of information systems. Together, they form the foundation of information security and are the key elements that must be protected to ensure the safe and secure handling of sensitive information.

However, it's often observed that cybersecurity priorities for IT and OT are inverted. These requirements are addressed by the relevant standards and organisations must understand that one standard cannot be applied across both areas of the manufacturing infrastructure.

ISO/IEC 27001/2 addresses the establishment of an information security management system for the IT infrastructure of an organization.

The ISA/IEC 62443 explicitly addresses Cybersecurity in OT environments; this helps an organization to maintain conformance with ISO/IEC 27001 through common approaches wherever feasible, while highlighting differences in IT vs. OT approach where needed.



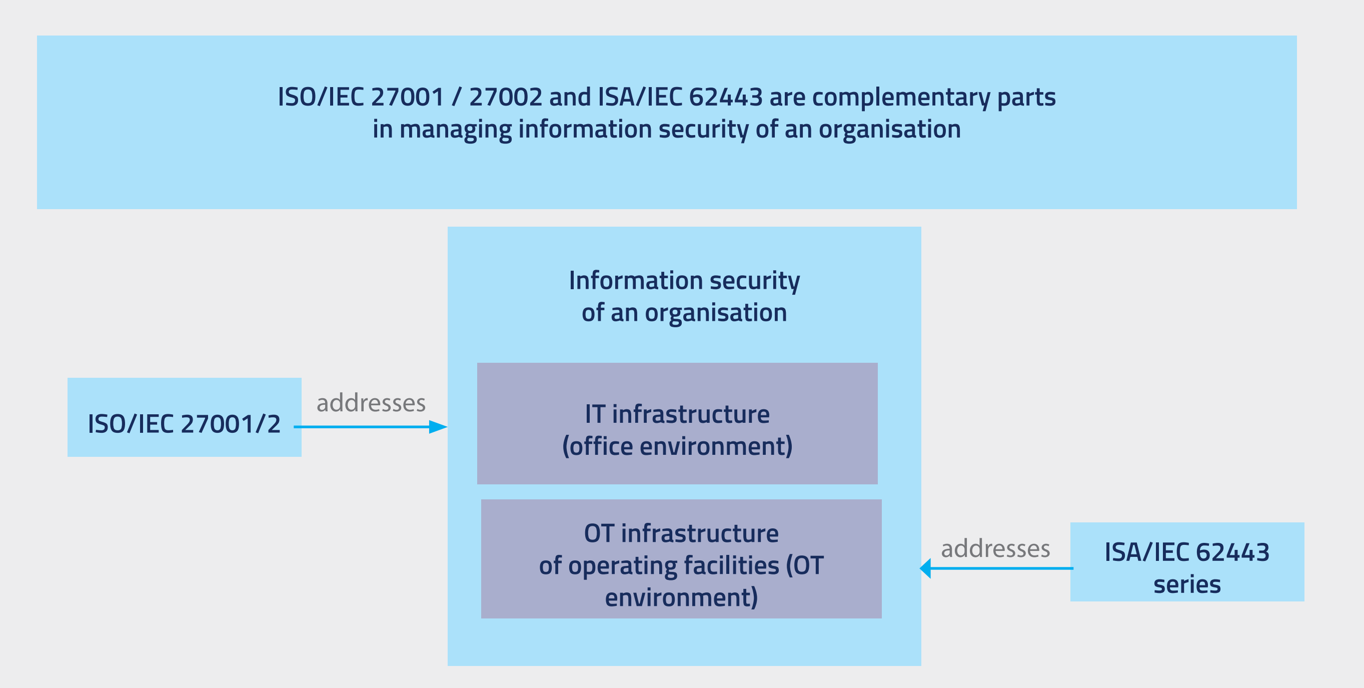
Information Technology

Confidentiality
Integrity
Availability

Top Priority

Industrial Automation and Control Systems

Availability
Integrity
Confidentiality



ISO/IEC 27001 / 27002 and ISA/IEC 62443 are complementary parts in managing information security of an organisation

Information security of an organisation

IT infrastructure (office environment)

OT infrastructure of operating facilities (OT environment)

ISO/IEC 27001/2 addresses

addresses ISA/IEC 62443 series

Source: Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments

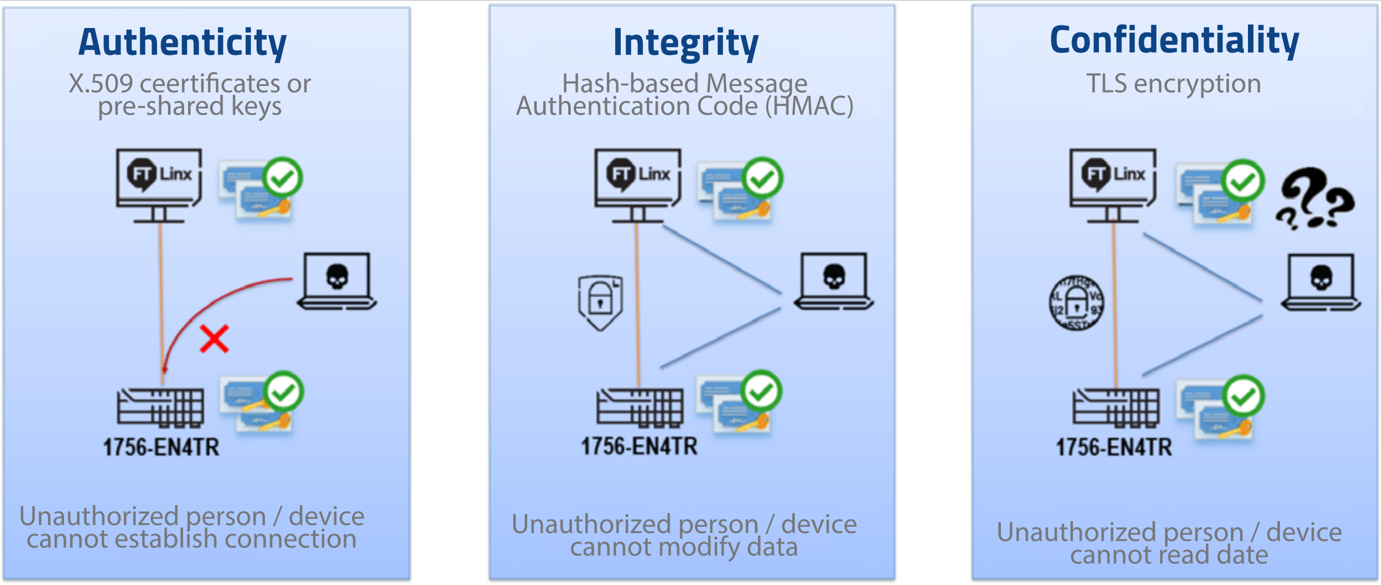
What is the CIP Security protocol?

Common Industrial Protocol (CIP™) Security is an open-standard secure communication protocol developed by ODVA for EtherNet/IP™ communications. CIP Security protocol provides security for industrial control systems that use Ethernet/IP, a communication network based on standard Ethernet and TCP/IP technologies.

CIP Security is designed to meet a significant number of the requirements specified in IEC 62443-4-2, which is a part of the IEC 62443 standard that focuses on the technical security capabilities of devices. CIP Security implements robust and ubiquitous security technologies, such as TLS and DTLS, to achieve protection of the control system device from unauthorized access, modification, or disclosure of data.

Secure ICS Communications

CIP Security protocol helps provide a secure transport for an EtherNet/IP network.


Authenticity
X.509 ceertificates or pre-shared keys
FT Linx
1756-EN4TR
Unauthorized person / device cannot establish connection
Integrity
Hash-based Message Authentication Code (HMAC)
FT Linx
1756-EN4TR
Unauthorized person / device cannot modify data
Confidentiality
TLS encryption
FT Linx
1756-EN4TR
Unauthorized person / device cannot read date

Enables an EtherNet/IP connected to help protect itself from malicious communications

CIP Security maintains availability of a system by preserving authenticity, integrity and confidentiality

CIP Security delivers new capabilities

Secure communications with EtherNet/IP

Authentication - helps prevent unauthorised devices from establishing connections.

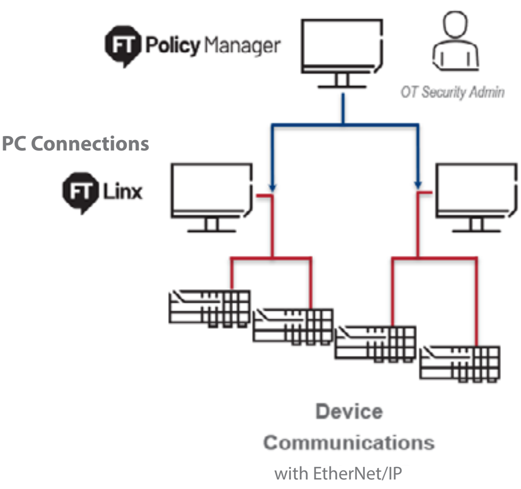
Integrity - helps prevent tampering or modification of communication.

Confidentiality - helps prevent snooping or disclosure of date.

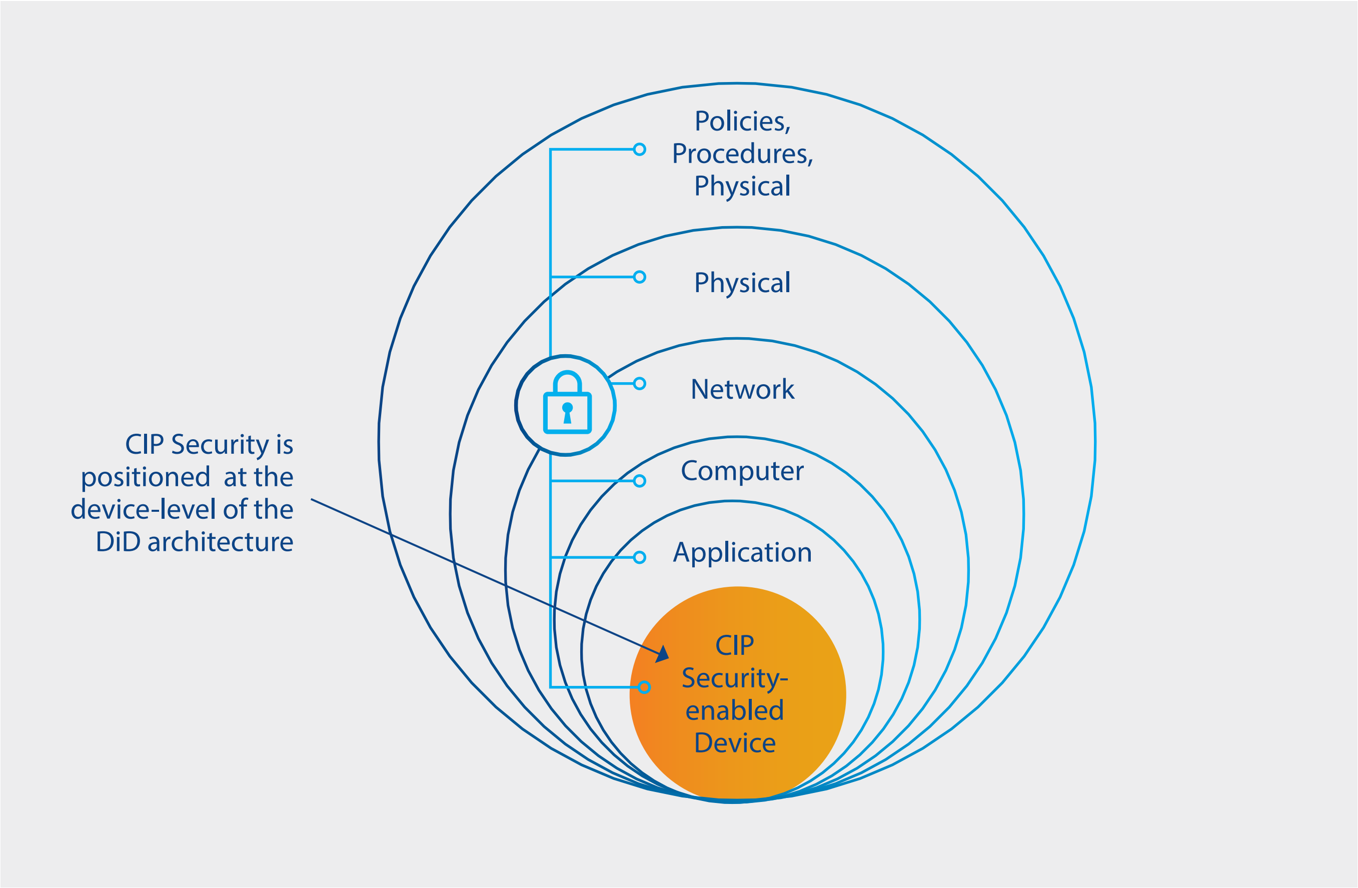
Notable features

- **System management**
  – Easily create and deploy security policies to manay devices, all at once.
- **Micro-segmentation**
  – Segment your automation application into smaller cell/zones.
- **Device-based firewall**
  – Enable/disable available ports/protocols of devices (i.e. / HTTP/NTTPS).
- **Legacy Systems Support**
  – Trusted IP - authorize specific communications based on IP address.
  – Retrofit 1756 based systems with the new 1756-EN4TR.
  – Leverage 1783-CSP proxy device in front of legacy products.

System Components

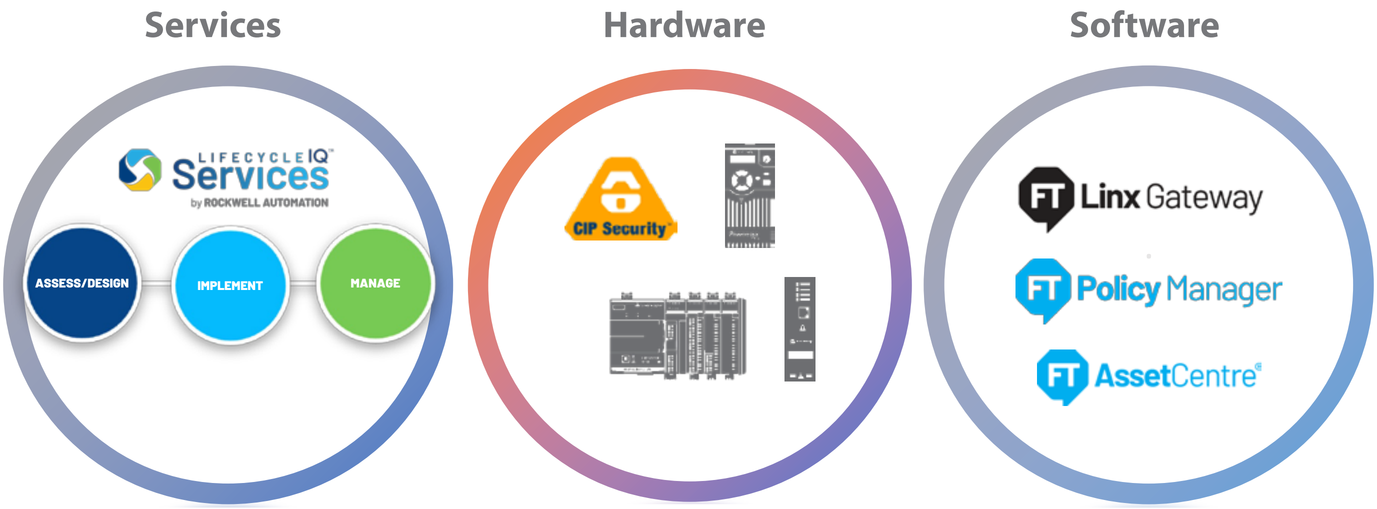


CIP Security as part of Defense in Depth architecture


Policies, Procedures, Physical
Physical
Network
Computer
Application
CIP Security-enabled Device
CIP Security is positioned at the device-level of the DiD architecture

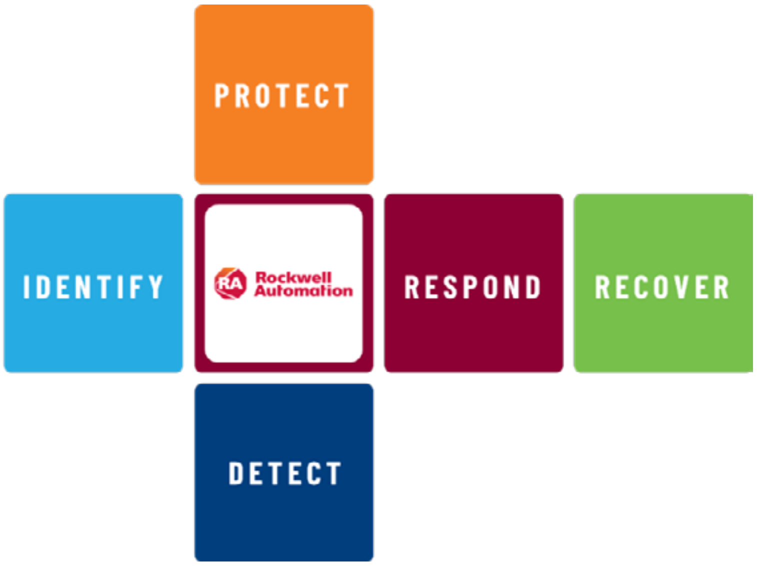
NHP Security portfolio

A complete portfolio aligned and certified with the most robust industry standards and frameworks - ISA/IEC 62443 and National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).



Cybersecurity Services

Has anyone tried to hack your site?
The cybersecurity threat is no longer just an IT concern. NHP's Services and Solutions team service team can help you build a NIST cybersecurity framework strategy to provide resilience into your site network infrastructure, no matter what hardware is installed.



NHP and its teams of partners bring both cybersecurity and IT domain knowledge to provide a solution that proactively discovers your vulnerabilities, misconfigurations, and unsecured network connections. Cybersecurity requires a multiprong approach in identifying threats, all the way to developing a plan on how to recover from an attack.

Email servicenz@nhp-nz.com to discover more on this topic.

Our partner capabilities and offerings aligning to NIST categories

	Capabilities / Offerings	Benefit
Identity	Asset inventory	Understand potential risks and exposures
	Network security assessment	Comprehensive future state logical and physical design blueprint
	Risk assessment	Get a full view of organizational cyber risk to strengthen security posture
	Penetration Testing	Discover vulnerabilities through ethical hacking and then flagging them for ease of attack and difficulty
	Vulnerability assessment	Test industrial security effectiveness & identify external and internal security risks
	Capabilities / Offerings	Benefit
Protect	Network segmentation	Protects the network from attacks moving laterally and improves security risk posture
	Industrial Demilitarized Zone (IDMZ)	Build architecture that separates the IT business systems from OT networks/ICS
	Secure Remote Access	Mitigate stolen credential & insider attacks
	Patch Management	Keep operating systems up to date and secure
	Data Backup & recovery plans	Increase the reliability of your network and reduce downtime
	Trainings and alerts	Reduce human error and insider threats; respond to threats with greater speed
	Capabilities / Offerings	Benefit
Detect	Threat Detection Implementation	Detect threats across networks, assets, and endpoints
	24/7 Managed Threat Detection Services	Quickly detect anomalous behavior to identify potential threats
	24/7 Managed Network and Infrastructure Services	Providing real-time monitoring of OT network infrastructure, data center and asset lifecycle
	Capabilities / Offerings	Benefit
Respond	Incident response, containment & mitigation	Prevent expansion of an event, mitigate its effects, and eradicate the incident
	Coordinated communication plan & execution	Coordinated and effective response activities
	Capabilities / Offerings	Benefit
Recover	Recovery Support	Restore operations to get back up and running quickly, limiting downtime
	Investigation & analysis	More targeted response and recovery activities
	Resilience planning	Refining cybersecurity strategy

Email servicenz@nhp-nz.com to discover more on this topic.

NHP’s offering aligning to NIST Categories

Install Base Evaluations (IBE)

To understand risk from a cybersecurity perspective, it is important to know what is on site. By initiating a site assessment NHP, with the support of Rockwell Automation, NHP will provide information that enables you to make data-driven decisions.

Reduce operational costs

- Lower inventory carrying costs
- Build spares strategies
- Reduce data collection costs

Decrease enterprise risk

- Gain instant visibility into product cybersecurity vulnerabilites
- Asses and mitigate obsolescence risk
- Receive proactive alerts for devices impacted by obsolescence status change and product safety advisories

Improve asset utilisation

- Enhance device availability for critical inventory
- Enable compatibility planning
- Reduce downtime associated with extended device replacements

Network services

The wide adoption of networked devices on the operational level of a site has introduced a host of new challenges. NHP offers a host of network services from network design to network implementation.

A site assessment of all devices connected to the network infrastructure will result in a report that highlights the health of the network infrastructure and the potential security risks. Not knowing what is happening on your network is no longer an option.

Outcomes and Benefits

DECREASE DOWNTIME and improve reliability by modernizing their network infrastructure all at ones (Physical & Logical)

We **BRIDGE THE** customer’s workforce **SKILLS GAP** with ASP network engineers who have the expertise in physical and logical network technology

REDUCE SECURITY RISKS while improving Overall Equipment Effectiveness (OEE)

Contact NHP Service servicenz@nhp-nz.com to discuss a site audit.

Allen Bradley Stratix Industrial Networking switches

Rockwell's partnership with Cisco has resulted in co-developed industrial network switch technology. Stratix switches that offer the Cisco® IOS enable IT and OT team members to efficiently manage their unique aspects of the industrial control system.

Allen-Bradley® Stratix® switches provide a secure switching/routing infrastructure that supports the needs of a wide range of industrial operations.

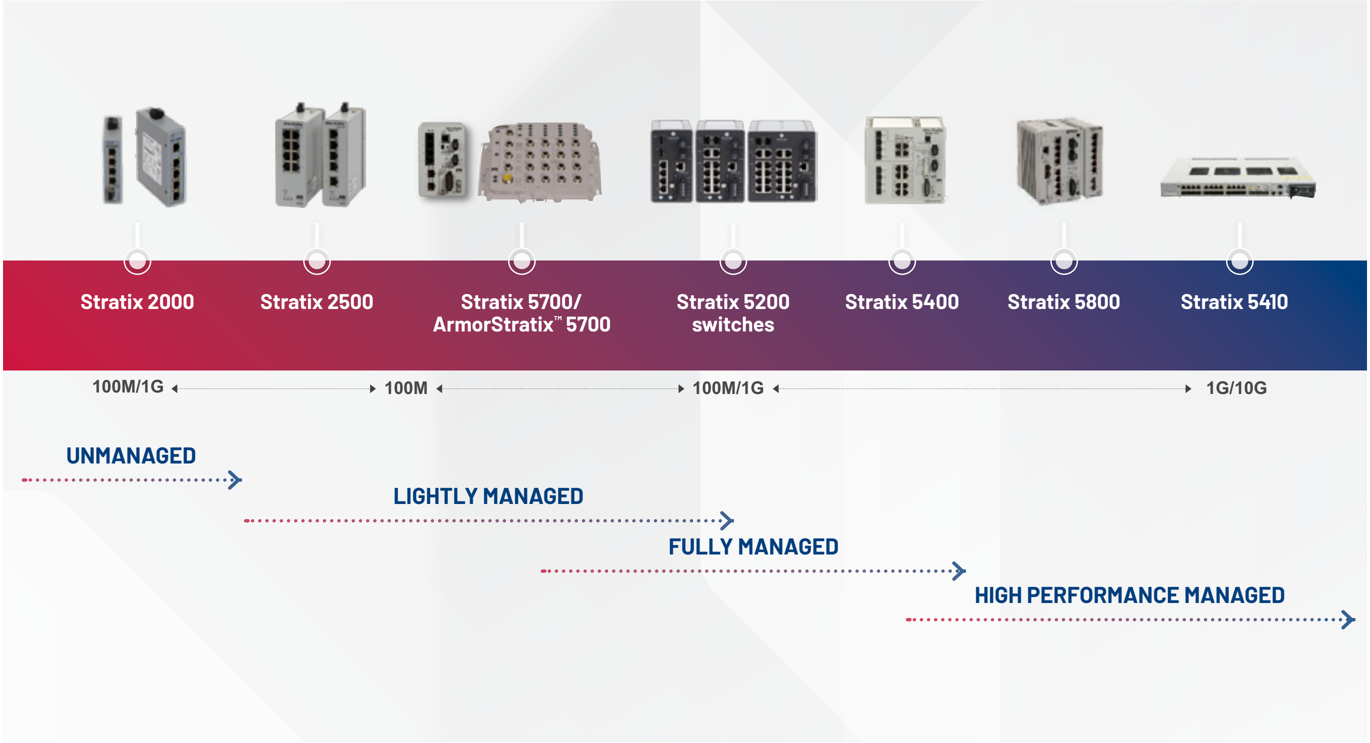
Security capabilities continue to evolve to improve operations and productivity of industrial control systems:

- Visibility features, like integrated NetFlow and RSPAN, work to identify threats in the environment. The ability to detect events on networks allows for faster response and resolution.
- Access control features, like port security, access control lists and integration into Cisco security tools help mitigate the risk of threats to your networked assets. Stratix networks are designed with world-class, market-leading security attributes.
- Enabled IT and OT features provide collaboration with response and recovery from security events that tie into asset management systems and the ability to back up and restore.

Allen-Bradley Stratix switches offer a wide range of design options, which help you meet the evolving needs of IT and OT industrial work environments.

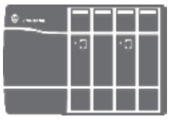
Network switch portfolio overview

Supporting secure network infrastructure for a wide range of industrial applications.

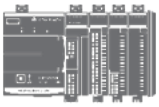


Portfolio of CIP Security enabled devices - Automation Hardware

FT Linx



ControlLogix® 5580
GuardLogix® 5580
1756-EN4TR



CompactLogix™ 5380
Compact GuardLogix® 5380

Kinetix® 5700
Kinetix® 5300

PowerFlex® 755T/S
PowerFlex® 6000T
Armor™ PowerFlex®

CIP Security Proxy

Logix Controllers with CIP Security

	Controller	RSLogix 5000	Studio 5000 Logix Designer				
		V16-V20	V21 - V30	V31	V32	V33	V34
Standard	ControlLogix 5580	N/A	N/A	CIP Security is supported by using either of the following: • A 1756-EN4TR communication module in the • same chassis. • A CIP Security Proxy.(1)	CIP Security is supported by using one of the following: • The controller Ethernet port. • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)		
	ControlLogix 5570	N/A	N/A	CIP Security is supported by using either of the following: • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)			
	ControlLogix 5560	N/A	N/A	N/A	N/A	N/A	N/A
	ControlLogix 5550	N/A	N/A	N/A	N/A	N/A	N/A
	CompactLogix 5380	N/A	N/A	CIP Security is supported by using a CIP Security Proxy. (1)			CIP Security is supported by using one of the following: • The controller Ethernet port. • A CIP Security Proxy.(1)
	CompactLogix 5370	N/A	N/A	CIP Security is supported by using a CIP Security Proxy. (1)			
	CompactLogix 5480	N/A	N/A	N/A	N/A	N/A	N/A
	1768 CompactLogix	N/A	N/A	N/A	N/A	N/A	N/A
	1769 CompactLogix	N/A	N/A	N/A	N/A	N/A	N/A
	SLC Controllers (All)	N/A	N/A	N/A	N/A	N/A	N/A

Logix Controllers with CIP Security

	Controller	RSLogix 5000	Studio 5000 Logix Designer				
		V16-V20	V21 - V30	V31	V32	V33	V34
Safety	GuardLogix 5580	N/A	N/A	CIP Security is supported by using either of the following: • A 1756-EN4TR communication module in the • same chassis. • A CIP Security Proxy.(1)	CIP Security is supported by using one of the following: • The controller Ethernet port. • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)		
	GuardLogix 5570	N/A	N/A	CIP Security is supported by using either of the following: • A 1756-EN4TR communication module in the same chassis. • A CIP Security Proxy.(1)			
	GuardLogix 5560	N/A	N/A	N/A	N/A	N/A	N/A
	Compact GuardLogix 5380 SIL2	N/A	N/A	CIP Security is supported by using a CIP Security Proxy. (1)			CIP Security is supported by using one of the following: • The controller Ethernet port. • A CIP Security Proxy.(1)
	Compact GuardLogix 5370	N/A	N/A		CIP Security is supported by using a CIP Security Proxy. (1)		
	1768 Compact GuardLogix	N/A	N/A	N/A	N/A	N/A	N/A
Redundancy	ControlLogix 5580 Redundancy	N/A	N/A	N/A	N/A	CIP Security is supported by using a single CIP Security Proxy through an Ethernet switch to 1756-EN2x communication modules in a redundant chassis pair. (1)	CIP Security is supported by using one of the following: • A single CIP Security Proxy through an Ethernet switch to • 1756-EN2x EtherNet/IP communication modules in a redundant chassis pair. (1) • A pair of 1756-EN4TR communication modules, firmware revision 4.001 or later. (2)
	ControlLogix 5570 Redundancy	N/A	N/A	CIP Security is supported by using a single CIP Security Proxy through an Ethernet switch to 1756-EN2x EtherNet/IP communication modules in a redundant chassis pair.(1)			

Other devices with CIP Security

Device	Firmware Revision
1756-EN4TR EtherNet/IP communication module	Any
Armor™ PowerFlex® drives	10.001 or later
PowerFlex® 755T drives	10.001 or later
PowerFlex 755TS drives	11.001 or later
Kinetix® 5300 drives	13.003 or later
Kinetix 5700 drives	11.001 or later
1783-CSP CIP Security Proxy	Any
Proxied devices that have been tested with the 1783-CSP CIP Security Proxy	For information on the devices that have been tested with a CIP Security Proxy and can be used in a system with CIP Security implemented, see the CIP Security Proxy User Manual, publication 1783-UM013 click here

(1) IMPORTANT: This is only for workstation programming, upload/download, and data collection, not for I/O.
For more information, see the CIP Security Proxy User Manual, publication 1783UM013.
(2) IMPORTANT: This is only for workstation programming, upload/download, and data collection, not for I/O.
For more information, see the High Availability Systems Reference Manual, publication HIGHAV-RM002

Stratus - Edge computing solutions

Minimising your Cyber Security risk from Edge to Enterprise

Cyber threats can come from anywhere. Although sometimes they come from the top down, we have seen many cyber intrusions begin at the edge. For this reason it is important to have layers of defence that can identify and react at the source without communication latency impacts. The edge often times can be your first level of defence and isolation before an attacker finds a way to spread out across your entire infrastructure.

ftServer

ztC Edge server

The need for compute and protection at the Edge

- Latency agnostic
- Allow threats to be detected and blocked quickly – seconds matter to act.
- It is critical to have an appliance that can detect and respond at the edge even if a connection to the enterprise is severed.

Why Stratus?

- Consolidation/virtualisation of Automation and Cyber applications at the Edge mandating resilient compute.
- Protect the Rockwell Automation / CrowdStrike Proxy ensuring continuous connection from Endpoints to the CrowdStrike Cloud and Cyber Security Operations Center
- Eliminate deployment complexity eg Claroty SRA and redundancy.
- Sized and tested.

Software Solutions

FactoryTalk Policy Manager

Use FactoryTalk® Policy Manager to configure, deploy and view the system communication security policies. FactoryTalk Policy Manager divides the system security policy into different components:

- Zones - groups of devices
- Devices - computers, controllers, modules, HMI panels and drives
- Conduits - communication routes between components.

Use these components to design security models that control the permissions and usage of devices within the system.

FactoryTalk Policy Manager Getting Results Guide

FactoryTalk Linx

FactoryTalk® Linx is the most modern, secure, best performing and preferred communications platform for integrated architecture. Our premier communication platform software provides one access point to your data, allowing both FactoryTalk and third-party software shared access to control equipment.

Discover: FactoryTalk Linx | FactoryTalk

FactoryTalk Security

FactoryTalk Security improves the security of your automation system by limiting access to those with a legitimate need. FactoryTalk Security authenticates the identities of users, and authorizes user requests to access a FactoryTalk system against a set of defined user accounts and access permissions held in the FactoryTalk local directory or FactoryTalk local directory.

FactoryTalk Security System Configuration Guide (rockwellautomation.com)

FactoryTalk AssetCentre

FactoryTalk® AssetCentre monitors your factory automation system, provides centralised tools to minimise downtime due to unauthorised actions or failing devices, and manages the life cycle of Rockwell Automation hardware devices in the system. It does this by:

- Securing access to actions within the FactoryTalk AssetCentre system.
- Managing device configuration files.
- Providing a disaster recovery system that verifies your devices' program and configuration files against protected master files, ensuring quick and accurate recovery if a problem should occur.
- Monitoring FactoryTalk-enabled software products and logging system events and user actions (recorded in the event log and audit log respectively).
- Providing version control and archiving of program files and documents.
- Synchronising life-cycle information in the FactoryTalk AssetCentre server and client with the data on the Rockwell Automation life cycle website.

FactoryTalk AssetCentre | FactoryTalk (rockwellautomation.com)

Thinmanager

Rockwell Automation ThinManager is a software solution that provides a safe and secure environment for end device management and content delivery in industrial settings.

It is purpose-built to mitigate the risks associated with devices and enterprise-level networks into industrial control environments by providing a platform to deliver content to end devices such as mobile devices or zero clients without the need to locally host applications or data on any of those end devices or terminals when used together with ThinManager Ready or ThinManager Compatable devices.

Thin Client Management Software | FactoryTalk (rockwellautomation.com)

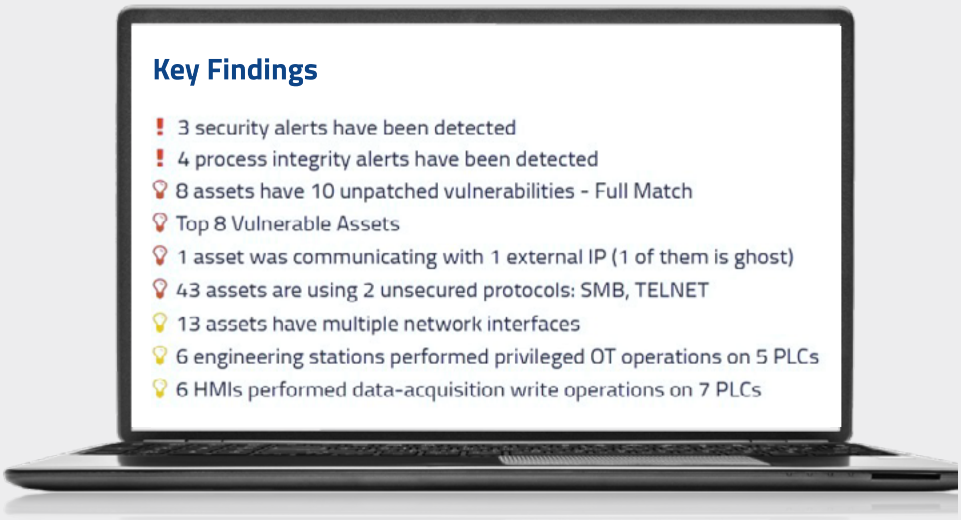
Claroty

Continuous Threat Detection with Alert and Risk Management.Detect threats across networks, assets, and endpoints, Improve your visibility into OT networks by monitoring network traffic and system logs. This can help security personnel to better understand the OT environment and identify potential threats.

Claroty helps to prioritize threats, so that security personnel can focus on the most critical ones. This can help to reduce the amount of time and resources that are wasted on investigating false positives

- Correlate known and proprietary common threats, abnormal behaviors vulnerabilities and exposures (CVE) with asset inventory.
- Prioritize patches and compensating controls based on VCVE classification and asset function
- Secure Remote Access

Network-based threat / Vulnerability assessment and mitigation



Key Findings

! 3 security alerts have been detected
! 4 process integrity alerts have been detected
💡 8 assets have 10 unpatched vulnerabilities - Full Match
💡 Top 8 Vulnerable Assets
💡 1 asset was communicating with 1 external IP (1 of them is ghost)
💡 43 assets are using 2 unsecured protocols: SMB, TELNET
💡 13 assets have multiple network interfaces
💡 6 engineering stations performed privileged OT operations on 5 PLCs
💡 6 HMIs performed data-acquisition write operations on 7 PLCs

Rockwell Automation and Claroty:
Comprehensive OT Cybersecurity | Rockwell Automation

Additional Resources

- Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments.
- Safeguarding Australia and New Zealand's Industrial Systems. (Whitepaper)
- Anatomy of 100+ Cybersecurity Incidents in Industrial Operations. (Whitepaper)
- Importance of OT Cybersecurity (Whitepaper)
- Understanding CIP Security (Video)
- OT Cybersecurity Quick Assessment (Tool)
- CIP Security with Rockwell Automation Products (Manual)
- The NIST Cybersecurity Framework
- ISA/IEC 62443 Standard
- ISO/IEC 27001/2 Standard

nhpnz.co.nz
SALES 0800 647 647
sales@nhp-nz.com

NHP ELECTRICAL ENGINEERING PRODUCTS

A.B.N. 84 004 304 812

67BCH 07/24