



ENGINEER
NEXT

VIP2017

The logo features the words "ENGINEER" and "NEXT" in a bold, white, sans-serif font, stacked vertically. A yellow graphic element, resembling a stylized 'X' or a folded ribbon, is positioned between the two words. To the left of the word "NEXT", the text "VIP2017" is enclosed within a white rectangular border. The entire logo is set against a blue background with diagonal stripes in various shades of blue, orange, and green.




Assessing Security for NI Linux Real-Time Using the NIST Cybersecurity Framework

National Instruments
Application Engineering Specialist
Stefan Egeler

Agenda

- Security is Everyone's Matter
 - Security is a Continuum
 - Security is Collective Effort
 - Security is About Doing
-
- Security Management Using NIST CSF
 - Security Decisions for NILRT Using NIST CSF
-
- Conclusion
 - Outlook
 - Key Resources

Security is Everyone's Matter



Zombie Computing	<ul style="list-style-type: none">• Hazard: Enhances system load• Hazard: Be part of sabotage• i.e.: Dyn servers down in 2016
Industrial Espionage	<ul style="list-style-type: none">• Hazard: Theft of sensitive data• i.e.: Trojans• i.e.: OpenSSL Heartbleed
Sabotage	<ul style="list-style-type: none">• Hazard: Data or function loss• i.e.: Get attacked by a botnet• i.e.: Ransomware

Security is a Continuum

Standardized attacks like WannaCry typically use multiple old vulnerabilities

Vulnerability exploit reaches 95 % after 60 days

„Of course I will get into every system. Security is about how long it takes.“
- A corporate pentester

Security is a Continuum

Standardized attacks like WannaCry typically use multiple old vulnerabilities

Vulnerability exploit reaches 95 % after 60 days

„Of course I will get into every system. Security is about how long it takes.“
- A corporate pentester



Security is a Continuum

Standardized attacks like WannaCry typically use multiple old vulnerabilities

Vulnerability exploit reaches 95 % after 60 days

„Never change a running system“

„Of course I will get into every system. Security is about how long it takes.“
- A corporate pentester

Security is Collective Effort

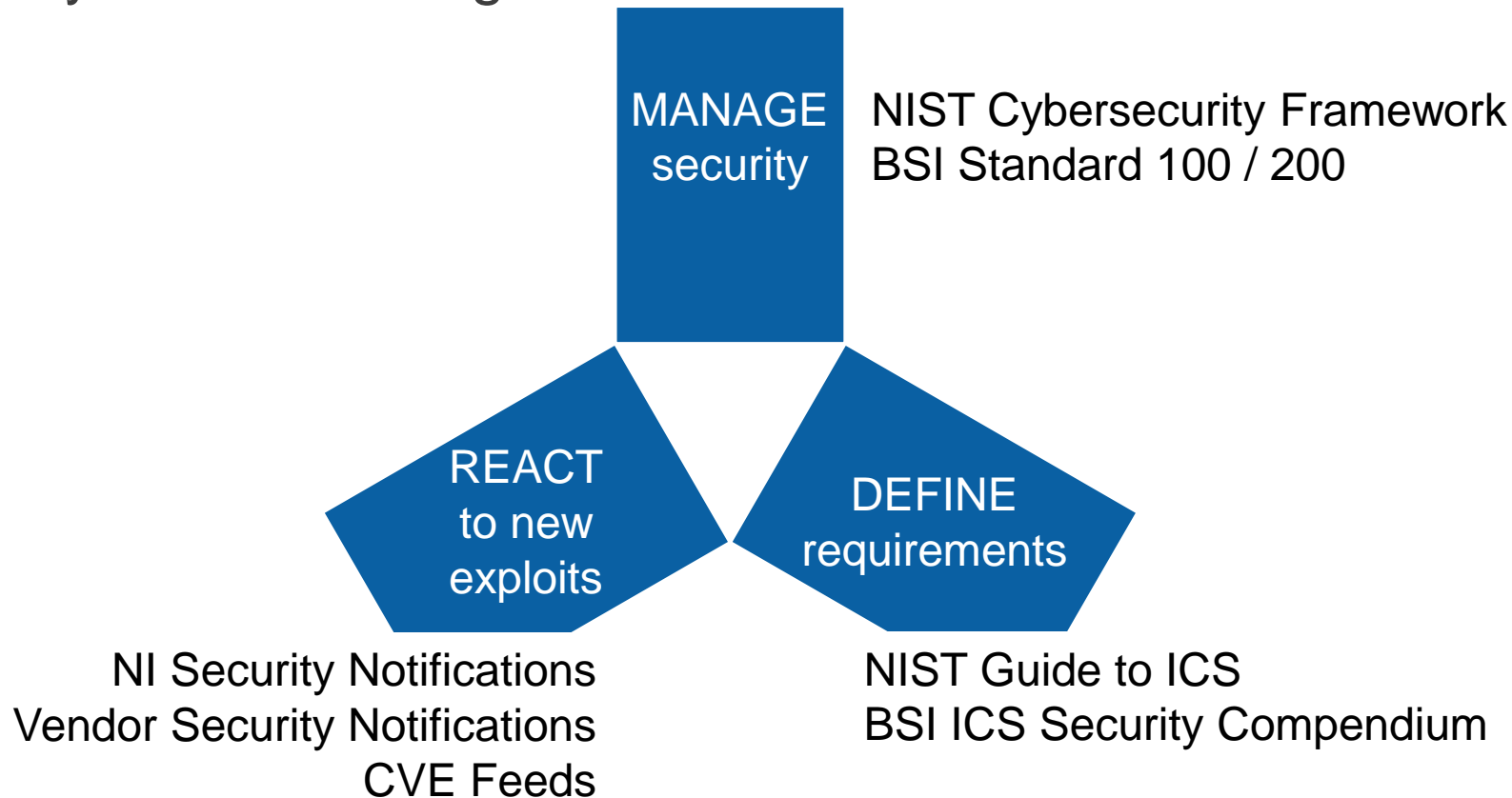
Start knowing
ni.com/security

Get NI consulting
(Contact NI Sales)

Reach out to the
community
ni.com/linuxrtforum

Get IT consulting
(Consider your IT & big
players like Tresys)

Security is About Doing



Security Management Using NIST CSF

Function	
Identify	What processes and assets need protection?
Protect	What safeguards are available?
Detect	What techniques can identify incidents?
Respond	What techniques can contain impacts on incidents?
Recover	What techniques can restore capabilities?

Security Management Using NIST CSF

Function	Categories	Subcategories	References
Identify (ID)	ID.AM Asset Management	ID.AM-2: Software platforms and applications within the organization are inventoried	
Protect (PR)			
Detect (DE)			
Respond (RS)			
Recover (RC)			

Security Decisions for NILRT Using NIST CSF

Function			
Identify	ID.AM Asset Management		
	ID.AM-2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none">■ List Linux software<ul style="list-style-type: none">▪ Use <code>opkg list</code> via PuTTY▪ PuTTY and <code>opkg</code> are explained in NI Linux Real-Time User Guide	User Guide
		<ul style="list-style-type: none">■ List NI software<ul style="list-style-type: none">▪ Get a MAX Report▪ Includes installed NI SW and SW version▪ Also documents firmware and kernel version	NI MAX
		<ul style="list-style-type: none">■ List your software<ul style="list-style-type: none">▪ Use source code control, i.e. SVN or Git▪ Create a tag for every release	Web

Security Decisions for NILRT Using NIST CSF

Function				
Identify				
Protect	PR.AC Access Control			
	PR.AC-1	Identities and credentials are managed for authorized devices and users	■ Set admin pw	User Guide
	PR.AC-2	Physical access to assets is managed and protected	■ Lead seals or locks	
	PR.AC-3	Remote access is managed	■ VPN	Consulting
	PR.AC-4	Access permissions are managed, incorporating the principles of least privilege and separation of duties	■ SELinux	Consulting
	PR.AC-5	Network integrity is protected, incorporating network segregation where appropriate	■ Firewall ■ VPN	User Guide Consulting







Security Decisions for NILRT Using NIST CSF

Function				
Identify				
Protect	PR.DS Data Security			
	PR.DS-1	Data-at-rest is protected	 Access Control  Cryptography  Firewall  Integrity Checking	Guide / Cons Web User Guide Guide / Web
	PR.DS-2	Data-in-transit is protected	 Cryptography  Firewall  VPN	Web User Guide Consulting








Security Decisions for NILRT Using NIST CSF

Function				
Identify				
Protect	PR.PT Protective Tech			
	PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	<div>■ Linux Logs</div> <div>■ SW Logs</div>	Web
	PR.PT-2	Removable media is protected and its use restricted according to policy	<div>■ Disable USB</div>	Web
	PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	<div>■ Access Control</div> <div>■ Physical Control</div>	Guide / Cons
	PR.PT-4	Communications and control networks are protected	<div>■ Firewall</div> <div>■ VPN</div>	User Guide Consulting

Security Decisions for NILRT Using NIST CSF

Function				
Identify				
Protect				
Detect	DE.CM Continuous Mon			
	DE.CM-1	The network is monitored to detect potential cybersecurity events	 Firewall  Intrusion Detection	Guide / Web Web / Cons
	DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	 Surveillance	
	DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	 Access Control  Intrusion Detection  Surveillance	Guide / Cons Web / Cons

Security Decisions for NILRT Using NIST CSF

Function				
Identify				
Protect				
Detect	DE.CM Continuous Mon			
	DE.CM-4	Malicious code is detected	 Virus Scanner	Web
	DE.CM-5	Unauthorized mobile code is detected	 Integrity Checking  Intrusion Detection  Virus Scanner	Guide / Web Web / Cons Web
	DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	 Access Control  Integrity Checking  Intrusion Detection	Web / Cons Web / Cons Consulting

Security Decisions for NILRT Using NIST CSF

Function	
Identify	
Protect	RS.MI-1 Incidents are contained
Detect	RS.MI-2 Incidents are mitigated
Respond	RS.MI Mitigation

Access Control
Cryptography
Firewall
Intrusion Prev
Virus Scanner

Guide / Cons
Web
User Guide
Consulting
Web

Security Decisions for NILRT Using NIST CSF

Function			
Identify	RC.RP-1: Recovery plan is executed during or after an event	■ Standalone: Replication and Development (RAD) Utility	NI Web
Protect		■ Automatized replication via LabVIEW: nisyscfg.lvlib	NI Help
Detect		■ Rescue data using a live CD, i.e. <ul style="list-style-type: none">▪ Gparted▪ System Rescue CD▪ Ubuntu	Web
Respond		■ In case of not-recoverable OS contact NI Support	NI Support
Recover		RC.RP Recovery Planning	

Conclusion

- The IIoT forces ICS developers to address cybersecurity
- A scalable framework like the NIST Cybersecurity Framework helps assessing the right amount of effort
- NI Linux Real-Time enables you to implement state-of-the-art security features

Outlook

- “Never change a running system” versus cybersecurity
- Understanding the consequences of general, intermediate, and extreme security implementations
- Creating a toolchain that is security-aware

Key Resources

- ni.com/security
 - NI Linux Real-Time Security User Guide
 - Security Updates
- ni.com/linuxrtforum
 - Tutorials & documentation
 - NI-attended discussion forum
- <https://www.nist.gov/cyberframework>
 - Manage Security with the CSF

NI LINUX REAL-TIME SECURITY USER GUIDE

OVERVIEW AND TUTORIAL

Summary

NI Linux Real-Time is a publicly available Linux operating system that is used across various National Instruments real-time systems.

This document is a guide for engineers working with products based on NI Linux Real-Time. It is intended to help you

NI Linux Real-Time Latest Activity: 4 hours ago

Overview Members (258) Discussions (143) Documents (24) Blog Polls

Welcome to the NI Linux Real-Time Community!

If you are new to NI Linux Real-Time, please read our [Introduction](#) and our [FAQ](#). Keep pace with the improvements we are making by checking the [Feature Updates and Changelog](#) for NI Linux Real-Time.

To take take advantage of the new NI-hosted package repository, upgrade your NI Linux Real-Time supported device to LabVIEW 2014.

Visit [OPKG Package Manager](#) at the OpenWrt Wiki for information on how to manage packages on your device. To obtain the source code for the NI Linux Real-Time distribution, visit github.com/ni.

To learn more about using C/C++, visit [C/C++ Embedded System Design Tools](#).

NIST

CYBERSECURITY FRAMEWORK

Recognizing that the national and economic security of the United States depends on the functioning of critical infrastructure

Cybersecurity Framework (PDF)

Cybersecurity Framework (Excel)

Latest Updates

- The NIST Cybersecurity Framework [Manufacturing Profile](#) was published. It provides Framework implementation details developed for the manufacturing sector.

Stay Connected During and After VIPDays



ni.com/niweekcommunity



facebook.com/NationalInstruments



twitter.com/niglobal



youtube.com/nationalinstruments