
ENGINEER
NEXT
VIP2017


NATIONAL
INSTRUMENTS™

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

National Instruments

Application Engineering Specialist

Stefan Egeler

NATIONAL INSTRUMENTS

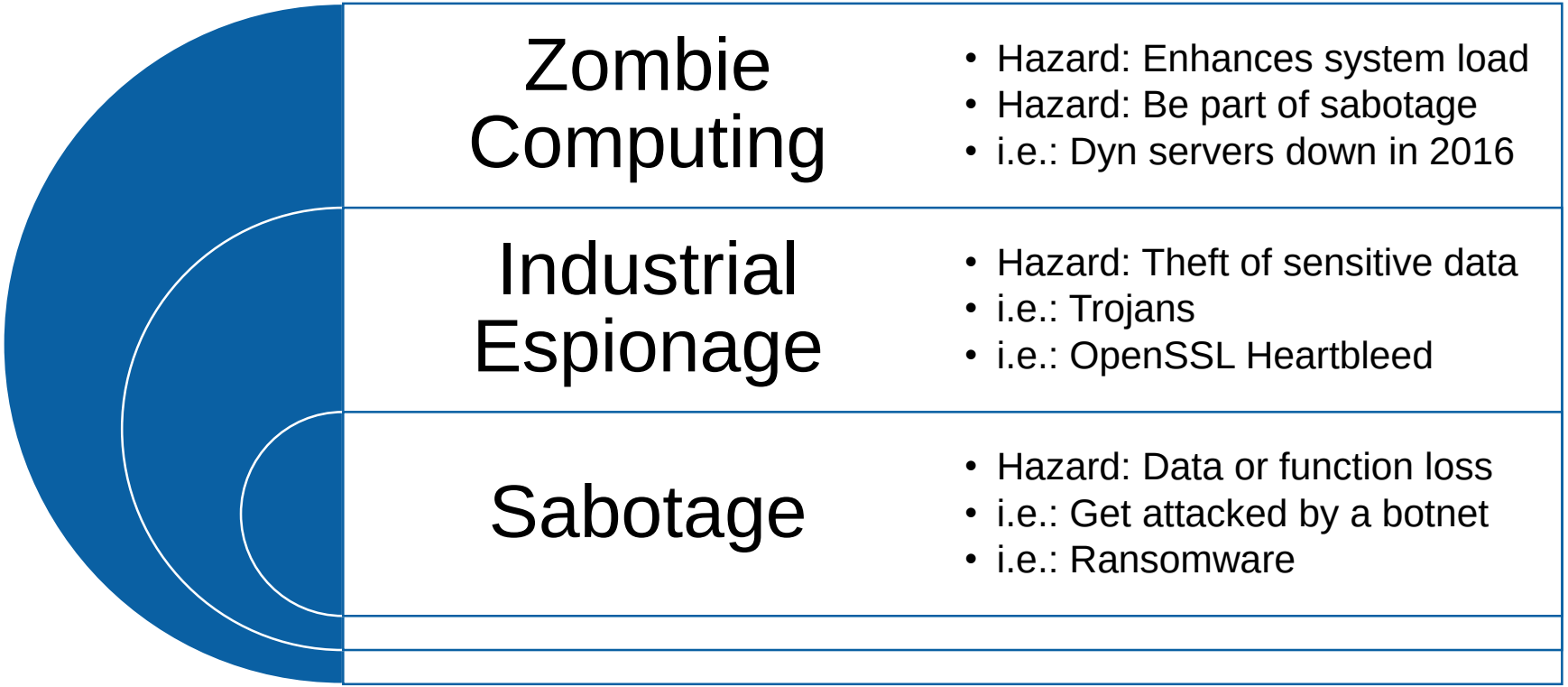
Agenda

- Security is Everyone‘s Matter
- Security is a Continuum
- Security is Collective Effort
- Security is About Doing

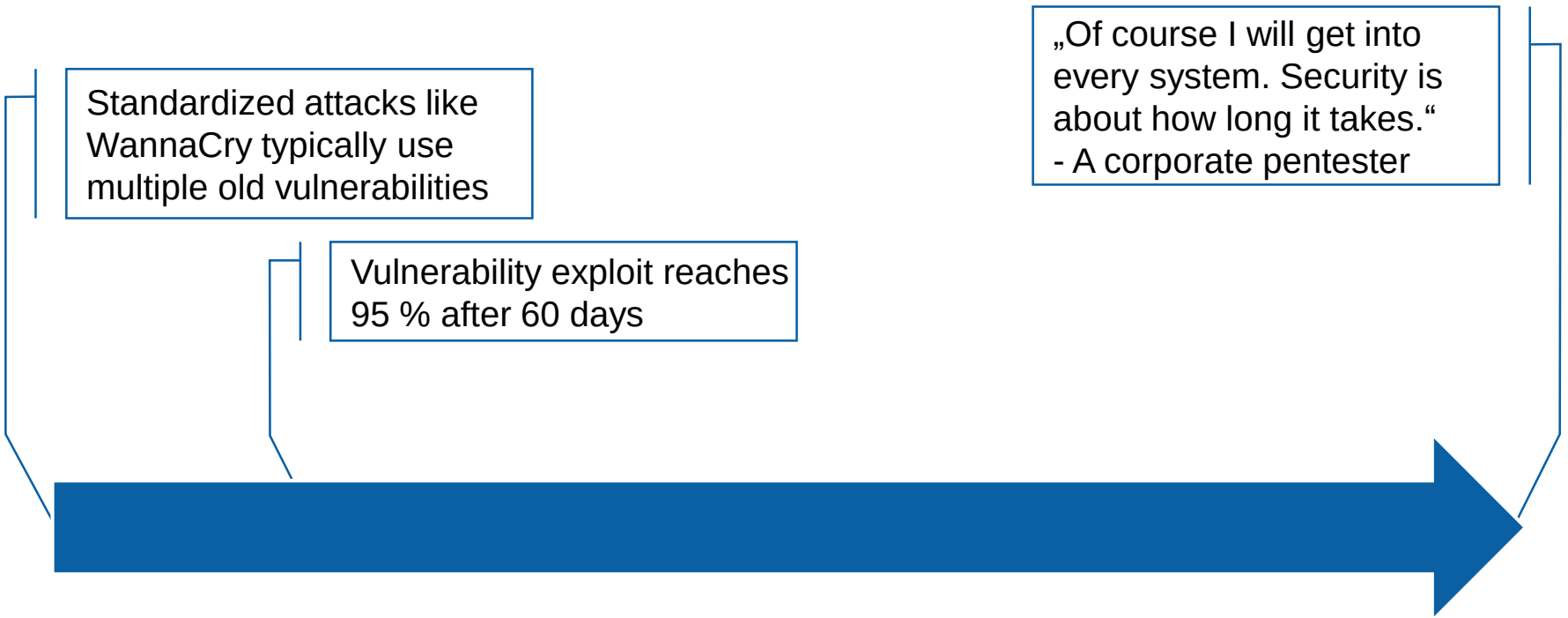
- Security Management Using NIST CSF
- Security Decisions for NILRT Using NIST CSF

- Conclusion
- Outlook
- Key Resources

Security is Everyone‘s Matter



Security is a Continuum



Security is a Continuum

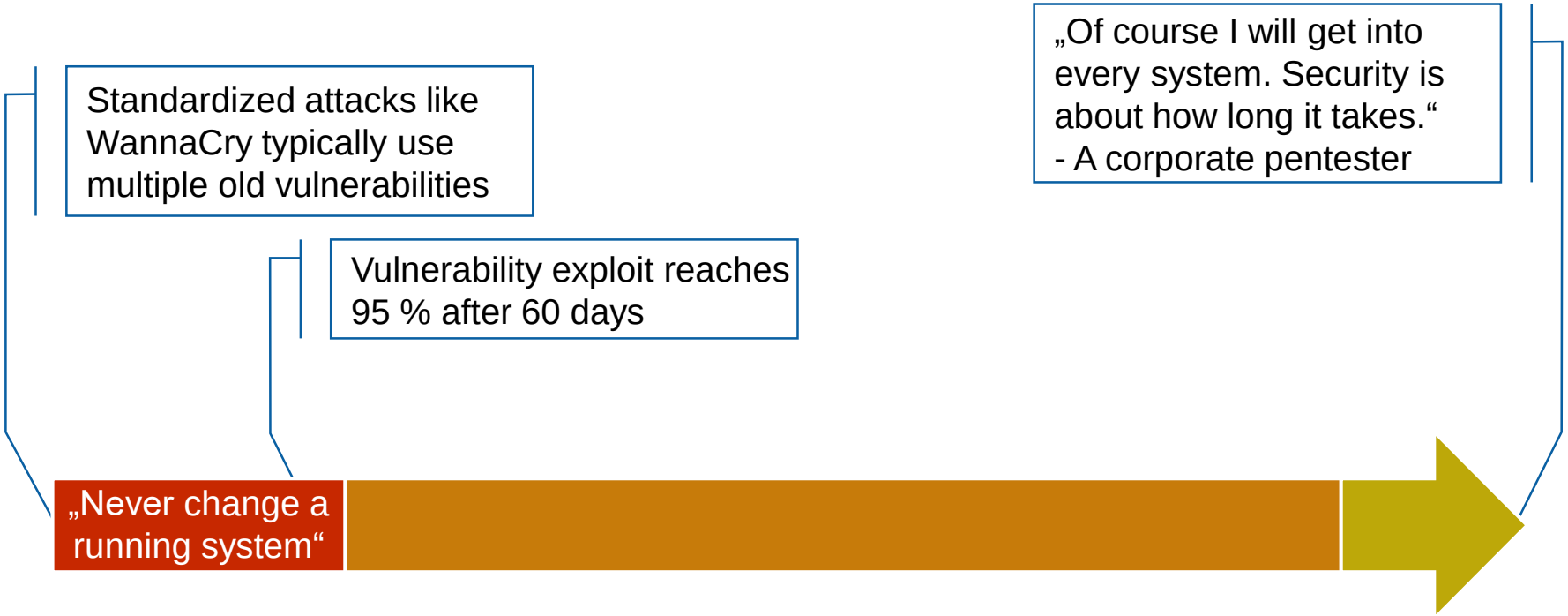
Standardized attacks like WannaCry typically use multiple old vulnerabilities

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

NATIONAL INSTRUMENTS

Security is a Continuum



NATIONAL INSTRUMENTS

Security is Collective Effort

Start knowing

ni.com/security

Get NI consulting

(Contact NI Sales)

Reach out to the community

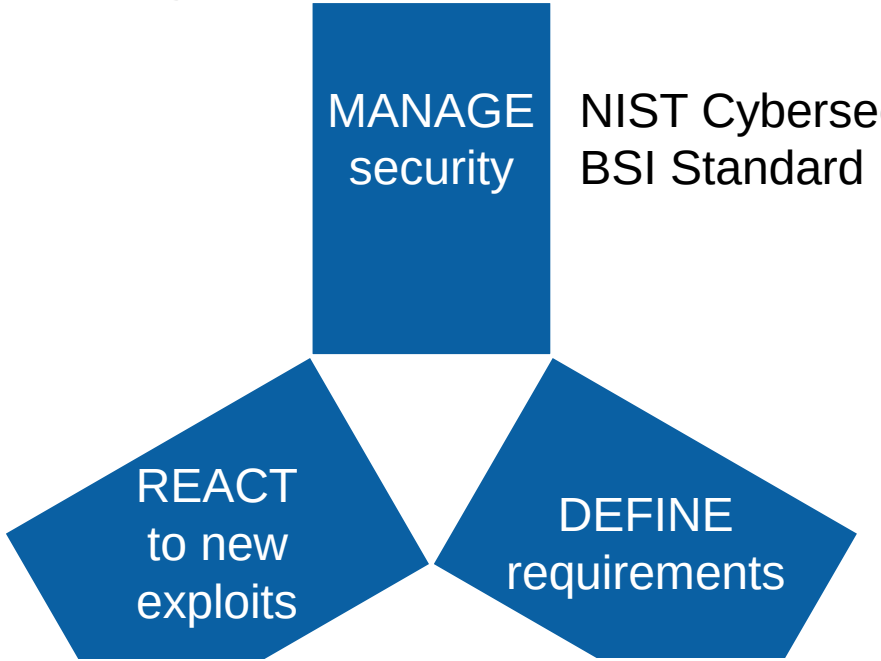
ni.com/linuxrtforum

Get IT consulting

(Consider your IT & big players like Tresys)

NATIONAL INSTRUMENTS

Security is About Doing



NIST Cybersecurity Framework
BSI Standard 100 / 200

NI Security Notifications
Vendor Security Notifications
CVE Feeds

NIST Guide to ICS
BSI ICS Security Compendium

NATIONAL INSTRUMENTS

Security Management Using NIST CSF

NATIONAL INSTRUMENTS

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)			

NATIONAL INSTRUMENTS

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	List Linux software ▪ Use `opkg list` via PuTTY ▪ PuTTY and opkg are explained in NI Linux Real-Time User Guide	User Guide
		List NI software ▪ Get a MAX Report ▪ Includes installed NI SW and SW version ▪ Also documents firmware and kernel version	NI MAX
		List your software ▪ Use source code control, i.e. SVN or Git ▪ Create a tag for every release	Web

NATIONAL INSTRUMENTS

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

NATIONAL INSTRUMENTS

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

NATIONAL INSTRUMENTS

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	Linux Logs SW Logs	Web
	PR.PT-2	Removable media is protected and its use restricted according to policy	Disable USB	Web
	PR.PT-3	Access to systems and assets is controlled, incorporating the principle of least functionality	Access Control Physical Control	Guide / Cons
	PR.PT-4	Communications and control networks are protected	Firewall VPN	User Guide Consulting

NATIONAL INSTRUMENTS

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

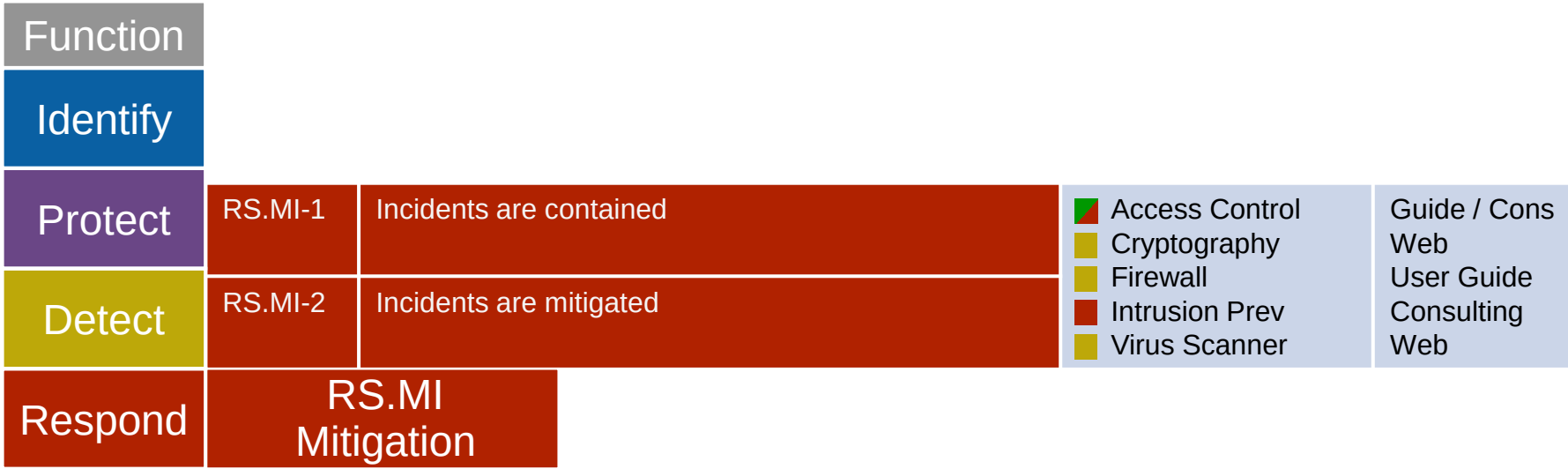
NATIONAL INSTRUMENTS

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

NATIONAL INSTRUMENTS

Security Decisions for NILRT Using NIST CSF



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. ▪ Gparted ▪ System Rescue CD ▪ Ubuntu	Web
Respond		In case of not-recoverable OS contact NI Support	NI Support
Recover	RC.RP Recovery Planning		

NATIONAL INSTRUMENTS

Conclusion

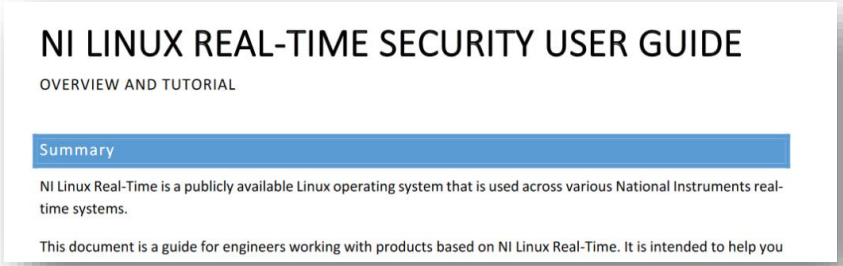
- The IIoT forces ICS developers to address cybersecurity
- A scalable framework like the NIST Cybersecurity Framework helps assessing the right amount of effort
- NI Linux Real-Time enables you to implement state-of-the-art security features

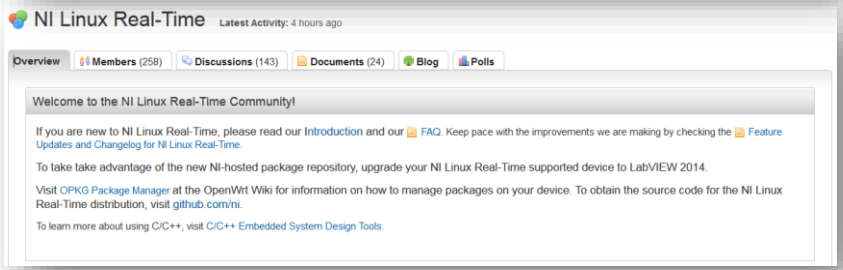
Outlook

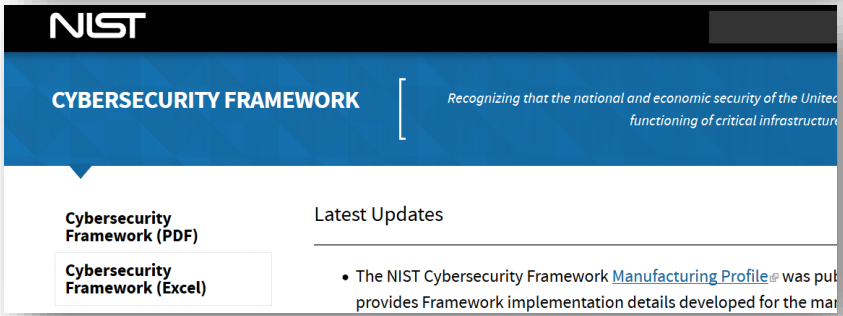
- “Never change a running system” versus cybersecurity
- Understanding the consequences of general, intermediate, and extreme security implementations
- Creating a toolchain that is security-aware

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







NATIONAL INSTRUMENTS

Stay Connected During and After VIPDays

ni.com/niweekcommunity

facebook.com/NationalInstruments

twitter.com/niglobal

youtube.com/nationalinstruments