Training Title	Practical hardening & testing for ICS environments
Abstract	Hardening is one of the various ways to protect your systems and environment from attacks. Being it remote or insider threats that you are protecting against. However, with the ever-increasing connectivity between different IT and industrial environments for data transfer to the business, for remote access or for integration between different industrial environments these systems and environments are more and more exposed to several threats. Therefore, additional protective measures need to be deployed to these systems and environments. Next to patching and the like, hardening is a way or reducing risks for the environment, but it takes a well-thought approach and actions to be performed. Hardening is not only part of the security best practices but is also (lightly) enforced through policies and standards. That is why the links and references towards the IEC62443 are going to be highlighted in the training. This training will give the student insights on the various aspects of a hardening process, the ins and outs of hardening will be explained, how to perform hardening, why the concerned hardening settings are important and what to strengthen to reduce potential attack vectors. Potential consequences of the taken hardening steps will be explained and students will be guided towards creating a (basic) hardening script and system policies to assist in doing the actual hardening for similar systems within their environments. The potential pitfalls you might run into while performing hardening of standalone or domain-joined systems will be explained as well. The training covers operating systems such as Windows 10/11 and Windows Server (as it is the most used operating system to provide Human Machine Interfaces to operators) but also Linux elements, network components security and industrial control system devices will be explained. Attendees will understand after the training how to verify hardening using common security tools and will understand what steps are to be taken for the hardening of systems and environments. Through real-world scenario-based exercises, attendees will get a thorough understanding of what can and should be done to protect their industrial environments.
Speaker	Dieter Sarrazyn
Contact Information	dieter@secudea.be +32 476 87 85 37
Twitter	@dietersar (https://twitter.com/dietersar)
LinkedIn	https://www.linkedin.com/in/dietersarrazyn/
Bio	Dieter has experience as practitioner, mentor, and trainer in several areas of cyber security. His work includes positions where he performed and/or security assessment projects and SCADA/ICS security projects such as penetration testing, risk assessments, assistance in securing these environments and providing training and awareness sessions. He helps customers managing security of deployed solutions security requirements management and performing security FAT/SAT tests.
Delivery	Training – 2 days
Delivery Format	In Person only
Delivery location(s)	**1. At a conference or public training event**: These will be announced on the training page (https://secudea.be/training) – registration will be handled by the conference/event organizer **2. Private training**: If you prefer to take our class in a more intimate setting, we can also bring our training to your offices. Contact me for more information about our private training offerings.
Knowledge requirements	Novice - Intermediate

Training Requirements	Training attendees should bring a laptop with a **working** virtualisation software installed (any is good, preferably VMWare), Required virtual machines (all of these are necessary): - default installation of Windows 10 or 11 - default installation of Windows 2019 server - default installation of Ubuntu LTS (last version available)

Covered topics	• Hardening explained
	  ○ Strategy
	  ○ Why/When/How/What
	  ○ Process (OS-agnostic)
	• Potential problems you might run into...
	• Hardening & IEC62443
	• Hardening step by step
	  ○ Different hardening steps & several labs in which students will perform actual hardening themselves
	  ○ Standalone systems <> domain joined systems
	  ○ Operator Jails
	  ○ Create your own hardening script/toolset
	• Network hardening
	• Physical hardening
	• User hardening
	• PLC hardening
	• Verifying hardening
	• Scenario based exercises