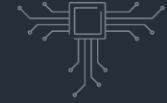**LEONARDO**

Leonardo Cyber & Security Solutions

Closing the professional skills gap

LEONARDO CONTRIBUTION FOR A
CYBER SAFER & MORE SECURE EUROPEAN UNION

2nd European Cybersecurity Skills Conference

Segovia, 21 September 2023

Electronics

Helicopters

Aircraft

Cyber & Security

Space

Unmanned Systems

Aerostructures

About me

Alberto Longhi
Training and Program Development Manager
at Leonardo Cyber & Security Academy

alberto.longhi@leonardo.com
cyberacademy.leonardo.com/en/alberto-longhi
linkedin.com/in/albertolonghi/
PhD in Physics
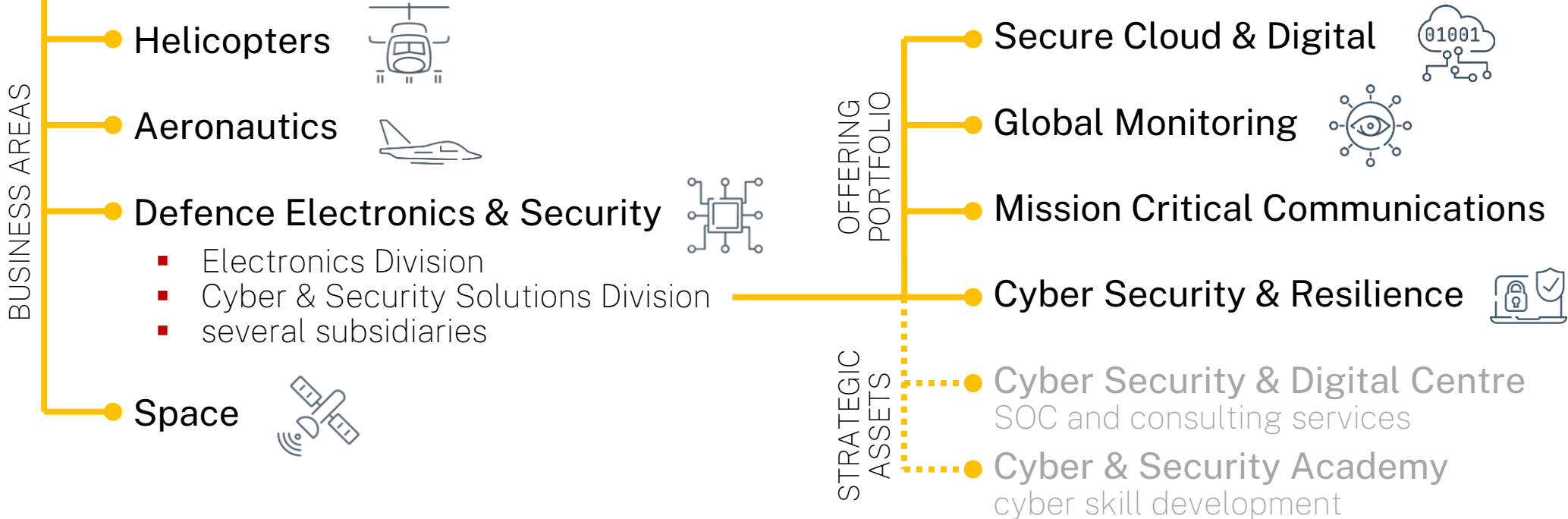CISSP, CISM, CRISC, ISO 27001 LA
Cybersecurity in Leonardo since 2003

About Leonardo

32,327 Italy   **7,540** United Kingdom   **7,143** United States   **2,578** Poland   **248** Israel   **1,556** Rest of the world
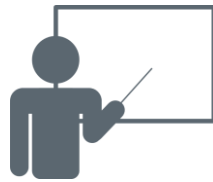
Leonardo is Italy's leading industrial company and one of the world's top Aerospace, Defence and Security firms, with an integrated offering of multi-domain operational capabilities for military and civil applications.

BUSINESS AREAS

- Helicopters
- Aeronautics
- Defence Electronics & Security
  - Electronics Division
  - Cyber & Security Solutions Division
  - several subsidiaries
- Space

OFFERING PORTFOLIO

- Secure Cloud & Digital
- Global Monitoring
- Mission Critical Communications
- Cyber Security & Resilience

STRATEGIC ASSETS

- Cyber Security & Digital Centre
  SOC and consulting services
- Cyber & Security Academy
  cyber skill development

LEONARDO

CYBER·&
SECURITY
ACADEMY

LEONARDO CONTRIBUTION FOR A CYBER SAFER & MORE SECURE EUROPEAN UNION

About Leonardo Cyber & Security Academy

LEARNING SERVICES

- Standard & custom courses
- Cybersecurity awareness
- Cyber exercise and white phishing

TECHNICAL PLATFORMS

- Cyber Trainer (LMS)
- Cyber Range
- Cyber Game (Capture the flag)

FACILITIES

- Human-tech: comfort & technology
- High-tech classrooms
- Relax area, arcade games
- Recording studio

LEONARDO CONTRIBUTION FOR A CYBER SAFER & MORE SECURE EUROPEAN UNION

Cybersecurity skills gap

Non-cybersecurity role profiles lack skills too!

Cyber & information security training is needed at several levels in an organisation, not only by cybersecurity professionals.

A cybersecurity education organisation should address several use cases.

Profile	Expected outcomes from cyber & information security training
User	■ Secure behaviour in usage of PCs, phones, email, social media etc.
Manager (non-technical)	■ Commitment to cyber and information security ■ Awareness of company risks when handling sensitive and critical information
CISO IT Manager (CIO)	■ Knowledge of all relevant cyber and information security issues and best practices ■ Assurance of the organisation's information by means of processes, people and technologies ■ Competent management of suppliers of IT and cybersecurity services
IT administrator Developer	■ Secure development and management of networks, systems, software, data ■ Secure user and customer support ■ Competent management of suppliers of IT and cybersecurity services
Legal Security	■ Awareness of the organisation's security compliance expectations ■ Integration of cyber risk with enterprise risks
Cybersecurity specialist	■ Correct and aware administration of cybersecurity technologies and execution of procedures ■ Understanding and management of cybersecurity operations and processes ■ Competent management of suppliers of IT and cybersecurity services

Our framework

Competence areas

The Cyber & Security Academy specialistic course catalogue builds upon three main tracks:

PREVENTION
GOLD TRACK
Cyber secure infrastructure

DEFENCE
FIRE TRACK
Cybersecurity in action — offence vs. defence

GOVERNANCE
IRON TRACK
Security governance, risk & compliance

PREVENTION						DEFENCE					GOVERNANCE						
ARCHITECTURE DESIGN	NETWORK SECURITY	SYSTEM SECURITY	CLOUD SECURITY	SECURE CODING	SECURITY OF CYBER-PHYSICAL SYSTEMS	THREAT INTELLIGENCE	MONITORING	INCIDENT RESPONSE	DIGITAL FORENSICS	PENETRATION TESTING	SECURITY STRATEGY & PROGRAMME	SECURITY OPERATIONS	SECURE DEVELOPMENT	SUPPLY CHAIN SECURITY	BUSINESS CONTINUITY	RISK MANAGEMENT	COMPLIANCE
RES	RES	RES	RES	RES	RES	DEF	DEF	DEF	DEF	DEF	MGT	MGT	MGT	MGT	MGT	MGT	MGT
A	N	S	C	D	P	I	M	H	F	P	P	O	D	S	B	R	C

Each **track** encompasses several **competence areas** identified by a unique code
Each competence area comprises several **competences** (not represented here)

ECSF applied

Leonardo competence areas vs. ENISA European Cybersecurity Skills Framework (ECSF)

enisa

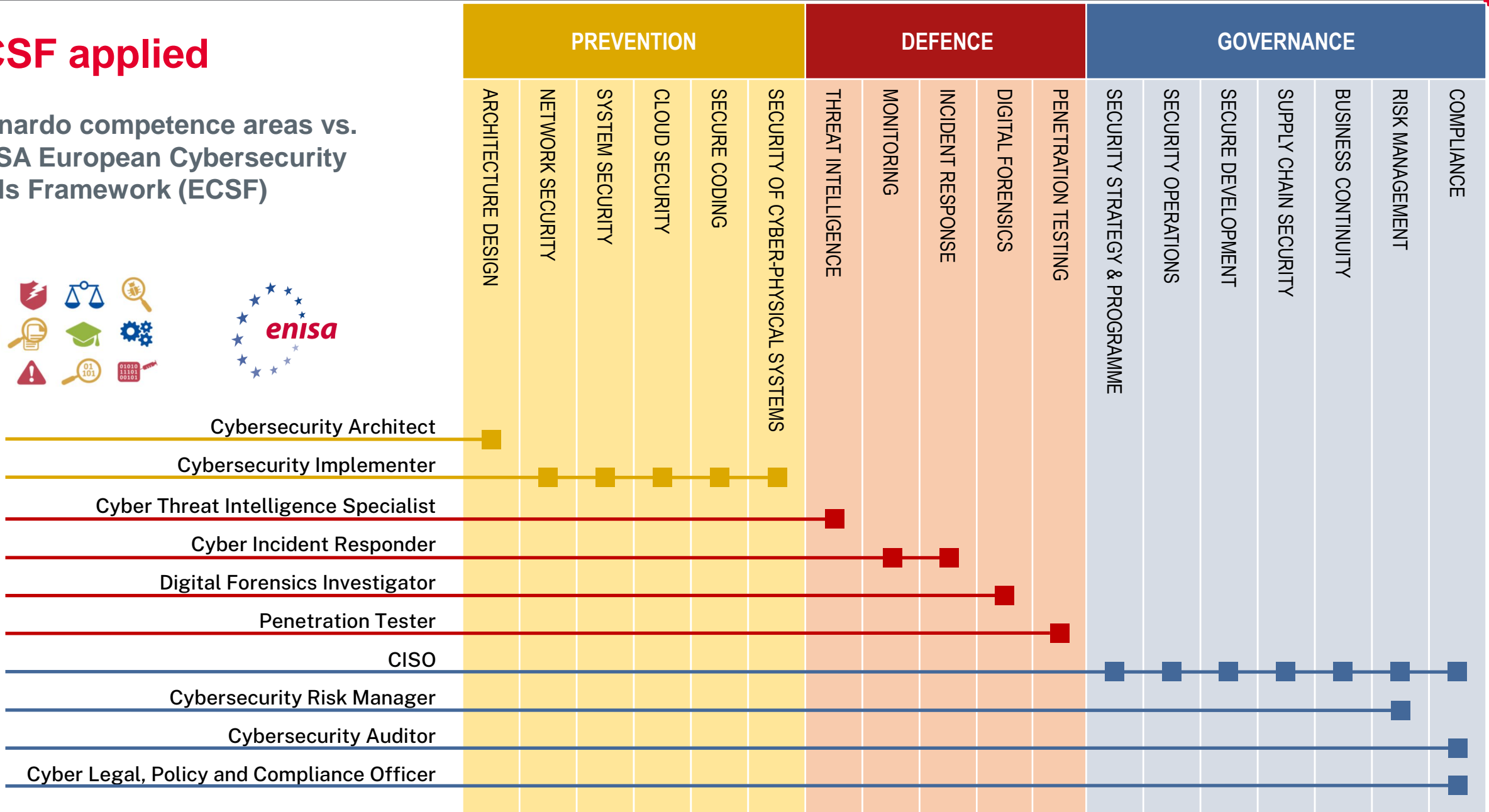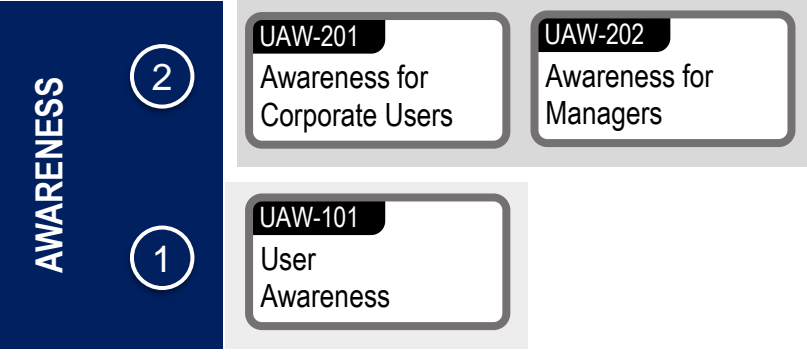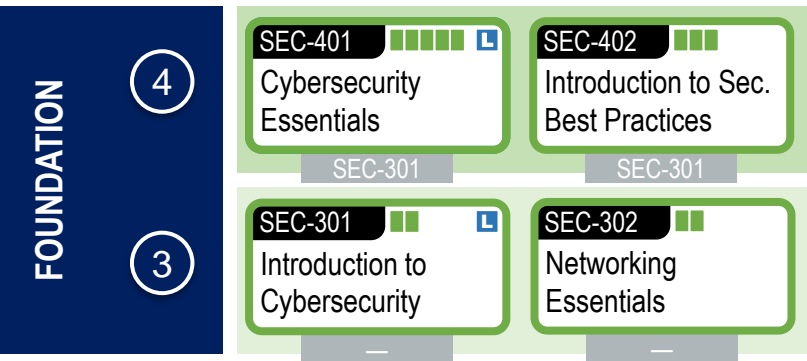|	PREVENTION						DEFENCE					GOVERNANCE						
	ARCHITECTURE DESIGN	NETWORK SECURITY	SYSTEM SECURITY	CLOUD SECURITY	SECURE CODING	SECURITY OF CYBER-PHYSICAL SYSTEMS	THREAT INTELLIGENCE	MONITORING	INCIDENT RESPONSE	DIGITAL FORENSICS	PENETRATION TESTING	SECURITY STRATEGY & PROGRAMME	SECURITY OPERATIONS	SECURE DEVELOPMENT	SUPPLY CHAIN SECURITY	BUSINESS CONTINUITY	RISK MANAGEMENT	COMPLIANCE
Cybersecurity Architect	■																	
Cybersecurity Implementer		■	■	■	■	■												
Cyber Threat Intelligence Specialist							■											
Cyber Incident Responder								■	■									
Digital Forensics Investigator										■								
Penetration Tester											■							
CISO												■	■	■	■	■	■	■
Cybersecurity Risk Manager																	■	
Cybersecurity Auditor																		■
Cyber Legal, Policy and Compliance Officer																		■

LEONARDO CONTRIBUTION FOR A CYBER SAFER & MORE SECURE EUROPEAN UNION

COURSE CATALOGUE EXAMPLE *(watermark)*

		ARCHITECTURE	CODING	CYBER-PHYSICAL	INTELLIGENCE	RESPONSE	PENTESTING	BCM	COMPLIANCE
SPECIALISATION	⑦								
	⑥				DEF-M60... Blue Team	DEF-P601 Red Team			MGT-C601 Compliance in Depth
	⑤	RES-A501 Security Architecture & Engineering	RES-D501 Secure Coding	RES-P501 Introduction to Security of CPS	DEF-I501 Cyber Threat Intelligence B/camp	DEF-H601 Advanced IR & Threat Hunting	DEF-P501 Penetration Testing	MGT-B501 Business Continuity & Disaster Recovery	MGT-C553 Security of CNI/OES
FOUNDATION	④	SEC-401 Cybersecurity Essentials *(SEC-301)*	SEC-402 Introduction to Sec. Best Practices *(SEC-301)*						
	③	SEC-301 Introduction to Cybersecurity *(—)*	SEC-302 Networking Essentials *(—)*						
AWARENESS	②	UAW-201 Awareness for Corporate Users	UAW-202 Awareness for Managers						
	①	UAW-101 User Awareness							

Legend:

- ⑦ **Warrior level**
- ⑥ **Advanced level**
- ⑤ **Intermediate level**
- ③ ④ **Foundation level**
- ① ② **User level**

Hands-on labs included
Duration (days)
Course ID
Course title

SEC-401 Cybersecurity Essentials
Prerequisite — SEC-301
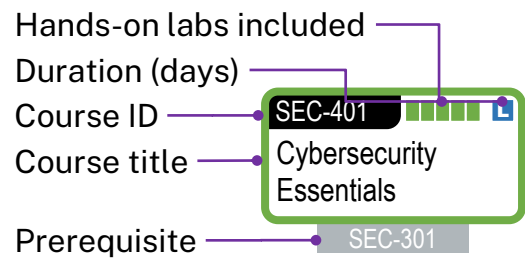
- **IRON TRACK** [GOVERNANCE] » *Security governance, risk & compliance*
- **FIRE TRACK** [DEFENCE] » *Cybersecurity in action — offence vs. defence*
- **GOLD TRACK** [PREVENTION] » *Cyber secure infrastructure*
- **GREENFIELD TRACK** » *A foundation for any cyber specialist*
- **HUMAN TRACK** » *Cyber awareness for non-specialists*

LEONARDO

THANK **YOU**
FOR YOUR ATTENTION

leonardo.com