Cultivating Cybersecurity Defence Expertise with Mindful Readiness and Skills

cadmus-project.eu

Mark Ruijsendaal (HSD)

GAP in courses

Education & Training Provision

Personnel Development

Problem Management

Information Security Strategy Development

Risk Management

<-*->

Systems Management

Testing

Quality Management & Compliance
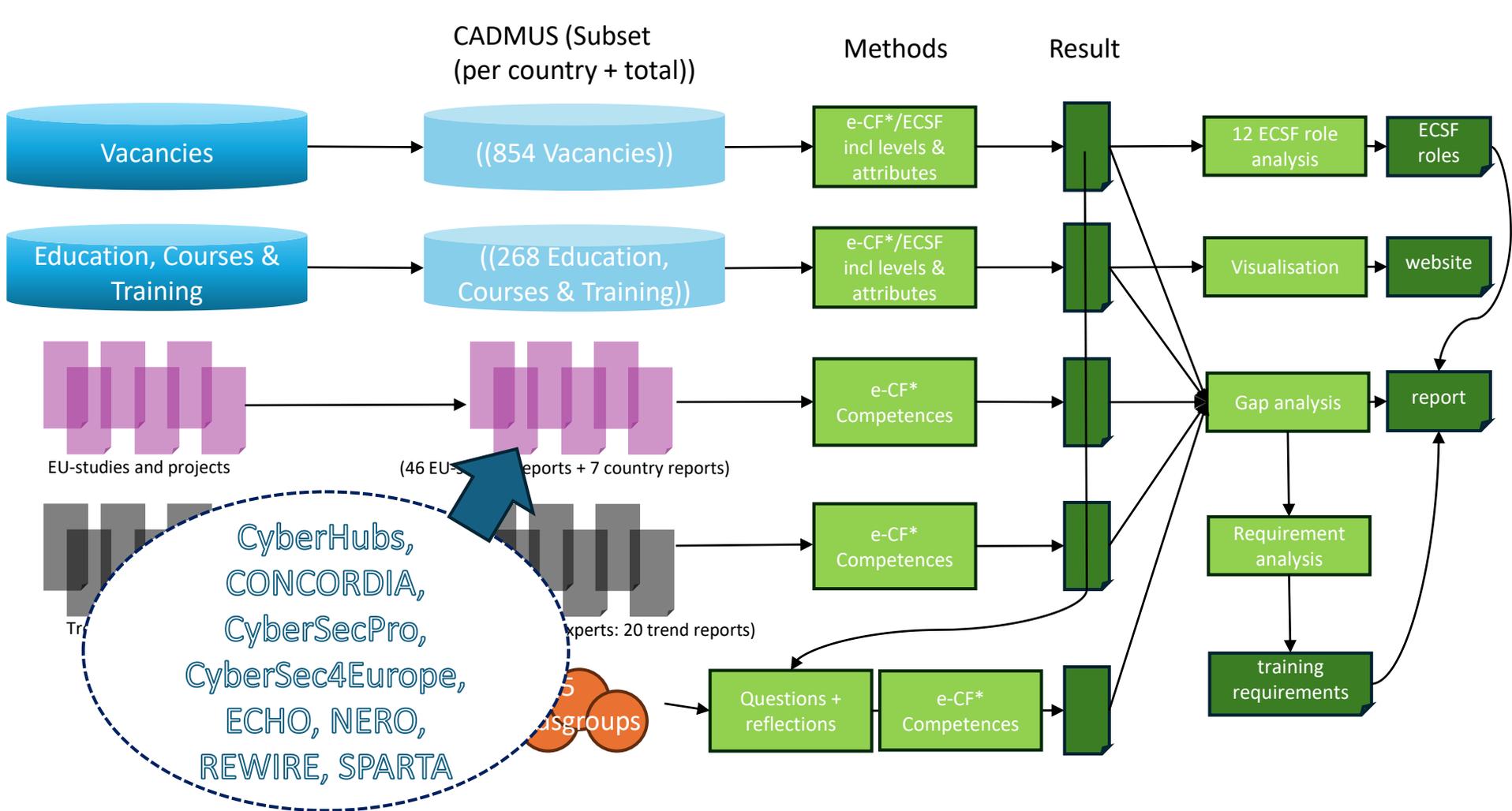
Left chart x-axis labels:
A1. IS and Business Strategy Alignment
A2. Service Level Management
A3. Business Plan Development
A4. Product/Service Planning
A5. Architecture Design
A6. Application/Product Design
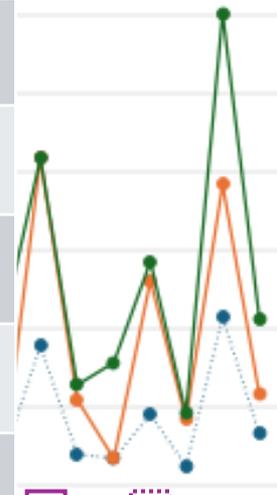
Right chart x-axis labels:
E3. Risk Management
E4. Relationship Management
E5. Process Improvement
E6. Quality Management and Compliance
E7. Business Change Management
E8. Information Security Management
E9. Information Systems Governance

ECSF Role	Recommended changes	New role suggestions
Chief Information Security Officer (CISO)	Change: E8 (e3) to E8 (e4) Add: A1(e5)	Security Governance Manager
Cyber Incident Responder	Change: C4 (e4) to C4 (e3) Add: D1(e4)	
Cyber Legal, Policy & Compliance Officer	None, the competences seem well placed in relation to labour market demand	Compliance Officer
Cyber Threat Intelligence Specialist	None, the competences seem well placed in relation to labour market demand	Threat Innovation Analyst
Cybersecurity Architect	Add: E4 (e4) Remove: B3	
Cybersecurity Auditor	Remove: B3 Change: E3 (e4) to E3 (e3) Add: E4 (e3)	
Cybersecurity Educator	Redefine or remove D9 Add: B1(e3)	
Cybersecurity Implementer	Add: C5 (e3)	
Cybersecurity Researcher	Remove: C4 Add: E4 (e4) Add: D9 (e3) Change: A7 (e5) to A7 (e4) Change: A9 (e5) to A7 (e4)	
Cybersecurity Risk Manager	Add: B5 (e2)	
Digital Forensics Investigator	Change: B3 (e4) to B3 (e3) Add: D7 (e3)	
Penetration Tester	None, the competences seem well placed in relation to labour market demand	

	LOS Title	What learners will be able to do	Training type & platform bundle	EQF level	Evidence (why this LOS)	Primary role
1	**Incident Response & Business Continuity (Problem Management)**	Detect, contain, and recover from ransomware; maintain critical ops.	Cyber-Range blue-team lab + incident SG&TTX; optional 2-3 days boot-camp.	5-6	C.4. sees double-digit (33% for courses and 37% for trainings) future relevance despite current oversupply; focus groups stress the need for tested run-books.	Incident Responder, SOC Analyst
2	**Zero-Trust Systems Management & Cloud Identity**	Deploy conditional access, micro-segment workloads, and run continuous posture assessments.	Guided Azure/AWS labs + SG&TTX "compromised M365 tenant" scenario.	5	C.5. shows (28% and 34% for courses and trainings) shortage; focus/trend stress "securing cloud environments, managing identities, enforcing zero-trust architectures".	Security Administrator, Cybersecurity Architect
3	**Basic Network & Endpoint Security**	Harden Small Office/Home Office (SOHO) routers, configure patching & logging.	Hands-on lab images + video walkthroughs.	4—5	Same focus-group evidence as #24; provides prereq for DevSecOps & IR LOS, in line with C.5. Systems Management (28% in courses and 34% in training).	Security Administrator
4	**Cyber-Education & Training Toolkit**	Design learner-centred labs; run awareness campaigns.	Mentor-guided design studio (LMS) +	4-7	D.3. gap (29% for both courses and trainings); ed... focus groups made mod... refresh.	...ersecurity ...
5	**Risk Management**	Identify, analyse, and treat risk; quantify risk; draft and present mitigation plans.	Blended micro-credential (LMS) + workshop on risk register & KRIs + board-level tabletop briefing.	6-7	E.3. Ris... 27%; tra...	...r, CISO
6	**Pen-Testing & Ethical Hacking**	Plan & execute IoT/OT pentests; report Common Vulnerability Scoring System (CVSS) findings.	2-3 days boot-camp + red-team CTF arena.	5	B.3. Test... 21% and t... explicit call... skills.	...on Tester, ...ility Assessor
7	**Security Management**	Establish and maintain an Information Security	Instructor-led workshops +	6-7	E.8. Information Security Management (courses 19%;	Legal/Policy & Compliance Officer

24 Learning Objectives Sets (LOS)

CADMUS

CADMUS-CR-04	CADMUS-CR-05	CADMUS-CR-06	CADMUS-CR-07	CADMUS-CR-08	CADMUS-CR-09	CADMUS
Firewall Configuration and Security Management	Linux OS Security Hardening and Compliance Validation	Windows OS Security Hardening and Active Directory Defence	Android Device Security and Hardening	Business Continuity Planning and Resilience Simulation	Disaster Recovery Operations and Technical Restoration	CISO Com Securi
Cyber Range + LMS	Cyber Range + LMS	Cyber Range + LMS	Cyber Range + LMS	Cyber Range + LMS	Cyber Range + LMS	Cyber F
Basic–Intermediate	Basic–Intermediate	Basic–Intermediate	Basic–Intermediate	Intermediate	Intermediate	Inte
5-6	5-6	5-6	5-6	6-7	6-7	

Configure and manage network firewalls to enforce security policies.
Implement secure management and access control on firewall systems.
Apply CIS benchmark controls to minimize attack surfaces.
Log, monitor, and

Solid understanding of TCP/IP networking and routing concepts.

Prior exposure to

Explain the role of firewalls in network segmentation and threat prevention.
Apply CIS pfSense recommendations to secure firewall operations.
Configure secure management access, password policies, and session controls.
Implement rule-based

Delivery methods
- Cyber Range Scenarios
- Serious Games and Table-Top Exercises
- Bootcamps and Traineeships
- Instructor/self-directed Short Courses

Currently 55 learning modules defined
Operational in 2026

• Configure system logging, auditing, and integrity monitoring

and password policies, audit policies, and privilege assignments

• Configure Android device policies for lock screen, updates

dependencies, and continuity requirements

• Execute restoration procedures for servers, applications, and data