CyberSecPro

in collaboration with

CURIUM

Comparative Analysis

of the Cybersecurity Incident Responder Role Across Frameworks

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

CyberSecPro Project Agreement no. 101083594. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

CURIUM The project is supported by the European Cybersecurity Industrial, Technology and Research Competence Centre ('granting authority'), under the powers delegated by the European Commission ('European Commission'), under the Grant Agreement No. 101190372.

CONTENTS

Introduction 3
Mission and Scope 3
Key Tasks and Responsibilities 4
Skills and Abilities 5
Knowledge Requirements 7
Comparative Summary Table of Components 9
Sector specific alignment of the incident responder profile 10
  Incident Responder – Health Sector 11
  Incident Responder – Energy Sector 13
  Incident Responder – Maritime Sector 15
Conclusion 17
References 18

LIST OF TABLES

Table 1 Comparative Summary of Incident Responder Components Across Frameworks . . 9
Table 2 Cyber Incident Responder – Health Sector Specialization Profile 11
Table 3 Cyber Incident Responder – Energy Sector Specialization Profile 13
Table 4 Cyber Incident Responder – Maritime Sector Specialization Profile 15

INTRODUCTION

Cybersecurity Incident Responders play a critical role in defending organizations by handling and mitigating cyber incidents. Multiple national and international skills frameworks define this role, each outlining the Incident Responder's mission, key tasks, required skills/abilities, and knowledge. In this analysis, we compare how the Incident Responder role is characterized across eight frameworks:

- **Australian ASD** – Australian Signals Directorate's incident responder profile [1]
- **U.S. CISA** – U.S. Cybersecurity and Infrastructure Security Agency's role (aligned with NICE framework) [2]
- **U.S. DoD** – U.S. Department of Defense cyber workforce role (aligned with NICE) [3]
- **NICE NIST** – U.S. NIST NICE Workforce Framework for Cybersecurity (Protect & Defend – Incident Response) [4]
- **ECSF (ENISA)** – European Cybersecurity Skills Framework (Incident Responder role) [5]
- **U.K. Framework** – UK Cyber Security Council/CIISec guidance for incident response roles [6]
- **Singapore** – Skills Framework (TechSkills Accelerator) Incident Investigator role [7]
- **Germany** – "Vorfall-Experte" certification (Incident Expert in the Cyber-Security Network) [8]

In the European context, the role of the incident responder is influenced by policy frameworks such as NIS2 and the EU Cybersecurity Act. These frameworks emphasize cross-sector coordination and information sharing between Computer Security Incident Response Teams (CSIRTs) and national competent authorities. Consequently, European frameworks place a greater emphasis on legal compliance, cooperation mechanisms, and resilience assessment than non-European frameworks do.

We examine commonalities and differences in mission, tasks, skills & abilities, and knowledge across these frameworks, highlighting where they converge and where each adds unique emphasis.

This whitepaper, a result of the collaboration between the CyberSecPro and CURIUM European funded projects. Both projects share a strong commitment to the development of cybersecurity skills and combined their shared knowledge and approach into providing the results summarized in this document. More information on each project can be found on the last page of this document.

During the preparation of this document, the authors used publicly available tools like (ChatGPT and Mistral) for content assistance, specifically to summarize information and to edit the text. The authors reviewed and revised the material generated and take full responsibility for the content herein.

MISSION AND SCOPE

All frameworks share a foundational mission for the Incident Responder: **to investigate and analyze cybersecurity incidents and minimize their impact**. For example, the U.S. NICE

framework [4] defines the role as one that "investigates, analyzes, and responds to cyber incidents within the network environment or enclave". The Australian ASD profile [1] similarly states that an Incident Responder "performs analysis and investigations of cyber security incidents, often malicious, to remediate networks and provide mitigation advice to protect and secure systems". In essence, across all frameworks the Incident Responder's purpose is to detect and contain threats quickly, reduce damage, and restore normal operations.

Beyond this common core, some frameworks extend the mission's scope. Most emphasize **preventing future incidents** by learning from attacks. The UK framework [6] explicitly notes that incident response includes "following up… to *minimise* damage… and prevent recurrence". The Singapore framework [7] highlights the role's responsibility to produce reports with "findings, conclusions and recommendations" and to recommend corrective actions to prevent future incidents. Many frameworks also stress **timeliness** – responding urgently to limit harm. Notably, the U.S. NICE/NIST description [4] even frames incident response as part of crisis management, invoking "mitigation, preparedness, response and recovery approaches… to maximize preservation of property and information security".

There are also unique emphases. The NICE [4] (and CISA [2]/DOD [3] aligned) definitions include coordination in broader emergencies, even mentioning the survival of life and property in crisis situations – an aspect not overtly mentioned in other frameworks. The ECSF (ENISA) framework [5] underscores adherence to organizational plans: the Incident Responder "according to the organisation's Incident Response Plan, restores systems… to an operational state". The UK [6] emphasizes the human element – staying "calm, ensuring clear communication" during incidents – as integral to the mission. Singapore's description [7] uniquely notes the need for on-call availability (including nights/weekends) and compliance with national law (the Cyber Security Act), reflecting operational realities of the role in that context. In Germany's "Vorfall-Experte" certification [8], the mission is implicit: these experts support organizations during serious IT security incidents as part of a national cyber defense network. In conclusion, **all frameworks align on the fundamental mission** of handling and remediating cyber incidents.

KEY TASKS AND RESPONSIBILITIES

Despite variations in phrasing, **the core tasks** of an Incident Responder are consistent across the frameworks. Fundamentally, an Incident Responder must monitor for potential incidents, investigate alerts, contain and eradicate threats, recover systems, and create necessary documentation for the incident.

For example, the U.K. framework [6] describes day-to-day actions such as responding to monitoring alerts, using tools/scripts to identify breaches, analyzing incidents and escalating as needed. Likewise, the U.S. CISA/NICE work role [2], [4] enumerates tasks including collecting intrusion artifacts, coordinating response efforts, and writing after-action reports. In Australia's ASD profile [1], the "Expectations" for an incident responder include "investigate… incidents," "analyse and resolve… incidents," and "contribute to digital forensic investigations," as well as communication of findings – all reflecting similar duties. Across all frameworks, **detecting and analyzing incidents** (through logs, alerts, or threat intelligence), **containing or mitigating the incident's impact**, and **recovering operations** are primary responsibilities.

All frameworks also highlight the importance of **incident documentation and reporting** as a task. For instance, the NICE/CISA role [2], [4] explicitly requires "write and publish after-action reviews" and incident findings reports, and the UK framework [6] stresses that every

significant action must be logged so that lessons can be learned. The Singapore Incident Investigator [7] similarly "develops reports that detail incident timeline, evidence, findings… and recommendations" and communicates findings to senior stakeholders. This shows a universal recognition that an incident responder's job is not done until the incident is analyzed and reported for improvement and possible legal/compliance needs.

Beyond these commonalities, certain tasks receive **special emphasis in specific frameworks**. The U.S. NICE [4] (and derived CISA [2]/DOD [3]) frameworks list detailed technical tasks such as performing trend analysis on incidents, correlating threat intelligence data, and triaging incidents by scope/impact – reflecting the granular approach of NIST's catalog of tasks. They even include liaison with law enforcement ("serve as technical expert and liaison to law enforcement") as a task, which is not explicitly mentioned in most other frameworks. The ECSF [5] tasks extend into preparation and process improvement: e.g. "develop, implement and assess procedures related to incident handling," and "measure cybersecurity incident detection and response effectiveness". This reflects a broader role in refining incident response plans and metrics in the European context. Similarly, Singapore [7] expects the Incident Investigator to "develop approaches to combat cyber threats," "implement processes and guidelines" for incident response, and even "propose mitigation techniques… to ensure cyber threats are kept at a minimum" – highlighting a proactive and improvement-oriented set of duties.

Another area of divergence is the extent of **leadership vs. technical focus**. Frameworks like Singapore's [7] (and to some degree ECSF [5]) include leading incident recovery and improving processes as tasks, suggesting this role may also manage incident response efforts. The ASD [1] and NICE [4] frameworks, while including coordination, put slightly more weight on technical analysis and immediate response actions (e.g. evidence collection, intrusion analysis). Nonetheless, even in technical-heavy frameworks, some management tasks appear (e.g. NICE's "coordinate incident response functions"). The UK description [6] interestingly notes that, incident responders might "draft or agree policies and procedures… or carry out exercises to test these", implying involvement in preparedness drills – a task not explicitly listed in others, though certainly implied in frameworks that mention testing incident handling techniques (ECSF [5]).

In summary, **all frameworks cover the incident lifecycle** – preparation (planning, monitoring), detection/analysis, containment/eradication, recovery, and post-incident learning. They align on tasks like alert monitoring, incident triage, evidence collection (forensics), incident handling/coordination, and reporting. Differences emerge in how much they emphasize tasks like developing IR plans, law enforcement liaison, proactive threat hunting or trend analysis, and process improvement. These differences often reflect the scope of the role in each context: some frameworks envision the Incident Responder also as an incident manager and planner, not just a reactive analyst.

Recent incident trends, particularly the surge of ransomware and supply-chain attacks, have also shifted expectations for responders. Frameworks increasingly require the ability to coordinate with business continuity teams, manage communication under crisis conditions, and support decisions such as ransom negotiation or disclosure.

SKILLS AND ABILITIES

The skillsets and abilities required for an effective performance of the Incident Responder role are broadly similar across frameworks, comprising both **technical cybersecurity skills** and

important soft skills. Common **technical skills** include the ability to analyze logs and network traffic, to recognize malware and indicators of compromise, and to conduct forensic analysis. For instance, the NICE framework [4] enumerates skills such as "recognizing and categorizing types of vulnerabilities and associated attacks", "securing network communications", and using security event correlation tools, as well as malware detection and analysis skills. The ECSF [5] similarly lists as key skills the ability to "collect, analyse and correlate cyber threat information from multiple sources," to "manage and analyse log files," and to carry out all technical aspects of incident handling. The UK framework [6] echoes this, expecting Incident Responders to be adept at "interpreting the output of monitoring systems," "investigating complex problems and finding solutions," and "analysing unexpected network or system events… and devising actions to stop them". Across all frameworks, the ability to perform **in-depth technical analysis under pressure** is a core skill.

Equally emphasized are **communication and coordination abilities** abilities. An incident responder must not only find and fix issues but also clearly communicate with others (technical teams, management, possibly external stakeholders). All frameworks note this in some way. The NICE/CISA role [2], [4] includes communication implicitly (e.g. writing reports, coordinating across teams), while the UK [6] explicitly lists "collaborating with other specialists" and communicating clearly under stress as key personal attributes. The ECSF profile has "communicate, present and report to relevant stakeholders" as a key skill. Singapore's framework requires stakeholder management and strong communication as well (rated at "Intermediate" proficiency). In Germany's incident expert program, communication is broken down into specific skills like conflict management and "persuasiveness," along with the ability to convey technical information in an understandable way (didactic skill). Thus, being able to coordinate incident response efforts and explain findings is universally important.

Another crucial ability across all frameworks is **working calmly and effectively under pressure**. Cyber incidents can be high-stakes crises, and the ability to remain level-headed is highlighted in several frameworks. The UK [6] notes the importance of "remaining calm under pressure" and methodical action. The ECSF [5] lists "work under pressure" as a key ability for the role. The German framework [8] stresses "resilience in stressful situations" as a personal trait of an incident expert. Even where not explicitly stated, this capability is implied given the urgent nature of incident response (for example, Singapore's profile hints at this by mentioning the need for being on standby and dealing with incidents in a timely manner). All frameworks also value **problem-solving skills** – the ability to troubleshoot and think critically through an unfolding incident.

Frameworks diverge by adding unique skill requirements relevant to their context or scope. **Leadership and crisis management skills** are explicitly mentioned in some. The German "Vorfall-Experte" enumerates leadership abilities (e.g. "leading in a crisis situation," "solution orientation," "ability to motivate"), reflecting that an incident expert may direct response efforts and guide others. The NICE framework [4] includes a technology related skill: "design incident response for cloud service models" (and a corresponding ability), acknowledging the growing need to handle incidents in cloud environments – a specificity not seen in other frameworks. The UK [6] emphasizes ethical and contextual judgment, expecting responders to consider the "commercial, cultural, ethical and environmental consequences" of actions, aligning with broader professional standards in the UK. Soft skills like didactic ability (i.e., teaching or guiding others during incidents) appear in the German framework [8].

In the Singapore framework [7], beyond technical competencies (which are mapped to specific skill categories like Incident Management, Forensics, Threat Analysis at certain proficiency levels), there is emphasis on critical thinking and "sense-making" as general skills – reflecting a need to interpret information and derive insights during investigations. This is conceptually similar to the analytical skills highlighted elsewhere, but Singapore's framework explicitly names those cognitive skills.

Another growing requirement across all frameworks is continuous learning through simulated exercises, such as cyber ranges. Incident responders must maintain technical and behavioral readiness by participating in regular, scenario-based training that reflects real-world attack patterns.

In summary, **technical and soft skills go together** for incident responders in all frameworks. They must possess strong technical abilities in cybersecurity detection and response, and be effective communicators, coordinators, and problem-solvers. The balance can vary, U.S. frameworks (NICE [4], DoD [3], CISA [2]) provide exhaustive lists of technical skills (malware analysis, log analysis, etc.), while European and other frameworks put relatively more emphasis on teamwork, communication, and even leadership. Ultimately, however, all agree that an Incident Responder must be a well-rounded professional capable of both deep technical work and effective collaboration under pressure.

KNOWLEDGE REQUIREMENTS

The knowledge base for a Cyber Incident Responder is extensive, covering technical, procedural, and contextual domains. There is strong agreement across frameworks on the **core knowledge areas** required. All frameworks expect knowledge of fundamental **network and system security concepts**, various forms of **cyber threats and vulnerabilities**, and **incident response processes**. In the NICE/NIST framework [4], for example, the responder needs knowledge of networking protocols and security methodologies, knowledge of cyber threats and vulnerabilities, and specific knowledge of incident response procedures (e.g. "incident categories, incident responses, and timelines" and handling methodologies). The Australian ASD profile [1] similarly requires understanding the organization's threat environment (threat actors, attack methods), as well as knowledge of legal/regulatory obligations and governance within which incidents occur. The ECSF [5] lists "Key knowledge" including "computer networks security," "computer systems vulnerabilities," "cyber threats," and "cybersecurity attack procedures" – again reflecting technical foundations in networks, vulnerabilities, and attack tactics. All frameworks also highlight knowledge of incident response tools and techniques. For instance, ECSF [5] mentions incident handling tools and methodologies as knowledge areas, and the UK framework [6] requires understanding of "the detection of and response to security incidents and the collection and use of threat intelligence" as core knowledge.

Another universally cited knowledge area is the **governing policies, laws, and standards** relevant to cybersecurity and incident handling. Incident responders must operate within legal and organizational policy constraints. The NICE framework [4] explicitly includes knowledge of applicable laws, regulations, and ethics. Australia's ASD role expects knowledge of the "legal and regulatory environment" of ASD operations. The ECSF [5] and Singapore [7] frameworks list understanding cybersecurity-related laws and regulations as key knowledge. This reflects that incident response often involves compliance (for example, reporting requirements under breach notification laws) and ethical considerations. The UK framework [6] similarly implies this through its emphasis on incident responders knowing not just technical aspects but also having context for their work including human factors and possibly compliance (though UK's explicit knowledge categories focus more on technical and behavioral science areas).

Many frameworks require knowledge in **digital forensics** or evidence handling. CISA/NICE [2], [4] lists skill in evidence preservation and knowledge of forensic concepts (implied in tasks and skills), while ECSF [5] expects knowledge of how CSIRTs operate and incident handling

best practices, which includes forensic procedures. The UK framework [6] lists Forensics as part of wider knowledge, defined as "collection, analysis and reporting of digital evidence in support of incidents" – indicating an incident responder should understand forensic principles even if dedicated specialists may do deep forensics.

There are **unique knowledge requirements or emphases** in certain frameworks reflecting regional or scope differences. For example, the German certification [8] demands knowledge of national structures: understanding "the cyber security network, the roles and tasks of each participant," and the specifics of the national incident response framework. It also highlights knowledge of BSI's IT baseline protection and emergency management framework. These are country-specific details to ensure responders fit into Germany's federal incident response system. The UK framework [6], interestingly, includes knowledge of "Human Factors" (usability, security culture, human behavior) and "Hardware Security," as part of broader contextual knowledge for the role. This suggests a holistic approach, where understanding how humans interact with security and the hardware aspects of security can provide context to incidents (for instance, social engineering aspects or hardware tampering). The NICE framework [4] (and by extension CISA [2]/DOD [3]) uniquely calls out knowledge of privacy laws and principles alongside cybersecurity ones– acknowledging that incident responders deal with personal data breaches and thus should know privacy obligations (most other frameworks focus on cybersecurity laws and don't explicitly mention privacy).

Industrial control system (ICS) or OT (Operational Technology) security knowledge is another specialized area: the UK [6] notes that if working with industrial systems, one needs additional knowledge of ICS security (cyber-physical systems). Other frameworks do not explicitly mention this, likely assuming it as a niche case or covered under broader threat knowledge. ECSF [5] and NICE [4] frameworks, being more general, do not list ICS explicitly but would consider it part of environment-specific knowledge if applicable. **Cloud security** is implicitly covered (NICE's skill statements on cloud IR suggest knowledge of cloud models is needed), though not always spelled out as a knowledge area; some knowledge statements in NICE like understanding virtualization or cloud service models appear in updated lists.

Moreover, frameworks differ in how they categorize knowledge vs skills. For example, NICE [4] delineates dozens of specific knowledge (K) items (e.g., K0042 "knowledge of incident response and handling methodologies"). The ECSF provides a more concise list of knowledge topics where as Singapore's description notes knowledge of "cyber security standards, protocols and frameworks", aligning with the idea that a responder should know the prevailing security standards (e.g., ISO 27001, NIST guidelines) and best practices.

Most frameworks have yet to fully address an emerging area: incident response in cloud-native, Internet of Things (IoT), and artificial intelligence (AI)-driven environments. As such, responders are increasingly expected to handle security events in distributed, containerized, and automated infrastructures where telemetry, orchestration tools, and AI-assisted detection play critical roles. Future frameworks should incorporate cloud forensics, API threat monitoring, and secure AI system handling skills into their incident response strategies.

In summary, **the knowledge required is comprehensive and largely shared**: Incident Responders everywhere need a strong grounding in technical security (networks, systems, malware, forensics), a clear understanding of incident response processes and threat landscapes, and familiarity with the legal/policy context of cybersecurity. Unique elements tend to reflect local context (national frameworks, specific domains like ICS, or emerging domains like cloud and privacy). All frameworks stress that an Incident Responder must be a continuous learner, staying current with evolving threats and tools – evidenced by the inclusion of threat intelligence and trend analysis in many profiles [1], [5]. Thus, a deep and broad knowledge base underpins the role across all compared frameworks.

COMPARATIVE SUMMARY TABLE OF COMPONENTS

The table below summarizes key components of the Incident Responder role across the analyzed frameworks, indicating which aspects are common to all and which are emphasized or unique in specific frameworks:

DIMENSION	COMMON COMPONENTS (ALL FRAMEWORKS)	UNIQUE/EMPHASIZED IN SPECIFIC FRAMEWORKS
Mission	– Investigate and analyze cybersecurity incidents to determine causes. – Contain, mitigate, and remediate incidents to minimize damage and restore operations. – Prevent future incidents through lessons learned and improved defenses (implied in all).	– Crisis management emphasis (life/property safety) – **NICE (US)**. – Following formal IR plan – **ECSF (EU)**. – Calm and clear communication as part of mission – **UK**. – On-call readiness (24/7 availability) – **Singapore**. – National cyber network support – **Germany** (Vorfall-Experte integrates into national incident support structure).
Tasks	– **Monitoring/Detection:** Continuously monitor networks/alerts for signs of incidents. – **Analysis/Triage:** Analyze alerts and events to determine incident scope, severity, and nature. – **Containment/Eradication:** Take action to stop the attack (e.g. isolate systems, remove malware) and mitigate damage. – **Evidence Collection:** Collect and preserve forensic evidence (disk images, logs, malware samples) for analysis. – **Response Coordination:** Coordinate with team members (SOC, IT, management) to execute the incident response plan. – **Recovery:** Restore affected systems and services to normal operation once threats are removed. – **Reporting/Lessons Learned:** Document the incident and actions taken; produce incident reports or after-action reviews for stakeholders.	– Developing and updating IR plans/procedures – e.g. testing and maintaining an Incident Response Plan (**ECSF**), conducting incident response exercises (**UK**). – Law enforcement liaison – serving as technical expert for police/Federal authorities during incidents (**NICE/CISA**). – Threat trend analysis – performing strategic analysis of incident trends and threat intel to inform defense (**NICE**). – Proactive vulnerability management – scanning for and addressing vulnerabilities as part of IR (**ECSF**, **Singapore**). – Leading incident recovery – taking charge of incident resolution efforts (**Singapore**). – Continuous improvement – measuring response effectiveness and refining processes after incidents (**ECSF**, **Singapore**).
Skills & Abilities	– **Technical Cyber Skills:** Intrusion detection, log analysis, malware analysis, and general analytical skills to investigate incidents. – **Incident Handling Skills:** Containment, eradication and recovery techniques; following defined procedures and play-	– Crisis leadership: Ability to lead and make decisions in a crisis (**Germany** – emphasizes leadership, decisiveness, motivating team). – Cloud incident response skills: Expertise in handling incidents in cloud environments (**NICE** e.g. designing IR for

DIMENSION	COMMON COMPONENTS (ALL FRAMEWORKS)	UNIQUE/EMPHASIZED IN SPECIFIC FRAMEWORKS
	books to handle incidents. – **Communication Skills:** Clearly communicate technical findings and incident status to varied stakeholders. This includes report writing and briefing abilities. – **Teamwork & Coordination:** Ability to collaborate with cross-functional teams (IT ops, management, forensic specialists) during response. – **Problem-Solving Under Pressure:** Remain calm and methodical in high-stress situations, apply critical thinking to novel problems, and make quick decisions to mitigate damage.	cloud models). – Collaboration with external parties: e.g. working with law enforcement or external CSIRTs (**NICE/CISA**, **ECSF**). – Stakeholder management & communication strategy: Strong focus in **Singapore** and **UK** (emphasis on clear, calm communication). – Resilience and empathy: Personal resilience, stress management, and empathy in handling incident aftermath (**Germany**).
Knowledge	– **Networking & Systems:** Knowledge of computer networks, protocols (TCP/IP, DNS, etc.), operating systems, and security architectures (defense-in-depth). – **Threats & Vulnerabilities:** In-depth knowledge of cyber threats (malware, attack techniques, adversary tactics) and system/application vulnerabilities. – **Incident Response Process:** Knowledge of incident handling methodologies, phases of incident response, and best practices/standards (e.g. NIST guidelines, ISO standards). – **Policies, Laws, Regulations:** Understanding of relevant cybersecurity laws, data breach regulations, organizational policies, and ethical considerations. – **Business Continuity/Recovery:** Knowledge of business continuity and disaster recovery principles.	– Country/sector-specific frameworks: e.g. **Germany** responders must know BSI IT-Grundschutz; **Singapore** expects knowledge of the Cybersecurity Act. – Privacy and data protection: Detailed knowledge of privacy laws and principles (**NICE**). – Industrial Control Systems (ICS): Knowledge of ICS/SCADA security and safety (**UK**). – Human factors and social engineering: Understanding attacker psychology and user behavior (**UK**). – Emerging technologies and trends: Keeping up with new technologies (**ASD**, **ECSF**). – Certifications and standards: Awareness of industry-recognized certifications (**ECSF**).

Table 1: Comparative Summary of Incident Responder Components Across Frameworks

SECTOR SPECIFIC ALIGNMENT OF THE INCIDENT RESPONDER PROFILE

CyberSecPro's ambition is to enhance the role of the Higher Education Institutes (HEIs) in offering hands-on and working-life skills for driving a trustworthy digital transformation in critical sectors of the economy. As part of the activities, CyberSecPro has created cybersecurity curricula targeted to health, the energy sector and the maritime sector.

D2.1 – Cybersecurity Practical Skills Gaps in Europe, the cybersecurity skills required in the Health, Energy, and Maritime Sectors are presented. For example, one major concern for the health sector is the reliance on access to patient data and information and the handling of

this information. Whereas, core assets in all sectors belong to the category of operational technology (e.g. SCADA systems, programmable logic controllers (PLCs), propulsion plants, dynamic positioning systems, monitoring and control systems) and specific knowledge and skills related to this technology and assets should be included.

The Cybersecpro project, taking into consideration the analysis of the different frameworks presented in the previous sections, and the needs analysis of each sector performed by the project, proposes the following sector specific adaptations of the ECSF incident responder role profile.

Incident Responder – Health Sector

PROFILE COMPONENT	DESCRIPTION
Profile Title	Cyber Incident Responder (Health Sector Specialization)
Alternative Title(s)	• Cyber Crisis Expert • Cyber Fighter/Defender • Cyber Incident Handler • Cyber Incident Responder • Cybersecurity SIEM Manager • Incident Response Engineer • Security Operation Analyst (SOC Analyst) • Security Operations Center (SOC) Analyst • Health Data Security Analyst • Medical Device Security Engineer
Summary Statement	Monitor the organisation's cybersecurity state, handle incidents involving medical and IT systems, and assure the continued operations of healthcare services.
Mission	Monitors and assesses systems' cybersecurity state with a focus on patient safety and data privacy. Analyses and mitigates incidents ensuring continuity of critical medical services. Identifies root causes and restores systems (e.g., HIS, PACS) to operational state while strictly preserving PHI/PII evidence for regulatory compliance.
Deliverable(s)	• Cyber Incident Report • Incident Response Plan • Medical Device Impact Assessment
Main Task(s)	• Data Leakage Analysis: Specifically investigate vectors for PII/PHI exfiltration. • Adopt and develop incident handling testing techniques. • Assess and manage technical vulnerabilities. • Contribute to the development, maintenance and assessment of the Incident Response Plan. • Cooperate with key personnel for reporting of security incidents according to applicable legal framework. • Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs). • Develop, implement and assess procedures related to incident handling. • Document incident results analysis and incident handling actions.

PROFILE COMPONENT	DESCRIPTION
	• Establish procedures for incident results analysis and incident handling reporting. • Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity or data breach incident. • Identify, analyse, mitigate and communicate cybersecurity incidents. • Measure cybersecurity incidents detection and response effectiveness in clinical environments.
Key Skill(s)	• Medical Log Analysis: Ability to parse and interpret logs from proprietary medical devices and HL7 messages. • Collect, analyse and correlate cyber threat information originating from multiple sources. • Communicate, present and report to relevant stakeholders (including clinical staff). • Manage and analyse log files. • Practice all technical, functional and operational aspects of cybersecurity incident handling and response. • Work on operating systems, servers, clouds and relevant infrastructures. • Work under pressure in life-critical environments.
Key Knowledge	• Health Information Systems (HIS): Architecture of HIS, PACS/DICOM standards, and e-Health exchange protocols. • Medical IoT (IoMT) Security: Vulnerabilities in connected devices (infusion pumps, monitors) and legacy medical OS limitations. • Computer networks security. • Computer Security Incident Response Teams (CSIRTs) operation. • Computer systems vulnerabilities & Cyber threats. • Cybersecurity attack procedures. • Cybersecurity related laws, regulations and legislations. • Cybersecurity-related certifications. • Incident handling communication procedures. • Incident handling recommendations and best practices. • Incident handling standards (NIST/ENISA) adapted for healthcare. • Incident handling tools. • Operating systems security. • Secure Operation Centres (SOCs) operation.
e-Competences (from e-CF)	• A.7. Technology Trend Monitoring (Level 3) • B.2. Component Integration (Level 2) • B.3. Testing (Level 3) • B.5. Documentation Production (Level 3) • C.4. Problem Management (Level 4)

Table 2: Cyber Incident Responder – Health Sector Specialization Profile

Incident Responder – Energy Sector

PROFILE COMPONENT	DESCRIPTION
Profile Title	Cyber Incident Responder (Energy Sector Specialization)
Alternative Title(s)	• Cyber Crisis Expert • Cyber Fighter/Defender • Cyber Incident Handler • Cyber Incident Responder • Cybersecurity SIEM Manager • Incident Response Engineer • Security Operation Analyst (SOC Analyst) • Security Operations Center (SOC) Analyst • OT Security Analyst • SCADA Security Engineer • ICS Defender
Summary Statement	Monitor the organisation's cybersecurity state, handle incidents in IT and OT environments, and assure the continued operations of critical energy infrastructure.
Mission	Monitors and assesses the security of IT and Operational Technology (OT) environments. Mitigates incidents prioritizing Health, Safety, and Environment (HSE) and Availability. Restores SCADA/ICS functionality ensuring physical process stability and safety.
Deliverable(s)	• Cyber Incident Report • Incident Response Plan • Operational Safety Impact Report
Main Task(s)	• Adopt and develop incident handling testing techniques. • Assess and manage technical vulnerabilities. • Contribute to the development, maintenance and assessment of the Incident Response Plan. • Cooperate with key personnel for reporting of security incidents according to applicable legal framework. • Cooperate with Secure Operation Centres (SOCs) and CSIRTs. • Develop, implement and assess procedures related to incident handling. • Document incident results analysis and incident handling actions. • Establish procedures for incident results analysis and incident handling reporting. • Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity incident. • Identify, analyse, mitigate and communicate cybersecurity incidents. • Measure cybersecurity incidents detection and response effectiveness.
Key Skill(s)	• Safety-Critical Decision Making: Understanding the physical impact of digital countermeasures. • Collect, analyse and correlate cyber threat information originating from multiple sources. • Communicate, present and report to relevant stakeholders.

PROFILE COMPONENT	DESCRIPTION
	• Manage and analyse log files. • Practice all technical, functional and operational aspects of cybersecurity incident handling and response. • Work on operating systems, servers, clouds and relevant infrastructures. • Work under pressure.
Key Knowledge	• ICS/OT Protocols: In-depth knowledge of industrial protocols (Modbus, DNP3, IEC 60870-5-104, IEC 61850). • SCADA & PLC Architecture: Understanding of RTUs, PLCs, HMIs, and the Purdue Enterprise Reference Architecture. • Safety Systems: Knowledge of Safety Instrumented Systems (SIS) and fail-safe principles. • OT Security Standards (e.g., IEC 62443). • Computer networks security. • Computer Security Incident Response Teams (CSIRTs) operation. • Computer systems vulnerabilities & Cyber threats. • Cybersecurity attack procedures. • Cybersecurity related laws, regulations and legislations. • Cybersecurity-related certifications. • Incident handling communication procedures. • Incident handling recommendations and best practices. • Incident handling standards, methodologies and frameworks. • Incident handling tools. • Operating systems security. • Secure Operation Centres (SOCs) operation.
e-Competences (from e-CF)	• A.7. Technology Trend Monitoring (Level 3) • B.2. Component Integration (Level 2) • B.3. Testing (Level 3) • B.5. Documentation Production (Level 3) • C.4. Problem Management (Level 4)

Table 3: Cyber Incident Responder – Energy Sector Specialization Profile

Incident Responder – Maritime Sector

PROFILE COMPONENT	DESCRIPTION
Profile Title	Cyber Incident Responder (Maritime Sector Specialization)
Alternative Title(s)	• Cyber Crisis Expert • Cyber Fighter/Defender • Cyber Incident Handler • Cyber Incident Responder • Cybersecurity SIEM Manager • Incident Response Engineer • Security Operation Analyst (SOC Analyst) • Security Operations Center (SOC) Analyst • Maritime Cyber Security Officer
Summary Statement	Monitor the vessel and shore-based cybersecurity state, handle incidents at sea and in port, and assure the safety of navigation and vessel operations.
Mission	Monitors and assesses cybersecurity on vessel and shore-based systems. Manages incidents in environments with intermittent connectivity, focusing on the safety of navigation and crew. Restores critical onboard systems (Bridge, Propulsion, Cargo) compliant with maritime regulations.
Deliverable(s)	• Cyber Incident Report • Incident Response Plan • Vessel Incident Report (IMO compliant)
Main Task(s)	• Remote Incident Triage: Coordinate response actions with crew onboard vessels characterized by high latency/low bandwidth (SatCom). • Analyze isolation of IT (Crew welfare) vs OT (Vessel control) networks. • Adopt and develop incident handling testing techniques. • Assess and manage technical vulnerabilities. • Contribute to the development, maintenance and assessment of the Incident Response Plan. • Cooperate with key personnel for reporting of security incidents according to applicable legal framework. • Cooperate with Secure Operation Centres (SOCs) and CSIRTs. • Develop, implement and assess procedures related to incident handling. • Document incident results analysis and incident handling actions. • Establish procedures for incident results analysis and incident handling reporting. • Evaluate the resilience of the cybersecurity controls and mitigation actions taken after a cybersecurity incident. • Identify, analyse, mitigate and communicate cybersecurity incidents. • Report incidents to maritime authorities as per IMO guidelines. • Measure cybersecurity incidents detection and response effectiveness.
Key Skill(s)	• Remote Response: Ability to guide non-technical crew (Captain/Officers) through incident handling procedures remotely.

PROFILE COMPONENT	DESCRIPTION
	• SatCom Traffic Analysis: Detecting anomalies in satellite links (VSAT, FBB, Inmarsat). • Collect, analyse and correlate cyber threat information originating from multiple sources. • Communicate, present and report to relevant stakeholders. • Manage and analyse log files. • Practice all technical, functional and operational aspects of cybersecurity incident handling and response. • Work on operating systems, servers, clouds and relevant infrastructures. • Crisis communication with shore-based fleet management. • Work under pressure.
Key Knowledge	• Vessel Onboard Systems: Specifics of ECDIS (Electronic Charts), VDR (Voyage Data Recorders), and AIS. • SatCom Security: Vulnerabilities and bandwidth constraints of satellite communications. • Maritime Regulations: Familiarity with IMO MSC.428(98) and TMSA 3 cyber security guidelines. • Understanding of vessel network segmentation (IT vs OT onboard). • Computer networks security. • Computer Security Incident Response Teams (CSIRTs) operation. • Computer systems vulnerabilities & Cyber threats. • Cybersecurity attack procedures. • Cybersecurity related laws, regulations and legislations. • Cybersecurity-related certifications. • Incident handling communication procedures. • Incident handling recommendations and best practices. • Incident handling standards, methodologies and frameworks. • Incident handling tools. • Operating systems security. • Secure Operation Centres (SOCs) operation.
e-Competences (from e-CF)	• A.7. Technology Trend Monitoring (Level 3) • B.2. Component Integration (Level 2) • B.3. Testing (Level 3) • B.5. Documentation Production (Level 3) • C.4. Problem Management (Level 4)

Table 4: Cyber Incident Responder – Maritime Sector Specialization Profile

CONCLUSION

In summary, **the knowledge required is comprehensive and largely shared**: Incident Responders everywhere need a strong grounding in technical security (networks, systems, malware, forensics), a clear understanding of incident response processes and threat landscapes, and familiarity with the legal/policy context of cybersecurity. Unique elements tend to reflect local context (national frameworks, specific domains like ICS, or emerging domains like cloud and privacy). All frameworks stress that an Incident Responder must be a continuous learner, staying current with evolving threats and tools – evidenced by the inclusion of threat intelligence and trend analysis in many profiles [1], [5]. Thus, a deep and broad knowledge base underpins the role across all compared frameworks.

REFERENCES

[1] Australian Signals Directorate, “Cyber Skills Framework – Incident Responder Role Profile,” Framework, 2023.

[2] Cybersecurity and Infrastructure Security Agency, “Cyber Defense Incident Responder (Work Role 531),” Work Role Profile, 2023.

[3] U.S. Department of Defense, “DoD Cyber Workforce Framework,” Framework, 2023.

[4] National Initiative for Cybersecurity Education, “NICE Framework Workforce Framework for Cybersecurity (NIST Special Publication 800-181 Rev. 1),” Special Publication 800–181, 2020.

[5] European Union Agency for Cybersecurity, “European Cybersecurity Skills Framework (ECSF) – Incident Responder Role Profile,” Framework, 2022.

[6] UK Cyber Security Council, “Cyber Security Body of Knowledge – Incident Response Role Profile,” Role Profile, 2023.

[7] SkillsFuture Singapore, “Skills Framework for Infocomm Technology – Incident Investigator,” Skills Framework, 2023.

[8] Bundesamt für Sicherheit in der Informationstechnik, “Vorfall-Experte Certification Program,” Certification Framework, 2023.

CYBERSECPRO

CyberSecPro aims to bridge the gap between degrees, working life, and marketable cybersecurity skill sets necessary in today's digitalization efforts and provide examples of best practices for cybersecurity training programs.

CyberSecPro's ambition is to enhance the role of the Higher Education Institutes (HEIs) in offering hands-on and working-life skills for driving a trustworthy digital transformation in critical sectors of the economy. The enhanced HEIs will equip the workforce with the necessary capabilities to address the digital challenges and be capable to develop secure privacy aware innovative ICT and industrial products that serve people, businesses and working-life communities practicing their democratic values and rights. By establishing a unique Learning Factory, CyberSecPro will be an authentic environment to link innovation, research, industry, academia and SME support. The outcome of the CyberSecPro is to empower the NextGen Europe.

More information: https://cybersecpro.eu/

CURIUM

The CURIUM project envisions a more secure and resilient digital landscape by strengthening the security, privacy, and accountability of hardware and software products with digital elements. At its core, CURIUM introduces a novel Compliance Continuum – a suite of cybersecurity-oriented tools and services designed to provide information, guidance, trustworthy security testing, and streamlined compliance with the Cyber Resilience Act (CRA).

By simplifying and automating compliance, CURIUM empowers European SMEs – especially micro and small enterprises – to conduct self-assessments, prepare for third-party certification, and reduce costs while accelerating time to market.

More information: https://curium-project.eu/