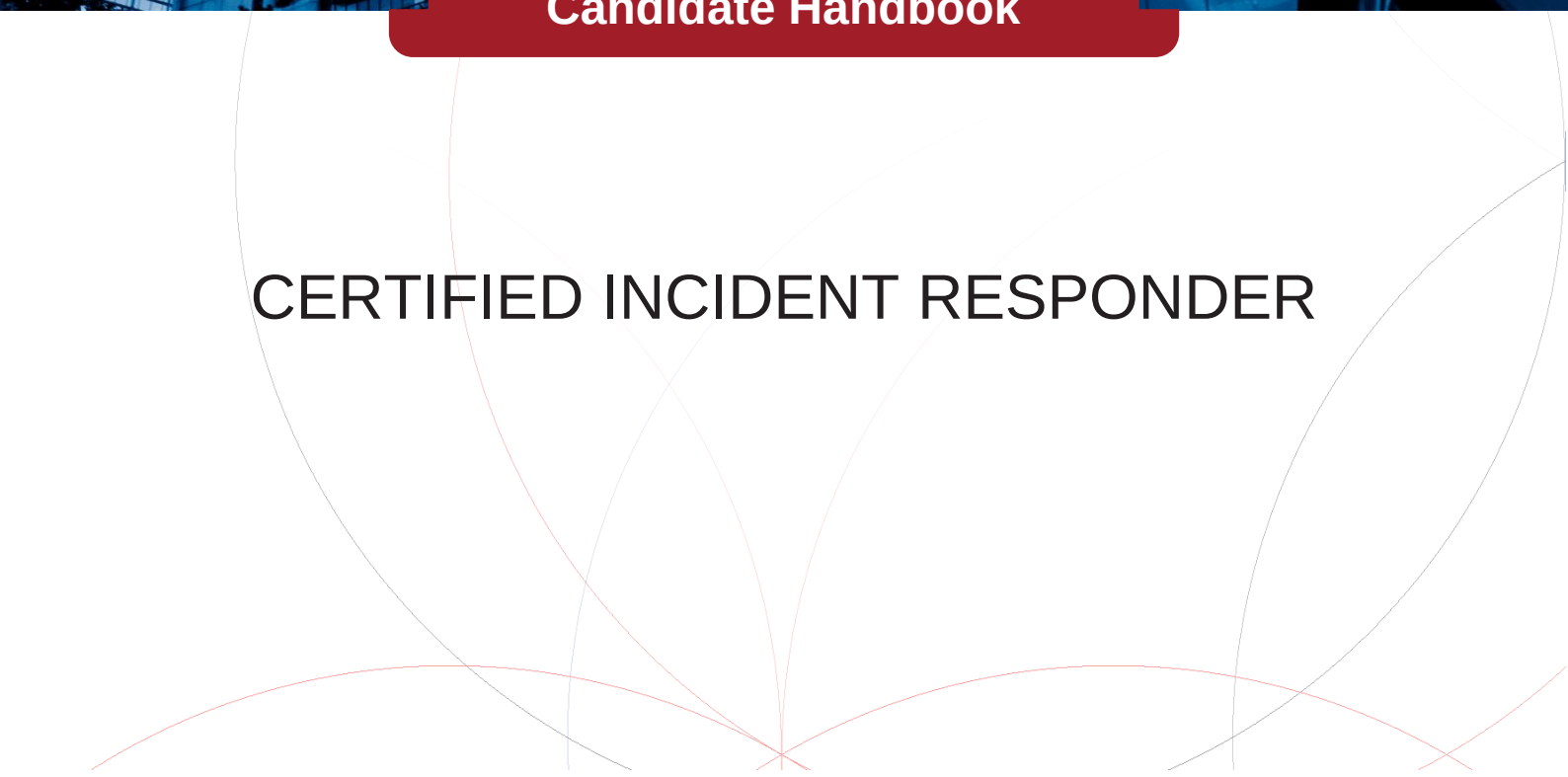




PECB

Candidate Handbook

CERTIFIED INCIDENT RESPONDER



Contents

SECTION I: INTRODUCTION.....	3
About PECB.....	3
Accreditations and Affiliations	3
PECB Code of Ethics.....	3
Introduction to Certified Incident Responder Certification	4
SECTION II: EXAM PROCESS, RULES AND POLICIES	5
Preparing For and Scheduling the Exam.....	5
Special Accommodations.....	5
Taking the Exam.....	5
Exam Results.....	6
Exam Retake Policy.....	6
Exam Security Policy	6
Exam Competency Domains	7
Sample Exam Questions.....	13
SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES	15
PECB Certified Incident Responder Credentials.....	15
Applying for Certification	15
Professional Experience	15
Professional References	16
Project Experience	16
Evaluation of Certification Applications.....	16
SECTION IV: CERTIFICATION MAINTENANCE POLICY	17
Renewing the Certification	17
Upgrade Credentials.....	17
Suspension of Certification	17
Revocation of Certification.....	17
Other Statuses.....	17
SECTION V: OTHER POLICIES	18
Application Fees for Examination and Certification	18
Complaint and Appeal Policy	18
Exams from Other Accredited Certification Bodies.....	18
Refund Policy.....	18

SECTION I: INTRODUCTION

About PECB¹

PECB is a leading certification body dedicated to fostering digital trust through comprehensive education, certification, and certificate programs across various disciplines. We empower professionals to develop and demonstrate their competence in digital security and other areas of expertise by providing world-class certification programs that adhere to internationally recognized standards.

Vision: As the global leader in digital trust education and certification, our vision is to empower and inspire professionals by enhancing their skills and fostering their professional success.

Mission: Our mission is to empower professionals with the knowledge and skills to protect their digital assets and ensure business continuity. Through our comprehensive programs, we aim to foster a secure digital ecosystem where innovation thrives and risks are managed effectively.

Values: Growth, Change, Harmony, Simplicity, Reliability, and Quality

Accreditations and Affiliations

At PECB, we are driven and culturally powered by a systemic process of continual improvement and professional development. As a testament to our high standards and commitment to providing quality services to our clients, PECB is accredited by a number of bodies and is a member of many professional organizations.

For detailed information on our accreditations and affiliations, click [here](#).

PECB Code of Ethics

The Code of Ethics is the set of values that PECB is committed to following, and defines the responsibilities of PECB professionals, including employees, trainers, examiners, invigilators, members of different committees, partners, distributors, certified individuals, and certificate holders. To read the PECB's Code of Ethics, click [here](#).

¹ Notes:

- The legal name of PECB is "PECB Group Pte. Ltd."
- PECB is an acronym that stands for "Professional Evaluation and Certification Board."
- Education (used in the first sentence of this page) refers to training courses developed by PECB, and offered globally through its network of partners.
- Certification refers to certification services provided according to ISO/IEC 17024. Certificate Program refers to certificate program services provided according to ANSI/ASTM E2659.
- "Certified" refers to ISO/IEC 17024 certifications' requirements and "Certificate holder" refers to ASTM E2659 certificate programs' requirements. Certificate holders are not certified, licensed, accredited, or registered to engage in a specific occupation or profession.

Introduction to Certified Incident Responder Certification

In a world where cyber threats are constant and ever-evolving, organizations must be equipped not only to defend against attacks but to respond swiftly and effectively when they occur. As the frequency and sophistication of cyber incidents continue to rise, from ransomware campaigns and data breaches to advanced persistent threats and living-off-the-land intrusions, the ability to manage them efficiently has become a critical organizational competency. The consequences of an unmanaged or poorly handled incident extend far beyond technical disruption: they carry financial, reputational, regulatory, and operational costs that can be severe and lasting.

The PECB Certified Incident Responder (CIR) certification is a globally recognized credential that validates the knowledge, skills, and competencies required to plan, execute, and manage cybersecurity incident response in a structured and efficient manner. Developed in alignment with internationally recognized frameworks the certification prepares professionals to lead and coordinate incident response operations that minimize damage, reduce recovery time, and prevent future occurrences.

The CIR training course provides candidates with a comprehensive understanding of the principles, methodologies, and techniques involved in every stage of the incident response life cycle. From preparation and threat intelligence through detection, containment, eradication, and recovery to post-incident analysis and organizational improvement, the course equips participants with both the theoretical grounding and the practical skills needed to respond effectively to a wide range of security incidents. Through hands-on labs and applied exercises using industry-standard tools, candidates develop the operational competencies required to perform under pressure and lead coordinated response efforts across technical and organizational boundaries.

Achieving the PECB Certified Incident Responder credential demonstrates a professional's ability to analyze threats, coordinate multidisciplinary teams and implement proactive measures that strengthen an organization's overall security posture. Certified professionals are equipped not only to respond to incidents but also to contribute strategically to an organization's cybersecurity governance and risk management framework, ensuring that every incident becomes an opportunity for continual improvement and long-term resilience.

This document specifies the PECB Certified Incident Responder certification scheme in compliance with ISO/IEC 17024. It also outlines the steps that candidates should take to obtain and maintain their credentials. As such, it is very important to carefully read all the information included in this document before completing and submitting your certification application.

If you have questions or need further information after reading it, please contact support@pecb.com.

SECTION II: EXAM PROCESS, RULES AND POLICIES

For detailed and most up-to-date information, you are advised to refer to the online **Exam Rules and Policies** by clicking [here](#).

Preparing For and Scheduling the Exam

To schedule the exam, candidates have two options:

1. **Online:** Through the [PECB Exams application](#). To schedule a remote exam, please go to the following link: [Exam Events](#).
2. **Paper-based:** By contacting the PECB authorized partner that provided the training course. The partner arranges the date, time, and location where the candidate is going to attend the exam.

For any changes with regard to the exam date, time, location, or other details, please contact support@pecb.com.

Special Accommodations

To ensure equal opportunities for all qualified persons, PECB will make reasonable accommodations for candidates, when appropriate. If candidates need special accommodations because of special needs (dyslexia, dyspraxia, ADHD, vision impairment, but not limited to) and temporary conditions (pregnancy, surgery, postoperative recovery, but not limited to), they can apply for such arrangements through the [myPECB](#) dashboard/ Enroll for an Exam. Any information that candidates provide regarding their special needs will be treated with confidentiality.

Taking the Exam

Candidates are required to arrive/be present at least 30 minutes before the exam starts. Candidates who arrive late will not receive additional time to make up for the delay and may not be allowed to sit for the exam.

Candidates are required to bring a valid identity card (national ID card, driver's license, or passport) and show it to the invigilator.

Online Exam Rules	Paper-Based Exam Rules
• Exams are provided electronically via the PECB Exams application. • The use of secondary electronic devices, such as tablets and phones, is not allowed during the exam. • The exam session is supervised remotely by a PECB Invigilator via the PECB Exams application and an external/integrated camera. • If requested on the day of the exam, additional time can be provided to candidates taking the exam in a non-native language, as follows: – 10 additional minutes for Foundation exams – 20 additional minutes for Manager exams – 30 additional minutes for Lead exams	• Exams are provided on paper, where candidates are not allowed to use anything but the exam paper and a pen. • The use of electronic devices, such as laptops, tablets, or phones, is not allowed. • The exam session is supervised by a PECB approved Invigilator at the location where the Partner has organized the training course. • If requested on the day of the exam, additional time can be provided to candidates taking the exam in a non-native language, as follows: – 10 additional minutes for Foundation exams – 20 additional minutes for Manager exams – 30 additional minutes for Lead exams

For specific information on exam types, languages available, and other details, please check the [List of PECB Exams](#).

Exam Results

Exam results will be communicated via email.

- The time span for the communication of exam results starts from the exam date and lasts three to eight weeks for essay type exams and two to four weeks for multiple-choice paper-based exams.
- For online multiple-choice exams, candidates receive their results instantly.

Candidates who successfully complete the exam will be able to apply for one of the credentials of the respective certification scheme.

For candidates who fail the exam, a list of the domains where they have performed poorly will be added to the email to help them prepare better for a retake.

If candidates disagree with the evaluation, they may request a re-evaluation of their exam results within 30 days from the date they receive their exam results. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

Exam Retake Policy

There is no limit to the number of times a candidate can retake an exam. However, there are certain limitations in terms of the time span between exam retakes. For more information, please visit this link: [Exam Rules and Policies - PECB](#).

Exam Security Policy

A significant component of a professional certification credential is maintaining the security and confidentiality of the exam. PECB relies upon the ethical behavior of certification holders and applicants to maintain the security and confidentiality of PECB exams.

Any disclosure of information about the content of PECB exams is a direct violation of PECB's Code of Ethics. PECB will take action against any individuals who violate such rules and policies, including permanently banning individuals from pursuing PECB credentials and revoking/invalidating any previous ones. PECB will also pursue legal action against individuals or organizations who infringe upon its copyrights, proprietary rights, and intellectual property.

Exam Competency Domains

The content of the exam is divided as follows:

Domain 1: Fundamental concepts of incident response

Main objective: Ensure that the candidate is able to interpret and apply fundamental concepts, phases, and methodologies of incident response.

Competencies	Knowledge statements
1. Ability to explain the main concepts of the incident response management system	1. Knowledge of the core principles and objectives of incident response
2. Ability to identify key stakeholders and roles in the incident response process	2. Knowledge of types and categories of cybersecurity incidents
3. Ability to explain the main phases of the incident response lifecycle (preparation, detection, containment, eradication, recovery, and lessons learned)	3. Knowledge of methods and tools used to identify the full path of malicious files and executables
4. Ability to identify indicators of compromise (IoCs) and recognize malicious artifacts within system directories and logs	4. Knowledge of distinguishing characteristics between ransomware, trojans, worms, and downloaders
5. Ability to determine the source and execution path of a malicious executable	5. Knowledge of common ransomware behaviors and ransom note structures
6. Ability to classify malware types based on behavior and observed indicators	6. Knowledge of best practices in evidence collection, documentation, and chain of custody
7. Ability to interpret and analyze ransom notes and other post-compromise artifacts	7. Knowledge of techniques to determine infection spread and affected assets
8. Ability to document and report findings accurately according to organizational policy	8. Knowledge of internal communication protocols and escalation paths during incident response
9. Ability to assess the impact and scope of an incident using available system data	9. Knowledge of common forensic tools and utilities used in incident response investigations
10. Ability to coordinate with stakeholders and communicate incident status clearly	10. Knowledge of post-incident review methodologies and improvement frameworks
11. Ability to use analysis tools (e.g., Process Explorer, Event Viewer, PowerShell commands) to gather relevant data	
12. Ability to evaluate the effectiveness of response activities and identify lessons learned	

Domain 2: Ransomware incident response

Main objective: Ensure the candidate is able to analyze, contain, and respond effectively to ransomware incident while preserving evidence.

Competencies	Knowledge statements
1. Ability to explain the ransomware attack lifecycle and identify its stages 2. Ability to analyze and differentiate the tactics, techniques, and procedures (TTPs) of major ransomware families, including Conti and Ryuk 3. Ability to detect ransomware activity using endpoint telemetry, network indicators, and SIEM correlation rules 4. Ability to perform evidence preservation and forensic artifact collection in a ransomware incident 5. Ability to apply a structured ransomware response playbook across all incident phases 6. Ability to contain, eradicate, and recover from a ransomware incident while minimizing business impact 7. Ability to assess legal, regulatory, and communication obligations arising from a ransomware incident 8. Ability to implement preventive and resilience controls to reduce the organization's exposure to ransomware 9. Ability to perform process analysis to identify ransomware activity in endpoint telemetry 10. Ability to evaluate backup architecture and recovery procedures for ransomware resilience 11. Ability to analyze RaaS operational models and their implications for incident attribution and response	1. Knowledge of ransomware taxonomy, including crypto ransomware, locker ransomware, wiper ransomware, doxware, and the Ransomware-as-a-Service (RaaS) model 2. Knowledge of the ransomware kill chain and its seven stages, from initial access through ransom demand 3. Knowledge of common initial access vectors exploited by ransomware actors, including phishing, exposed RDP, and supply chain compromise 4. Knowledge of the TTPs associated with Conti, Ryuk, and LockBit ransomware families and their respective MITRE ATT&CK mappings 5. Knowledge of double extortion and triple extortion techniques and their impact on response strategy 6. Knowledge of endpoint, network, and identity-based indicators of compromise applicable to ransomware detection 7. Knowledge of SIEM correlation rule logic for ransomware behavioral signatures, including shadow copy deletion, mass file modification, and C2 beaconing 8. Knowledge of forensic artifact types collected during ransomware investigations, including memory images, event logs, prefetch files, and MFT dumps 9. Knowledge of the procedures for containment, eradication, and recovery in ransomware incidents 10. Knowledge of backup strategy principles, including the 3-2-1-1-0 rule and immutable backup requirements 11. Knowledge of network segmentation, least-privilege principles, and multi-factor authentication as ransomware preventive controls

Domain 3: Malware in incident response

Main objective: Ensure that the candidate is able to analyze malware and respond effectively to malware incidents using structured analysis and response procedures.

Competencies	Knowledge statements
1. Ability to classify malware types and select the appropriate analysis technique for each 2. Ability to configure and use an isolated virtual analysis environment for safe malware examination 3. Ability to submit malware samples to sandbox platforms and interpret the resulting behavioral reports 4. Ability to conduct static analysis of suspicious files to extract indicators of compromise 5. Ability to triage and scope a malware incident based on capability assessment and system context 6. Ability to apply the NIST SP 800-61 incident handling phases to a malware incident 7. Ability to apply containment strategies appropriate to the malware's capability profile 8. Ability to identify and remove malware persistence mechanisms during eradication 9. Ability to restore systems and validate recovery integrity following a malware incident 10. Ability to integrate threat intelligence findings into detection rules and response workflows 11. Ability to produce a complete malware incident report with documented evidence and chain of custody 12. Ability to map malware behaviors to MITRE ATT&CK techniques and identify detection gaps	1. Knowledge of the main project management concepts, terminology, processes, and best practices 2. Knowledge of malware taxonomy, including viruses, worms, Trojans, rootkits, spyware, infostealers, botnet agents, and fileless malware 3. Knowledge of the three levels of malware analysis: automated dynamic analysis, targeted static analysis, and full reverse engineering 4. Knowledge of analysis environment configuration, isolation requirements, and sandbox evasion techniques employed by malware 5. Knowledge of static analysis tools and techniques, including strings extraction, PE structure inspection, import table analysis, and entropy analysis 6. Knowledge of the NIST SP 800-61 incident handling phases as applied to malware incidents: preparation, detection and analysis, containment, eradication, recovery, and post-incident activity 7. Knowledge of malware triage factors and incident severity classification criteria, including system criticality, data sensitivity, and malware capability 8. Knowledge of containment strategies applicable to different malware capability profiles, including infostealers, backdoors, and lateral movement malware 9. Knowledge of malware persistence mechanisms, including registry Run keys, scheduled tasks, Windows services, WMI subscriptions, and startup folders 10. Knowledge of eradication procedures and the conditions under which system rebuild is preferred over malware removal 11. Knowledge of recovery procedures, including system restoration from verified clean media and post-recovery monitoring requirements

Domain 4: Perimeter threat detection and response

Main objective: Ensure that the candidate is able to identify, analyze, and respond to external threats and perimeter breaches while building organizational resilience.

Competencies	Knowledge statements
1. Ability to identify and analyze perimeter breach indicators across network, firewall, and security event logs 2. Ability to classify external attack vectors and assess their scope and impact on the organization's perimeter 3. Ability to investigate and respond to content management system (CMS) compromise incidents, including web shell deployment 4. Ability to apply a structured detection-to-alert workflow for external threat events 5. Ability to correlate external threat indicators across multiple detection sources to produce an accurate incident timeline 6. Ability to assess the scope and business impact of a perimeter breach on organizational assets and services 7. Ability to develop and execute response procedures that address the root cause of a perimeter security incident 8. Ability to recommend and implement compensating controls following a perimeter security incident 9. Ability to translate incident findings into resilience improvements that reduce future exposure to external threats	1. Knowledge of perimeter breach indicators, including unauthorized access attempts, firewall rule violations, anomalous outbound connections, and failed authentication spikes 2. Knowledge of common external attack vectors, including web application attacks, credential stuffing, DNS hijacking, man-in-the-middle attacks, and exploitation of public-facing services 3. Knowledge of CMS vulnerabilities, common exploitation techniques, web shell characteristics, and indicators of CMS compromise 4. Knowledge of the detection-to-alert workflow, including log correlation logic, alert triage procedures, and escalation thresholds 5. Knowledge of network perimeter security technologies, including firewalls, intrusion detection and prevention systems (IDS/IPS), web application firewalls (WAF), and DMZ architecture 6. Knowledge of resilience principles applicable to perimeter security, including defense-in-depth, zero trust architecture, and network segmentation 7. Knowledge of external threat intelligence sources and their integration into perimeter detection and response capabilities 8. Knowledge of incident scope assessment procedures for perimeter breach scenarios, including affected asset identification and data-at-risk classification 9. Knowledge of post-incident hardening measures and compensating controls for perimeter security 10. Knowledge of the procedures for communicating perimeter breach findings to technical and non-technical stakeholders

Domain 5: Incident response to persistent mechanisms

Main objective: Ensure that the candidate is able to identify, analyze, and eradicate persistence mechanisms installed by threat actors during an incident, including fileless and living-off-the-land techniques.

Competencies	Knowledge statements
1. Ability to identify and catalog common persistence techniques used by threat actors across endpoint and server environments 2. Ability to detect and analyze fileless persistence mechanisms, including registry-based payload storage and PowerShell-based techniques 3. Ability to identify living-off-the-land (LotL) persistence techniques that abuse legitimate Windows system tools and built-in scripting capabilities 4. Ability to differentiate between malicious persistence artifacts and legitimate administrative scheduled tasks, services, and registry entries 5. Ability to develop detection rules targeting persistence behaviors in endpoint telemetry, Windows Event Logs, and SIEM platforms 6. Ability to map identified persistence techniques to the MITRE ATT&CK Persistence tactic and its sub-techniques 7. Ability to remove all identified persistence mechanisms during the eradication phase of incident response 8. Ability to verify the completeness of eradication by confirming the removal of all persistence artifacts before initiating recovery	1. Knowledge of common persistence techniques, including registry Run and RunOnce keys, scheduled tasks, Windows services, startup folder entries, and WMI event subscription 2. Knowledge of fileless persistence mechanisms, including PowerShell profile modification, registry-based shellcode storage, and AMSI bypass techniques 3. Knowledge of registry-based persistence locations most commonly abused by threat actors, including HKCU\Software\Microsoft\Windows\CurrentVersion\Run and related keys 4. Knowledge of living-off-the-land (LotL) persistence techniques that abuse legitimate Windows tools, including PowerShell, WMI, COM object hijacking, and DLL search-order hijacking 5. Knowledge of the MITRE ATT&CK Persistence tactic, its sub-techniques, and their corresponding detection and mitigation guidance 6. Knowledge of the forensic artifacts associated with persistence mechanism installation and execution, including registry hive entries, Prefetch files, and Sysmon event records 7. Knowledge of detection methods for persistence behaviors using Sysmon event IDs, Windows Security Event Log entries, and EDR behavioral analytics 8. Knowledge of eradication procedures specific to each persistence mechanism category, including registry key removal, scheduled task deletion, and service deregistration 9. Knowledge of the conditions under which system rebuild is required to achieve complete eradication of persistence 10. Knowledge of post-eradication validation procedures used to confirm that no residual persistence artifacts remain before recovery begins

Based on the above-mentioned domains and their relevance, the exam contains **20 hands-on questions**, as summarized in the table below:

			Level of understanding (Cognitive/Taxonomy) required	
			Questions that measure comprehension, application, and analysis	Questions that measure evaluation
Competency domains	Fundamental concepts of incident response	Number of questions/points per competency domain	% of the exam devoted/points to/for each competency domain	
	Ransomware incident response	4	20	X
	Malware incident response	4	20	X
	Perimeter threat detection and response	4	20	X
	Incident response to persistent mechanisms	5	25	
		3	15	X
Total		20	100%	
Number of questions per level of understanding			12	8
% of the exam devoted to each level of understanding (cognitive/taxonomy)			60%	40%

The passing score of the exam is **70%**.

This exam comprises hands-on technical questions: The hands-on lab exam is designed to evaluate candidates' ability to apply their knowledge and skills in practical, real-world contexts. Candidates are expected to demonstrate technical proficiency by configuring, troubleshooting, and optimizing systems; analyzing and solving problems; and integrating multiple concepts to achieve functional solutions. The exam emphasizes practical competence, accuracy, and efficiency, focusing on how well candidates can translate theoretical understanding into effective technical execution.

This is an open-book exam. The candidate is allowed to use the following reference materials:

- Training course materials (accessed through the PECB Exams app and/or printed)
- Any personal notes taken during the training course (accessed through the PECB Exams app and/or printed)

A sample of exam questions will be provided below.

Sample Exam Questions

Assume you are in a production environment investigating a user-reported issue on Windows06 where files are inaccessible. Look for common ransomware indicators, such as:

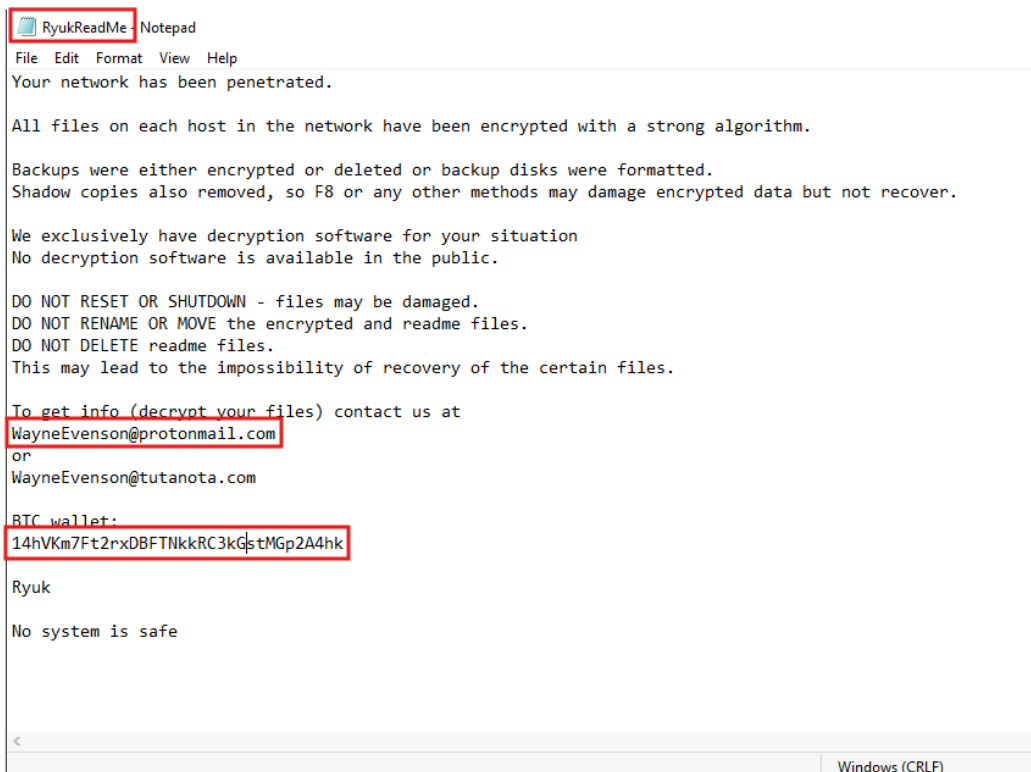
- Ransom notes present in various folders
- Error messages when attempting to open files
- Files that open but display unreadable, encrypted content

These observations strongly suggest a ransomware infection.

Review the ransom note created by Ryuk executable file and answer the following questions:

Questions:

1. What is the file name of the ransom note?
2. The ransom note provides two email addresses for the user to contact in order to get their data decrypted. What is the full ProtonMail address?
3. What Bitcoin (BTC) wallet address has been provided?



```
RyukReadMe - Notepad
File Edit Format View Help
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
WayneEvenson@protonmail.com
or
WayneEvenson@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk

No system is safe

Windows (CRLF)
```

Answers:

1. RyukReadMe
2. WayneEvenson@protonmail.com
3. 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Review the Sysmon logs in Splunk to identify the necessary information and answer the following questions.

Questions:

1. At which registry location is the new key added?
2. What is the name of the new registry entry that is added?
3. What is the associated executable image of the first (chronologically) event seen?
4. What is the associated executable image of the second (chronologically) event seen?

Event

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}' /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2025-06-24T06:08:57.939754300Z' /><EventRecordID>2606</EventRecordID><Correlation><Execution ProcessID='3008' ThreadID='3552' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>windows06</Computer><Security UserID='S-1-5-18' /></System><EventData><Data Name='RuleName'>technique_id=T1012,technique_name=Query Registry</Data><Data Name='UtcTime'>2025-06-24 06:08:57.935</Data><Data Name='ProcessGuid'>{772e1828-40f9-685a-1901-000000001000}</Data><Data Name='ProcessId'>6540</Data><Data Name='Image'>C:\Windows\System32\reg.exe</Data><Data Name='FileVersion'>10.0.17763.1 (WinBuild.160101.0800)</Data><Data Name='Description'>Registry Console Tool</Data><Data Name='Product'>Microsoft® Windows® Operating System</Data><Data Name='Company'>Microsoft Corporation</Data><Data Name='OriginalFileName'>reg.exe</Data><Data Name='CommandLine'>REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ /d "C:\users\Public\jMxwR.exe" /f</Data><Data Name='CurrentDirectory'>C:\Users\ComtechAdmin\Desktop</Data><Data Name='User'>WINDOWS06\ComtechAdmin</Data><Data Name='LogonGuid'>{772e1828-4085-685a-899f-050000000000}</Data><Data Name='LogonId'>0x59f89</Data><Data Name='TerminalSessionId'>1</Data><Data Name='IntegrityLevel'>High</Data><Data Name='Hashes'>SHA1=429DF8371B437209D79DC97978C33157D1A71C4B,MD5=8A93ACAC33151793F8D5200071C0B06,SHA256=19316D4266D0B776D9B2A05D5903D8CBC8F0EA1520E9C2A7E6D5960B6FA4DCAF,IMPHASH=BE482BE427FE212CFEF2CDA0E61F19AC</Data><Data Name='ParentProcessGuid'>{772e1828-40f9-685a-1701-000000001000}</Data><Data Name='ParentProcessId'>6436</Data><Data Name='ParentImage'>C:\Windows\System32\cmd.exe</Data><Data Name='ParentCommandLine'>"C:\Windows\System32\cmd.exe" /C REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ /d "C:\users\Public\jMxwR.exe" /f</Data><Data Name='ParentUser'>WINDOWS06\ComtechAdmin</Data></EventData></Event>
```

host = windows06 | source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | sourcetype = xmlwineventlog

Answers:

1. HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
2. Svchos
3. C:\Windows\System32\cmd.exe
4. C:\Windows\System32\reg.exe

SECTION III: CERTIFICATION PROCESS, RULES AND POLICIES

PECB Certified Incident Responder Credentials

All PECB certifications have specific requirements regarding professional experience. To determine which credential is right for you, take into account your professional needs and analyze the criteria for the certifications.

The credentials in the PECB Certified Incident Responder scheme have the following requirements:

Credential	Exam	Professional experience	Project experience	Other requirements
PECB Certified Provisional Incident Responder	PECB Certified Incident Responder exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified Incident Responder (CIR)		Five years: two years of work experience in incident response or cybersecurity	300 hours	

To be considered valid, the implementation activities should follow best implementation and management practices and include the following:

1. Monitoring and analyzing system and network logs to detect suspicious activities
2. Conducting initial triage and classification of security events and incidents
3. Assisting in the containment, eradication, and recovery phases of security incidents
4. Collaborating with IT and security teams to execute incident response playbooks
5. Engaging in post-incident reviews to capture lessons learned and recommend improvements
6. Maintaining up-to-date knowledge of common attack techniques and threat actor behaviors

For detailed and most up-to-date information, you are advised to refer to the online **Certification Process** by clicking [here](#).

Applying for Certification

All participants who successfully pass their certification exam (or an equivalent accepted by PECB) are entitled to apply for the PECB credentials they were examined for. Specific professional requirements will need to be fulfilled to be PECB certified.

The application process is very simple and takes only a few minutes:

- [Create](#) your account
- Check your email for the confirmation link
- [Log in](#) and click on Apply for Certificate

The approval of the application occurs when the Certification Department validates that you fulfil all the certification requirements regarding the credential you have applied for. An email will be sent to the address you provided during your application to update you on your application status. If approved, you will then be able to download your certificate and digital badge from your member account.

Professional Experience

Candidates must provide complete and correct information regarding their professional experience, including job title(s), start and end date(s), job description(s), and more. Candidates are advised to

summarize their previous or current assignments, providing sufficient details to describe the nature of the responsibilities for each job. More detailed information can be included in the CV.

Professional References

For each application, two professional references are required. Professional references shall be individuals who have worked with you in a professional environment and can validate your expertise in the respective field, current, and previous work history. You cannot use as a reference the persons who fall under your supervision or are a relative of yours.

Project Experience

The candidate's project log will be checked to ensure that the candidate has the required number of implementation hours.

Evaluation of Certification Applications

The Certification Department will evaluate each application to validate the candidates' eligibility for certification or certificate program. A candidate whose application is being reviewed will be notified in writing and, if necessary, given a reasonable time frame to provide any additional documentation. If a candidate does not respond by the deadline or does not provide the required documentation within the given time frame, the Certification Department will validate the application based on the initial information provided, which may lead to the candidates' credential downgrade.

PECB can deny certification/certificate program if candidates:

- Falsify the application
- Violate the exam procedures
- Violate the PECB Code of Ethics
- Fail the exam

If applicants have any concerns regarding the denial of certification/certificate program, they may file an appeal by following the complaint and appeal process [Complaint and Appeal Policy](#).

The application payment for the certification/certificate program is nonrefundable. This is due to the application verification process, the evidence submitted by the candidates, and the involvement of the relevant departments.

If candidates pass the exam, they can apply for the certificate within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats. Even though the certification period expires, candidates have the right to reopen their case. However, PECB will no longer be responsible for any changes regarding the conditions, standards, policies, and candidate handbook that were applicable before the case was closed. A candidate requesting their case to reopen must do so in writing to certification.team@pecb.com and pay the required fee.

SECTION IV: CERTIFICATION MAINTENANCE POLICY

For detailed and most up-to-date information, you are advised to refer to the online **Certification Maintenance Policy** by clicking [here](#).

Renewing the Certification

PECB certifications are valid for three years. To maintain them, PECB certified professionals must meet the requirements related to the designated credential, e.g., they must fulfill the required number of continuing professional development (CPD) hours. In addition, they need to pay the annual maintenance fee.

Upgrade Credentials

PECB Certifications can be upgraded online through your dashboard by logging in [here](#), clicking **View Certificate**, and then clicking the **Upgrade** button. For more information on the upgrade requirements and fees, go to the [Certification Maintenance](#) page on the PECB website.

Suspension of Certification

Failure to submit the CPD and AMF payment during the certification cycle will result in a 12-month suspension period, during which you can address any outstanding AMFs and CPDs. In addition to these, the certification may be suspended for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been suspended are not authorized to further promote their certification while it is suspended.

Suspended members must remediate their suspension within a maximum period of 12 months.

Revocation of Certification

PECB can revoke (that is, withdraw) certification if the candidate fails to address the outstanding AMFs and CPDs during the 12-month suspension period. In addition to these, certification may be revoked for other reasons listed in the **Certification Maintenance Policy**. Individuals whose certification has been revoked are not authorized to use any references to a certified status.

If candidates disagree with any certification decision (certification level, suspension, or revocation) they may request a re-evaluation within 30 days from the date they receive their certification decision. If still not satisfied, they can file an appeal through the [PECB Ticketing System](#) within 30 days from the date they receive the re-evaluation decision. Appeals received after 30 days will not be processed. For more detailed information, please refer to [Complaint and Appeal Policy](#).

Other Statuses

Besides being active, suspended, or revoked, a certification can be voluntary withdrawn, or designated as Emeritus. For more information, go to the [Certification Maintenance](#) page on the PECB website.

SECTION V: OTHER POLICIES

Application Fees for Examination and Certification

Candidates may take the exam without attending the training course. The applicable prices are as follows:

- Lead Exam: \$1000²
- Manager Exam: \$700
- Foundation Exam: \$500
- Transition Exam: \$500

The application fee for certification is as follows:

- Master Certification: \$100
- Foundation Certification: \$200
- Transition Certification: \$200
- All other Certifications: \$500

For candidates who complete a training, eLearning, or self-study course delivered by a PECB Partner, the training fee includes the first exam attempt, one free retake, the certification application fee, and the first year of the Annual Maintenance Fee (AMF). This cycle must be completed within 12 months from the course completion date for instructor-led training, or within 12 months from the purchase date for self-study and eLearning formats.

Complaint and Appeal Policy

A person wishing to file a complaint or an appeal can do so by submitting a [service ticket](#) and selecting the corresponding category in the topic dropdown menu: “file a complaint” or “file a certification/certificate program appeal”. Before filing a complaint or an appeal, make sure to follow the [complaint and appeal policy](#).

Exams from Other Accredited Certification Bodies

PECB accepts exams from other recognized accredited certification bodies. PECB will evaluate the requests through its equivalence process to decide whether the respective exam(s) can be accepted as equivalent to the respective PECB certification.

Refund Policy

PECB will refund your payment if the requirements of the Refund Policy are met. To read the Refund Policy, click [here](#).

² All prices listed in this document are in US dollars.



Contact PECB Support at
support@pecb.com



Telephone number
+1-844-426-7322



Visit our [Help Center](#) to access manuals, FAQs, and quick guides, or reach us directly via Live Chat or by submitting a ticket [here](#).

Follow us on:



www.pecb.com