OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen ITS Cybersecurity

Cybersécurité
(IT Specialist niveau fondations)

Certification : IT Specialist: Cybersecurity

Niveau : Foundation / Entry-level | Public : Analystes SOC juniors / Techniciens cybersécurité / Étudiants

1. Présentation de la certification

L'examen **IT Specialist: Cybersecurity (ITS Cybersecurity)**, délivré par **Pearson** via Certiport, valide les compétences fondamentales en les fondamentaux de la cybersécurité, la protection des systèmes et la réponse aux incidents. Cette certification atteste de votre capacité à maîtriser les concepts et pratiques essentiels du domaine, selon les bonnes pratiques de l'industrie.

La réussite de cet examen unique conduit à l'obtention de la certification **IT Specialist en Cybersecurity**, reconnue internationalement par les employeurs et les institutions éducatives. Les ITS sont des certifications **entry-level** posées comme première brique du parcours IT, souvent validées avant les certifications constructeurs (Microsoft, Cisco, AWS, Google).

Informations clés

Code de l'examen	ITS Cybersecurity (ITS-Cybersec)
Intitulé officiel	IT Specialist: Cybersecurity
Certification obtenue	IT Specialist en Cybersecurity
Technologie ciblée	Cybersecurity
Éditeur officiel	Pearson (Pearson VUE / Certiport)
Centre de test	Certiport (Pearson VUE) — OpenCertif est centre Certiport autorisé
Niveau	Foundation / Entry-level
Programme	IT Specialist (ITS) — certifications industry-recognized
Format de l'examen	QCM scenarios + drag-and-drop + matching items + hot spot questions
Durée de l'examen	50 minutes
Nombre de questions	Environ 40 questions
Score requis	700 sur 1000 (≈ 70 %)
Prérequis recommandé	Environ 150 heures de pratique (recommandation Pearson / Certiport)

Langue de l’examen	Anglais (autres langues selon disponibilité régionale)
Âge minimum recommandé	13 ans et plus
Validité de la certification	Permanente sur la version passée (liée à la version technologique ciblée)
Politique de reprise	Délai d’attente de 24 heures avant la 1re reprise (voucher retake à utiliser sous 60 jours)
Modalité	En centre Certiport agréé (CATC) avec Compass — OpenCertif est centre Certiport autorisé
Badge numérique	Badge officiel délivré via Credly après réussite
Position dans le catalogue	Brique fondamentale du parcours IT — souvent passée avant les certifications constructeurs (Microsoft, Cisco, AWS, etc.)

2. Profil du candidat

En tant que candidat à l'examen ITS Cybersecurity, vous développez et validez des compétences fondamentales en cybersecurity. Vous êtes capable de :

- Comprendre les **fondamentaux de la cybersécurité** et son importance.
- Connaître la **CIA Triad** : Confidentiality, Integrity, Availability.
- Identifier les **menaces (threats)** et **acteurs malveillants** : script kiddies, insiders, hacktivists, APT, nation-states.
- Comprendre les types d'**attaques** : malware, phishing, DoS, MITM, ransomware.
- Comprendre la **cryptographie** de base : symétrique, asymétrique, hashing.
- Gérer l'**authentication** : passwords, MFA, biometrics, SSO.
- Configurer l'**authorization** : RBAC, ACL, principle of least privilege.
- Comprendre la **sécurité réseau** : firewall, IDS / IPS, VPN, segmentation.
- Gérer la **sécurité endpoint** : antivirus, EDR, patch management.
- Gérer la **sécurité applicative** : OWASP Top 10, secure coding.
- Comprendre les fondamentaux de l'**incident response** : NIST 800-61.
- Connaître les **frameworks** : NIST CSF, ISO 27001, MITRE ATT&CK.;
- Gérer la **compliance** : RGPD, PCI DSS, HIPAA.
- Sensibiliser aux **bonnes pratiques** : security awareness, phishing simulations.

L'examen évalue spécifiquement les familles de compétences essentielles à tout débutant en cybersecurity :

- Security fundamentals et CIA Triad
- Threats, attacks et adversaires
- Cryptographie
- Authentication et authorization
- Network et endpoint security
- Incident response et compliance

3. Prérequis et public cible OpenCertif

Aucun prérequis académique formel n'est exigé. Pearson et Certiport recommandent toutefois :

- **150 heures de pratique cybersécurité et concepts**.
- Connaissance préalable des fondamentaux réseau (ITS Networking recommandé).
- Notions d'OS Windows et Linux.
- Accès à un lab : VirtualBox, Kali Linux pour les manipulations.
- Anglais niveau intermédiaire (vocabulaire technique).
- Curiosité pour les enjeux de sécurité et veille technique.

Public cible OpenCertif

- Analystes SOC juniors (niveau 1).

- Techniciens cybersécurité débutants.
- Étudiants en BTS SIO option SISR, BTS cybersécurité, DUT Réseaux.
- Profils en reconversion vers la cybersécurité.
- Auditeurs IT juniors.
- Candidats aux certifs avancées : **CompTIA Security+**, **CEH**, Cisco CCNA Security.
- Officers sécurité IT juniors.
- Profils en parcours d’initiation (avant CEH, EHE EC-Council).

4. Domaines de compétences mesurées

L'examen est structuré autour de 6 grands domaines de compétences. Le tableau ci-dessous indique le poids relatif de chaque domaine dans l'évaluation finale (version 2026 — aligné sur la version actuelle ITS Pearson). Les pondérations sont des estimations issues du guide officiel Unity / Certiport.

Domaine	Intitulé	Pondération
1	Security fundamentals et CIA Triad	15 %
2	Threats, attacks et adversaires	20 %
3	Cryptographie	15 %
4	Authentication et authorization	15 %
5	Network et endpoint security	20 %
6	Incident response et compliance	15 %

*Remarque : l'examen UCU Programmer dure environ 50 minutes pour 40 questions, soit environ 1 minute 15 par question. La gestion du temps est essentielle. Le score requis pour valider est de **500 sur 700** (sur une échelle officielle Unity de 200 à 700 points).*

5. Détail des compétences mesurées

Cette section détaille de manière exhaustive l'ensemble des compétences couvertes par l'examen ITS Cybersecurity, en s'appuyant sur les Objective Domains publiés par Certiport et Unity Technologies (version 2026 — aligné sur la version actuelle ITS Pearson).

1 Security fundamentals et CIA Triad — 15 %

1.1 Concepts fondamentaux

- **Confidentiality** : empêcher la divulgation.
- **Integrity** : assurer que la donnée n'est pas altérée.
- **Availability** : la donnée est accessible quand nécessaire.
- Non-repudiation et accountability.

1.2 Defense in Depth

- Couches : physical, perimeter, network, host, app, data.
- Defense in Depth strategy.
- Zero Trust Architecture (notions).

1.3 Risk Management

- Risk = Threat × Vulnerability × Impact.
- Risk treatment : avoid, transfer, mitigate, accept.
- Business Impact Analysis (BIA).

2 Threats, attacks et adversaires — 20 %

2.1 Threat actors

- Script kiddies (débutants).
- Hacktivists (motivations politiques).
- **APT** (Advanced Persistent Threats), nation-states.
- Insiders (intentionnels et accidentels).
- Cybercriminels et organized crime.

2.2 Types de malware

- **Virus**, **worm**, **trojan**, **ransomware**.
- **Spyware**, **adware**, **keylogger**.
- **Rootkit** et bootkit.
- **RAT** (Remote Access Trojan).
- Fileless malware.

2.3 Attaques courantes

- **Phishing**, spear phishing, whaling, vishing, smishing.
- **Social engineering** : pretexting, baiting.
- **DoS / DDoS**.
- **MITM** (Man-In-The-Middle).
- **SQL injection**, **XSS**, **CSRF**.
- **Brute force** et credential stuffing.

2.4 Kill chain et MITRE ATT&CK;

- **Cyber Kill Chain** (Lockheed Martin).
- **MITRE ATT&CK;** : tactics, techniques, procedures (TTPs).
- Diamond Model.

3 Cryptographie — 15 %

3.1 Symétrique

- **AES** (128, 192, 256 bits).
- DES, 3DES (legacy), ChaCha20.
- Clé partagée.

3.2 Asymétrique

- **RSA**, **ECC**, **Diffie-Hellman**.
- Public key / private key.
- Signatures numériques.

3.3 Hashing

- **SHA-256**, SHA-3.
- MD5 et SHA-1 obsolètes.
- **bcrypt**, Argon2 pour passwords.
- Salt et pepper.

3.4 PKI et TLS

- **PKI** (Public Key Infrastructure).
- Certificats X.509.
- CA (Certificate Authority).
- **TLS / SSL** handshake.

4 Authentication et authorization — 15 %

4.1 Authentication factors

- Something you **know** (password).
- Something you **have** (token, card).
- Something you **are** (biometrics).
- Somewhere you **are** (location).
- Something you **do** (behavior).

4.2 Passwords et MFA

- Password policies : complexity, length, expiration.
- Password managers.
- **MFA** (Multi-Factor Authentication) : TOTP, SMS, push.
- Hardware tokens : YubiKey, FIDO2.

4.3 SSO et federation

- **SSO** (Single Sign-On).
- **SAML**, **OAuth 2.0**, **OIDC**.
- Identity providers : Okta, Azure AD, Google Workspace.

4.4 Authorization

- **RBAC** (Role-Based Access Control).
- **ABAC** (Attribute-Based Access Control).
- ACL (Access Control Lists).
- Principle of least privilege.

5 Network et endpoint security — 20 %

5.1 Network security

- **Firewalls** : stateful, NGFW.
- **IDS / IPS**.
- **VPN** : IPsec, SSL.
- Network segmentation et VLANs.
- DMZ.

5.2 Endpoint security

- **Antivirus** et **EDR** (Endpoint Detection and Response).
- Host-based firewall.
- Patch management.
- Application whitelisting.

5.3 Web et app security

- **OWASP Top 10** : Injection, Broken Auth, XSS, etc.
- **WAF** (Web Application Firewall).
- Secure coding practices.
- Input validation et output encoding.

5.4 Cloud security

- Shared Responsibility Model.
- IAM cloud.
- Encryption at rest et in transit.
- Cloud Access Security Broker (CASB).

6 Incident response et compliance — 15 %

6.1 Incident Response

- **NIST 800-61** 4 phases : Preparation, Detection & Analysis, Containment Eradication Recovery, Post-Incident.
- Incident Response Plan (IRP).
- Communication et reporting.

6.2 SOC et SIEM

- **Security Operations Center (SOC)**.
- **SIEM** : Splunk, ELK, QRadar, Sentinel.
- Log analysis.
- Threat intelligence.

6.3 Forensics basics

- Chain of custody.
- Acquisition d’artefacts.
- Memory et disk forensics.

6.4 Compliance et frameworks

- **NIST Cybersecurity Framework** (Identify, Protect, Detect, Respond, Recover).
- **ISO 27001** ISMS.
- **RGPD / GDPR**.
- **PCI DSS**, **HIPAA**, **SOC 2**.
- **MITRE ATT&CK;** et CIS Controls.

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au ITS Cybersecurity à travers un parcours blended-learning complet, combinant ressources e-learning interactives, projets pratiques en CIA Triad, threats, malware, encryption, authentication, incident response et compliance et accompagnement tutoré.

Format de la formation

Durée recommandée	150 heures de pratique Cybersecurity recommandées par Pearson / Certiport (OpenCertif structure ce parcours sur 50 à 70 heures de formation tutorée complétées par 80 à 100 heures de projet et exercices)
Modalité	100 % distanciel asynchrone, ou blended (distanciel + classes virtuelles)
Support pédagogique	Unity Certified User Courseware officiel (GMetrix) + ressources OpenCertif (modules Rise 360, scénarios immersifs)
Plateforme LMS	lmsopencertif.fr (Moodle) — accès 24/7 pendant 12 mois
Encadrement	Tutorat asynchrone par expert Unity certifié + classes virtuelles bimensuelles
Pratique requise	Au moins 150 heures de pratique Unity (recommandation officielle Unity Technologies)
Évaluations	Quiz formatifs par module, 3 projets pratiques Unity, examens blancs CertPREP
Certification finale	Passage de l’examen ITS Cybersecurity en centre OpenCertif (CATC Certiport)

Parcours d’apprentissage proposé

- **Module 1 :** CIA Triad et fondamentaux.
- **Module 2 :** Defense in Depth et Zero Trust.
- **Module 3 :** Risk Management.
- **Module 4 :** Threat actors et APT.
- **Module 5 :** Types de malware.
- **Module 6 :** Phishing et social engineering.
- **Module 7 :** DoS / DDoS et MITM.
- **Module 8 :** Attaques web : SQLi, XSS, CSRF.

- **Module 9 :** Cyber Kill Chain et MITRE ATT&CK.;
- **Module 10 :** Cryptographie symétrique et asymétrique.
- **Module 11 :** Hashing et PKI.
- **Module 12 :** TLS / SSL.
- **Module 13 :** Authentication factors et MFA.
- **Module 14 :** SSO, SAML, OAuth, OIDC.
- **Module 15 :** Authorization : RBAC, ABAC, ACL.
- **Module 16 :** Firewalls, IDS / IPS, VPN.
- **Module 17 :** Endpoint security : antivirus, EDR.
- **Module 18 :** OWASP Top 10 et WAF.
- **Module 19 :** Cloud security.
- **Module 20 :** Incident Response NIST 800-61.
- **Module 21 :** SOC et SIEM.
- **Module 22 :** Forensics basics.
- **Module 23 :** NIST CSF et ISO 27001.
- **Module 24 :** RGPD, PCI DSS, HIPAA.
- **Module 25 :** Examen blanc CertPREP.

7. Ressources d’étude officielles

En complément du parcours OpenCertif, les ressources officielles Unity Technologies et Certiport suivantes sont fortement recommandées :

- Documentation officielle Cybersecurity (sources éditeur).
- Page Certiport officielle : certiport.pearsonvue.com/Certifications/IT-Specialist.
- Page Pearson IT Specialist : pearson.com / itspecialist.
- **CertPREP Practice Tests (GMetrix)** — examens blancs Certiport pour ITS.
- **LearnKey courses** pour IT Specialist — self-paced video learning.
- Tutoriels gratuits et documentation Cybersecurity.
- Communautés : **Stack Overflow**, **GitHub**, **Reddit** (selon technologie).
- Plateformes d’apprentissage : **Coursera**, **edX**, **Udemy**, **Pluralsight**.
- Badge officiel délivré via **Credly** (credly.com).
- Page Pearson VUE pour la réservation : home.pearsonvue.com.
- Pages OpenCertif dédiées : opencertif.fr / its.

8. Modalités de passage de l’examen

Inscription	Via OpenCertif ou directement auprès d’un centre Certiport
Centre d’examen	OpenCertif — Centre Certiport Authorized Testing Center (CATC) / Pearson VUE
Mode de passage	En centre uniquement (Unity n’autorise pas l’examen OnVUE à distance pour les certifications UCU — présence sur site requise)
Pièce d’identité	1 pièce d’identité avec photo obligatoire le jour de l’examen (pour les mineurs : autorisation parentale et CNI / passeport)
Aménagements	Demande possible auprès de Certiport (temps additionnel, assistance technique)
Résultat	Score communiqué immédiatement à la fin de l’examen (échelle 200-700, seuil de réussite 500)
Validité de la certification	3 ans à partir de la date de réussite — attribuée une seule fois (stackable, pas de renouvellement payant requis)
Politique de reprise	Délai d’attente de 24 heures avant la 1re reprise. Voucher retake à utiliser sous 60 jours après l’échec.

Badge numérique	Badge officiel délivré via Credly et intégrable à LinkedIn, CV, portfolio, sites de recrutement

9. Contact et inscription

Pour toute information complémentaire, demande de devis ou inscription à la formation préparatoire au ITS Cybersecurity, l'équipe OpenCertif reste à votre disposition. OpenCertif est un Centre Certiport Authorized Testing Center (CATC) habilité à délivrer les certifications Unity Certified User.

OpenCertif
Centre de formation et de certification

app.opencertif.fr
lmsopencertif.fr

Centre agréé Certiport / Pearson VUE
Certifié Qualiopi — Actions de formation

10. Mentions légales et version

Ce syllabus est établi par OpenCertif sur la base des Objective Domains officiels publiés par Certiport pour la certification ITS Cybersecurity, dans sa version applicable (version 2026 — aligné sur la version actuelle ITS Pearson). Les compétences mesurées, les pondérations et les objectifs présentés reflètent fidèlement la structure de l'examen telle que publiée par Unity Technologies via Certiport.

Version du syllabus : 2026.05 — Édition mai 2026
Source officielle Certiport : certiport.pearsonvue.com/Certifications/Unity/Certified-User/Certify
Source officielle Unity : unity.com/products/unity-certifications/user-programmer
Page OpenCertif : opencertif.fr/unity-user-programmer