OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen ITS Network Security

Sécurité réseau
(IT Specialist niveau fondations)

Certification : IT Specialist: Network Security

Niveau : Foundation / Entry-level | Public : Techniciens sécurité réseau / Analystes SOC juniors

1. Présentation de la certification

L'examen **IT Specialist: Network Security (ITS Network Security)**, délivré par **Pearson** via Certiport, valide les compétences fondamentales en la sécurité des réseaux et la protection des systèmes contre les menaces. 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 Network Security**, 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 Network Security (ITS-NetSec)
Intitulé officiel	IT Specialist: Network Security
Certification obtenue	IT Specialist en Network Security
Technologie ciblée	Network Security
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 Network Security, vous développez et validez des compétences fondamentales en network security. Vous êtes capable de :

- Comprendre les principes de **Defense in Depth**.
- Connaître la **CIA Triad** : Confidentiality, Integrity, Availability.
- Identifier les **types de menaces** : malware, phishing, DDoS, MITM, social engineering.
- Configurer un **firewall** avec règles d'entrée et sortie.
- Différencier **IDS** (Intrusion Detection) et **IPS** (Prevention).
- Configurer un **VPN** : site-to-site et remote access.
- Comprendre les bases de **cryptographie** : symétrique, asymétrique, hashing.
- Connaître les **protocoles sécurisés** : HTTPS, SSH, SFTP, IPsec, TLS / SSL.
- Connaître les **standards** : WPA2, WPA3, 802.1X.
- Gérer l'**AAA** : Authentication, Authorization, Accounting.
- Configurer le **hardening** Windows et Linux.
- Mettre en place des contre-mesures basiques contre attaques web (XSS, SQLi).
- Notions d'incident response et de log analysis.
- Connaître les frameworks compliance : ISO 27001, NIST, RGPD.

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

- Defense in Depth et fondamentaux
- Network Security et firewall
- Software et OS Security
- Threats, attacks et vulnérabilités
- Cryptographie et protocoles
- Wireless security et compliance

3. Prérequis et public cible OpenCertif

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

- **150 heures de pratique réseau et sécurité**.
- Connaissance préalable des fondamentaux réseau (ITS Networking en prerequis recommandé).
- Accès à un lab de tests : Packet Tracer, Kali Linux, VirtualBox.
- Notions de systèmes d'exploitation Windows et Linux.
- Anglais niveau intermédiaire (vocabulaire technique).

Public cible OpenCertif

- Techniciens sécurité réseau juniors.
- Sysadmins se spécialisant en sécurité.

- Analystes SOC juniors (niveau 1).
- Étudiants en BTS SIO option SISR, DUT Réseaux et Télécoms.
- Profils en reconversion vers la cybersécurité.
- Candidats aux certifs avancées : **CompTIA Security+**, CCNA Security.
- Auditeurs réseau juniors.

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	Defense in Depth et fondamentaux	20 %
2	Network Security et firewall	20 %
3	Software et OS Security	15 %
4	Threats, attacks et vulnérabilités	20 %
5	Cryptographie et protocoles	15 %
6	Wireless security et compliance	10 %

*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 Network Security, en s'appuyant sur les Objective Domains publiés par Certiport et Unity Technologies (version 2026 — aligné sur la version actuelle ITS Pearson).

1 Defense in Depth et fondamentaux — 20 %

1.1 Principes fondamentaux

- **CIA Triad** : Confidentiality, Integrity, Availability.
- AAA : Authentication, Authorization, Accounting.
- Principle of **Least Privilege** et Separation of Duties.
- Non-repudiation et accountability.

1.2 Defense in Depth

- Couches : physique, réseau, host, application, données.
- Zero Trust Architecture (notions).
- Security through obscurity et ses limites.

1.3 Risk Management

- Risk = Threat × Vulnerability × Impact.
- Risk assessment et mitigation strategies.
- Business Impact Analysis (BIA).

2 Network Security et firewall — 20 %

2.1 Firewalls

- Types : packet filtering, stateful, application-layer, NGFW.
- Règles : source, destination, port, protocol, action.
- ACL (Access Control Lists).
- DMZ (Demilitarized Zone).

2.2 IDS / IPS

- **IDS** : Detection only (passive).
- **IPS** : Detection + Prevention (active).
- Signature-based vs anomaly-based.
- Snort, Suricata, OSSEC.

2.3 VPN

- Site-to-site VPN (entreprise).
- Remote access VPN (utilisateurs nomades).
- **IPsec** : AH, ESP, IKE.
- **SSL / TLS VPN** (OpenVPN).

2.4 Network segmentation

- VLANs pour isoler les segments.
- Microsegmentation.
- Air gap (isolation physique).

3 Software et OS Security — 15 %

3.1 Hardening

- **Windows hardening** : disable services, patch, AV, GPO.
- **Linux hardening** : permissions, iptables, ufw, SELinux / AppArmor.
- **CIS Benchmarks** et NIST guidelines.

3.2 Patch management

- Vulnerability management lifecycle.
- Patch tuesdays et hotfixes.
- Test environments avant production.

3.3 Application security

- Secure coding practices : OWASP Top 10.
- Input validation et output encoding.
- Web Application Firewall (WAF).

4 Threats, attacks et vulnérabilités — 20 %

4.1 Types d'attaques

- **Malware** : virus, worm, trojan, ransomware, spyware, rootkit.
- **Phishing**, spear phishing, vishing, smishing.
- **Social engineering** : pretexting, baiting, tailgating.
- **DoS / DDoS** : volumetric, protocol, application.
- **MITM** : ARP poisoning, DNS poisoning.
- **SQL injection**, **XSS**, **CSRF**.
- **Brute force** et password attacks.

4.2 Vulnérabilités

- **CVE** (Common Vulnerabilities and Exposures).
- **CVSS** (Common Vulnerability Scoring System).
- Zero-day vs N-day.
- Misconfigurations.

4.3 Incident response

- Phases : Preparation, Identification, Containment, Eradication, Recovery, Lessons learned.
- Log analysis et SIEM.
- Forensics de base.

5 Cryptographie et protocoles — 15 %

5.1 Cryptographie symétrique

- Algorithmes : **AES** (128, 192, 256), DES, 3DES, ChaCha20.
- Modes : ECB, CBC, GCM.
- Clés partagées.

5.2 Cryptographie asymétrique

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

5.3 Hashing

- **SHA-256**, SHA-3, MD5 (obsolète).
- **bcrypt**, Argon2 pour passwords.
- Salt et pepper.

5.4 PKI et TLS

- **PKI** et certificats X.509.
- CA (Certificate Authority) et chain of trust.
- **TLS / SSL** handshake.
- Protocoles : **HTTPS**, **SSH**, **SFTP**, **IPsec**.

6 Wireless security et compliance — 10 %

6.1 WiFi security

- WEP (cassé), **WPA**, **WPA2**, **WPA3**.
- PSK vs Enterprise (802.1X, RADIUS).
- Rogue AP et evil twin attacks.

6.2 Compliance et standards

- **ISO 27001 / 27002** : ISMS.
- **NIST Cybersecurity Framework**.
- **RGPD / GDPR** : protection données personnelles UE.
- **PCI DSS** : données bancaires.

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au ITS Network Security à travers un parcours blended-learning complet, combinant ressources e-learning interactives, projets pratiques en Defense in Depth, firewalls, IDS / IPS, VPN, cryptography, threats et accompagnement tutoré.

Format de la formation

Durée recommandée	150 heures de pratique Network Security 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 Network Security en centre OpenCertif (CATC Certiport)

Parcours d’apprentissage proposé

- **Module 1 :** CIA Triad et fondamentaux sécurité.
- **Module 2 :** Defense in Depth et Zero Trust.
- **Module 3 :** Risk Management et BIA.
- **Module 4 :** Firewalls et ACL.
- **Module 5 :** DMZ et network segmentation.
- **Module 6 :** IDS / IPS et SIEM.
- **Module 7 :** VPN — IPsec et SSL.
- **Module 8 :** OS hardening Windows et Linux.
- **Module 9 :** Patch management.

- **Module 10 :** Types d’attaques et malware.
- **Module 11 :** Social engineering et phishing.
- **Module 12 :** DoS / DDoS et MITM.
- **Module 13 :** OWASP Top 10 et web attacks.
- **Module 14 :** CVE, CVSS, vulnerability management.
- **Module 15 :** Incident response process.
- **Module 16 :** Cryptographie symétrique / asymétrique.
- **Module 17 :** Hashing et PKI.
- **Module 18 :** TLS / SSL et HTTPS.
- **Module 19 :** WiFi security : WPA2 / WPA3.
- **Module 20 :** Compliance : ISO, NIST, RGPD.
- **Module 21 :** 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 Network Security (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 Network Security.
- 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 Network Security, 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 Network Security, 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