Comparatif de solutions IT

*

leGymnase

↘ Sommaire

↘ Contexte et objectifs

Introduction

Face à l'évolution constante des menaces cyber et à l'obligation de garantir la continuité pédagogique et administrative, notre établissement a engagé une réflexion sur le renforcement de son infrastructure informatique et de sa posture de cybersécurité.

L’entrée en vigueur de nouvelles obligations réglementaires (directive NIS2, RGPD, exigences ANSSI), renforcent la nécessité d’un audit structuré et d’un accompagnement dans la sécurisation du système d’information.

Le besoin initial s’articule autour de trois axes :

- Réaliser un **audit de cybersécurité** complet (technique et organisationnel)
- Disposer d’une **vision claire des vulnérabilités existantes**
- Étudier les solutions de **remédiation, supervision continue et accompagnement IT**

Objectifs de la consultation

L’objectif principal de cette consultation est de comparer plusieurs offres de prestataires spécialisés à savoir, Lunarr, Athéo Ingénierie, et Orange Cyberdefense, dans le but de sélectionner la solution :

- La plus adaptée à nos besoins techniques et organisationnels
- La plus efficace en termes de sécurité et de suivi
- La plus réaliste en termes de budget

La démarche doit permettre de :

- Évaluer objectivement les forces et faiblesses de chaque offre
- Prendre une décision éclairée, en lien avec nos priorités stratégiques

Enjeux pour la structure

Les enjeux de ce projet sont multiples :

- Conformité : Alignement avec les exigences ANSSI, RGPD
- Sécurité : Réduction du risque de compromission des données sensibles (élèves, personnel, enseignants, comptabilité)
- Performance : Amélioration de la résilience du SI, capacité de réponse rapide aux incidents
- Budget : Optimisation du rapport qualité/prix sur le court et le long terme

↘ Méthodologie

Démarche de sélection des prestataires

Dans le cadre de cette étude comparative, trois prestataires spécialisés en cybersécurité ont été identifiés :

- **Lunarr**, jeune acteur 100 % dédié à la cybersécurité, adossé au Groupe Mentor
- **Athéo Ingénierie**, intégrateur IT historique avec une forte spécialisation cyber, rattaché au groupe OCI
- **Orange Cyberdefense**, leader européen de la cybersécurité, filiale du groupe Orange

La sélection s'est appuyée sur :

- L'analyse de **documents commerciaux et techniques fournis** par chaque prestataire (fiches d'offre, devis, méthodologies, présentations)
- Des **entretiens** et échanges avec les équipes commerciales et techniques
- La **prise en compte de retours d'expérience publics** (témoignages clients, références) ou disponibles dans les médias spécialisés

Critères de comparaison

Pour assurer une évaluation équitable, les offres ont été comparées selon **des critères objectifs** répartis en cinq grandes catégories :

- **Contenu et qualité des prestations proposées** : audit organisationnel, technique, test d'intrusion, plan de remédiation
- **Réactivité et supervision** : présence d'un SOC, accompagnement post-audit, gestion d'incident

- **Support & relation client** : proximité, interlocuteur dédié, services complémentaires
- **Réputation & retour d'expérience** : références clients, notoriété du prestataire, certifications
- **Aspects économiques** : coût total TTC, rapport qualité/prix

↘ Présentation des préstataires

Lunarr

Lunarr est une entreprise française spécialisée dans la cybersécurité, basée à Nancy. Elle accompagne diverses organisations, des TPE et PME aux administrations publiques et établissements de santé, dans la sécurisation de leurs systèmes d'information face aux cyber menaces.

L'approche de Lunarr est structurée autour de cinq axes principaux :

• Gouvernance, gestion des risques et conformité (GRC) : Lunarr aide les entreprises à développer et mettre en œuvre des politiques de sécurité efficaces, assurant une conformité aux normes en vigueur.

• Audits de sécurité et tests d'intrusion (Pentests) : Ses experts certifiés réalisent des audits offensifs pour identifier les vulnérabilités des systèmes avant qu'elles ne soient exploitées par des attaquants.

• Détection et réponse aux incidents : Grâce à son Centre d'opérations de sécurité (SOC), Lunarr surveille en continu les systèmes d'information pour détecter et neutraliser les cybermenaces en temps réel.

• Formation et sensibilisation : Reconnaissant que la cybersécurité passe avant tout par les collaborateurs, Lunarr propose des programmes de formation adaptés pour renforcer les compétences internes en matière de sécurité.

• Conseil stratégique en cybersécurité : Lunarr accompagne les organisations dans la définition et la mise en œuvre de stratégies globales de sécurité numérique alignées sur leurs enjeux métiers.

En avril 2024, Lunarr a renforcé son pôle formation en acquérant César Hub, un organisme de formation basé à Reims, rebaptisé depuis Cesarr. Cette acquisition s'inscrit dans la volonté de l'entreprise d'étendre son réseau de centres de formation à travers la France, avec pour objectif d'en ouvrir dix d'ici trois ans.

Athéo

Athéo Ingénierie est une entreprise française spécialisée dans l'intégration d'infrastructures informatiques et la cybersécurité, fondée en 2013 et basée à Strasbourg. Elle compte environ 80 collaborateurs répartis sur quatre sites : Strasbourg, Nancy, Besançon et Paris.

L'entreprise offre une gamme complète de services, notamment :

• Intégration d'infrastructures IT : Athéo Ingénierie se distingue par son expertise en gestion multicloud, virtualisation et protection des données critiques.

• Services cloud managés : Elle propose des solutions innovantes pour l'optimisation des infrastructures cloud, permettant aux entreprises de piloter leurs ressources en temps réel.

• Cybersécurité : Consciente des enjeux majeurs liés à la sécurité numérique, Athéo Ingénierie accompagne les organisations dans la mise en place de politiques de sécurité efficaces, assurant la disponibilité, l'intégrité et la confidentialité des informations.

En novembre 2021, Athéo Ingénierie a été acquise par le groupe OCI Informatique, renforçant ainsi sa présence nationale et consolidant son positionnement parmi les principaux intégrateurs d'infrastructures IT dans le Grand Est.

Orange Cyberdefense

Orange Cyberdefense est la filiale du Groupe Orange dédiée à la cybersécurité, créée en 2016 suite au rachat d'Atheos. Basée à Paris La Défense, elle compte environ 3 000 collaborateurs répartis dans 12 pays.

L'entreprise offre une gamme complète de services, notamment :

- **Services managés de sécurité** : Orange Cyberdefense fournit des services de gestion de la sécurité, de détection et de réponse aux menaces pour les organisations du monde entier.

- **Conseil en cybersécurité** : Elle accompagne les entreprises de toutes tailles sur l'ensemble du cycle de vie de la menace, offrant des services de conseil technologique en sécurité, d'audit de contrôle et conformité, et de gouvernance et gestion des risques.

- **Formation et sensibilisation** : Consciente des enjeux liés à la sécurité numérique, Orange Cyberdefense propose des programmes de formation et de sensibilisation pour aider les organisations à renforcer leur posture de sécurité.

En tant que leader européen des services de cybersécurité, Orange Cyberdefense s'efforce de protéger les libertés individuelles et de construire une société numérique plus sûre. Elle compte plus de 8 700 clients dans le monde.

↘ Comparaison générale

Critères	Lunarr	Athéo Ingénierie	Orange Cyberdefense
Réputation & Retour d'expérience	Jeune acteur (lancé en 2023) adossé au Groupe Mentor. Premiers clients satisfaits : un témoignage salue le renforcement de la sécurité interne et la qualité des formations dispensées. Mise sur des relations durables et la confiance, avec une approche humaine.	Présent depuis 2013, reconnu comme l'un des leaders du Grand Est. Plus de 500 clients, avec de "très belles références" régionales et nationales. Fidélisation élevée : clients industriels (ex. Socomec, De Dietrich) témoignent du professionnalisme et de la fiabilité de ses services.	Leader européen de la cybersécurité avec plus de 8 700 clients dans 12 pays. Filiale d'Orange, reconnue par les institutions et les analystes (Forrester, IDC, MSSP Alert). Certifications ANSSI (PASSI, PDIS). Réputation solide auprès des grands groupes comme du mid-market.
Services proposés	100 % spécialisé en cybersécurité. Offre sur-mesure autour de 5 axes : gouvernance & conformité, audits de sécurité/Pentests, détection & réponse aux incidents (SOC/CSIRT),	Intégrateur IT global avec volet cybersécurité. Couvre l'infrastructure (stockage, virtualisation, réseaux, systèmes) et la sécurité associée. Propose	Offre complète couvrant l'ensemble du cycle de cybersécurité : audits certifiés PASSI, SOC 24/7, CSIRT, MSS/MDR, conseil en gouvernance, pentests (200+

	formation/sensibilisation, conseil stratégique. Cible aussi bien les PME que les collectivités et hôpitaux, avec une expertise pointue.	infogérance et services cloud managés, protection des données, supervision de sécurité continue (offre “Safety SOC”) et solutions sur mesure. Expertise notable en multicloud, virtualisation et sécurité des infrastructures critiques.	experts), threat intelligence, sécurité cloud et OT, formations techniques et sensibilisation. S’adapte aux PME comme aux grands groupes.
Réactivité & gestion d’incidents	Dispose d’un service de surveillance et réponse aux cyberattaques (SOC/CSIRT) dédié. Équipe à taille humaine (≈13 employés) garantissant agilité et interventions rapides en cas d’incident. Aucune faille de sécurité publique connue à ce jour, signe d’une bonne proactivité.	Organisation rodée pour la gestion d’incidents. Maîtrise des outils de détection avancés (EDR/XDR, SIEM, etc.) et de réponse (analyses forensiques, malwares). Capacité à mobiliser ses experts en urgence dans le cadre de contrats	Réseau mondial de 18 SOCs et 14 CyberSOC. CSIRT activable 24/7 avec astreinte continue. Intervient sur les plus grandes cybercrises (ex : SolarWinds, NotPetya, WannaCry). Réactivité démontrée : cellule de crise activée en moins de 2h lors d’un incident interne.

		de service, y compris via son SOC interne pour une surveillance 24/7. Aucun incident majeur public, gage d'efficacité.	Capacité à coordonner des réponses globales à grande échelle.
Support client & accompagnement	Relation de proximité privilégiée. Lunarr met l'humain au centre de sa démarche et tisse des relations durables. Accompagnement personnalisé : conseils adaptés, formation du personnel et suivi post-mission pour assurer la pérennité des bonnes pratiques.	Support structuré et étendu. Athéo dispose d'une équipe dédiée au support et à l'infogérance, avec des abonnements de services managés pour le suivi au quotidien. Les clients bénéficient d'un interlocuteur unique pour l'ensemble de leur IT, et d'un suivi réactif post-déploiement (maintenance, mises à jour sécurité, etc.).	Suivi personnalisé avec interlocuteur dédié. Présence locale dans toute la France. Offres packagées pour PME et solutions sur-mesure pour les grands comptes. Rapports, comités de pilotage et accompagnement complet de la stratégie de cybersécurité. Initiatives Micro-SOC pour les structures de taille intermédiaire.
Innovation & évolutivité	Entreprise récente, fondée pour adresser les	Capacité avérée à se réinventer. Athéo a fait	250+ analystes et chercheurs. R&D intégrée au

	menaces émergentes (contexte NIS2, etc.). Évolutive par nature : intègre la formation continue des employés dans sa stratégie (acquisition d'un centre de formation rebaptisé Cesarr) pour anticiper les futures menaces. Culture de l'innovation portée par le Groupe Mentor, favorisant l'adaptation rapide aux nouvelles cyberattaques.	évoluer son modèle vers le cloud et les services managés pour suivre les besoins du marché. Investit dans des solutions innovantes (ex : partenariat avec un éditeur pour piloter le cloud hybride en toute sécurité). Mise à jour constante de ses offres cybersécurité (ex : intégration de l'EDR français HarfangLab) pour rester à la pointe.	groupe Orange. Utilisation d'IA, XDR, SOAR. Rapports annuels (Security Navigator). Intégration rapide des nouvelles menaces. Partenariats stratégiques (Microsoft, Netskope, Fortinet). Offre évolutive, adaptée à tous les niveaux de maturité cybersécurité.
Événements marquants & incidents	Création en 2023 en tant que filiale cybersécurité de Mentor. 2024 : rachat de l'organisme de formation César Hub (rebaptisé "Cesarr") pour renforcer son pôle formation. Pas d'incident de	Parcours jalonné de succès. Fondée par D. Nicoletti en 2013, croissance rapide (50 % en deux ans) qui l'a mené à ~25 M€ de CA en 2021. Rachat par le Groupe OCI fin 2021,	Rachats successifs (Atheos, SecureLink, SensePost, SCRT) pour bâtir un acteur paneuropéen. Membre fondateur du Campus Cyber. Incidents

	sécurité connu publiquement étant donné son jeune âge. Lunarr se fait surtout remarquer par cette expansion rapide et son positionnement de « gardien de la cybersécurité » en Lorraine.	consolidant son leadership dans l'Est. Partenaire de formations locales (école 42 Mulhouse) pour soutenir la filière cyber. Aucune controverse ou faille majeure publique en plus de 10 ans d'existence, reflétant une gestion solide.	maîtrisés avec transparence (ex : Micro-SOC 2022). Réputation renforcée par son expérience sur des cas d'attaques à grande échelle. Croissance continue, +14 % de CA annuel.

↘ Comparaison des devis

Devis 1 : Athéo

📌 Prestations proposées :

• Audit de sécurité basé sur des analyses de vulnérabilités

• Évaluation des menaces incluant des scénarios d'attaques modernes

• Supervision et réponse aux incidents (SOC et solutions avancées)

• Approche pédagogique pour sensibiliser les utilisateurs aux cyberattaques

Devis 2 : Lunarr

📌 Prestations proposées :

1. Diag Cyber - Audit d'organisation

• Examen des documents de cybersécurité de l’entreprise (analyse de risques, politique SI, PCA/PRA, charte informatique, etc.).

• Entretiens individuels et ateliers pour identifier les bonnes pratiques et les points faibles.

• Contrôle des points clés selon les recommandations de l’ANSSI, avec analyse des résultats et recommandations.

2. Diag Cyber - Audit technique

• Tests d’intrusion sur le système d’information.

• Revue de configuration des équipements informatiques.

• Analyse des résultats et mise en place d’un plan de traitement des vulnérabilités.

Devis 3 : Orange Cyberdefense

CyberDiag – Offre Premium

• Diagnostic complet des volets organisationnel, technique et humain.

• Évaluation de la gouvernance cybersécurité, des processus et configurations SI.

• Identification des vulnérabilités internes et externes.

• Élaboration d’un plan d’action priorisé avec recommandations de remédiation.

• Rapport de synthèse, restitution orale, attribution d’un cyberscore.

• Sensibilisation des équipes et accompagnement à la mise en œuvre des actions.

Critères	Athéo	Lunarr	Orange Cyberdéfense
Audit organisationnel	✅ Basé sur l'ANSSI, contrôle des bonnes pratiques	✅ Basé sur l'ANSSI, audit documentaire et entretiens	✅ Basé sur l'ANSSI, audit de gouvernance, processus et sécurité organisationnelle
Audit technique	✅ Scan des vulnérabilités internes & externes	✅ Tests d'intrusion, scan SI, analyse des vulnérabilités	✅ Tests d'intrusion, scans de vulnérabilités, SOC 24/7 et CSIRT
Test d'intrusion	✅ Mentionné dans l'audit technique	✅ Inclus avec scoring des vulnérabilités	✅ Réalisés par des experts certifiés (PASSI), plus de 200 pentesters
Analyse des risques	✅ Basé sur ANSSI & analyse des menaces actuelles	✅ Audit documentaire et analyse des risques	✅ Analyse documentée des risques et des menaces, cartographie complète
Supervision et surveillance	✅ SOC & CSIRT pour détection et réponse aux incidents	❌ Non inclus, pas de SOC	✅ SOC 24/7 dans 18 pays + CSIRT pour réponse aux

			incidents
Formation et sensibilisation	✅ E-learning, simulation de phishing, formation des employés	❌ Non inclus, uniquement recommandations	✅ Formations sur mesure, e-learning, sensibilisation utilisateurs & IT
Gestion de crise	✅ PCA/PRA, gestion des incidents, accompagnement après attaque	❌ Non inclus	✅ CSIRT activable 24/7, cellules de crise, retour d'expérience d'attaques majeures
Protection avancée	✅ Gestion des accès, protection des données, messagerie sécurisée	❌ Non mentionné	✅ Plan d'action personnalisé avec accompagnement expert
Plan de remédiation	✅ Plan détaillé suite à l'audit	✅ Plan d'action après l'audit	✅ Plan d'action personnalisé avec accompagnement expert
Accompagnement post-audit	✅ Assistance et suivi des recommandations	✅ Remédiation et suivi des corrections	✅ Suivi personnalisé, interlocuteur dédié, accompagnement long terme
Coût total	13 080,00 € TTC	9 600,00 € TTC	11 880,00 € TTC

↘ Pour et contre de chacuns

ATHEO

POUR

- Accompagnement complet et long terme : Athéo ne se limite pas à un audit, mais propose un suivi post-audit, une surveillance continue via un SOC et des formations.
- Offre tout-en-un : Audit organisationnel, audit technique, supervision des menaces et réponse aux incidents.
- Supervision 24/7 : Athéo inclut un SOC (Security Operations Center) et un CSIRT pour réagir en cas de cyberattaque.
- Formation et sensibilisation des employés : E-learning, simulation de phishing, tests de sensibilisation inclus.

CONTRE

- Peut être coûteux sur le long terme : Avec un SOC et une assistance continue, les frais d'abonnement pourraient être élevés si un suivi long terme est choisi.
- Athéo est principalement conçu pour un accompagnement long terme, ce qui peut ne pas convenir aux entreprises recherchant uniquement un audit ponctuel et actionnable.

LUNARR

POUR

- Audit technique approfondi : Tests d'intrusion, scan du système d'information, scoring des vulnérabilités et analyse détaillée des configurations SI.
- Plan d'action précis : Suite aux audits, Lunarr fournit un rapport détaillé avec recommandations et plan de correction des failles.
- Approche pragmatique et efficace : Axée sur la correction des vulnérabilités immédiates.
- Indépendance : Ne nécessite pas d'abonnement ou de suivi à long terme, parfait pour une évaluation ponctuelle.
- Remédiation et suivi : Accompagnement dans la correction des vulnérabilités avec des tests réguliers pour vérifier l'efficacité des corrections.

CONTRE

- Aucune surveillance continue : Pas de SOC ni de CSIRT pour la réponse aux incidents en temps réel.
- Aucune formation ou sensibilisation des employés : Contrairement à Athéo, Lunarr ne propose pas de formation post-audit.
- Pas de gestion de crise : Si une attaque survient après l'audit, aucune assistance n'est prévue.

ORANGE CYBERDEFENSE

POUR

- Accompagnement global : Orange Cyberdefense prend en charge l'ensemble du cycle de cybersécurité avec un diagnostic, un plan de remédiation et un suivi personnalisé.
- Audit complet : Analyse de la gouvernance, des processus techniques et humains, cartographie des risques, identification des vulnérabilités.
- Conformité avec les standards : Diagnostic structuré selon le cadre de l'ANSSI
- Formation et sensibilisation incluses : Transmission des bonnes pratiques en continu, posture pédagogique.

CONTRE

- Peut être coûteux sur le long terme : Avec un SOC et une assistance continue, les frais d'abonnement pourraient être élevés si un suivi long terme est choisi.

↘ Conclusion

Athéo se distingue par une approche complète de la cybersécurité, incluant une **surveillance continue via un SOC, une gestion des incidents (CSIRT) et des formations dédiées aux utilisateurs**. Cette solution est particulièrement adaptée aux structures nécessitant un **suivi long terme, une protection renforcée des données et une réponse rapide en cas d'incident**. L'accompagnement proposé permet de réduire les risques liés aux cyberattaques, tout en intégrant des actions de sensibilisation et de formation pour renforcer la posture de sécurité globale.

Lunarr, quant à lui, propose une approche plus ciblée, centrée sur **un audit ponctuel et une analyse technique approfondie des vulnérabilités**. L'offre

inclut des **tests d'intrusion, un scan du système d'information et un plan d'action correctif**.

Orange Cyberdefense, de son côté, va encore plus loin avec une couverture complète du cycle de cybersécurité. Leader européen du secteur, elle propose un ensemble de services hautement structurés allant des audits certifiés PASSI à la supervision 24/7 via ses SOCs internationaux, en passant par la réponse aux incidents (CSIRT), la gestion des risques, la formation et la veille stratégique. Cette solution s'adresse particulièrement aux structures souhaitant un partenaire de cybersécurité expérimenté, capable de gérer aussi bien des attaques complexes que des déploiements à grande échelle, avec une capacité d'accompagnement sur mesure et une réactivité prouvée en situation de crise.

Dans notre cas **Athéo** ou **Orange Cyberdéfense** seraient donc plus pertinents si nous souhaitons un **suivi longue durée** des infrastructures informatiques tandis que **Lunarr**, de son côté, adopte une approche axée sur un **diagnostic à court terme**, avec une analyse des vulnérabilités et des points faibles de nos infrastructures, accompagnée d'une remédiation et d'un suivi des corrections, mais **sans proposer de service de supervision continue (SOC).**

↘ Annexes

Sources des différents retours d'expérience

Retours sur Athéo :

nelson.news

twinl.com

Retours sur Lunarr :

Témoignages clients et site officiel de Lunarr :

lunarr.fr

welcometothejungle.com

Articles de presse régionaux sur leurs actualités :

scoop.it

Fiches Grand Est Transformation soulignant leurs offres et réussites

grandest-transformation.fr

Retours sur Orange Cyberdefense :

Orange Cyberdefense – site officiel et communiqués de presse Orange

orangecyberdefense.com

newsroom.orange.com

newsroom.orange.com

Analyses sectorielles et rapports d’experts

orangecyberdefense.com

orangecyberdefense.com

Articles de presse spécialisés et contenus officiels (ANSSI, etc.)

orange-business.com

canalys.com

Glossaire

Terme	Signification	Définition / Rôle
SOC	Security Operations Center	Centre de supervision de la sécurité. Surveille en temps réel les systèmes informatiques, détecte les menaces et déclenche des alertes.
CSIRT	Computer Security Incident Response Team	Équipe spécialisée dans la gestion des incidents de sécurité (analyse, confinement, remédiation). Intervient en cas d'attaque.
Audit organisationnel	-	Évaluation des pratiques de sécurité à l'échelle de la structure (gouvernance, politiques internes, sensibilisation du personnel…).
Audit technique	-	Analyse de la sécurité des systèmes informatiques : réseau, serveurs, pare-feu, configurations, etc.
Pentest	Penetration Test	Test d'intrusion. Simulation d'une attaque réelle pour identifier les failles exploitables par un pirate.

Scan de vulnérabilités	-	Analyse automatisée du système pour détecter les failles techniques connues (ports ouverts, failles logicielles, etc.).
Plan de remédiation	-	Document listant les mesures correctives à mettre en place suite à un audit (actions techniques ou organisationnelles).
XDR	Extended Detection & Response	Outil de sécurité qui croise plusieurs sources (endpoint, mail, réseau...) pour détecter les attaques de manière intelligente.
SIEM	Security Information & Event Management	Outil qui centralise et analyse les journaux d'événements des équipements pour détecter les anomalies ou comportements suspects.
SOAR	Security Orchestration, Automation and Response	Plateforme qui automatise la détection et la réponse aux incidents pour soulager les analystes sécurité.
EDR	Endpoint Detection & Response	Solution installée sur les postes de travail/serveurs qui

		détecte les menaces et y réagit (ex : isolement d'un poste infecté).
CyberScore	-	Note de maturité ou de niveau de cybersécurité attribuée à une organisation (souvent utilisée dans les audits ANSSI).
Conformité RGPD	Règlement Général sur la Protection des Données	Ensemble d'obligations liées à la gestion et protection des données personnelles (ex : données élèves ou salariés).
NIS2	Directive européenne sur la sécurité des réseaux et systèmes d'information (2023)	Norme européenne imposant un niveau minimal de cybersécurité à certaines structures publiques et privées.
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information	Certification délivrée par l'ANSSI à des prestataires jugés compétents pour réaliser des audits de sécurité.
PDIS	Prestataire de détection d'incidents de sécurité	Qualification ANSSI pour les prestataires capables d'assurer une détection avancée des cyberincidents.

Colin MONTERASTELLI

Le 12/03/2025

leGymnase