NAROK

Audit IA

Présentation de l'offre

narok.fr | contact@narok.fr | 06 49 50 39 86

Narok, société spécialisée en cybersécurité offensive

Narok est une société spécialisée dans la **cybersécurité offensive** fondée en 2025.
Nous aidons les entreprises à identifier et corriger leurs vulnérabilités avant qu'elles ne soient exploitées.

Nos audits s'appuient sur des référentiels éprouvés (OWASP, CIS, ANSSI, etc.) , et sur une approche réaliste fondée sur les techniques d'attaque réelles.

NOTRE VISION

Jeune et indépendante, **Narok combine agilité et exigence.**

Nous plaçons la **transparence,** la **pédagogie** et la **qualité technique** au cœur de chaque mission.

NOTRE MISSION

Fournir des prestations offensives de haut niveau :

- Tests d'intrusion
- Campagnes de phishing
- Audits techniques
- Sensibilisations

Ce qui nous distingue

Expertise 100% offensive

acquise par le biais de plusieurs années d'expérience

Méthodologie rigoureuse

documentée et éprouvée

Recommandations concrètes

et priorisées

Relation de confiance

proximité, clarté et accompagnement

L’offre IA – Pourquoi ?

L’adoption rapide de l’IA générative crée de nouvelles opportunités… mais ouvre également des surfaces d’attaque inédites : manipulation via les prompts, exfiltration de données, contournement des garde-fous, compromission des pipelines RAG, exposition d’API internes, erreurs métier induites par l’IA, etc…

Face à ces risques, Narok propose une offre structurée autour de 2 modules complémentaires :

Sécurité des usages IA

Pentest des Usages IA (Front)

Évaluer la robustesse des LLM, copilots, agents et interfaces IA face à des attaques réelles.

+

Sécurité des architectures IA

Audit d’Architecture IA & Sécurité des Pipelines

Vérifier la sécurité des pipelines RAG, des vector stores, des orchestrateurs et des API internes. Cette approche permet de couvrir l’ensemble de la chaîne IA, du point d’entrée utilisateur jusqu’aux composants techniques internes.

Présentation technique

Pentest des usages IA

NAROK

Sécurité des Usages IA (LLM, Agents & fonctionnalités IA)

Raison d'être

Les assistants IA, copilots, chatbots et intégrations LLM deviennent des points d'entrée critiques.

Mal configurés ou manipulés, ils peuvent exposer des données sensibles, contourner des contrôles, exécuter des actions dangereuses ou générer des réponses compromettantes.

Par le biais de l'offre Sécurité des Usages IA, Narok propose un pentest spécialisé, ciblé sur la couche "front" : ce que voient les utilisateurs, les applications, et les services exposant les fonctionnalités IA.

Notre solution technique – Le test d’intrusion

Un test d’intrusion (pentest) reproduit, dans un cadre contrôlé et autorisé, les techniques d’un attaquant afin d’identifier des vulnérabilités exploitables et d’évaluer leur impact métier.

Objectif

- Détecter les vulnérabilités exploitables via les prompts et les interactions utilisateur
- Tester la robustesse des LLM, copilots et agents IA face aux attaques
- Identifier les risques de fuite, manipulation ou exécution indésirable
- Valider la sécurité des fonctionnalités reposant sur l’IA de vos applications
- Preuves concrètes des risques métier associés aux usages IA

STANDARDS

Les tests seront effectués selon la méthodologie OWASP.

Ce que nous ciblons et auditons typiquement dans le cadre du test d'intrusion :

- LLM internes / copilots métiers
- Chatbots IA et assistants internes
- Agents IA déclenchant des actions (API, automatisations)
- Intégrations via API front (Azure/OpenAI/Claude/Mistral…)
- Interfaces métiers connectées à un modèle IA
- Portails ou applications donnant accès à des capacités LLM

RÈGLES D’ENGAGEMENT

Tests réalisés uniquement après validation du périmètre, signature d’un accord d’intervention (et d’un NDA si nécessaire).
Toute exploitation destructive est proscrite.
Nos adresses IPs vous sont communiquées avant les tests.

Exclusions par défaut

- Tests de déni de service / stress (DoS) — risque pour la production ; à planifier séparément si nécessaire
- Ingénierie sociale (phishing)
- Tests sur composants tiers non couverts par le périmètre validé

Sécurité des Usages IA – tests usuels

Tests sur les Agents & Copilots

Méthodes clés

- Exécution non autorisée d'actions par l'agent
- Détournement de workflows (création ticket, mise à jour donnée, etc.)
- Manipulation des outils internes exposés à l'IA (plugins, actions)
- Validation de l'isolation entre les actions autorisées et interdites
- Tests sur les mécanismes de transformation des inputs/outputs

Tests sur les interfaces LLM

Méthodes clés

- Prompt injection directe, indirecte, multi-turn
- Contournement des restrictions
- Extraction d'informations sensibles
- Débordement de contexte (context overflow)
- Manipulation des instructions métier ("action hijacking")
- Induction d'erreurs ou de comportements inattendus

API Front reliées aux outils IA

Méthodes clés

- Contrôles d'accès
- Fuite d'informations dans les réponses / erreurs
- Mauvaises configurations de proxies ou gateways IA
- Contournement des limitations (tokens, taux, contrôles)
- Tests de payloads malveillants envoyés aux endpoints IA

Sécurité des Usages IA (LLM, Agents & fonctionnalités IA) - Bénéfices

Quels sont les bénéfices ?

- Identifier rapidement les failles visibles et exploitables
- Réduire les risques opérationnels (actions inattendues, erreurs, manipulation)
- Sécuriser les assistants et workflows IA avant généralisation
- Aligner les usages LLM avec les politiques internes de sécurité
- Protéger les données métier face aux risques d’exfiltration

Présentation technique

Sécurité des Architectures IA

NAROK

Sécurité des Architectures IA (Architecture IA & Sécurité des Pipelines)

Raison d'être

L'intégration d'IA générative et d'assistants métier repose sur une chaîne technique complexe : ingestion de données, vectorisation, stockage, orchestrateurs, API internes, RAG, modèles hébergés ou externalisés.

Si cette architecture n'est pas sécurisée, l'organisation s'expose à des risques majeurs : fuite de données, compromission de sources, contournement d'ACL, altération silencieuse du contexte, ou exposition d'API sensibles.

Narok propose un audit complet de la stack IA côté back : pipelines, vector stores, orchestrateurs, API IA, architecture cloud/on-prem - Une évaluation de la sécurité des composants techniques, pipelines, orchestrateurs et intégrations IA.

Sécurité des Architectures IA – Notre solution

Un audit d'architecture consiste à analyser la conception globale d'un système afin d'évaluer la manière dont ses composants interagissent, se protègent et s'isolent.

L'objectif est d'identifier les risques structurels liés au design, aux flux de données, au cloisonnement, aux dépendances techniques et aux choix d'intégration.

Un audit de configuration consiste à examiner en détail les paramètres, réglages et contrôles effectifs d'un composant ou d'un service pour vérifier qu'ils sont conformes aux bonnes pratiques et ne présentent pas de vulnérabilités.

OBJECTIFS

- Évaluer la robustesse et l'isolation des composants IA
- Identifier les points faibles du RAG, de l'ingestion et de la vectorisation
- Vérifier la sécurité des API internes exposant des capacités IA
- Analyser la gouvernance, les flux de données et les modalités d'accès.
- Proposer des recommandations structurelles pour un déploiement IA sécurisé

PÉRIMÈTRE TYPIQUE :

- Pipelines RAG (Retriever / Loader / Index / Query)
- Ingestion de fichiers, bases documentaires, APIs internes
- Vector stores : Elasticsearch, Pinecone, Chroma, Opensearch…
- Orchestrateurs IA : LangChain, LlamaIndex, Flowise, frameworks internes
- Connecteurs applicatifs (CRM, SharePoint, Confluence…)
- API IA internes : gateways, proxies, microservices
- Architecture cloud/on-prem : Azure, AWS, GCP, Kubernetes

Sécurité des Architectures IA – tests usuels

Sécurité des API IA Internes

- Exposition et topologie réseau.
- Authentification (API keys, OAuth, mTLS…).
- Autorisation & gestion des rôles.
- Vérification des quotas, contrôles, filtrages et logs.
- Risques de contournement ou d'escalade d’accès.

Analyse d’Architecture IA

- Cartographie de la chaîne IA (data → vectorisation → requêtes → réponses).
- Vérification du cloisonnement et du principe de moindre privilège.
- Revue des interactions entre composants (API, bus, workers).
- Bonnes pratiques d’architecture (durcissement, isolation, gestion secrets).
- Vérification des environnements (dev/staging/prod) et de l’isolation.

Sécurité du Pipeline RAG & de l’Ingestion

- Analyse des connecteurs (Chargeurs de documents, loaders).
- Tests de robustesse aux sources malveillantes.
- Audit des mécanismes d’extraction et normalisation.
- Verification de l’intégrité du contenu ingéré.
- Détection de risques de corruption ou confusion des données.

Audit des Vector Stores

- Vérification des ACL, authentification, autorisation.
- Cloisonnement des espaces clients/projets.
- Risques de fuite ou d’inversion d’embeddings.
- Vérification de l’exposition réseau et des dépendances.
- Sécurisation du schéma d’indexation/documentation.

Sécurité des Architectures IA (Architecture IA & Sécurité des Pipelines) - Bénéfices

Quels sont les bénéfices ?

- Comprendre précisément les risques structurels associés à votre utilisation de l'IA
- Garantir la conformité des flux IA aux bonnes pratiques de sécurité
- Sécuriser l’ingestion, la vectorisation et l’accès aux données
- Assurer une intégration durable, scalable et sécurisée de l’IA dans votre SI
- Protéger les pipelines IA contre les intrusions et corruptions silencieuses

Livrables

NAROK

Livrables fournis

À l’issue de la mission, **trois livrables complémentaires** sont transmis à l'audité, en français ou en anglais, selon les besoins exprimés.

Ils permettent à la fois une analyse technique approfondie et une exploitation opérationnelle et managériale des résultats.

RAPPORT D’AUDIT DÉTAILLÉ

- Document complet structuré en trois parties : synthèse managériale, synthèse technique et détails des vulnérabilités
- Contient l’intégralité des constats, preuves, démarches d’exploitation et recommandations associées
- Référence principale pour le suivi des corrections

SLIDES DE SYNTHÈSE MANAGÉRIALE

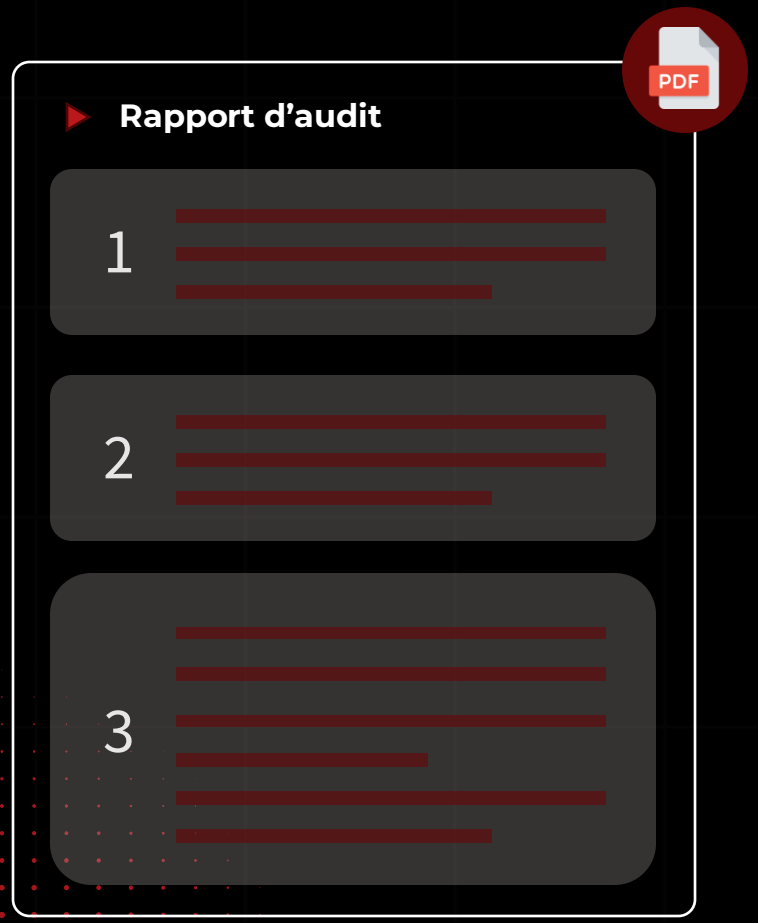
- Présentation visuelle reprenant les éléments clés du rapport (risques, indicateurs, recommandations)
- Support de restitution orale et de communication interne auprès des décideurs
- Fournit une vision claire du niveau de sécurité global et des actions prioritaires

PLAN D’ACTION

- Tableau de suivi regroupant l’ensemble des recommandations et vulnérabilités associées
- Hiérarchisation selon le niveau de risque et l’effort de correction estimé
- Permet un pilotage opérationnel de la remédiation

Détail du rapport d’audit

Structure du rapport détaillé



1 SYNTHÈSE MANAGÉRIALE

- Résumé global de la mission et des conclusions principales
- Présentation des **risques identifiés** selon la **matrice à quatre niveaux** vraisemblance / impact de l’ANSSI
- S’adresse aux **décideurs** : priorisation, tendances, indicateurs globaux

2 SYNTHÈSE TECHNIQUE

- **Indicateurs clés (KPI)** : nombre de vulnérabilités par criticité, conformité au référentiel d’audit, etc.
- **Synthèse des vulnérabilités / non-conformités et des recommandations**
- Vision consolidée pour les **équipes techniques** et les responsables de la sécurité

3 DÉTAILS TECHNIQUES

Pour chaque vulnérabilité / non-conformité :

- **Description, contexte et évaluation (via score CVSS pour les vulnérabilités)**
- **Preuve** et **démarche d'identification détaillée** (pour la reproductibilité)
- **Recommandation corrective** la plus précise possible

+ annexes et éventuels scripts / captures / extraits pertinents

Informations complémentaires

NAROK

Déroulement et organisation de l’audit

Acceptation de l’offre commerciale

Réalisation de l'audit sur site ou à distance

Livraison finale : rapport audit technique, plan d’action

2 – 3 semaines

10 jours

Réunion de lancement & Validation des prérequis

Fin de l'audit et débriefing à chaud

En option
Réunion de restitution

Sur demande : destruction des données d’audit

Présentation de l'équipe d'audit

Une équipe expérimentée et complémentaire

Narok est une entreprise crée par trois experts pentesters bénéficiant chacun de plusieurs années d'expérience

Antoine Clairotte

Président - cofondateur

Responsable d'audit

Victor Josso

Auditeur - cofondateur

Auditeur

Nicola KALAHE

Auditeur - cofondateur

Auditeur

CV des auditeurs – Nicola

Nicola est un auditeur expérimenté spécialisé dans la sécurité offensive. Au cours de ces **quatre dernières années**, il a pu mener des tests d'intrusion sur de nombreuses typologies d'environnements (infrastructures, applicatifs web, applicatifs mobiles et systèmes embarqués).

2021 -2023

Master *Sécurité Informatique* en alternance
Sorbonne Université

2021 - 2025

OWN
Auditeur cybersécurité (pentester)

Depuis 2025

Narok
Cofondateur & Auditeur cybersécurité (pentester)

RÉFÉRENCES

- **Test d'intrusion applicatif**

Audits d'applications web métiers et grand public selon la méthodologie OWASP
Nombreuses campagnes réalisées pour les secteurs logiciel, assurance, bancaire, transport, finance et télécom

- **Test d'intrusion interne**

Tests d'intrusion sur les environnements Active Directory et Wi-Fi
Audits d'architecture réseau et d'organisation interne
Réalisés dans des environnements sensibles des secteurs santé, banque, assurance et finance

- **Test d'intrusion mobile**

Audits de sécurité d'applications Android et iOS pour une banque et une application de rencontre

- **Test d'intrusion objets connectés**

Audits de sécurité sur les box Internet d'un opérateur télécom
Autres interventions pour un opérateur satellite

- **Revue d'architecture et de configuration**

Audits de postes de travail Windows dans le *secteur assurance, finance et satellite*

Audits de configurations des serveurs Linux / AS400 et de pare-feu pour les *secteurs télécom et banque*

COMPÉTENCES

PASSI – Prestataire d'Audit de la Sécurité des Systèmes d'Information qualifié

2024 – 2025 : Qualification sur les portées audit de configuration et test d'intrusion
Statut : Expirée

CTF (Capture The Flag)

- BreizhCTF 2024
- TRACS 2022 / 2023 – 3e place
- DEFNET 2021 / 2022

FORMATEUR

Depuis 2023 : Intervenant en cybersécurité à Sorbonne Université

Développement d'outillage interne

Conception et maintenance d'outils internes d'audit et d'automatisation

CV des auditeurs – Victor

Victor est un auditeur expérimenté spécialisé dans la sécurité offensive et le phishing. Au cours de ces **trois dernières années**, il a pu mener des tests d'intrusion sur de nombreuses typologies d'environnements (infrastructures, applicatifs web, applicatifs mobiles et systèmes embarqués), et gérer de multiples exercices de phishing.

2022 - 2024

Master *Expert de la sécurité des données, des réseaux et des systèmes* en alternance
Ecole 2600

2022 - 2025

OWN
Auditeur cybersécurité (pentester)

Depuis 2025

Narok
Cofondateur & Auditeur cybersécurité (pentester)

RÉFÉRENCES

- **Test d'intrusion applicatif**

Audits d'applications web métiers et grand public selon la méthodologie OWASP
Nombreuses campagnes réalisées pour les secteurs assurance, bancaire, transport, finance, télécom et divers TPE/PME

- **Test d'intrusion interne**

Tests d'intrusion sur les environnements Active Directory et Wi-Fi
Audits d'architecture réseau et d'organisation interne
Réalisés dans des environnements sensibles des secteurs santé, assurance et énergie

- **Test d'intrusion mobile**

Audits de sécurité d'applications Android pour le secteur bancaire et de la grande distribution

- **Test d'intrusion systèmes embarqués**

Audits de sécurité sur des systèmes embarqués dans le *secteur aéronautique (portail multimédia, connectivité en vol, Wi-Fi)*

- **Revue d'architecture et de configuration**

Audits de postes de travail Windows dans le *secteur banque, assurance et santé*
Audits de configurations des serveurs Linux et de pare-feu pour les *secteurs télécom, bancaire et étatique*

COMPÉTENCES

PASSI – Prestataire d'Audit de la Sécurité des Systèmes d'Information qualifié

2025: Qualification sur les portées test d'intrusion, audit de configuration et audit de code
Statut : Expirée

Développement logiciel

- Développement d'un outil de simulation de campagne de phishing
- Développement d'outillage offensif (interceptions réseau)
- Développement d'applicatifs internes

Conception d'exercices de phishing

- Elaboration de scénarii adaptés au contexte client
- Copie des pages web légitimes
- Gestion du MFA

Notre valeur ajoutée

Pourquoi choisir
Narok ?

Une entreprise agile, à taille humaine et pour qui la satisfaction client est cruciale

Une équipe expérimentée, compétente et qui saura s'adapter aux enjeux et spécificités de chaque client

Des livrables exhaustifs et précis

Une disponibilité assurée pendant la période de l'audit et à posteriori si nécessaire

NAROK

narok.fr | contact@narok.fr | 06 49 50 39 86

Si vis pacem, para bellum