
NEVERHACK
YOUR CYBER PERFORMANCE PARTNER

Votre partenaire en matière de cyberperformance

Bienvenue dans le monde de NEVERHACK, où l'excellence et l'expertise convergent pour protéger vos données et vos systèmes. Dans cette présentation, vous découvrirez notre dévouement à la qualité et à la sécurité des projets que nous réalisons grâce à notre équipe qualifiée. Fruit de nos efforts et de notre collaboration, cette présentation constitue un guide précieux de nos offres et de nos solutions.

NEVERHACK

PARTENAIRE DE VOTRE PERFORMANCE CYBER

SÉCURITÉ OFFENSIVE
AUDIT & PENTEST

NOTRE CENTRE D'AUDIT NEVERHACK

Un centre qualifié PASSI
et France Cybersecurity en 2021.

30 Experts offensifs / auditeurs techniques & certifiés

+ de 40 auditeurs fonctionnels

Maitrisant de nombreux référentiels
- NIST V2
- ISO 27002.2022
- ENISA

Nos prestations (PASSI)

- TESTS D'INTRUSIONS
- AUDIT DE CONFIGURATION
- AUDIT DE CODE SOURCES
- AUDIT D'ARCHITECTURE

En milieu Industriel

- AUDIT DE SITE INDUSTRIEL
- AUDIT HARDWARE & OT

Autres expertises

- AUDIT D'APPLICATION
- CAMPAGNE DE PHISHING
- AUDIT ORGANISATIONNEL
- AUDIT DE FORGE LOGICIELLE

OPÉRATION RED TEAM & SOC ASSESSMENT

SERIOUS GAME & SIMULATION D'ATTAQUE (CTF, sensibilisation)

ILS NOUS FONT CONFIANCE

Secteurs concernés

- Aérospatiale & Défense
- Banques & Assurances
- Energie & Utilitaires
- Services Financiers
- Gouvernement & Secteur Publique
- Santé
- Luxe & Hospitalité
- Industrie manufacturière
- Retail & E-commerce
- Technologie & Logiciel
- Télécommunications
- Transport & Logistique

Liste non exhaustive

ÉVALUER VOS SURFACES D'ATTAQUE

Notre offre d'audit technique couvre l'ensemble de la surface d'attaque de votre organisation et permet de sécuriser vos actifs

INTERNE

- Réseau interne [LAN]
  Active Directory
- Audit des mots de passe
- Active Directory
- WIFI [WAN]

EXTERNE

- Infrastructure Externe
- Application WEB
- Application MOBILE
- OSINT

COMPORTEMENTAL

- PHISHING & SMISHING
- Intrusion physique
- VISHING
- Social Engineering

NOS ENGAGEMENTS & NORMES

01 | **EXPERTISE**

Une analyse et un diagnostic exhaustif des périmètres à auditer basés sur l'expérience et l'expertise de notre équipe

02 | **COMMUNICATION**

Un accompagnement réalisé par des hackers éthiques à l'écoute de vos objectifs et de vos contraintes

03 | **RESULTATS**

Les résultats des audits sont communiqués via des synthèses managériales et techniques afin qu'elles puissent être comprises par l'ensemble de votre organisation

04 | **CONFIDENTIALITÉ & SÉCURITÉ**

Nous garantissons la confidentialité et l'innocuité de nos interventions et de vos données. Autorisations d'audit et NDA sont globalement proposés en amont des missions

Référentiels & Normes

DISPOSITIF & LOCALISATION

NEVERHACK déploie plusieurs équipes européennes d'auditeurs techniques & pentesters pour répondre aux enjeux de sécurité offensive de ses clients. Ces équipes permettent à NEVERHACK d'assurer un niveau de réactivité important à ses clients internationaux. Nous permettant également de nous adapter aux contextes anglophones de nos clients.

- **FRANCE**
  Paris, Toulouse & Rennes
  15 Pentester
- **ITALIE**
  Milan
  10 Pentester
- **ESTONIE**
  Tallinn
  3 Pentester
- **ESPAGNE**
  Madrid
  2 Pentester

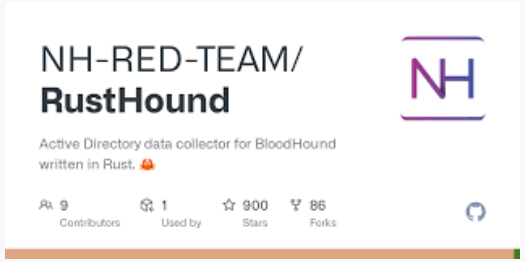
PUBLICATIONS & INNOVATIONS

Les experts en sécurité offensive de NEVERHACK sont amenés à utiliser différents outils dans le cadre de leurs missions.
Ils développent également de nouveaux outils innovants comme RustHound en 2022.

01 | RUSTHOUND

Outil Open Sources d'audit d'AD développé par les équipes NEVERHACK - 2022

RustHound est un outil de collecte BloodHound multiplateforme écrit en Rust, ce qui le rend compatible avec Linux, Windows et macOS.



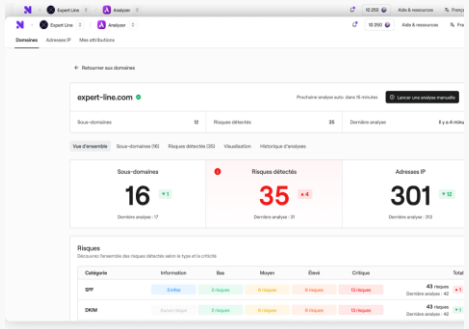
02 | CVE's

Dans le cadre de nos activités de recherche vulnerability, l'un des auditeurs NEVERHACK a relevé 3 vulnérabilités dans GLPI. Ces vulnérabilités ont été corrigées dans la version 10.0.10 du logiciel après les avoir divulguées à l'éditeur.

03 | Analyzer

Plateforme d'analyse de l'exposition à la sécurité de votre internet

Analyser vous permet de mesurer les vulnérabilités de votre exposition à internet :
- Nom de domaine
- Sécurité des sites web
- Sécurité des applications



04 | KRAKEN

KRAKEN redéfinit les standards des solutions BAS grâce à son moteur d'exécution avancé orchestrant des scénarios d'attaque complexes couvrant l'intégralité du framework MITRE ATT&CK.
La solution se distingue par :

- Des attaques réalistes et sophistiquées incluant des techniques furtives
- Une évaluation complète mesurant tant la réactivité des équipes SOC que l'efficacité réelle des solutions de sécurité déployées
- Une architecture extensible conçue pour intégrer de nouvelles technologies d'automatisation

ÉVÈNEMENTS & ANIMATIONS

NEVERHACK déploie une offre de "Serious Game" ou de "Capture The Flag" (CTF) en cybersécurité, adaptée aux besoins de formation des entreprises, des établissements éducatifs ou des équipes de sécurité.

CTF organisés par NEVERHACK

Développement d'une plateforme de sensibilisation pour les équipes IT

- Elaboration, écriture et intégration d'un programme de e-learning pour sensibiliser ses populations IT aux bonnes pratiques de sécurité.

Résultats:

- Structure et démarche pédagogique
- Fichiers source des supports produits
- E-learning IT complet intégré sur le LMS

LVMH

Sensibilisation des développeurs aux bonnes pratiques de développement

- Définition des programmes de sensibilisation
- Intégrer des principes de Serious Game
- Elaboration d'un support E-learning
- Animation d'une journée de formation (Formateur + Pentester)

Référentiel

- TOP 10 OWASP
- TOP 25 OWASP

LIVRABLES

RAPPORT

- Rapport détaillé et associé à une matrice de risques
- Slide pour représenter les failles lors de la restitution technique et la restitution métier
- Tableau de suivi des vulnérabilités

LIVRABLES HYPOTHESES

Un support de présentation technique est formalisé à l'attention des intervenants techniques permettant de présenter de façon synthétique l'ensemble du rapport d'intervention.

EVALUATION DES VULNÉRABILITÉS

Dans le cadre de sa démarche qualité et de son approche globale, NEVERHACK propose d'utiliser la même forme et les mêmes conventions pour l'ensemble des rapports d'audit et de tests d'intrusion fournis. Ainsi, tous les rapports d'intrusion utiliseront les mêmes métriques (CVSSv3.1 pour la qualification des vulnérabilités ou échelle de l'ANSSI si un score CVSS n'est pas calculable) et observeront la même structure pyramidale, quel que soit le domaine concerné

CVSS	0	1	2	3	4	5	6	7	8	9	10
Niveau de risque	Faible				Modéré			Important		Critique	

PV DE DESTRUCTION

NEVERHACK communique l'ensemble des rapports d'audit et les conserve pendant 1 mois après la restitution technique. Un PV de destruction doit être transmis par la suite au pilote de l'audit après ce délai.

LIVRABLES HYPOTHESES

PV de destruction

Plan d'actions

6.2 Mauvaise configuration des droits sudoers

La présence de la ligne :

```
(root) /usr/bin/rootsh -i -u oracle($|[ ].*)
```

Dans le fichier **/etc/sudoers** permet à un utilisateur d'ajouter des arguments à la suite de la commande:

```
sudo /usr/bin/rootsh -i -u oracle
```

En rajoutant "-u root" à la fin de la commande, il est possible d'élever ces privilèges et de passer **root** sur le serveur.

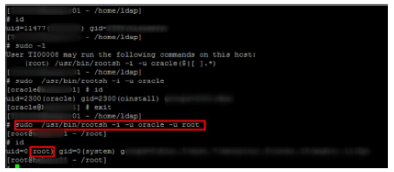


Figure 14: Élévation des privilèges à **root**

NOM	Mauvaise configuration des droits sudoers
CRITICITÉ	**MAJEURE**

DESCRIPTION	Le fichier **/etc/sudoers** permet entre autre de donner des accès à des commandes en tant que root à des utilisateurs n'ayant pas de droits sudo.
	
	Dans notre cas, l'utilisateur **USER02** peut effectuer la commande suivante avec les droits root:
	`(root) /usr/bin/rootsh -i -u oracle($|[ ].*)`
	Cette commande permet de passer à l'utilisateur **oracle**. Cependant, il est possible de passer **root** via la commande :
	`sudo /usr/bin/rootsh -i -u oracle -u root`
	En effet, le problème ici est la regex à la droite de oracle
	`oracle(\$|[ ].*)`
	qui permet à un utilisateur d'ajouter les paramètres qu'il souhaite à la suite de la commande.
	En rajoutant le paramètre '-u root', cela permet de passer en tant qu'utilisateur "root".

Tableau récapitulatif

4.2 Récapitulatif des vulnérabilités

Le tableau ci-dessous regroupe les vulnérabilités par ordre de criticité.

ID	VULNÉRABILITÉ	CRITICITÉ	AUTHENTIFIÉE	CVSS
3	XML eXternal Entity (XXE)	CRITIQUE	NON	9.3
1	Fuite d'informations	MODÉRÉE	NON	5.3
2	Composant déprécié et vulnérable	MODÉRÉE	NON	4.8

4.3 Plan d'actions de correction des vulnérabilités

Le tableau ci-dessous regroupe les actions correctives par ordre de priorité selon la criticité, l'impact et la facilité de correction des différentes vulnérabilités.

ID	VULNÉRABILITÉ	ACTION	EFFORT DE CORRECTION
3	XML eXternal Entity (XXE)	Correctement configurer le parseur XML. Filtrer les entrées utilisateurs. Dans le cas de projet2, l'endpoint **ibp** n'étant pas utilisé, il a été décidé de retirer son exposition d'Internet.	MOYENNE
2	Composant déprécié et vulnérable	Mettre à jour le composant/logiciel impacté. Toutes les applications doivent être maintenues à jour.	FACILE
1	Fuite d'informations	Cacher les informations pouvant aider un attaquant à comprendre et connaître la configuration d'un serveur.	FACILE

Synthèse technique

5. SYNTHÈSE TECHNIQUE

L'audit de sécurité a révélé plusieurs vulnérabilités critiques qui compromettent globale de l'infrastructure. Au total 13 vulnérabilités ou mauvaise configurations identifiées dont trois critiques : l'accès a des applications web avec les droits adm la présence d'un mot de passe Wi-Fi faible et la réutilisation de mots de pa comptes windows.

Lors de l'audit interne, 4 plages d'IP ont pût être identifiées :

- 10.0.0.1/24 et 10.0.0.2/24, comprenant entre autre le Domaine Controlle Directory et les machines utilisateurs des sites de Hackme sur Seine et l mer
- 10.0.0.3/24 et 10.0.0.4/24 hébergeant les serveurs de sauvegarde et c données.

Il est à noter que les réseaux avec les plages d'adresses IP sont les mieux sécurisés machine windows n'a pût être compromis sur ces réseaux. Cependant, sur le Hackme sur Seine, un des principaux problème identifié qui doit être corrigé d' la présence **d'un mot de passe Wi-Fi faible** sur le SSID "ACME-DATA" qui peut-ê

Synthèse managériale

4. SYNTHÈSE MANAGÉRIALE

L'audit de sécurité a mis en évidence plusieurs problèmes importants dans le réseau de ACME, affectant la sécurité globale de leurs systèmes. En tout, 13 vulnérabilités ou erreurs de configuration ont été identifiées, dont trois principales : un mot de passe Wi-Fi trop faible, un accès non sécurisé à certaines applications web, et la réutilisation de mots de passe sur les comptes Windows.

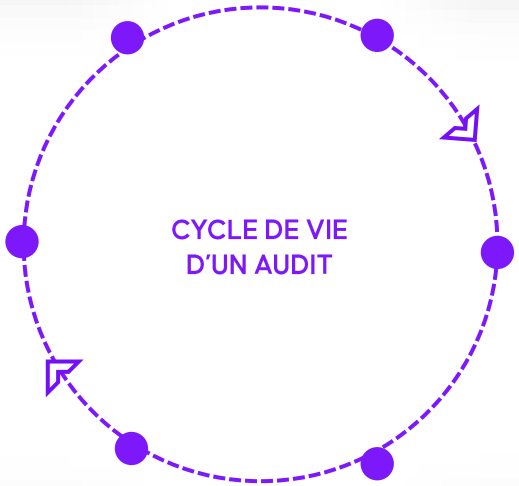
Certaines parties du réseau de ACME sont bien protégées, mais d'autres montrent des faiblesses notables. Par exemple, le mot de passe pour le Wi-Fi est trop simple, ce qui pourrait permettre à n'importe qui de se connecter facilement et d'accéder à l'ensemble du réseau interne. De plus, certains services sont accessibles sans les protections nécessaires, ce qui expose les systèmes à des risques de sécurité.

Il a également été observé que le manque de séparation entre différentes parties du réseau augmente les risques. Des informations sensibles ont été trouvées dans des partages mal configurés, et la réutilisation des mots de passe pour les comptes administratifs a facilité des accès non autorisés.

Concernant la gestion des mots de passe, la politique actuelle est insuffisante. Les mots de passe sont trop courts et certains comptes utilisent encore des mots de passe par défaut, ce qui pourrait permettre un accès facile à des comptes importants.

Les recommandations incluent de renforcer les mots de passe, de désactiver les services non essentiels, et de mieux gérer les configurations et les accès. En suivant ces conseils, il sera possible de corriger les faiblesses identifiées et d'améliorer la sécurité globale du réseau de ACME.

NOTRE DÉMARCHE :



01

Réception de la demande d'audit et envoie de la proposition commerciale.

- Note de cadrage
- NEVERHACK accuse réception de la demande(≈72h)
- NEVERHACK transmets une proposition technique et financière (≈7 jours)

LIVRABLES & HYPOTHESES

- 1 réunion de cadrage
- 1 réunion de présentation de l'offre

02

Planification de la mission

- Identification du périmètre de la mission
- NDA et Autorisation d'audit
- Travaux préliminaires: revue documentaire, analyse de risques et élaboration du programme d'audit

LIVRABLES & HYPOTHESES

- Planning d'intervention
- Méthodologie d'audit technique
- Liste des prérequis administratifs et techniques
- Autorisation d'audit

03

Lancement de la mission

- Validation des interlocuteurs
- Rappel du besoin (type de prestation, périmètre et objectifs)
- Logistique et planning

LIVRABLES & HYPOTHESES

- Réunion de lancement
- Format du rapport final
- Autorisation d'audit signé

04

Réalisation de l'audit

- Réalisation des tests techniques (tests d'intrusion, audit d'application mobile, etc.)
- Évaluation de la criticité des vulnérabilités
- Réunion à chaud en fin d'audit

LIVRABLES & HYPOTHESES

- Point quotidien ou hebdomadaire de suivi de la mission
- Réunion de préclôture (restitution à chaud)

05

Restitution de l'audit

- Consolidation et rédaction des livrables intégrant les synthèses managériale et technique, le descriptif de chaque vulnérabilité découverte
- Présentation des résultats d'audit technique (observations, et actions correctrices)

LIVRABLES & HYPOTHESES

- 1 réunion de clôture (restitution au COMEX et équipes techniques)
- Rapport d'audit technique
- Slides de restitution au travers d'une soutenance orale

06

CAPITALISATION

- Réunion semestrielle avec présentation des vulnérabilités par périmètre sur 6 mois.
- Exemple planning & suivi des vulnérabilités
- Optimisation d'intervention en mode contre audit
- Qualification des nouveaux périmètres

LIVRABLES & HYPOTHESES

- Tableau de suivi des vulnérabilités
- Point semestriel (Slides tendance vulnérabilité par périmètre)

NOTRE DÉMARCHE :

	LIVRABLES	HYPOTHÈSES
1 PHASE 1 – PLANIFICATION DE LA MISSION • Identification du périmètre de la mission • NDA et Autorisation d'audit • Travaux préliminaires: revue documentaire, analyse de risques et élaboration du programme d'audit	• Note de cadrage • Planning d'intervention • Méthodologie d'audit technique • Liste des prérequis administratifs et techniques • Format du rapport final	• 1 réunion de cadrage
2 PHASE 2 – LANCEMENT DE LA MISSION • Validation des interlocuteurs • Rappel du besoin (type de prestation, périmètre et objectifs) • Logistique et planning	• Autorisation d'audit signé	• Réunion de lancement
3 PHASE 3 – REALISATION DES TESTS TECHNIQUES • Réalisation des tests techniques (tests d'intrusion Externe & Interne) • Évaluation de la criticité des vulnérabilités	• Preuves d'audit formalisées • Tests techniques documentés • Constats formalisés	• Réalisation des tests techniques • Point hebdomadaire de suivi de la mission • Réunion de préclôture (restitution à chaud)
4 PHASE 4 – COMMUNICATION DES RESULTATS • Consolidation et rédaction des livrables intégrant les synthèses managériale et technique, le descriptif de chaque vulnérabilité découverte • Présentation des résultats d'audit technique (observations, et actions correctrices)	• Slides de restitution • Rapport d'audit	• 1 réunion de clôture (restitution au COMEX)

Notre méthodologie d'intervention est conforme avec les exigences spécifiques du référentiels PASSI.

GOUVERNANCE

Process & Outils

Une efficience de processus mesurée par des indicateurs de performances.

RÉACTIVITÉ

- NEVERHACK d'accusé de réception d'une demande de prestation sous 24H.
- NEVERHACK fournit une réponse chiffrée aux demandes de ses clients sous 7 jours ouvrés.

Une seule adresse mail de contact :
redteam@neverhack.com

KPI's

- Respect des délais de réponse aux sollicitations
- Respect des délais de démarrage
- Respect des délais de livraison des rapports
- Respect des délais de remplacement de ressources (absences non planifiées)
- Qualité des propositions techniques des projets
- Qualité des rapports d'audit technique
- Respect des fréquences des instances de gouvernance

Comitologie

Une comitologie à plusieurs niveaux : au niveau du contrat-cadre (pilotage de la sous-traitance) et au niveau de chaque besoin unitaire (maitrise de la qualité des livrables)

• **KOM / RLA**	• Prescripteur technique, • PenTester NEVERHACK • Resp. Projet NH
• **Réunion de restitution**	• Prescripteur technique, • PenTester NEVERHACK • Resp. Projet NH

Org-Chart

Une organisation dédiée à nos clients, adressant les métiers achat, pilotage de la sous-traitance et technique.

BUSINESS MANAGER
ACHAT

- Relation commerciale
- Gestion des demandes, réponses au niveau commercial,
- Garant des KPI globaux.

DIRECTEUR DE PROJET
HEAD OF, Prescripteurs

- Management global des équipes
- Allocation des activités
- Management des plans de charge
- Vérification de la conformité des Livrables

RESPONSABLE D'AUDIT & PENTESTER
EQUIPE Technique

- Delivery des activités
- Cross-Check
- Présentation des résultats
- Workshop si nécessaire

TEST D'INTRUSION

1 Expertise

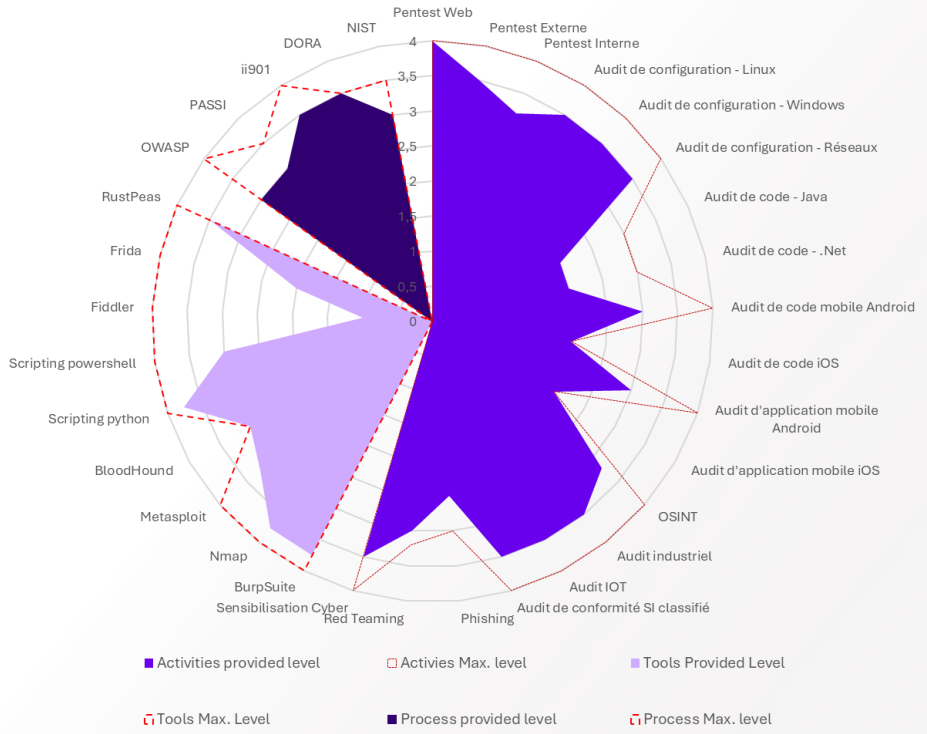
- Test d'intrusion interne
- Test d'intrusion externe
- Test d'intrusion web
- Audit d'application mobile

NEVERHACK est qualifié prestataire d'audit PASSI RGS par l'ANSSI. Chacune de nos prestations bénéficie des procédures et du savoir-faire PASSI, en particulier sur la confidentialité des données client.

2 Référentiels & Normes

3 Valeur ajoutée

- Test d'intrusion interne
- Test d'intrusion externe
- Test d'intrusion web
- Audit d'application mobile



75 tests d'intrusion web réalisé en 2023

35 tests d'intrusion d'application mobile réalisés en 2023

120 tests d'intrusions réalisés en 2023

1,09 M € CA 2023

4 Méthodologie & livrables

1. Prise d'empreinte
2. Recherche de vulnérabilités
3. Exploitation
4. Rebond & latéralisation
5. « Nettoyage »

- Liste des vulnérabilités identifiées, classées par criticité (faible, moyenne, élevée).
- Description détaillée des vulnérabilités, y compris les preuves d'exploitation.
- Recommandations de correction et bonnes pratiques.
- Synthèse des risques et propositions d'amélioration.

TEST D'INTRUSION

Black BOX

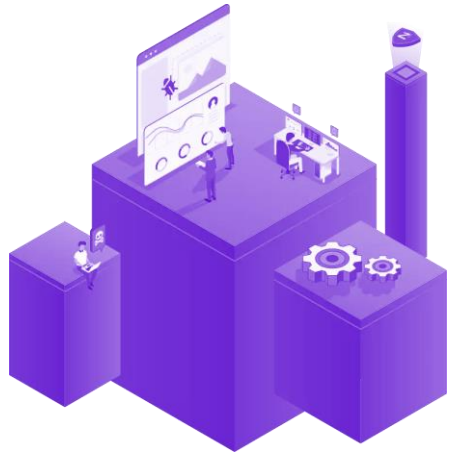
Approche de la boîte noire : Cette approche se concentre sur l'évaluation d'un système sans connaissance détaillée de sa structure ou de ses processus internes. Elle simule le point de vue d'un attaquant externe qui n'a pas accès aux informations internes de l'entreprise ou du système qu'il examine.

Grey BOX

Cette approche implique une certaine connaissance interne du système ou de l'organisation faisant l'objet de l'audit, mais pas une connaissance complète. L'auditeur dispose ainsi d'une vision plus nuancée et contextualisée de la situation. Elle simule le point de vue d'un utilisateur malveillant ou d'un attaquant qui a réussi à obtenir des informations d'identification.

White BOX

Cette approche implique une connaissance complète de la structure interne du système ou de l'organisation qui fait l'objet de l'audit. Les auditeurs ont un accès total aux informations internes, y compris les processus, les systèmes et les données. Cela leur permet d'évaluer en détail la conformité, les performances et les vulnérabilités.



AUDIT DE CODE SOURCE

1 Expertise

Un audit de code source en cybersécurité consiste à analyser le code d'une application pour identifier des vulnérabilités, des failles de sécurité et des mauvaises pratiques de développement.

2 Valeur ajoutée

- NEVERHACK est qualifié prestataire d'audit PASSI RGS par l'ANSSI. Chacune de nos prestations bénéficie des procédures et du savoir-faire PASSI, en particulier sur la confidentialité des données client.
- Les audits de code source réalisés par NEVERHACK peuvent s'effectuer sur tout type de langage informatique :

PHP JavaScript HTML CSS JAVA python C C#
C++ COBOL J2SS GO .Net

3 Référentiels & Normes

Software Engineering Institute

MISRA

OWASP

VISA DE SÉCURITÉ

Checkmarx

4 Méthodologie & livrables

- Scan des sources à l'aide d'outils automatisés ;
- Revue manuelle des résultats ;
- Audit et évaluation manuelle des parties de code les plus sensibles.

Liste non exhaustive des outils pouvant être utilisés lors de la phase de recherche automatisée:

- Semgrep : Outil d'analyse statique de code. Il permet de rechercher des motifs dans le code source,
- Visual Code Grepper : VCG est un outil de revue automatisée de la sécurité du code qui prend en charge C/C++, Java, C#, VB et PL/SQL.

- Dépôt du code sources et des rapports sur notre plateforme **Oodrive**.
- Identification des failles de sécurité dans le code (injections, mauvaises pratiques, etc.).
- Analyse de la qualité du code, de sa maintenabilité et de sa sécurité.
- Recommandations pour corriger les vulnérabilités et améliorer la sécurité du code.
- Conseils pour l'implémentation des bonnes pratiques de développement sécurisé.
- Exemple de code sécurisé ou bonnes pratiques de refactoring.

5 Key Figures

79 audits de code sources réalisés en 2023

632 000 K € CA 2023

AUDITS DE CONFIGURATION

1 Expertise

Un audit de configuration en cybersécurité consiste à évaluer les configurations des équipements systèmes & réseaux ainsi que les applications pour identifier des failles potentielles.

2 Nos Atouts

- NEVERHACK est qualifié prestataire d'audit PASSI RGS par l'ANSSI. Chacune de nos prestations bénéficie des procédures et du savoir-faire PASSI, en particulier sur la confidentialité des données client.
- Les audits de configuration réalisés par NEVERHACK peuvent s'effectuer sur tout type d'élément informatique :

Logiciel Applications Bases de données Equipement réseaux Forge logicielle Serveurs OT

3 Référentiels & Normes

4 Méthodologie & livrables

Analyse des configurations
- Comparer les configurations collectées avec les bonnes pratiques et standards de sécurité.
- Identifier les écarts, les mauvaises configurations, et les vulnérabilités potentielles.

Évaluation des risques
- Analyser l'impact potentiel des mauvaises configurations sur la sécurité globale.
- Prioriser les risques en fonction de leur gravité et de leur probabilité d'exploitation.

- Liste des erreurs de configuration ou des configurations non conformes aux bonnes pratiques.
- Analyse des impacts potentiels des mauvaises configurations.
- Recommandations pour corriger les configurations et aligner avec les standards de sécurité.
- Liste de contrôle (checklist) des configurations sécurisées.

5 Key Figures

55 missions d'audits de configuration réalisées en 2023

60 technologies et versions rencontrés par nos auditeurs

655 K € CA 2023

AUDIT ORGANISATIONNEL

1 Expertise

Un audit organisationnel consiste à évaluer le niveau de maturité de l'organisme audité, sur la base d'un référentiel sélectionné. Cette évaluation s'effectue via la conduite d'ateliers « déclaratifs », de l'analyse documentaire, et le cas échéant certains tests non techniques.

2 Nos Atouts

- Notre démarche est outillée, via la production de nombreux référentiels internes, prêt à l'emploi sur les principaux standards
- NeverHack est certifié PASSI, notamment sur la portée d'audit organisationnel
- ~30% de nos consultants sont certifiés ISO27001 Lead Auditor / Implémenter
- De nombreuses références nous permettent de bénéficier du retour & des bonnes pratiques du marché
- La transversalité des expertises NeverHack nous permet de faire appel à un pool d'experts le cas échéant (par exemple sur des sujets d'IAM)

3 Référentiels & Normes

4 Méthodologie & livrables

Nos équipes interviennent sur tout ou partie des étapes suivantes lors d'audits organisationnels :

- **Cadrage de l'audit** (étude du contexte, sélection/conception du référentiel d'audit adéquat, présentation de la démarche aux parties prenantes, etc.)
- **Conduite de l'audit**, sur base d'ateliers, d'analyses documentaires et le cas échéant de tests
- **Formalisation du rapport d'audit**, avec les résultats et le plan d'action associé

Principaux livrables

- Référentiel d'audit à compléter
- Supports de communication sur l'audit (flyer, kick-off, etc.)
- Référentiel d'audit complété
- Support de restitution de l'audit
- Feuille de route détaillée (projets identifiés, RACI associés, priorisation, etc.)
- Feuille de route niveau managérial
- Supports de comités

5 Key Figures

30% de nos consultants certifiés ISO27001

2 livres blancs parus en S1 2024 (NIS2 & DORA)

>10 référentiels couverts au sein de nos modèles

500 K € CA 2023

AUDIT DE SITE INDUSTRIEL

1 Expertise

- Audits OT/cybersécurité (orga./phy, techniques, architecture).
- Cartographies des systèmes,
- Audits & plans de conformité (IEC 62443, LPM, NIS/NIS2, TISAX, ...).

Nous réalisons des audits pour évaluer le niveau de sécurité OT/cyber, des cartographies via sondes passives, et nos intervenants possèdent une double expertise, pour une approche technique et opérationnelle.

2 Nos Atouts

- Notre équipe combine des années d'expérience en systèmes industriels ainsi qu'en cybersécurité, offrant une compréhension unique des contraintes et des risques spécifiques aux environnements industriels critiques, garantissant des solutions adaptées et efficaces.
- Grâce à notre double expertise, nous assurons une protection complète, alliant sécurité opérationnelle et physique, en suivant des standards éprouvés dans le secteur industriel et des audits méthodiques pour répondre aux standards les plus exigeants.

3 Référentiels & Normes

ISA/IEC 62443 CYBERSECURITY EXPERT ISA — IEC — AirCyber Boost — NIS2 — 82 Rev. 3 — TISAX®

4 Méthodologie & livrables

1. Définition des objectifs et périmètre
2. **Collecte de données** : Sondes passives OT et relevés techniques.
3. **Analyse** : Évaluation des vulnérabilités et écarts.
4. **Rapport** : Résultats, vulnérabilités, recommandations
5. **Restitution** : Présentation des résultats et plan d'action

- Évaluation du niveau de sécurité, vulnérabilités identifiées, écarts avec les référentiels.
- Plan d'action, recommandations d'amélioration, priorisation.
- Synthèse des écarts avec les référentiels et recommandations de mise en conformité.
- Cartographie réseau OT complète (plan d'architecture, matrice de flux, plan d'adressage, équipements critiques, etc.).

5 Key Figures

47 Audit de site industriel réalisés en 2023

564 K € CA 2023

AUDITS D'ARCHITECTURE

1 Expertise

L'audit d'architecture a pour but la vérification de la mise en œuvre des bonnes pratiques de sécurité sur un Système d'Information ou sur un périmètre donné de celui-ci.

2 Nos Atouts

- NEVERHACK est qualifié prestataire d'audit PASSI RGS par l'ANSSI. Chacune de nos prestations bénéficie des procédures et du savoir-faire PASSI, en particulier sur la confidentialité des données client.
- Les audits d'architecture réalisés par NEVERHACK peuvent s'effectuer sur ces différents environnements cloud :

Azure aws

3 Référentiels & Normes

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

ISO 19011 Auditor

VISA DE SÉCURITÉ

4 Méthodologie & livrables

Les thématiques de critères d'audit suivantes (si applicables) sont passées en revue :

- Défense périmétrique ;
- Défense en profondeur ;
- Cloisonnement ;
- Rupture protocolaire ;
- Gestion des flux ;
- Maintien en Condition Opérationnelle et Sécurité ;
- Traçabilité ;
- Sauvegarde ;
- Plan de continuité d'Activité / Plan de Reprise d'activité

- Analyse de la conception de l'architecture en termes de sécurité (segmentations, contrôles d'accès, etc.).
- Identification des points faibles dans la conception et des risques associés.
- Recommandations pour renforcer la sécurité de l'architecture (zonage, pare-feu, VPN, etc.).
- Plan d'amélioration pour l'évolution de l'architecture.

5 Key Figures

31 audits d'architecture réalisés en 2023

294 K € CA 2023

RED TEAMS

1 Expertise

L'objectif de notre service Red Team est de simuler une cyberattaque réaliste en récupérant des trophées que vous aurez définis (actifs sensibles de l'entreprise, données à caractères personnels, atteinte à l'image...) dans le but d'éprouver votre organisation.

2 Key Figures

6 Exercices Red Team réalisés en 2023

60 70 technologies et versions rencontrés par nos auditeurs

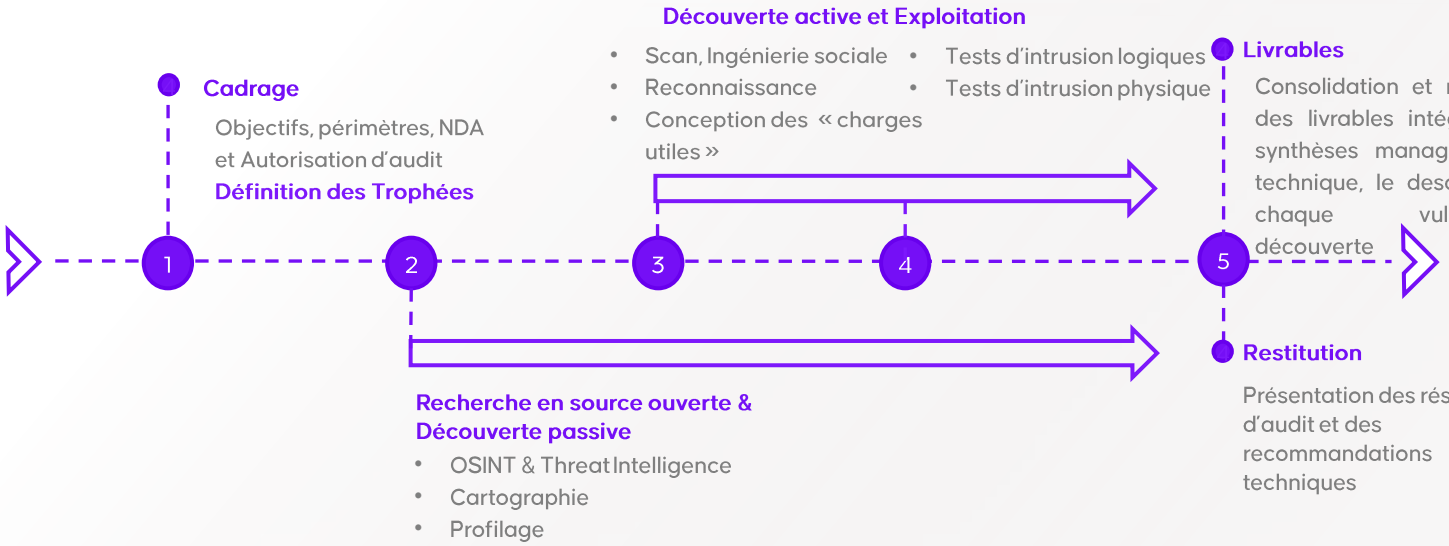
210 K € CA 2023

3 Référentiels & Normes

4 Méthodologie & livrables

Objectif : Effectuer un service dans le but de mener une attaque réaliste, généralement représentée en cinq étapes principales

- Recherche en source ouverte & Reconnaissance
- Ingénierie sociale
- Accès au SI
- Exploitation
- Obtention des trophées définis



SERIOUS GAME

1 Expertise

NEVERHACK déploie une offre de "Serious Game" ou de "Capture The Flag" (CTF) en cybersécurité, adaptée aux besoins de formation des entreprises, des établissements éducatifs ou des équipes de sécurité.

2 Valeur ajoutée

Capture The Flag (CTF) - Compétitions de Cybersécurité :

- CTF Jeopardy : Série de défis dans plusieurs catégories (cryptographie, exploitation de vulnérabilités, forensics, etc.) où les équipes gagnent des points pour chaque défi résolu.
- CTF Attack/Defense : Compétition où chaque équipe doit défendre ses propres services tout en essayant de pirater ceux des autres.

Scénarios de Simulation Réalistes : Jeux basés sur des scénarios réels où les participants doivent identifier et répondre à des cyberattaques simulées.

Formations Interactives et Ateliers : Sessions de formation en direct, avec des démonstrations pratiques et des exercices interactifs.

3 Référentiels & Normes

BattleHack

4 Méthodologie & livrables

PRODUCTION DE CONTENUS

SUPPORTS AUDIOVISUELS	E-learning, Mobile learning Vidéos, Motion design Démo. d'attaque Affiches, BD, Mails
JEUX	Serious Game, Escape Game Simulation, CTF
TESTS	Phishing, USB drop Ingénierie sociale Empreinte numérique Quiz

DÉPLOIEMENT

ANIMATION	Sessions en présentiel, table ronde, stands
INTÉGRATION ET LANCEMENT	Intégration au LMS Déploiement des contenus à distance
SUIVI DES INDICATEURS ET REPORTING	Taux de participation, succès (évolution des comportements) et satisfaction Amélioration continue

5 Key Figures

8 CTF organisés en 2023

3 Simulations d'attaques organisées en 2023

European Cyber Week
FIC Forum International de la Cybersécurité
ArcelorMittal
PRÉVOIR Assureur Solutions Vie
LVMH
LE GROUPE LA POSTE
CYBER ON BOARD
L'ORÉAL