Catalogue Cybersécurité

2025

actimac
SOLUTIONS PRO MAC & PC

osinx
PÔLE CYBERSÉCURITÉ

TABLE DES MATIÈRES

AUDIT / Serveur

Contexte

Le serveur est un élément central de l'infrastructure informatique. Sa sécurisation est primordiale pour garantir la disponibilité et la confidentialité des ressources.

Objectifs

- Évaluer la configuration matérielle et logicielle du serveur.
- Vérifier les mises à jour et correctifs appliqués.
- Contrôler la gestion des accès et des comptes utilisateurs.
- Analyser les paramètres de sécurité (firewall local, antivirus).
- Évaluer la qualité de supervision des incidents.

Prérequis

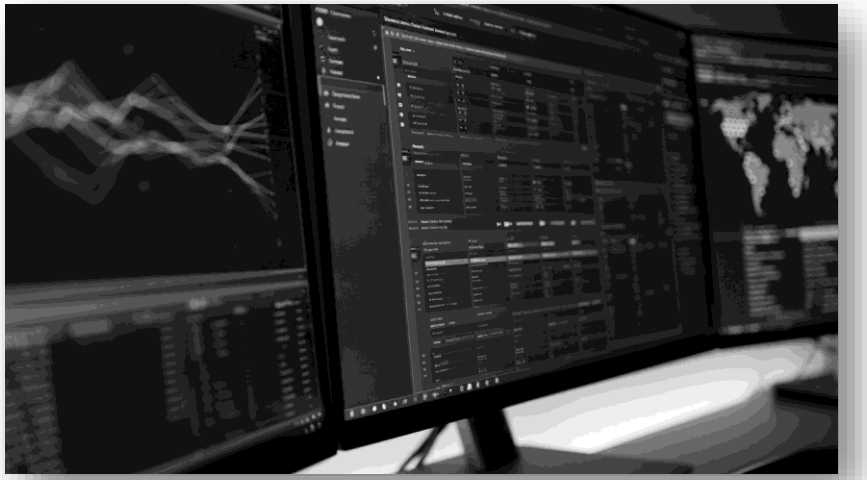
- Accès administrateur aux serveurs audités.
- Documentation technique et cartographie des serveurs.
- Disponibilité des responsables IT.
- Accès aux journaux système et de sécurité.

Durée

- 1 journée par serveur

Prestations

- Audit des configurations système et sécurité du serveur.
- Contrôle des accès et des privilèges.
- Analyse des logs et détection d'anomalies.
- Vérification des politiques de sauvegarde appliquées aux serveurs.
- Restitution de l'analyse et du plan d'action en visioconférence.



AUDIT / Active Directory

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

Active Directory est le service d'annuaire et d'authentification qui gère les identités et accès dans un réseau Windows. Son bon fonctionnement est crucial pour la sécurité globale du système d'information.

Objectifs

- Analyser la topologie AD (domaines, forêts, sites).
- Contrôler les rôles des contrôleurs de domaine (FSMO).
- Vérifier la gestion des comptes et groupes d'utilisateurs.
- Analyser les stratégies de groupe (GPO) appliquées.
- Vérifier les politiques de mots de passe et accès.
- Contrôler la réplication et la résilience des contrôleurs.
- Évaluer les mécanismes de journalisation et audit.

Prérequis

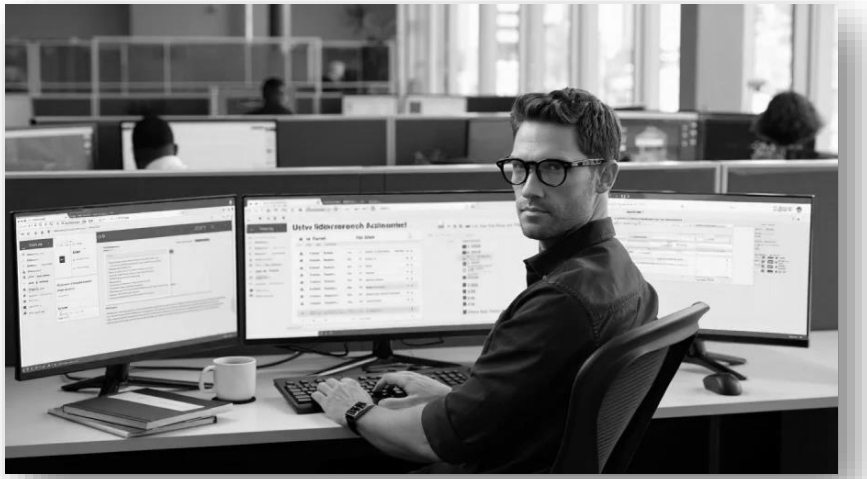
- Accès à un compte administrateur de l'AD.
- Documentation de l'architecture Active Directory.
- Disponibilité des responsables AD.

Durée

- 1 journée par Active Directory

Prestations

- Audit des contrôleurs de domaine et services AD.
- Analyse des politiques de sécurité appliquées.
- Contrôle des comptes à privilèges et délégations.
- Revue des processus de réplication.
- Restitution de l'analyse et du plan d'action en visioconférence



actimac
SOLUTIONS PRO MAC & PC

osinx
PÔLE CYBERSÉCURITÉ

AUDIT / Sauvegarde

Contexte

Les systèmes de sauvegarde sont la clé pour restaurer des données après incident. Sans contrôle, les sauvegardes peuvent s'avérer incomplètes ou inutilisables.

Objectifs

- Vérifier la politique de sauvegarde (fréquence, périmètre, supports, restauration).
- Évaluer la sécurisation des serveurs de sauvegarde.
- Contrôler la protection contre le chiffrement malveillant.
- S'assurer de la conformité aux obligations réglementaires.
- Vérifier la stratégie de rétention et d'archivage.

Prérequis

- Accès à la documentation des plans de sauvegarde.
- Disponibilité des administrateurs en charge de la sauvegarde.
- Accès en lecture seule aux consoles de restauration
- Accès administrateur pour les tests de restauration
- Disponibilité pour tests ponctuels.

Durée

- 1 journée par typologie de sauvegarde

Prestations

- Audit de la configuration du logiciel de sauvegarde.
- Tests de restauration à partir de différents jeux.
- Analyse des journaux de sauvegarde et erreurs.
- Vérification de la segmentation réseau / sécurisation.
- Restitution de l'analyse et du plan d'action en visioconférence.

AUDIT / Antivirus

Contexte

Dans le paysage numérique actuel, les antivirus sont essentiels pour détecter et neutraliser les charges virales, offrant ainsi une première ligne de défense contre les cybermenaces.

Objectifs

Se prémunir contre :

- Les virus informatiques (rançongiciel, cheval de Troie, malware…)
- La compromission ou la destruction de données
- Les interruptions d'activités par suite d'une attaque virale (rançongiciel)
- Une non-conformité réglementaire et/ou une non-application d'une assurance cyber.

Prérequis

- Disponibilité des prestataires infogérant la solution antivirale.
- Si possible, accès à la console d'administration de de l'antivirus avec un compte d'administration dédié et en lecture seule.

Durée

- 1 journée par solution antivirale

Prestations

- Évaluation de la couverture périmétrique (équipements protégés ou non par l'antivirus).
- Analyse des politiques de sécurité antivirale mises en place et des documentations associées.
- Vérification de la cohérence des configurations déployées (analyses comportementales, exclusions, sensibilité de détection).
- Évaluation des stratégies de maintien de service de l'antivirus.

AUDIT / Firewall

Contexte

Avec l'augmentation des menaces cybernétiques, les organisations doivent renforcer leur périmètre de sécurité pour protéger leurs réseaux et systèmes contre les intrusions.

Objectifs

La protection périmétrique inclut l'utilisation de systèmes de détection et de prévention des intrusions (IDS/IPS) et de technologies de filtrage avancées pour contrôler et surveiller le trafic entrant et sortant.

Prérequis

- Disponibilité des prestataires potentiels infogérant les Firewall.
- Accès au Firewall avec un compte d'administration dédié.

Durée

Selon le nombre de Firewall à analyser

Prestations

- Analyse de la configuration et des vulnérabilités du Firewall.
- Rapport d'audit : analyses, résultats, preuves et plan d'action.
- Restitution de l'analyse et du plan d'action en visioconférence.

AUDIT / Accès distants - VPN

Contexte

Les accès distants via VPN doivent être sécurisés pour éviter les compromissions. Leur contrôle est essentiel face à l'augmentation du travail en mobilité, du télétravail.

Objectifs

- Vérifier l'authentification des utilisateurs distants.
- Évaluer les mécanismes MFA intégrés.
- Contrôler la segmentation et restrictions d'accès.
- Analyser les configurations IPsec/SSL déployées.
- Vérifier la journalisation et détection d'anomalies.
- Étudier les droits accordés via le VPN.
- Évaluer la robustesse des clients VPN utilisés.

Prérequis

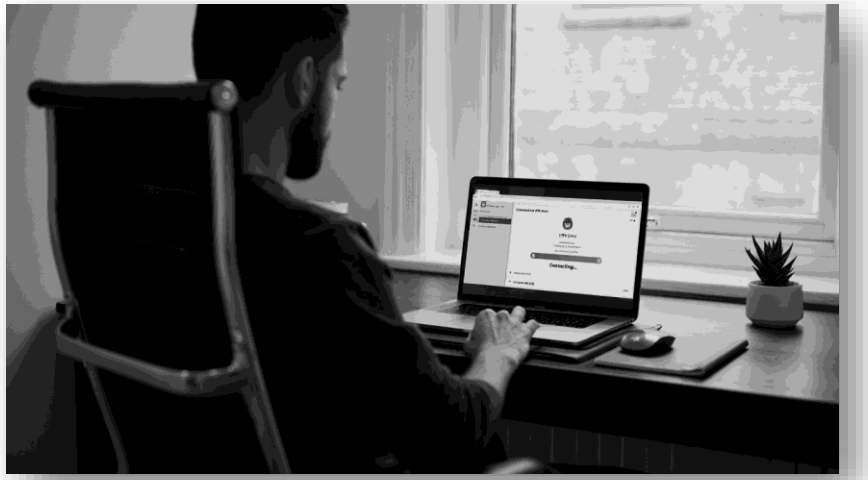
- Accès en lecture seule à la passerelle VPN.
- Documentation sur les profils distants des utilisateurs.
- Disponibilité des administrateurs réseau.
- Export des journaux récents d'accès VPN.

Durée

- 1 journée par accès distant à analyser

Prestations

- Audit de configuration des serveurs VPN.
- Analyse de la sécurité des protocoles utilisés.
- Vérification MFA et authentification.
- Contrôle des règles d'accès distants.
- Restitution de l'analyse et du plan d'action en visioconférence.



AUDIT / Wi-Fi

Contexte

Les réseaux Wi-Fi élargissent la surface d'attaque d'une organisation. Une configuration insuffisamment sécurisée permet des intrusions critiques.

Objectifs

- Évaluer la configuration de la sécurité (protocoles WPA…)
- Vérifier le cloisonnement entre les réseaux invités et internes.
- Contrôler les accès par certificats ou identifiants.
- Évaluer la robustesse des mots de passe et clés.
- Étudier l'intégration avec le SI (AD/RADIUS).
- Apprécier la qualité du monitoring du Wi-Fi.

Prérequis

- Plan de l'infrastructure du réseau sans fil.
- Accès en lecture seule aux contrôleurs et bornes Wi-Fi.
- Disponibilité d'un administrateur réseau.

Durée

- 1 journée par typologie de point d'accès

Prestations

- Audit des contrôleurs et points d'accès.
- Tests de sécurité (authentification, chiffrement).
- Analyse de la segmentation VLAN.
- Contrôle du monitoring et alertes.
- Restitution de l'analyse et du plan d'action en visioconférence

AUDIT / Messagerie Microsoft 365

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

La messagerie Microsoft 365 est une cible privilégiée des attaquants. Sa configuration doit être auditée pour limiter les phishing et compromissions.

Objectifs

- Vérifier les règles d'authentification (MFA, OAuth).
- Analyser les politiques de transport
- Évaluer la bonne configuration d'Exchange Online.
- Contrôler les flux SMTP entrants/sortants.
- Vérifier SPF, DKIM, et DMARC.
- Analyser la journalisation et la supervision des mails
- Contrôler la configuration des protections anti-spam.

Prérequis

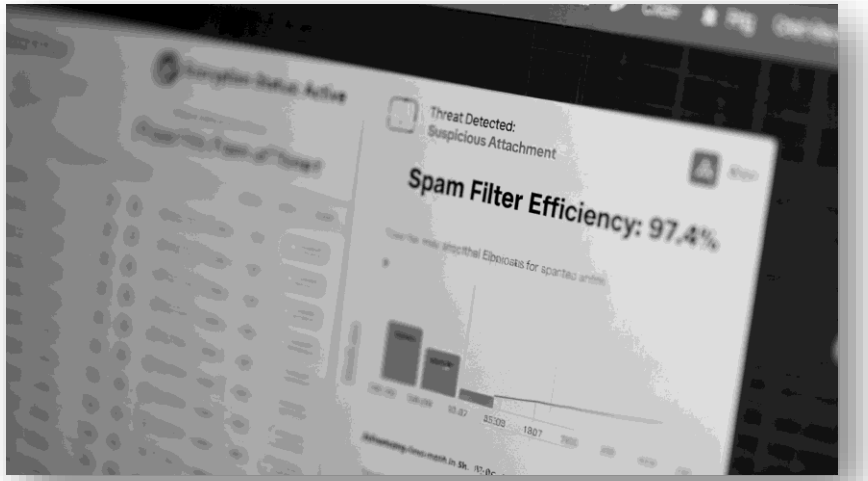
- Accès avec un compte administrateur dédié en lecture seule sur le tenant Microsoft 365.
- Disponibilité d'un administrateur Microsoft 365.
- Procédures et documentations actuelles des configurations.

Durée

- 1 journée par serveur Exchange Online

Prestations

- Analyse des configurations Exchange Online.
- Contrôle des règles d'authentification et sécurité.
- Vérification SPF, DKIM, DMARC.
- Analyse de la supervision et alertes.
- Restitution de l'analyse et du plan d'action en visioconférence



actimac
SOLUTIONS PRO MAC & PC

osinx
PÔLE CYBERSÉCURITÉ

AUDIT / Organisationnel

Contexte

Un audit organisationnel permet de mesurer la maturité cyber d'une organisation et tout particulièrement ses capacités de gouvernance des process liés à la cybersécurité.

Objectifs

- Évaluer les politiques de sécurité déjà en place.
- Vérifier la gestion des habilitations et accès.
- Contrôler les actions de sensibilisation des utilisateurs.
- Analyser les procédures de gestion d'incidents.
- Évaluer la gouvernance DSI & SSI.
- Vérifier le respect des obligations réglementaires.
- Contrôler la documentation et archivage des actions.

Prérequis

- Disponibilité d'un référent DSI/SSI.
- Documentation sécurité existante.
- Accès aux chartes et politiques interne.
- Disponibilité d'équipes métiers pour entretiens.

Durée

- devis personnalisé à définir

Prestations

- Analyse des procédures sécurité existantes.
- Revue des processus organisationnels SSI.
- Évaluation de la culture sécurité des équipes.
- Contrôle de la documentation et suivi.
- Restitution de l'analyse et du plan d'action en visioconférence

AUDIT / Téléphonie IP (VoIP)

Contexte

La VoIP simplifie, consolide la communication mais expose le système d'information à de nouveaux vecteurs d'attaque réseau. Son audit est crucial pour limiter les intrusions.

Objectifs

- Évaluer la sécurisation des serveurs de communication.
- Analyser les protocoles utilisés (SIP, RTP).
- Vérifier le chiffrement et l'authentification.
- Contrôler la segmentation entre VoIP et IT.
- Évaluer la résilience et la QoS.
- Contrôler la gestion des comptes et annuaires.
- Vérifier la journalisation et supervision.

Prérequis

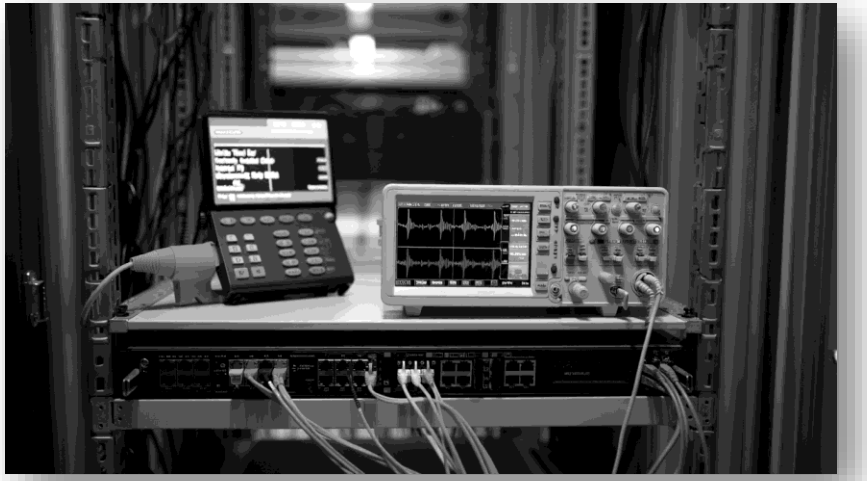
- Documentation de l'infrastructure VoIP.
- Accès en lecture seule aux consoles.
- Disponibilité d'un administrateur spécialisé dans les communications VoIP.
- Export des journaux récents.

Durée

- 1 journée par réseau VoIP

Prestations

- Analyse de la configuration des serveurs VoIP.
- Contrôle des protocoles et du chiffrement.
- Vérification des règles de segmentation.
- Audit des comptes utilisateurs.
- Restitution de l'analyse et du plan d'action en visioconférence



RSSI À TEMPS PARTAGÉ

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

La fonction de RSSI externalisé permet aux organisations n'ayant pas les ressources suffisantes de bénéficier d'une expertise en cybersécurité, d'un pilotage adapté des risques et de la conformité.

Objectifs

- Définir et piloter la stratégie de cybersécurité en cohérence avec les enjeux métier.
- Mettre en place et suivre un plan d'action sécurité.
- Superviser la conformité réglementaire (RGPD, NIS2, etc.).
- Gérer les incidents et sensibiliser les collaborateurs.
- Accompagner la direction dans les décisions de sécurité stratégique.

Prérequis

- Accès aux politiques et procédures internes existantes.
- Disponibilité des équipes techniques et métiers pour échanges réguliers.
- Mise à disposition des outils et tableaux de bord sécurité.
- Implication de la direction dans le suivi des actions.

Durée

- Sur devis

Prestations

- Audit initial de maturité et définition de la feuille de route sécurité.
- Gouvernance cybersécurité (comités, reporting, suivi des risques).
- Accompagnement en cas d'incident, de crise cyber.
- Déploiement de politiques de sensibilisation et de formation.
- Restitution régulière des indicateurs et plan d'amélioration en comité de direction.

actimac
SOLUTIONS PRO MAC & PC
osinx
PÔLE CYBERSÉCURITÉ

EDR MANAGÉ

Contexte

Le service ESET **M**anaged **D**etection & **R**esponse offre une protection avancée combinant l'expertise humaine d'un SOC dédié et l'intelligence artificielle, sans nécessiter de ressources dédiées en interne.

Objectifs

- Faire une surveillance continue des menaces 24/7
- Déployer une réponse immédiate aux incidents (confinement, remédiation).
- Bénéficier d'une équipe spécialisée externalisée
- Répondre aux exigences de conformité réglementaire (cyberassurance, NIS2 etc.).
- Avoir une visibilité et reporting automatiques (rapports avec analyse des incidents et recommandations.).

Prérequis

- Déploiement d'ESET sur l'ensemble des endpoints à surveiller.
- Connectivité réseau permettant la remontée des données de télémétrie vers la plateforme.
- Désignation d'un interlocuteur technique pour les échanges avec le SOC et la validation des actions.

Durée

- Selon devis personnalisé à définir.
- Optionnel : personne technique dédiée (TAM) pour un accompagnement renforcé en français 24/7.

Prestations

- Surveillance continue 24/7 (recherche d'IoC/IoA, analyse comportementale (UEBA), et corrélation des événements via IA et Threat Intelligence).
- Analyse, qualification automatiques et humaines des détections par des analystes SOC (criticité, investigation forensic avancée).
- Réponse aux incidents avec actions de remédiation immédiates (isolation d'endpoints, mise en quarantaine, blocage IP) avec escalade selon la sévérité.
- Optimisation continue par ajustement des règles de détection, d'exclusion et intégration des dernières menaces.
- Support et accompagnement via des alertes par e-mail, par la console. Création de rapports réguliers, et assistance d'experts pour la gestion de crise (avec option TAM francophone).

GESTION DES INCIDENTS

Contexte

Lors d'un incident cyber (intrusion, ransomware, compromission…), des réponses rapides et méthodiques sont essentielles pour contenir la menace et limiter les impacts.

Objectifs

- Identifier et qualifier rapidement l'incident.
- Contenir la menace et limiter sa propagation.
- Restaurer les systèmes critiques et la continuité d'activité.
- Analyser l'incident, faire un RETEX pour proposer des actions correctives afin de renforcer la sécurité et éviter la récurrence.

Prérequis

- Droits d'accès temporaires aux systèmes impactés.
- Accès aux journaux et éléments techniques (SIEM, antivirus, sauvegardes…).
- Disponibilité des équipes techniques.
- Contact désigné pour coordination et validation des actions.

Durée

- Sur devis

Prestations

- Analyse initiale et qualification de l'incident.
- Contention et éradication de la menace (isolation, nettoyage, correctifs).
- Assistance à la restauration des systèmes et données.
- Investigations forensiques et rapport d'incident.
- Recommandations d'amélioration et retour d'expérience.

PENTEST / Site internet

Contexte

Les sites web sont des cibles privilégiées des cyberattaques : un test d'intrusion permet d'identifier les failles pouvant être exploitées et leur résistance face à un attaquant potentiel.

Objectifs

- Détecter les vulnérabilités applicatives (injections, XSS, CSRF, etc.).
- Évaluer la sécurité des mécanismes d'authentification et de session.
- Identifier les faiblesses de configuration serveur et CMS.
- Mesurer le niveau de résistance face à une attaque réelle.

Prestations

- Cartographie et reconnaissance de la surface d'attaque du site.
- Tests manuels et automatisés des vulnérabilités connues (OWASP Top 10, WSTG), vérifications approfondies et tentatives d'exploitation contrôlées.
- Restitution de l'analyse et du plan d'action en visioconférence.

Prérequis

- Autorisation formelle de réaliser le test (contrat, périmètre défini).
- Accès technique au site (URL, environnements, comptes de test si nécessaire).
- Disponibilité des équipes techniques pour la coordination.
- Fenêtre de test validée afin de limiter les impacts en production.

Durée

- 3 jours

PENTEST / Réseau interne

Contexte

Un test d'intrusion depuis le réseau interne permet d'identifier les faiblesses exploitables par un attaquant déjà présent dans le SI (employé malveillant, accès ou ordinateur compromis).

Objectifs

- Détecter les vulnérabilités des systèmes, services et protocoles internes.
- Évaluer les risques liés aux partages de fichiers, à l'Active Directory et aux habilitations.
- Vérifier la segmentation et l'isolation des réseaux.
- Tester la propagation d'un attaquant dans le réseau interne.

Prérequis

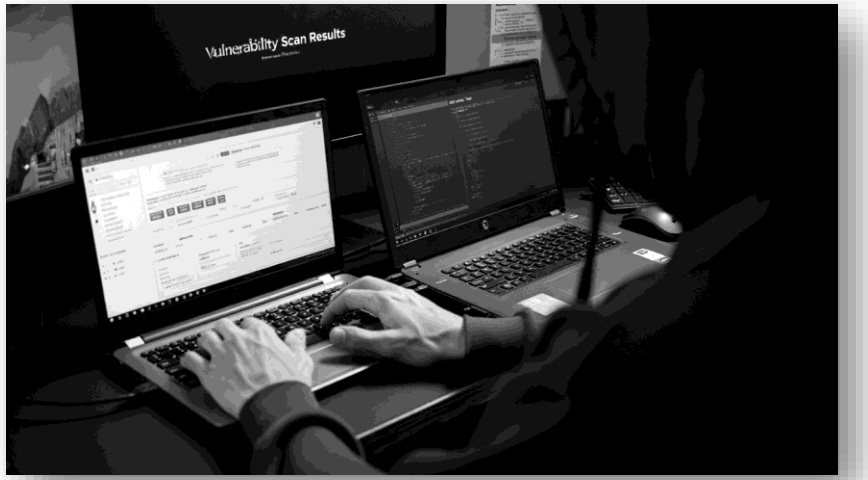
- Autorisation formelle de réaliser le test (contrat, périmètre défini).
- Accès au réseau interne via un point d'entrée défini (LAN, VPN, poste de test).
- Disponibilité des équipes techniques pour la coordination.
- Fenêtre de test planifiée pour éviter les perturbations.

Durée

- 3 jours

Prestations

- Reconnaissance et cartographie des ressources internes.
- Analyse des services exposés et identification des failles.
- Exploitation contrôlée (élévation de privilèges, mouvement latéral).
- Évaluation de la résistance d'Active Directory et des mécanismes de sécurité.
- Rapport détaillé avec criticité des failles et plan de remédiation et restitution en visioconférence.



PENTEST / Réseau externe

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

Un test d'intrusion depuis le réseau externe permet d'identifier les vulnérabilités exploitables par un attaquant à partir des infrastructures exposées sur Internet (serveurs, pare-feu, VPN, applications, etc.)

Objectifs

- Cartographier la surface d'exposition sur Internet.
- Identifier et tester les vulnérabilités des services et applications exposés.
- Évaluer la robustesse des mécanismes d'authentification et d'accès distant.
- Vérifier la résistance face aux attaques courantes (scan, exploitation, hors DDoS).

Prérequis

- Autorisation formelle de réaliser le test (contrat, périmètre validé).
- Liste des IP, domaines et services inclus dans le périmètre.
- Fenêtre de test validée pour limiter les perturbations éventuelles.
- Contact technique disponible pour la coordination.

Durée

- 3 jours

Prestations

- Reconnaissance et scan de la surface exposée.
- Tests automatisés et manuels des services et applications accessibles.
- Tentatives contrôlées d'exploitation des vulnérabilités.
- Vérification de la configuration des services critiques (VPN, firewalls, etc.).
- Rapport détaillé avec criticité des failles et plan de remédiation et restitution en visioconférence.

actimac
SOLUTIONS PRO MAC & PC
osinx
PÔLE CYBERSÉCURITÉ

HAMEÇONNAGE / Phishing par mail

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

Le phishing reste la première cause de compromission des systèmes d'information. Simuler des campagnes de phishing permet d'évaluer et de renforcer la maturité cyber des collaborateurs.

Objectifs

- Mesurer le niveau de maturité cyber des utilisateurs face aux attaques par mail.
- Identifier les comportements à risque (clic, ouverture de pièces jointes, saisie d'identifiants).
- Évaluer l'efficacité des dispositifs techniques (anti-spam, filtres).
- Sensibiliser et former les collaborateurs par la pratique.

Prérequis

- Liste des cibles et contenu de la campagne validés.
- Autorisation formelle de réaliser la campagne.
- Configurer les outils de protection pour exécuter la campagne de phishing
- Communication interne planifiée pour accompagner la démarche.

Prestations

- Conception, planification et envoi des campagnes de phishing.
- Suivi des comportements (clic, ouverture, saisie, signalement).
- Restitution des résultats auprès de la direction et des responsables.
- Option : renforcement de la maturité cyber par des sessions de sensibilisation adaptées.

actimac
SOLUTIONS PRO MAC & PC
osinx
PÔLE CYBERSÉCURITÉ

HAMEÇONNAGE / Smishing (SMS)

Contexte

Les attaques par SMS (smishing) exploitent la confiance des utilisateurs pour les inciter à cliquer sur des liens frauduleux, télécharger des applications malveillantes ou à divulguer des informations sensibles.

Objectifs

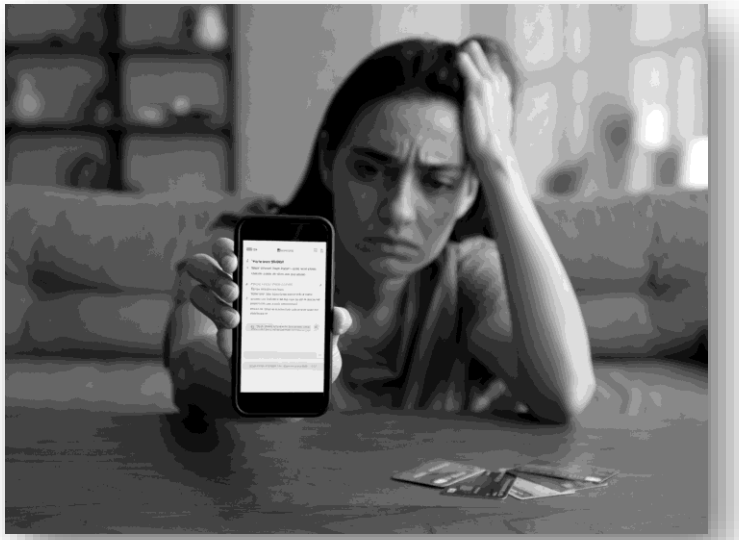
- Évaluer la sensibilité des utilisateurs aux attaques par SMS.
- Identifier les comportements à risque (clic, réponse, saisie d'identifiants).
- Vérifier la capacité des collaborateurs à détecter et signaler une tentative de compromission.
- Réduire le facteur humain comme point d'entrée des cyberattaques.

Prérequis

- Liste validée des numéros de téléphone cibles.
- Autorisation formelle de mener la campagne.
- Communication interne planifiée pour accompagner la démarche.
- Contact désigné pour suivi et restitution des résultats.

Prestations

- Conception et envoi de SMS de phishing réalistes.
- Suivi et mesure des comportements (clic, réponse, saisie).
- Restitution des résultats auprès de la direction et des équipes.
- Option : renforcement de la maturité cyber par des sessions de sensibilisation adaptées.



FORMATION / Sensibilisation à la cybersécurité

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

Les actions humaines sont déterminantes en cybersécurité : erreurs, clics malveillants ou négligences sont à l'origine de la majorité des incidents.

Objectifs

- Réduire le facteur humain dans les cyberattaques afin de limiter les risques
- Développer la culture cybersécurité au sein de l'organisation.
- Apprendre à reconnaître les menaces courantes (phishing, smishing, ransomware…).
- Adopter les bons réflexes de sécurité au quotidien.

Prérequis

- Disponibilité des collaborateurs ciblés.
- Présence des responsables de pôle, de service, fortement recommandée
- Salle équipée d'un système de projection

Durée

- Session de 3h en présentiel ou distanciel

Prestations

- Formation en présentiel ou distanciel
- Questionnaire d'évaluation de la maturité cyber des participants
- Diffusion de la présentation en PDF

actimac
SOLUTIONS PRO MAC & PC

osinx
PÔLE CYBERSÉCURITÉ

FORMATION / L'intelligence artificielle (IA)

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

L'intelligence artificielle transforme les usages numériques des organisations, mais elle induit aussi de nouveaux enjeux de confidentialité, de conformité et des nouveaux risques d'usage.

Objectifs

- Découvrir les usages pratiques de l'IA au service de la productivité.
- Comprendre les limites et les erreurs possibles des outils IA.
- Faire une utilisation sécurisée, responsable et éthique de l'IA au quotidien.

Prérequis

- Public cible identifié (collaborateurs, managers, direction).
- Identifier les outils IA utilisés dans l'organisation.
- Présence des responsables de pôle, de service, fortement recommandée
- Salle équipée d'un système de projection

Durée

- Session de 3h en présentiel ou distanciel

Prestations

- Formation en présentiel ou distanciel
- Questionnaire d'évaluation sur la compréhension des fondamentaux d'usage de l'IA
- Diffusion de la présentation en PDF.

actimac
SOLUTIONS PRO MAC & PC
osinx
PÔLE CYBERSÉCURITÉ

FORMATION / La gestion de crise cyber

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Contexte

Se préparer à la gestion de crise cyber permet de préparer les équipes à une situation critique, d'en limiter les impacts et assurer une meilleure résilience organisationnelle.

Objectifs

- Sensibiliser les équipes dirigeantes et opérationnelles aux enjeux d'une crise cyber.
- Comprendre les rôles et responsabilités au sein d'une cellule de crise.
- Maîtriser les bonnes pratiques de communication de crise (interne et externe).
- S'exercer à la prise de décision dans un contexte d'urgence.
- Renforcer la capacité de l'organisation à répondre efficacement à une crise.

Prérequis

- Identification des participants (direction, IT, métiers, communication).
- Si existants, outils de gestion de crise, PCA/PRA, procédure, etc.
- Salle équipée d'un système de projection.
- Validation du scénario de mise en situation avec l'organisation.

Durée

- 2 jours en présentiel

Prestations

- Présentation des fondamentaux de la gestion de crise cyber.
- Étude de cas réels et partage de bonnes pratiques.
- Simulation de crise (exercice simplifié et limité).
- Débriefing collectif avec analyse des réactions et axes d'amélioration (audit des risques, plan de continuité ou de reprise d'activité, etc.)

actimac
SOLUTIONS PRO MAC & PC
osinx
PÔLE CYBERSÉCURITÉ