synetis

wellcome by LA FRANÇAISE

Présentation des offres SSI
Audits

Version 1.1

VOS INTERLOCUTEURS

synetis

Antoine COUTANT
Practice manager Audits SSI & CERT

+33 6 67 22 02 34
antoine.coutant @synetis.com

Adrien DÉSIRÉ
Key Account Manager

+33 7 62 45 81 19
adrien.desire@synetis.com


01
SYNETIS

SYNETIS

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

VISA DE SÉCURITÉ

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

CLUSIF

membre de syntec numérique

FIC
Forum International de la Cybersécurité

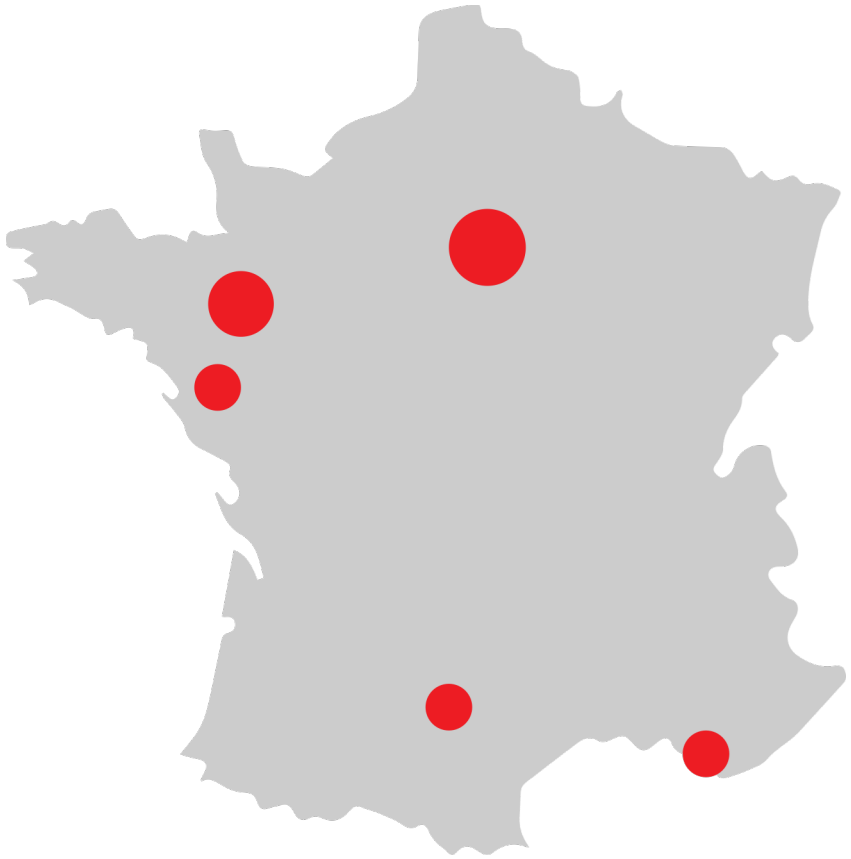
lesassises
de la sécurité et des systèmes d'information

certifopac

Happy index® AtWork

Les Echos
Champions de la croissance 2023

CROISSANCE CONTINUE

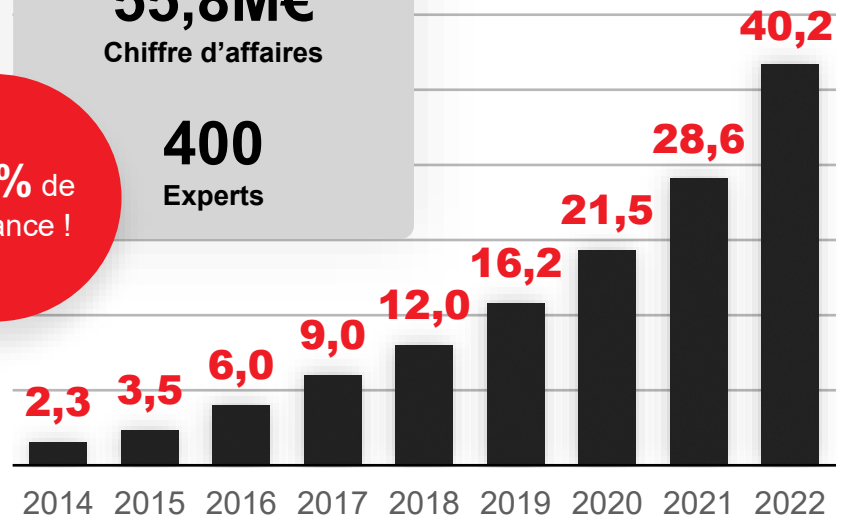


PRÉVISIONNEL 2023

55,8M€
Chiffre d'affaires

400
Experts

39,8% de croissance !



CHIFFRE D'AFFAIRES (M€)

EFFECTIFS

POURQUOI SYNETIS ?

Cabinet de **conseil** et d'**expertise**

Pure **player** de la **cybersécurité**

Membre actif d'**Hexatrust**

Forte imprégnation du **contexte** et des **enjeux** de votre écosystème

Labellisé **ExpertCyber** et qualifié **PASSI**

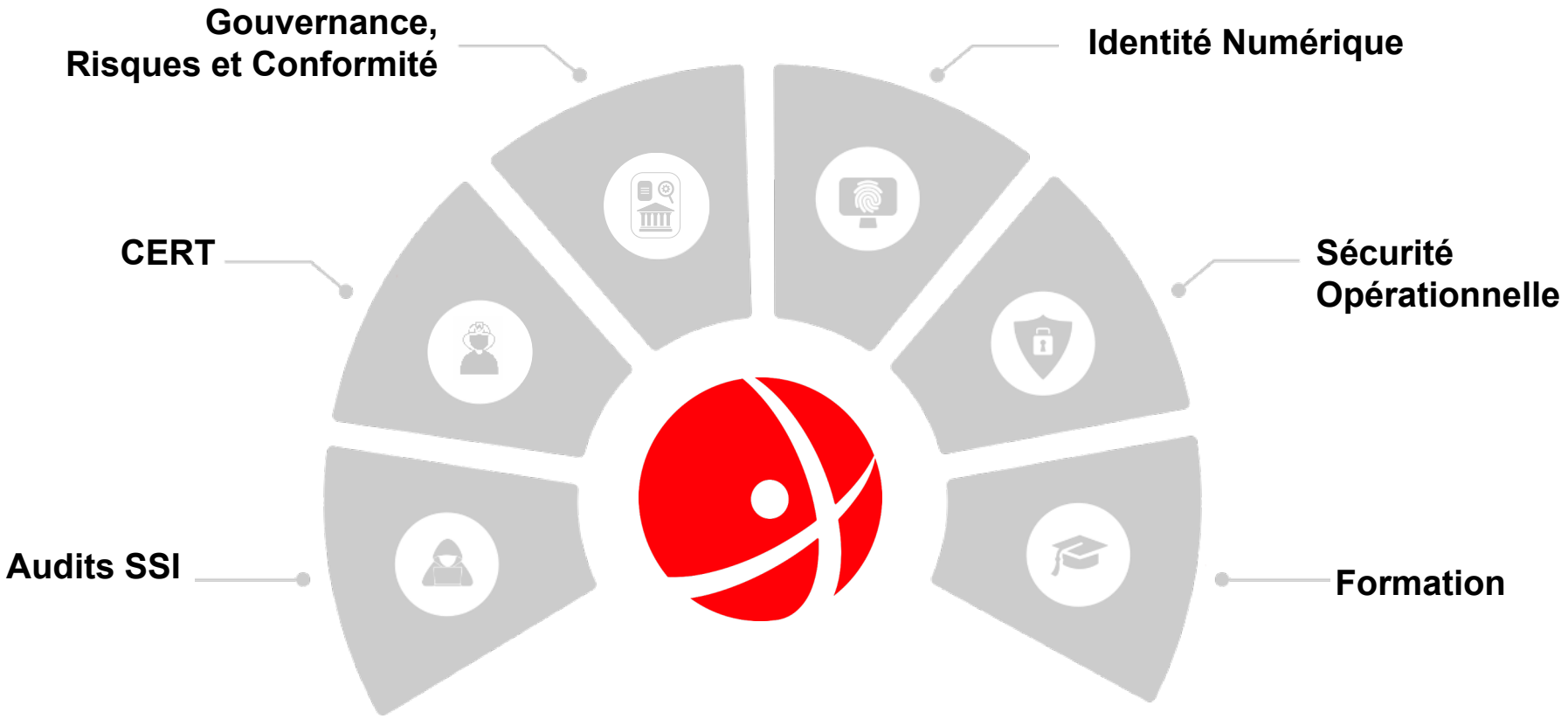
Offre de service **cybersécurité 360°**

02

OFFRES

synetis

OFFRES



Auditer → Conseiller → Construire → Opérer → Réagir

AUDITS SSI

Connaître son niveau d'exposition aux cybermenaces

Audits de sécurité

- Audits SSI : architecture, configuration, organisationnels et physiques, revue de code source, tests d'intrusion (interne, externe, applicatif)
- Audits transverses : systèmes industriels, WiFi, AD, redteam, etc.
- Campagnes de social engineering

Formation

- Catalogue de formations liées au thème majeur de la cybersécurité
- Formations sur mesure
- Formations de sécurité offensive

Cryptanalyse statistique

- Hygiène des mots de passe
- Indicateurs et métriques pour les sensibilisations
- Constat de la « solidité des secrets »

CERT SYNETIS

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

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

Prévenir et anticiper les menaces en cas d'incident

De la prévention…

- Veille de sécurité
- Threat intelligence

… à la réaction

- Réponse à incident
- Investigation numérique

GOUVERNANCE DE LA SÉCURITÉ, RISQUES ET CONFORMITÉ

Organiser et piloter sa cybersécurité

Définir la stratégie et l'organisation de la sécurité

- Schéma directeur / Roadmap SSI
- PSSI et politiques thématiques
- Diagnostics de maturité GHA / ISO 27002
- Gouvernance et organisation

Identifier, analyser et traiter les risques

- Cartographie de risques
- Intégration de la sécurité dans les projets
- Méthodologies eBIOS…

Viser et évaluer la conformité

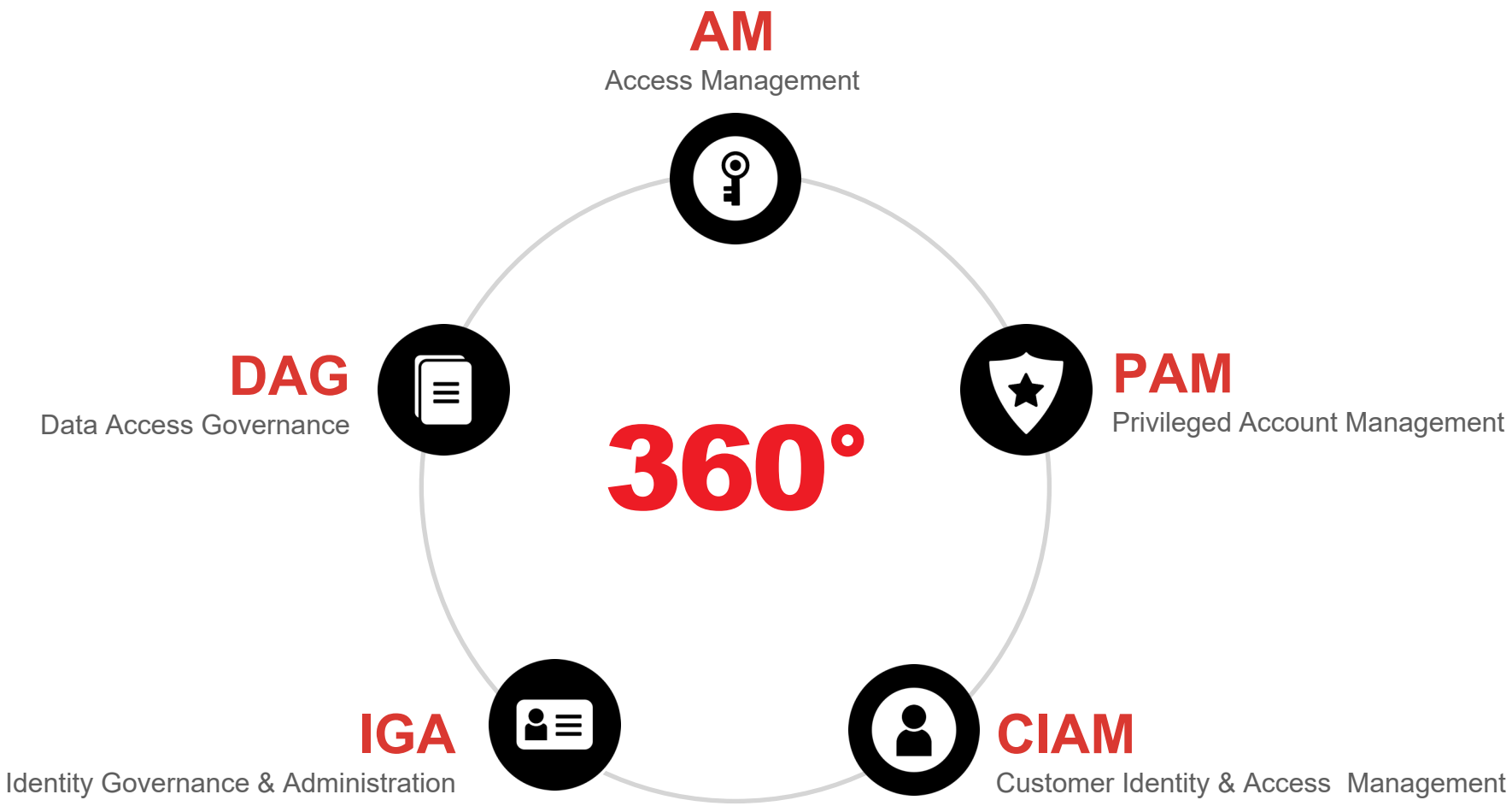
- Audits organisationnels de la sécurité (ISO 27001, NIS/LPM, NIST, SecNumCloud, PASSI…)
- Accompagnement à l'homologation (RGS)

Assurer la continuité et la résilience

- Plan de Continuité d'Activité
- Plan de Continuité Opérationnelle
- Plan de Gestion de Crise, exercice de crise, exercice de repli

IDENTITÉ NUMÉRIQUE

Maîtriser ses identités et ses accès



SÉCURITÉ OPÉRATIONNELLE

Déployer des solutions technologiques de protections des SI

Cryptographie, Infrastructures, Données, Réseau

Architecture & réseaux sensibles

Chiffrement & PKI

Prévention de fuite de données

Sécurité du cloud

Sécurité des réseaux

Sécurité des Infrastructures Microsoft

Sécurité & surveillance Active Directory

Sécurité & surveillance M365, AAD

Classification & protection des données

Détection & prévention des intrusions

Reconstruction SI

Détection & Services managés

Endpoint Detection & Response (EDR)

Network Detection & Response (NDR)

Logs & SIEM

SOC

Managed Security Services

DÉTECTION & SOLUTION

03

EXEMPLES DE PRESTATIONS D’AUDIT

synetis

PENTEST WEB

Objectifs

- Dérouler les tests techniques en boite noire (sans connaissance particulière sur une application cible ni de compte d'accès) puis en boite grise (avec une connaissance limitée de la cible et la possession d'au moins un compte d'accès)

Livrables

- Convention d'audit (rédigée en FR et au format PDF)
- Rapport détaillé de l'audit (rédigé en FR et au format PDF)
- Support de restitution / rapport managérial (rédigé en FR et au format PDF)

Hypothèses et limitations

- L'ensemble des phases est réalisé depuis les locaux de Synetis
- Le périmètre se limite au périmètre défini
- La période d'audit est limitée dans le temps, sur 1 semaine calendaire pour une cible web

- A partir de 5000€ HT (selon périmètre à auditer)

Approche

Etape 1 – Initialisation et cadrage

- Précision des besoins et des prérequis : définition du périmètre cible et de sa criticité
- Précision de la démarche et des impacts

Etape 2 – Tests d'intrusion externe

- Boîte noire
  - Découverte du périmètre cible, cartographie et recherche d'information en source ouverte (OSINT)
  - Analyse des technologies, frameworks et liaisons sécurisées SSL/TLS
  - Prise d'empreinte et analyse des équipements de sécurité identifiés (WAF)
  - Déroulement des tests de vulnérabilité passifs et outillés
  - Déroulement des tests intrusifs avancés, planifiés et principalement manuels
  - Focus sur les risques identifiés lors de la réunion de lancement
- Boîte grise
  - Déroulement des tests de vulnérabilité passifs et outillés
  - Déroulement des tests intrusifs avancés, planifiés et principalement manuels
  - Tests d'étanchéité entre les comptes, tentatives d'élévation de privilèges et usurpation d'identité

Etape 3 - Restitution des résultats

- Formalisation de l'analyse technique au sein d'un rapport détaillé
- Soutenance de restitution

CAMPAGNE DE PHISHING

Objectifs

- Evaluer la compréhension par les utilisateurs du SI du Commanditaire des mesures de sécurité dans leur environnement par la réalisation d'une campagne de social engineering de type hameçonnage de masse

Livrables

- En fin d'étape 1 : Stratégie de phishing au format PDF
- En fin d'étape 3 : Rapport de mise en œuvre et d'analyse des résultats de l'exercice, accompagné de recommandations rédigé en français et livré au format PDF

Hypothèses et limitations

- La reconnaissance active n'est pas employée lors de l'étape de profilage (prises de contact, filature, inspection physique, etc.).
- Une seule campagne de phishing réalisée (une seule population considérée soit un seul scénario)
- Aucune pièce jointe malveillante ne sera forgée pour la campagne, seuls des liens de redirection seront considérés
- L'achat d'un domaine typosquatté est inclus

- A partir de 3000€ HT

Approche

Etape 1 – Profilage

- Reconnaissance passive : recherche dans les sources d'informations publiquement accessibles (registres publics, sites web officiels et personnels, réseaux sociaux, forums, moteurs de recherche)
- Sélection des scénarios de phishing à privilégier :
  - Sujets susceptibles de présenter un fort intérêt pour le destinataire (actualité de l'entreprise, résultats, etc.)
  - Jeu-concours, information interne, etc., menant à un lien malveillant puis à une fausse mire d'authentification
  - Mail semblant provenir du support informatique, incitant par exemple les destinataires à télécharger et installer une mise à jour pour un logiciel du poste de travail

Etape 2 – Campagne de mailing

- Mise en place d'une plateforme de phishing/ portail malveillant reproduisant en tout point l'apparence d'une application cible, avec un nom de domaine le plus semblable possible à celui utilisé par cette dernière (typosquatting)
- Déroulement de la campagne de mailing et collecte des données associées

Etape 3 - Restitution des résultats

- Formalisation de l'analyse humaine au sein d'un rapport synthétique comprenant
  - Le(s) scénario(s) détaillé(s) de la campagne d'hameçonnage
  - Les données anonymisées et résultats statistiques de la campagne réalisée

PENTEST EXTERNE

Objectifs

- Auditer les composants exposés sur l'Internet (firewalls, routeurs, services et serveurs de DMZ exposés, etc.)

Livrables

- Convention d'audit (rédigée en FR et au format PDF)
- Rapport détaillé de l'audit (rédigé en FR et au format PDF)
- Support de restitution / rapport managérial (rédigé en FR et au format PDF)

Hypothèses et limitations

- L'ensemble des phases est réalisé depuis les locaux de Synetis
- Le périmètre se limite au périmètre défini
- La période d'audit est limitée dans le temps

- A partir de 5000€ HT (selon périmètre à auditer)

Approche

Etape 1 – Initialisation et cadrage

- Précision des besoins et des prérequis : définition du périmètre cible et de sa criticité
- Précision de la démarche et des impacts

Etape 2 – Tests d'intrusion externe

- Découverte du périmètre cible, cartographie et recherche d'information en source ouverte (OSINT)
- Découverte du périmètre de la cible exposé et cartographie des services
  - Identification des plages d'IP IANA, des domaines et sous-domaines
  - Analyses des services exposés, bannières, fingerprint, versions
  - Analyse de l'indexation, des versionning et des ressources
  - Cartographie et regroupement des assets (IP, serveurs)
- Déroulement des tests de vulnérabilités et identification des points d'entrées
- Analyse manuelle et approche offensive / intrusive à l'encontre des systèmes identifiés :
  - Contournement des règles de filtrage, des éventuelles protections en place
  - Routage des requêtes vers d'autres assets et identification des SPOF
  - Tentatives d'intrusions au travers de la DMZ pour des rebonds internes
- Validation des scénarios d'exploitation et vérification des faux-positifs
- Développement de preuves de concept / illustration des exploitations

Etape 3 - Restitution des résultats

- Formalisation de l'analyse technique au sein d'un rapport détaillé
- Soutenance de restitution

PENTEST INTERNE 1/3

Objectifs

- Auditer les composants exposés sur l'Internet (firewalls, routeurs, services et serveurs de DMZ exposés, etc.)

Livrables

- Convention d'audit (rédigée en FR et au format PDF)
- Rapport détaillé de l'audit (rédigé en FR et au format PDF)
- Support de restitution / rapport managérial (rédigé en FR et au format PDF)

Hypothèses et limitations

- L'ensemble des phases est réalisé depuis les locaux de Synetis ou sur site Audité
- Le périmètre se limite au périmètre défini
- La période d'audit est limitée dans le temps

- A partir de 5000€ HT (selon périmètre à auditer) + frais de déplacement

Approche

Etape 1 – Initialisation et cadrage

- Précision des besoins et des prérequis : définition du périmètre cible et de sa criticité
- Précision de la démarche et des impacts

Etape 2 – Tests d'intrusion externe

- Découverte du réseau et des composants de l'infrastructure auditée
  - Identification des segments réseaux, hôtes et services accessibles
  - Recherche de vulnérabilités et défauts de configuration
- Déroulement des tests intrusifs, planifiés et principalement outillés ou manuels :
  - Exploitation de vulnérabilités et défauts de segmentation et/ou de configuration
  - Attaques sur l'authentification et écoute active sur le réseau (MitM)
  - Déplacements latéraux, rebond, escalade de privilèges
  - Empoisonnements réseau (NBT-NS/LLMNR, IPv6, ARP, etc.)
  - Coerce (simple, authentifiée, avec rétrogradation, relay vers l'ADCS)
  - Exploitation de CVE (ZeroLogon, EternalBlue, PrintNightmare, etc.)
  - Attaques sur Kerberos, Wifi (le cas échéant)
  - Escalade de privilège au niveau du domaine Active Directory et du SI
- Validation des scénarios d'exploitation et vérification des faux positifs
- Développement de preuves de concept / illustration des exploitations

Etape 3 - Restitution des résultats

- Formalisation de l'analyse technique au sein d'un rapport détaillé
- Soutenance de restitution

PENTEST INTERNE 2/3

Ce type de test d'intrusion se focalise sur le réseau interne de l'audité. L'objectif ici est d'endosser le rôle d'un attaquant ayant réussi à entrer sur le réseau interne (via une intrusion externe réussie) ou bien le rôle d'un collaborateur de l'audité qui chercherait à lui nuire.

Dans ce type de test d'intrusion, l'attaque de l'annuaire (très souvent Active Directory) est une composante essentielle, car elle est souvent la colonne vertébrale du système d'information et permet de compromettre le réseau dans son ensemble.

Des tests de vulnérabilités sont également effectués à l'encontre des serveurs et postes de travails présents, ainsi que les différentes applications internes qui seraient présentes, car ils peuvent permettre la découverte de comptes pour un potentiel rebond.

Audit Simple

- Réseau unique, avec un annuaire Active Directory simple (mono-forêt mono-domaine) ou sans, moins de 100 serveurs
- A partir de 5 000€ HT (selon périmètre à auditer), frais de déplacement facturés en sus

Audit Moyen

- Réseau unique comprenant un annuaire Active Directory plus complexe (multi-forêt avec relations d'approbation, et/ou multi-domaine), entre 100 et 250 serveurs. Possibilité d'utiliser un poste de travail standard de collaborateur pour l'approche boîte grise.
- A partir de 9 000€ HT (selon périmètre à auditer), frais de déplacement facturés en sus

Audit Complexe

- Interconnexion de réseaux (rebonds nécessaires), annuaire Active Directory complexe (multi-forêt avec relations d'approbation, et/ou multi-domaine) ou autre type d'annuaire, plus de 250 serveurs. Possibilité d'utiliser un poste de travail standard de collaborateur pour l'approche boîte grise.
- A partir de 15 000€ HT (selon périmètre à auditer), frais de déplacement facturés en sus

PENTEST INTERNE 3/3 – AUDIT SPÉCIFIQUE WIFI

Souvent jugés sécurisés et robustes, les réseaux Wifi ou les implémentations qui gravitent autour de son usage présentent quelques faiblesses inhérentes au monde sans fil. Malgré tout, les attaques sur le Wifi ne sont pas simples à mettre en œuvre car elles nécessitent des cartes capables d'injecter des trames ce qui est un prérequis nécessaire pour les attaques Wifi et la plupart des PC ne disposent pas de cette capacité.

Dans le cadre de ses travaux d'audit de sécurité, Synetis a mis en place une méthodologie dédiée pour auditer un réseau Wifi. Cette dernière comprend une approche boîte noire, une approche boîte grise et également une approche Wifi open / invité.

Pour les tests boîte noire, la méthodologie consiste à cartographier les réseaux Wifi environnants afin de détecter la présence d'éventuels réseaux mal configurés. Une analyse des méthodes d'authentification EAP est également réalisée. Par écoute passive, l'auditeur s'attache à vérifier différentes faiblesses d'authentification (WEP, WPA PSK, WPA MGT). Bien que les versions PEAP et EAP-TLS intègrent une encapsulation TLS, les premiers échanges EAP Response / identity transitent par défaut en clair, divulguant potentiellement le nom de domaine Active Directory de l'entreprise et l'identifiant utilisateur. Ces informations présentant un intérêt pour attaquant sont alors recherchées. Enfin, la mise en place d'un point d'accès Wifi frauduleux (Rogue AP) permet de vérifier différents points de contrôle tels que les méthodes d'authentification, l'identité du serveur Radius, etc.

Pour l'approche boîte grise, l'auditeur cherche à vérifier le contrôle d'accès réseau (par adresse MAC par exemple) ainsi que le cloisonnement entre réseau. Un point d'attention porte sur la vérification de la/les interface(s) d'administration du point d'accès et si elle(s) est(sont) accessible(s) sur le réseau / VLAN courant. Enfin, les wifi open-guest disposent souvent d'un portail web captif. L'auditeur cherche alors à y contourner l'identification. En effet, les portails sont souvent équipés de "slots" de taille fixe autorisant X connexions simultanées. Ainsi, en automatisant de nombreuses connexions avec des adresses MAC générées à la volée, les slots peuvent être saturés provoquant un déni de service du point d'accès invité.

- A partir de 5 000€ HT (selon périmètre à auditer)
- Frais de déplacement facturés en sus.

contact@synetis.com
+33 1 47 64 48 66

www.synetis.com
19 rue du Général Foy, 75008 Paris
2 rue Claude Chappe, 35510 Cesson-Sévigné