ASTAR

CATALOGUE DES SERVICES

Désignation
Astar_Catalogue_Services

Rédacteur
David SORIA - dsoria@astar.org

Nature, Date et version
Catalogue des services 2025-10-15 v1.5

01

02

03

PRÉSENTATION D'ASTAR

Astar est une société spécialisée, exerçant exclusivement dans le secteur de la Sécurité des Systèmes d'Information (cybersécurité), dans tous ses sous-domaines du service :

RÉPONSE À INCIDENT | AUDIT | CONSEIL | FORMATION

Astar a été reconnu **Expert Cyber** par l'AFNOR. Ce titre valorise les entreprises ayant démontré un niveau d'expertise technique et de transparence dans le domaine de la cybersécurité.

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

Nous promouvons une approche de la sécurité *"by design"* en favorisant les fondations (minimisation, maintenabilité, processus, ...), plutôt que l'empilement d'outils qui complexifient et alourdissent le SI.
Notre ambition est que la sécurité informatique soit, un jour, pour les usagers, aussi simple que de mettre une serrure sur sa porte.

Les valeurs d'Astar

Nos engagements éthiques

Afin d'éviter tout conflit d'intérêt, qui pourrait orienter nos recommandations techniques ou le contenu de nos articles, Astar ne commercialise aucun produit de cybersécurité et n'accepte aucun sponsor.

Astar pratique des tarifs réduits pour les services publics, les associations d'intérêt général et les jeunes entreprises.
Nous essayons, autant que possible, de recourir à des prestataires labellisés B Corporation.

Astar s'engage socialement, auprès des plus jeunes, sur les problématiques de risques numériques (*"sextorsion"*, *"revenge porn"*, protection des données personnelles, ...) en animant des séances gratuites de sensibilisation dans divers établissements (lycée, MJC, ...).
Astar s'engage pour la protection du potentiel scientifique et technique (PPST) de la nation en animant des séances gratuites d'initiation aux thématiques de cybersécurité, dans les pépinières de Start-Up.

Astar s'engage sur la thématique de l'empreinte environnementale. Nous n'imprimons rien. Nous privilégions les transports faiblement carbonés. Nous utilisons, autant que possible, du matériel hautement réparable. Nous éteignons nos services qui ne nécessitent pas une disponibilité continue.

Nos engagements professionnels

Les lignes directrices de l'approche revendiquée par Astar sont les suivantes :

- **L'Utilité**
  Nous ne cherchons pas à paraître impressionnant avec un jargon cryptique. Nous ne cédons pas à la facilité des recettes toutes faites mais inapplicables à votre contexte. Nous voulons fournir un travail clair, exploitable et qui produira des effets. Nous personnalisons toutes nos missions.
- **L'Expertise**
  Rester au niveau, face à l'évolution toujours plus rapide des technologies, nécessite un temps conséquent dédié à la veille et à l'expérimentation. Nos experts allouent en moyenne 40 jours par an à de l'exploration technique non facturée.
- **Le soin**
  Toutes nos prestations se doivent de faire la fierté des ingénieurs qui les réalisent. Nous tenons à produire un résultat absolument impeccable et nous ne lésinons pas sur les efforts.

Carte d'identité

Nom	Astar
Forme sociale	Entreprise unipersonnelle à responsabilité limitée
Adresse (siège)	4 rue Alan Turing 33680 LACANAU
Capital	100 € (assurance RC Pro couvrant pour 100 000€ de dégats causés)
Immatriculation	843 134 842 (R.C.S. BORDEAUX)
Création	2018-10-16
Président	David SORIA
Actionnariat	Français 100% (David SORIA)
code APE	6202A (Conseil en systèmes et logiciels informatiques)
site Web	https://www.astar.org
Contacts	contact@astar.org - 09 83 20 01 30

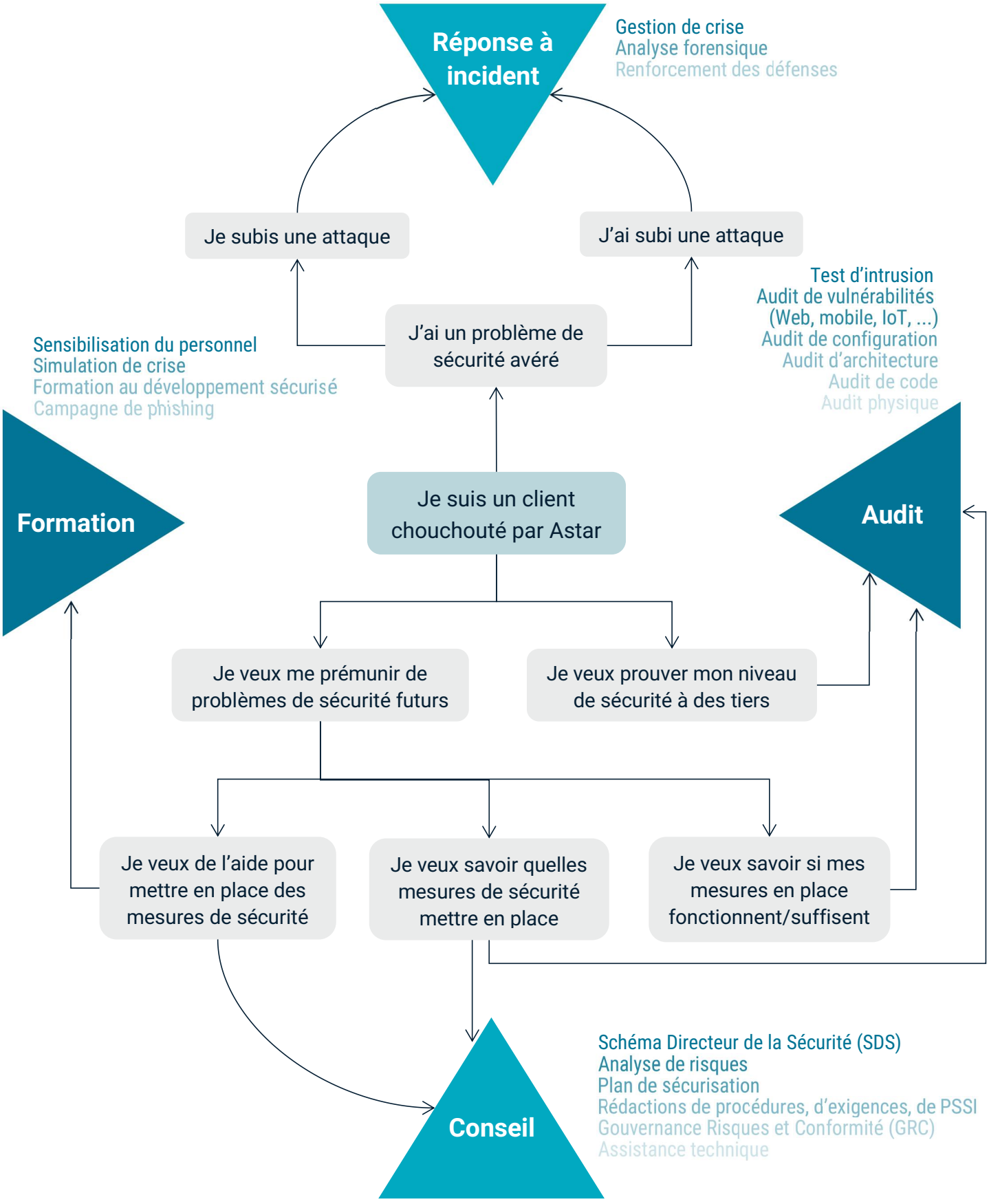
Clients

Astar intervient en France et à l'étranger, dans les entreprises de toute taille et dans tous les secteurs économiques. Nos clients incluent des sociétés du CAC 40 tout comme des Start-Up.
Nous avons une expérience très étendue dans l'audit des systèmes d'information de santé (à travers de nombreux hôpitaux audités et des Medtech produisant des objets connectés pour la santé). Mais aussi dans les domaines bancaires, industriels et du transport.

Quelques clients ayant accepté d'être cités :

PRESTATIONS

Le présent catalogue des prestations Astar est en permanence accessible à l'adresse suivante :
https://bonny.astar.org/Astar_Catalogue_Services.pdf



Vue d'ensemble

- **CSIR-CRI** : Gestion de crise - *150 € HT de l'heure en journée, 300 € HT la nuit et le weekend*
- **CSIR-FOR** : Analyse forensique - *Forfait à 5 000 € HT ou sur mesure à 500 € HT par demi-journée*
- **CSIR-DEF** : Renforcement des défenses - *450 € HT par demi-journée*

- **ASSI-EXT**: Audit de résistance aux intrusions externes - *900 € HT par jour*
- **ASSI-INT** : Audit de résistance aux intrusions internes - *900 € HT par jour*
- **ASSI-MOB** : Audit d'application mobile - *900 € HT par jour*
- **ASSI-IOT** : Audit d'objet connecté - *900 € HT par jour*
- **ASSI-AUT** : Audit d'automates et Systèmes Industriels - *900 € HT par jour*
- **ASSI-COD** : Audit de code - *900 € HT par jour*
- **ASSI-CNF** : Audit de configuration - *900 € HT par jour*
- **ASSI-ARC** : Audit d'architecture - *900 € HT par jour*
- **ASSI-PHY** : Audit physique - *900 € HT par jour*
- **ASSI-INC** : Audit incrémental - *900 € HT par jour*
- **ASSI-PAS** : Audit annuel des mots de passe - *Forfait 1 000 € HT*
- **ASSI-SOC** : Stress Test SOC - *900 € HT par jour*
- **ASSI-DOS** : Stress Test Déni de Service - *900 € HT par jour*
- **ASSI-EXP** : Audit d'exposition numérique - *900 € HT par jour*

- **CONS-STA** : StartSec - *Forfait 1 000€ HT*
- **CONS-GRC** : Audit Gouvernance Risque Conformité (GRC) - *Forfait 2 500 € HT*
- **CONS-SDS** : Schéma Directeur de la Sécurité - *Forfait 5000 € HT*
- **CONS-PDS** : Analyse des risques et Plan de Sécurité - *900 € HT par jour*
- **CONS-ORG** : Audit organisationnel - *900 € HT par jour*
- **CONS-AMO** : Assistance technique - 450 *€ HT par demi-journée*

- **SENS-SUA** : Sensibilisation à la cybersécurité (pour StartUp et associations) - *Gratuit*
- **SENS-ADO** : Sensibilisation aux risques numériques pour les adolescents - *Gratuit*
- **SENS-PER** : Sensibilisation au risque informatique (pour le personnel) - *1 jour, 1200€ HT*
- **SIMU-CRI** : Exercice de crise cyber - *900 € HT par jour*
- **SENS-PHI** : Campagne de phishing - *Forfait 3000 € HT*
- **FORM-DEV** : Formation au développement sécurisé (pour développeurs) - *3 jours, 3000 € HT*
- **FORM-SIA** : Formation au déploiement sécurisé de l'IA - *3 jours, 4000 € HT*
- **FORM-SAD** : Formation à la sécurisation d'Active Directory - *3 jours, 3000 € HT*
- **FORM-PER** : Formation à la sécurité offensive (pour les employés) - *5 jours, 5000 € HT*
- **FORM-RAP** : Formation rédaction de rapport (pour pentesters) - *1 jour, 2500 € HT*
- **COUR-SEC** : Module cybersécurité (pour l'enseignement supérieur) - *25 heures, 5000 € HT*

Réponse à incident

CSIR-CRI : Gestion de crise

Si vous subissez actuellement une attaque, vous pouvez faire appel à nous pour vous aider à gérer, en direct, cet événement.

Cette prestation consiste à monter une cellule de crise (où à rejoindre la votre si vous en avez déjà une), avec un ingénieur Astar, afin de vous assister dans la résolution de l'incident.
Dans ces moments de stress intense, il est difficile d'avoir les idées claires et de prendre les meilleures décisions. Disposer d'un point de vue extérieur, et expérimenté, favorise une résolution rapide de l'incident, tout en diminuant les risques de dommages collatéraux ou de nouveaux départs de feu.

Les consultants Astar s'occupent de dresser un plan de gestion ordonné afin d'accomplir les bonnes actions dans le bon ordre (communication, action, prise d'information, etc.).
Ils coordonnent les personnes capables d'agir sur place et suggèrent les moyens de résolution qu'ils jugent les plus adéquats.
Ils mettent à disposition une trousse à outils toute faite pour les opérations importantes (copie de la RAM, recherche de maliciel, ...). Ils prennent également soin de faciliter les investigations futures (recherche de l'origine de l'intrusion, des auteurs, de la portée réelle, ...) via la collecte et la sauvegarde des éléments clés.

Cette prestation est facturée à l'heure. Le client n'a pas besoin de s'engager sur un nombre minimal d'heures et il peut décider, à tout moment, de la fin de cette assistance.

Pour qui	Les entreprises en train de subir une attaque
Pour quoi	Éliminer la menace le plus vite possible et avec le moins de pertes possibles
Quand	Au cours de l'attaque subie
Tarif	150 € HT de l'heure en journée, 300 € HT la nuit et le weekend

CSIR-FOR : Analyse Forensique (Investigation numérique)

L'analyse forensique a pour objectif d'élucider, dans la mesure du possible, les sources, les causes, les techniques, les tactiques et la chronologie d'une attaque subie.

L'investigation en amont cherche à remonter la chaîne des causalités depuis les événements dommageables observés :

- Identifier le(s) programme(s) malveillant(s) (si l'attaque était automatisée) ou les commandes à l'origine des dommages observés
- Identifier les méthodes (tactiques et techniques) d'exécution de ce programme ou de ces commandes (escalade de privilège, vol d'identifiants, contournement des défenses, …)
- Identifier les moyens d'obtentions de ces méthodes (attaque par force brute, exploitation de vulnérabilité, ingénierie sociale, …)
- Identifier les sources ayant réalisé l'intrusion initiale

L'investigation en aval suit les actions des agents malveillants au sein du réseau :

- Lister les machines où les dommages ont été observés
- Identifier les sources depuis lesquelles les attaquants se sont connectés à ces machines puis les destinations vers lesquelles ils se sont propagés

- Identifier les méthodes (tactiques et techniques) de reconnaissance, de propagation et de compromission au sein du système d'information
- Identifier d'éventuels accès persistants ou des activités résiduelles de la menace, au sein du réseau

La méthodologie d'investigation d'Astar s'appuie sur le formalisme de la matrice ATT&CK mise à disposition par le MITRE pour décrire les tactiques et techniques.
Astar emploie uniquement des méthodes d'investigation conformes à l'état de l'art et non destructives vis-à-vis des preuves analysées.

Cette prestation est un engagement de moyens au cours duquel Astar explore les matériaux d'investigation à disposition (journaux d'événements, copie du maliciel, ...) et restitue un rapport contenant :

- Les constats et les déductions
- Les hypothèses et, le cas échéant, les certitudes, à propos de l'amont et de l'aval de l'attaque
- Les recommandations pour rétablir et améliorer le niveau de sécurité

Les analyses forensiques peuvent également être conduites dans le cadre d'une plainte. Dans ce cas, Astar propose une prestation sur mesure et suit une méthodologie très cadrées (collecte opposable des preuves, déclaration de tous les outils utilisés avec version et somme de contrôle, …).
Le livrable est un rapport d'expertise complet pouvant être produit comme preuve dans une démarche judiciaire.

Forfait d'analyse préliminaire

Après avoir subi un incident, on souhaite parfois ne pas perdre de temps sur les aspects commerciaux afin de démarrer l'analyse le plus tôt possible.
Pour les clients qui veulent limiter les allers-retours avec le service achat, nous proposons une analyse forensique préliminaire forfaitaire au prix de 5000 € HT (plus frais de déplacement).

Un ingénieur Astar est dépêché sur place et alloue environ 4 jours à l'investigation de l'incident.
Son objectif est d'établir des conclusions sur tous les sujets où cela est possible, dans le temps imparti. Puis de lister les hypothèses possibles pour les questions qui demeurent en suspens.
Le rapport d'intervention technique décrit toutes les investigations menées, les hypothèses et conclusions, les preuves collectées et une estimation du temps nécessaire pour faire la lumière sur les questions demeurées irrésolues.
Ce rapport est conçu pour servir de base exhaustive à toute investigation future qui viendrait en complément (même de la part d'un autre prestataire).

A l'issue de cette analyse préliminaire, le client peut se contenter des résultats ou bien demander une extension pour continuer les investigations sur un ou plusieurs points non élucidés.

Ce format forfaitaire est, de l'expérience d'Astar, souvent bien adapté. En effet, même si toutes les questions ne reçoivent pas une réponse certaine, il est fréquent que les actions à mener par le client diffèrent finalement peu selon que telle ou telle hypothèse soit vraie.
Par exemple: même si une intrusion par force brute est suspectée sans être avérée, le client doit de toute façon changer tous les mots de passe car la base Active Directory a été exposée.
Cette analyse préliminaire est donc souvent suffisante pour donner des recommandations pertinentes, même lorsque toutes les questions n'ont pas pu être élucidées.

Analyse sur mesure

Si vous souhaitez une prestation sur mesure, Astar vous proposera un devis de 20 jours d'analyse (au prix de 1000 € HT/Jour, plus les éventuels frais de déplacement) dont vous ne paierez finalement que les jours réellement consommés.

Un ingénieur Astar est envoyé sur place et mène les analyses sur les matériaux d'investigation à disposition. Il rend compte, chaque soir, de ses avancées de la journée, des pistes qu'il projette d'explorer le lendemain et des chances qu'il estime d'obtenir des réponses concluantes.
Si le client estime posséder assez d'éléments ou si les moyens, nécessaires pour en obtenir plus, sont trop couteux, il peut décider de mettre fin à l'analyse à tout moment. Il s'accordera avec l'ingénieur Astar sur le format de rapport attendu selon son besoin (simple note technique d'intervention ou rapport complet pouvant servir devant un tribunal).
Une fois le rapport terminé, seuls les jours réellement consommés sur le devis initial sont facturés.

Pour qui	Les entreprises ayant subi une attaque
Pour quoi	Déterminer comment les attaquants ont pénétré dans le réseau, ce qu'ils y ont fait et comment empêcher que cela se reproduise
Quand	Une fois que l'attaque a été circonscrite
Tarif	Forfait à 5 000 € HT ou sur mesure à 500 € HT par demi-journée

CSIR-DEF : Renforcement des défenses

Le rétablissement ou l'amélioration du niveau de sécurité, après une attaque, peut être une tâche délicate.
Il arrive notamment qu'il soit nécessaire de mobiliser des compétences en cybersécurité qu'on ne possède pas parmi son personnel mais qui n'auraient pas vocation à être internalisées de manière pérenne.

Dans ces cas-là, il est pertinent de recourir à une assistance technique ponctuelle de quelques jours/semaines. Astar peut détacher des ingénieurs chez ses clients pour les accompagner dans la résolution des points faibles (revue des permissions, recherche des machines obsolètes, sécurisation d'une interface Web, ...) ou la mise en place d'améliorations (déploiement d'un SIEM, d'un scanner de vulnérabilités, d'un outil de cartographie du SI, ...).

Astar propose un *pull* de jours/homme assez large et le client peut décider, à tout moment, de la fin de l'assistance technique, sans préavis, lorsqu'il est satisfait des avancées. Il ne paiera que les demi-journées effectivement consommées (450 € HT la demi-journée).

Pour qui	Les entreprises ayant subi une attaque
Pour quoi	Combler les points faibles du système d'information et élever le niveau de résistance face aux attaques
Quand	Quelques semaines après l'attaque subie
Tarif	450 € HT par demi-journée

Audit de Sécurité du Système d'Information

Test d'intrusion / Audit de vulnérabilité

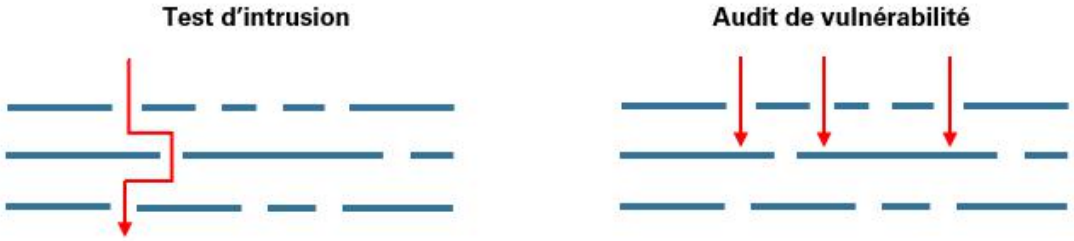
Le domaine de la cybersécurité fait souvent mention d'audit de vulnérabilité et de test d'intrusion de manière interchangeable. Pourtant, il existe des subtilités entre ces deux notions.

Elles ont en commun la démarche générale :

- Identification de la nature des cibles et découverte de leur agencement
- Acquisition d'informations et recherche de vulnérabilités
- Exploitation des vulnérabilités et tentatives d'intrusions
- Analyse des risques et proposition de contre-mesures

La première différence porte sur le but recherché. Un audit de sécurité sert à se mettre en conformité avec l'état de l'art. Un test d'intrusion sert à mettre à l'épreuve ses défenses.

La deuxième différence tient dans les phases de recherche et d'exploitation. L'audit de vulnérabilité est une démarche dite "**horizontale**" : il cherche à lister toutes les vulnérabilités visibles par un attaquant. Le test d'intrusion est une démarche "**verticale**" : il cherche à déterminer la profondeur à laquelle un attaquant peut s'introduire dans un système d'information (il n'a besoin d'identifier qu'une seule vulnérabilité à chaque étape).



L'expérience d'Astar montre que c'est souvent une approche hybride qui va correspondre au mieux à ce dont un client a besoin.
Les prestations d'**audit de résistance aux intrusions** (externes ou internes) d'Astar combinent donc l'audit de vulnérabilité et le test d'intrusion.
L'aspect prédominant dépend de ce qui motive la démarche initiale du client. L'approche du test d'intrusion est pertinente lorsque le client est soumis à une obligation de résultats. Celle de l'audit de vulnérabilité l'est lorsqu'il est soumis à une obligation de moyens.

Conformément à l'état de l'art, Astar propose des **contre-audits** (retest) et des **attestations d'audit**. Le contre-audit permet de valider les corrections effectuées par vos équipes, quelques semaines après l'audit initial. L'attestation vous permet de communiquer les résultats macroscopiques à des tiers, sans révéler les détails techniques (qui décrivent comment vous attaquer).

ASSI-EXT : Audit de résistance aux intrusions externes

L'audit externe sert à évaluer la résistance de votre système d'information vis-à-vis d'Internet: pirates, concurrents, robots automatisés, etc.
Il s'adresse donc aux actifs exposés à tout Internet : messagerie, site Web, extranet, portail fournisseur, VPN, etc. Mais aussi aux produits que vous vendez : progiciel, "appliance", ...

Le profil de ce type d'audit est généralement en "blackbox": l'auditeur ne dispose d'aucun accès ni d'aucune information préalable sur la cible. Lorsque le périmètre contient un ou des espaces authentifiés

(site Web par exemple), il est pertinent d'ajouter une partie "greybox" (un compte utilisateur valide est fourni). Ceci permet de couvrir le scénario d'un utilisateur hostile ou qui se serait fait voler son compte (en raison d'un mot de passe trop faible par exemple).

La méthodologie suivie pour ce type d'audit est celle de l'OWASP qui est la référence prédominante du domaine.

Bien que ce type d'audit couvre tous les scénarios de menace, nous proposons aussi, pour les clients qui le souhaitent, de le diviser en plusieurs prestations qui couvrent chacune un type précis de menace :

- **Niveau 1 : résistance face à une attaque automatisée**
  Attaquant dit "opportuniste" : maliciel exploitant uniquement des vulnérabilités connues (non patchées) et utilisant des moyens de propagation automatisables - 95% des attaques.
- **Niveau 2 : résistance face à une attaque avancée**
  Attaquant recourant à une approche semi-manuelle et qui oriente ses attaques de manière personnalisée selon le contexte. Les moyens de compromission et de propagation peuvent être sophistiqués (non automatisables) - environ 4% des attaques.
- **Niveau 3 : résistance face à une attaque ciblée**
  Attaquant recherchant activement des failles dans les produits ou le réseau de l'entreprise pour mener des attaques "supply chain" (compromettre les clients de cette entreprise). L'attaquant peut allouer un temps conséquent à la recherche de vulnérabilités et posséder des compétences très pointues (notamment en algorithmique, sécurité logicielle et cryptographie) - environ 1% des attaques.

Cette approche progressive permet de commencer par des prestations économiques mais qui couvrent la majorité des attaques subies.

Pour qui	Les entreprises qui ont déjà mis en place un socle de protections minimales vis-à-vis d'Internet
Pour quoi	Vérifier l'effectivité des protections en place et éliminer les angles morts résiduels Prouver/Témoigner son niveau de sécurité à des tiers
Quand	Tous les 2 ans environ
Tarif	900 € HT par jour

ASSI-INT : Audit de résistance aux intrusions internes

Ce type d'audit sert à évaluer la résistance de votre réseau face à une menace s'étant déjà introduite à l'intérieur : un maliciel ayant contourné l'antivirus, un employé déloyal, une personne s'introduisant physiquement dans les bâtiments, etc.

Généralement, cet d'audit est mené à minima en "greybox" : l'auditeur dispose d'un compte utilisateur valide, sans privilèges particuliers. Compte tenu de l'écrasante proportion des attaques réussies, qui ont démarré par un courriel de hameçonnage, le cas où un poste de travail (et l'utilisateur associé) devient hostile est LE scénario principal à couvrir.
Il est également fréquent de mener une partie de l'audit en "whitebox" : un compte administrateur du domaine est fourni pour mener certains tests automatisés (vérification des correctifs de sécurité, des configurations, ...) en parallèle des tests manuels qui ne peuvent être exhaustifs.

Bien qu'il existe des référentiels généraux sur la conduite de l'audit d'un point de vue organisationnel (ISO 19011, PASSI, etc.), la recherche technique des vulnérabilités ne dispose pas encore d'un standard établi

(comme c'est le cas pour la sécurité Web avec l'OWASP par exemple). Astar utilise donc une méthodologie développée en interne, publique, transparente et collaborative : OCNSP.

Pour qui	Les entreprises qui ont déjà mis en place un socle de protections minimales dans leur réseau interne
Pour quoi	Estimer l'étendue des impacts quand les protections périmétriques sont contournées (VPN compromis, maliciel qui contourne l'antivirus, hameçonnage, ...) Prouver/Témoigner son niveau de sécurité à des tiers
Quand	Tous les 2 ans environ
Tarif	900 € HT par jour

ASSI-MOB : Audit d'application mobile

L'audit d'applications mobiles Android et iOS évalue les risques de compromission par les menaces suivantes :

Une application mobile malveillante, installée sur le même appareil, qui tenterait d'exfiltrer les données des autres applications
Un adversaire ayant dérobé l'appareil sur lequel est installé l'application et qui tenterait d'en extirper des informations réutilisables
Un adversaire pouvant écouter les communications entre l'application et une ressource tierce (objet connecté, serveurs du propriétaire de l'application, ...)
etc.
Ce type d'audit doit être réalisée à l'aide d'un jeu de données représentatives si l'auditeur ne peut les créer lui-même (par exemple si l'application se synchronise à un objet connecté qui n'est pas fourni).

L'audit d'application mobile repose sur le standard MAS (Mobile Application Security) de l'OWASP, qui fournit à la fois les exigences attendues d'une application sécurisée et les moyens de les tester.

Selon que les applications iOS et Android sont développées depuis un code unique, exporté aux deux formats, ou bien indépendamment l'une de l'autre, le degré de mutualisation des tests est variable.

Pour qui	Les entreprises qui développent une application mobile.
Pour quoi	Connaître les risques de compromission de données et d'actions illégitimes depuis un environnement mobile hostile (applications espionne sur le même appareil, appareil volé, ...). Prouver/Témoigner son niveau de sécurité à des tiers
Quand	Tous les 2 ans environ
Tarif	900 € HT par jour

ASSI-IOT : Audit d'objet connecté (IoT)

L'audit d'objets connectés évalue les risques vis-à-vis des menaces suivantes :

Rétro-ingénierie permettant à un concurrent de copier la technologie

Altération du comportement de l'appareil pouvant menacer l'utilisateur
Extraction de données sensibles (données personnelles de l'utilisateur, secret codé en dur et réutilisable contre d'autres dispositifs, ...)
Pour cela, l'audit recours à des attaques électroniques (Uart, Vcan, Mcan, ...), protocolaires (bluetooth, radio fréquence, etc.) ou informatique bas niveau (firmware).

Les critères d'audit se basent essentiellement sur les standards ISO 30141 (Architecture de référence de l'Internet des objets), ETSI 303 645 et au guide l'ANSSI (Recommandations de sécurité pour un système d'objets connectés).

Généralement, ce type d'audit est mené en boite grise ou blanche. C'est-à-dire que l'auditeur dispose d'une description globale du produit et de schémas généraux, fournis par le client, de sorte à pouvoir trouver en quelques jours des erreurs qu'un adversaire mettrait potentiellement des semaines à détecter à l'aveugle.
En conditions idéales, nous demandons deux dispositifs car l'un d'entre eux sera démonté et inutilisable (soudure sur les connecteurs, ...).

Pour qui	Les entreprises qui développent ou utilisent un objet connecté
Pour quoi	Connaître les risques de compromission de données et d'actions illégitimes depuis un environnement hostile (client curieux, concurrent, hacker, appareil volé, ...). Prouver/Témoigner son niveau de sécurité à des tiers
Quand	À chaque modification majeure du matériel ou du firmware
Tarif	900 € HT par jour

ASSI-AUT : Audit d'automates et de systèmes industriels (OT : ICS - SCADA)

L'audit de systèmes industriels concerne les infrastructures critiques de production (chaîne d'assemblage, bras robotisés, ...).

Par nature, ces cibles sont difficiles à auditer. D'une part, elles sont souvent basées sur des technologies propriétaires, vétustes et mal documentées et peuvent donc réagir de manière imprévue lors des audits. D'autre part, comme ces équipements sont coûteux, il n'y a généralement pas d'environnement de pré-production ou de test, sur lesquels mener l'audit.
Pour ces raisons, les audits de systèmes industriels se font de manière très encadrée avec une connaissance initiale maximale de l'auditeur (présentation de l'architecture, des schémas, description des fonctions, ...).

Un des thème prépondérant de ces audits est l'isolation : physique et vis-à-vis des autres réseaux.
En effet, la correction des vulnérabilités des automates n'est généralement pas réalisable par le client lui-même, il doit effectuer une demande au fournisseur (sans maîtrise sur le délai de réponse). On considère donc que la priorité numéro 1 d'un système industriel est d'être étanche vis-à-vis des menaces.

Les standards communément utilisés sont le guide de l'ANSSI et le modèle Purdue.

Pour qui	Les entreprises qui développent ou utilisent des automates
Pour quoi	Connaître les risques de rupture et de faute de la production. Prouver/Témoigner son niveau de sécurité à des tiers

Quand	À chaque modification majeure du matériel ou du firmware
Tarif	900 € HT par jour

ASSI-COD : Audit de code

L'audit de code est le type d'évaluation de sécurité le plus poussé.
Il consiste en l'analyse de tout ou partie du code source, ou des conditions de compilation d'une application, dans le but d'y découvrir des vulnérabilités, liées à de mauvaises pratiques de programmation ou des erreurs de logique.
Il est parfois considéré comme la version "whitebox" d'un audit de vulnérabilité applicatif : l'auditeur dispose de la connaissance maximale du système. Ce type d'approche permet donc d'obtenir un haut niveau de confiance dans l'exhaustivité des résultats.
Un audit de code permet d'identifier, en quelques jours, des vulnérabilités qui seraient très difficiles à découvrir "à l'aveugle".

Ce type de prestation est pertinent lorsque votre activité est fortement basée sur la vente d'une solution logicielle (application mobile ou Web, client lourd). Dans ce cas, une vulnérabilité qui affecterait votre produit pourrait être utilisée contre tous vos clients (vous seriez la cause de leur incident de sécurité) et vous subiriez un choc en image de marque.
L'audit de code vous donne deux avantages face à ce risque :

- Vous avez les meilleures chances de détecter une vulnérabilité avant un pirate
- Dans le cas contraire, vous pouvez attester que vous avez employé les meilleurs moyens de l'état de l'art pour prévenir ce cas (donc on ne peut vous reprocher aucune négligence)

La réalisation d'un audit de code consiste à vérifier que les principes de secure coding sont bien respectés par la cible.
Ces principes sont précisément définis dans le référentiel de l'OWASP Secure Coding Practices. La méthodologie pour tester le respect de ces principes est également documentée par l'OWASP dans son référentiel Application Security Verification Standard (ASVS) . Trois niveaux d'exigence y sont définis selon la criticité de l'application cible.

Historiquement, l'audit de code concerne les "applications" : clients lourds, sites Web, applications mobiles. De nos jours, il peut s'étendre à de nouveaux sujets puisque le "code" s'immisce dans toujours plus de pans de l'informatique (Infrastructure as Code, DevOps, …). Pour ces cas-là, l'approche sera souvent hybride entre l'audit de code et l'audit de configuration (voir ci-après).

Pour qui	Pour les entreprises éditrices de solutions logicielles (progiciel, application mobile, ...)
Pour quoi	Prouver aux clients que les produits vendus sont sûrs
Quand	Avant la release d'une version majeure
Tarif	900 € HT par jour

ASSI-CNF : Audit de configuration

L'audit de configuration vise à établir la conformité du paramétrage d'une cible (un système d'exploitation, un logiciel, une application mobile, un équipement réseau, un site Web, …) avec un référentiel d'exigences de sécurité donné.

Ces référentiels peuvent être :

- CIS
- OWASP
- PCI DSS
- RGS de l'ANSSI
- NIST Security and Privacy Controls
- NIST Cybersecurity Framework
- ISO 270001
- RGPD
- …

Ce type de prestation est utile lorsque vous devez témoigner d'un niveau de conformité pour l'un de vos produits (un "tampon" à montrer à vos clients) ou bien si vous voulez valider la sécurité d'un élément qui sera largement déployé dans votre SI (un master Windows par exemple).

Pour qui	Des PME aux grandes entreprises
Pour quoi	Assurer la conformité d'un élément du SI avec l'état de l'art
Quand	Avant le déploiement d'un nouveau composant
Tarif	900 € HT par jour

ASSI-ARC : Audit d'architecture

L'audit d'architecture est une prestation visant à évaluer la nature, le choix, le positionnement et la mise en oeuvre des éléments d'un système d'information (généralement un réseau.), du point de vue de la sécurité. Là où l'audit de configuration s'intéresse au fonctionnement interne des machines, l'audit d'architecture étudie la sécurité des interactions entre toutes ces machines. L'audit de configuration peut être vu comme l'analyse microscopique et l'audit d'architecture comme l'analyse macroscopique.

L'audit d'architecture comprend généralement les étapes suivantes :

- Analyse des documentations, plans et schémas d'architecture du système d'information
- Contrôle de leur exactitude via des tests techniques
- Critique de l'agencement, de la nature et du dimensionnement des différentes briques du système d'information
- Propositions de corrections/améliorations
- Conseils sur les perspectives d'évolution

L'audit d'architecture est pertinent lors de l'initialisation de projets d'urbanisation du SI.
En effet, il est fortement recommandé de faire valider l'aspect "sécurité" d'une évolution d'architecture du SI, **avant** de la mettre en place. Toute modification à posteriori est souvent plus couteuse.

Avec le développement du DevOps, la frontière entre audit de configuration et audit d'architecture tend à s'effacer. Les prestations qui visent à valider une architecture Cloud, par exemple, combinent

généralement les deux approches (puisque les éléments du SI sont déployés via des fichiers de configuration).

Pour qui	Des PME aux grandes entreprises
Pour quoi	Assurer la conformité de l'organisation d'un Système d'Information avec l'état de l'art
Quand	Avant la validation d'une nouvelle architecture (ou de son évolution)
Tarif	900 € HT par jour

ASSI-PHY : Audit physique

L'audit de sécurité physique met à l'épreuve la première barrière de sécurité de votre SI : la protection périmétrique.
Il n'est pas rare que ce domaine soit négligé, particulièrement lorsqu'une entreprise possède plusieurs sites géographiques et/ou qu'elle accueille beaucoup de public.
Or, même si vos serveurs sont complétement à jour de leur correctifs de sécurité, que les mots de passe sont bons et que le réseau est bien segmenté … s'il est possible de partir avec un serveur sous le bras après être entré par la zone de livraison … vous avez quand même un problème.

L'audit de sécurité physique teste les voies d'accès physiques au SI de l'entreprise :
Entrée non surveillée

- Porte de secours laissée ouverte
- Absence de contrôle d'accès par badge (ou bien une porte sécurisée qui se ferme trop lentement permettant de se faufiler derrière un employé)
- Machines sensibles exposées (baie avec la clé sur la serrure, …)
- Wifi vulnérable
- Fouille des poubelles à la recherche d'informations sensibles
- Accès à des câbles du réseau depuis des parties publiques
- Mots de passe inscrits sur des post-it
- Informations sensibles visibles depuis les fenêtres
- Cartographie des locaux par images satellites et par drone
- Badges facilement imitables
- Possibilité d'obtenir des informations sensibles en écoutant les conversations des employés lors de leur pause déjeuner
- …

Cette catégorie de moyens d'infiltration est généralement utilisée lors des tests d'intrusion (voir plus haut). Néanmoins ceux-ci se contentent de trouver **UN SEUL** moyen d'accès physique qui leur permettra de s'attaquer à des vulnérabilités informatiques (vulnérabilités que l'on nomme "logiques" en opposition à "physiques").
L'audit purement physique, quant à lui, tente d'identifier exhaustivement toutes les vulnérabilités périmétriques.

Pour qui	Les entreprises qui habritent des données sensibles (secrets industriels, ...) ou bien qui possèdent plusieurs sites géographiques ou bien dont la taille implique que les

	employés ne se connaissent pas tous
Pour quoi	Connaître ses risques face aux menaces physiques (adversaire qui se rend sur place)
Quand	Tous les 4 ans environ
Tarif	900 € HT par jour

Les prestations décrites ci-après sont davantage conçues pour la récurrence (annuelle ou biennale) et s'inscrivent donc dans une démarche d'hygiène informatique et de contrôle continu de la sécurité.

ASSI-INC : Audit Incrémental

Si vous avez décidé d'intégrer pleinement les audits de sécurité aux processus courants de votre entreprise, l'audit incrémental est fait pour vous.
Il s'agit d'un audit de sécurité du système d'information (ASSI) conçu pour améliorer la sécurité de manière itérative.

Cet audit est :

- Récurrent : effectué chaque année avec un nombre de jours constant
- Continu : chaque année, les vulnérabilités de l'années précédente sont revérifiées pour valider leur correction
- Progressif : révérifier les vulnérabilités étant plus rapide que les découvrir, du temps est donc disponible pour en rechercher de nouvelles. Le périmètre couvert s'étend donc chaque année
- Orienté opérationnel : l'accent est mis sur la précision des informations nécessaires à la vérification et à la correction plutôt que sur la description de l'exploitation et des impacts
- Suivi : l'audit fournit des indicateurs managériaux d'aide à la décision (temps et compétences à allouer à la correction, efficacité des corrections passées, progression du périmètre couvert, progression du niveau de sécurité, etc…)
- Léger : un effort est porté sur le fait de diminuer autant que possible la charge administrative pour le client. Les informations sur le contexte sont donc enregistrées, d'une année sur l'autre, pour minimiser les échanges nécessaires au démarrage des tests.

L'avantage de cette approche est que vous gérez votre sécurité "par le budget". Chaque année vous allouez la même somme fixe à cet audit, mais votre niveau de sécurité, lui, augmente car l'audit couvre une partie de plus en plus étendue.

Pour qui	Les entreprises engagées dans un processus d'amélioration continue de leur sécurité
Pour quoi	Augmenter progressivement le périmètre de test tout en vérifiant les corrections passées. Prouver que l'on effectue des audits de sécurité régulièrement.
Quand	Tous les ans
Tarif	900 € HT par jour

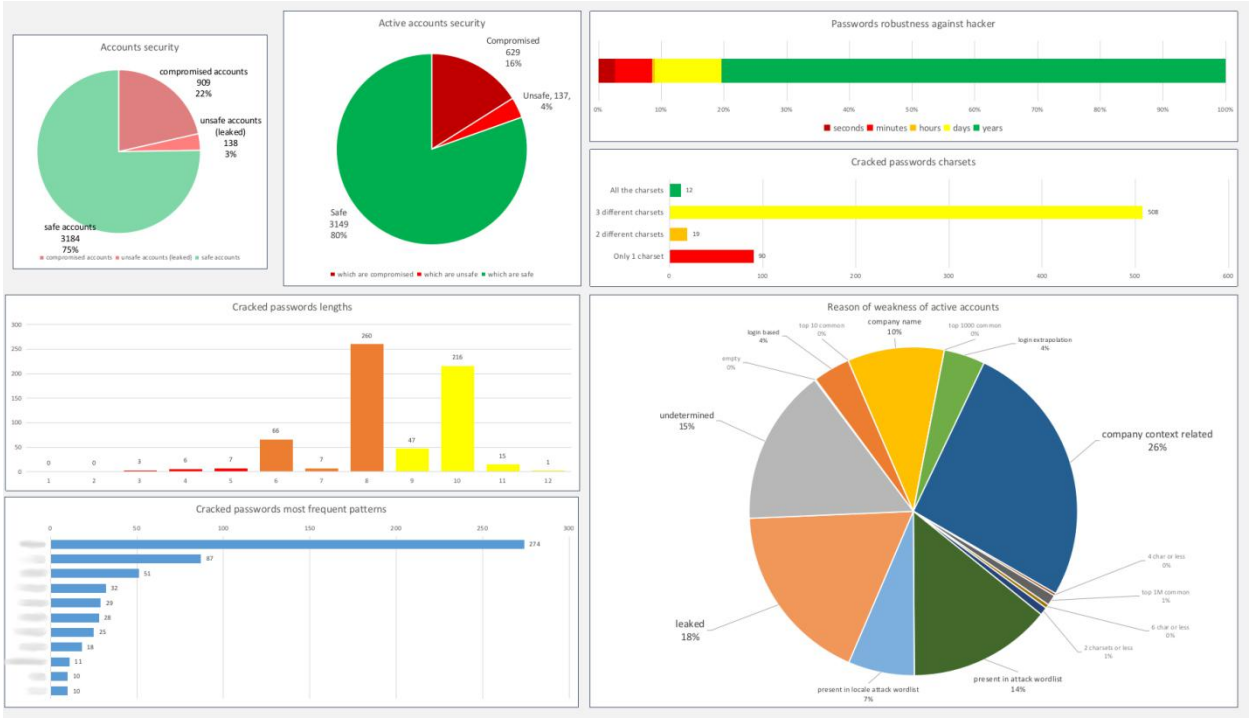
ASSI-PAS : Audit annuel des mots de passe

Il existe plusieurs moyens d'augmenter le niveau de robustesse des mots de passe de vos employés : forcer plusieurs jeux de caractères (minuscules, majuscules, chiffres, ponctuation), forcer une taille minimale, interdire d'utiliser certains mots (son propre nom, le nom de l'entreprise, …), former et sensibiliser les utilisateurs au choix d'un bon mot de passe, etc.
Mais malgré toutes ces dispositions, vous n'avez jamais la certitude que les employés n'ont pas utilisé un mot de passe prédictible (P@55word!, J34n-L0u!s, …). Les restrictions techniques seront toujours contournables.
C'est pourquoi une bonne politique de mot de passe ne se base pas uniquement sur les mesures préventives mais aussi sur les vérifications à posteriori.

Astar vous propose une vérification annuelle des mots de passe au prix forfaitaire de 1000 € HT.
Celle-ci comprend les vérifications suivantes :

- test des mots de passe courants internationaux et spécifiques à la langue du pays concerné
- test des mots de passe issus de fuites (data breach)
- test des mots de passe dérivés des noms d'utilisateur
- test des mots de passe dérivés des prénoms et dates de naissance
- test des mots de passe dérivés du nom de la société
- test des mots de passe dérivés des provenances géographiques (villes, départements, …)
- test par force brute
- test par dictionnaires avec dérivations (l33t, variations des majuscules, etc.)

Le résultat est présenté sous la forme d'un tableur et de graphiques qui restituent les comptes pouvant être compromis, à quelle vitesse (quelques secondes, quelques heures, quelques jours, …), leur criticité selon les groupes auxquels ils appartiennent, les raisons de leur faiblesse (mot de passe dérivé d'un prénom, du nom de l'entreprise, etc.).
Vous obtenez également des statistiques générales sur la campagne de vérification : pourcentage de comptes à risque, motifs les plus fréquemment utilisés dans les mots de passe, répartition des mots de passe compromis en nombre de caractères, etc.



Si vous contractualisez de manière régulière pour cette prestation, vous obtiendrez aussi le delta par rapport à l'année précédente.

Pour qui	Les entreprises qui ont un nombre conséquent d'employés (> 100)
Pour quoi	Vérifier qu'aucun compte ne puisse servir de porte d'entrée à un attaquant à cause de la faiblesse du mot de passe
Quand	Tous les 1 ou 2 ans
Tarif	Forfait 1 000 € HT

ASSI-SOC : StressTest SOC

Cette prestation vise à améliorer vos capacités de détection des attaques en les mettant à l'épreuve, pour repérer les scénarios qui passent encore au travers.

L'auditeur va mener plusieurs actions malveillantes (depuis Internet ou depuis l'intérieur du réseau) associées aux différentes catégories du référentiel ATT&CK du MITRE : reconnaissance, escalade de privilèges, mouvements latéraux, etc.
Pour chacune de ces catégories, il utilisera différents niveaux d'élaboration : des attaques bruyantes faciles à détecter jusqu'aux attaques très furtives.

Astar produit alors une matrice des tests menés qui fournit, pour chaque cas :

- les heures exactes de début et de fin (synchronisées avec le NTP interne)
- les lignes de commandes exactes (afin de permettre le rejeu)
- l'identifiant précis de la technique dans le référentiel ATT&CK (exemple: T1134)
- une capture des trames réseaux émises
- le degré d'élaboration du scénario
- la dangerosité du scénario
- son statut de détection (est-ce que le SIEM a reçu un événement, est-ce qu'une alerte a été émise, …)
- les logs pouvant permettre de le détecter
- etc.

Ceci vous permet de cartographier les étapes d'une attaque où vous êtes bien outillés et celles qui risquent de vous échapper. L'intérêt est de pouvoir prioriser les futurs ajouts de logs en faveur de ceux qui comblent vos angles morts.
Ceci permet également de tester la qualité de service de votre SOC si vous recourez à un prestataire externe (vitesse de compilation des événements en alertes, vitesse d'escalade, …).

Pour qui	Les entreprises qui disposent d'un SOC
Pour quoi	Répérer les angles morts dans les règles de détection, prioriser les futurs intégrations de logs, mesurer l'efficacité des règles et processus actuels (SLA, escalade, ...)
Quand	Tous les 2 ans environ
Tarif	900 € HT par jour

ASSI-DOS : StressTest Déni de Service

Si la disponibilité de vos services est un besoin crucial (salle de marché, datacenter, …), il est probable que vous ayez implémenté des mesures dédiées, dites de “haute disponibilité” : mise en cluster, PCA/PRA, fournisseur anti-DDOS, etc…
Le point faible de ces mesures est que, une fois mises en place, on est souvent réticent à les mettre à l’épreuve. En effet, tester ces dispositifs fait courir le risque d’une interruption en cas de défaut.

Cette réticence est en partie justifiée : pourquoi prendre un risque avéré d’interruption alors que vous serez probablement rarement attaqué sur ce terrain par les pirates ? D’un autre côté, il serait fâcheux de payer des mécanismes haute-disponibilité couteux si ceux-ci ne fournissent pas le service attendu (d’autant plus si vous vous en rendez-compte au cours d’une crise). Or il n’est pas si rare d’observer des mesures de haute disponibilité défaillantes car mal déployées.
Mieux vaut tester ses capacités lors d’un exercice contrôlé.

La prestation de StressTest DOS d’Astar propose de tester la résistance d’une infrastructure (interne ou externe) face à plusieurs types de menace :

- Saturation par le débit (depuis une puis plusieurs machines)
- Saturation logique (flood d’emails via un formulaire de contact, blocage des comptes par force brute, …)
- Saturation protocolaire (fuzzing des services provoquant des dysfonctionnements)
- Exploitation de configurations impropres (usurpation HSRP/VRRP, etc.)

Les attaques lancées sont progressives en termes de dangerosité et peuvent être stoppées en quelques secondes/minutes.

Pour qui	Les entreprises qui peuvent perdre des sommes importantes en cas d’interruption de quelques minutes ou dont le chiffre d’affaire est très concentré sur une courte période de l’année
Pour quoi	Valider l’efficacité des mécanismes de haute disponibilité mis en place
Quand	Tous les 2 ans environ
Tarif	900 € HT par jour

ASSI-EXP : Audit d’exposition numérique

Cet audit recherche et compile les informations de sources ouvertes (OSINT) utiles à un adversaire.

Les données recueillies peuvent concerner :

- Les noms de domaines et les adresses IP pouvant être associés à l’entreprise (serveur de test, de pré-production, accès VPN, ...)
- Les employés de l’entreprise pouvant être identifiés, les noms d’utilisateurs probables qui peuvent en être déduits et les éventuels moyens de vérifier si ces comptes sont valides
- Les adresses courriels pouvant être glanées depuis internet
- Les images satellites permettant de cartographier les sites géographiques de la société
- Les informations permettant de reconstituer l’organigramme interne
- Les fuites d’informations passées (“leak” ou “data breach”) exposant des données de l’entreprise

- L'existence de domaines clones malveillants (cdicsount.com au lieu de cdiscount.com, …)
- Les technologies utilisées en interne (via les offres d'emploi : "Cherche Expert MacAfee EPO" ou les rapports d'anciens stagiaires)
- etc …

Ce sujet est amené à devenir de plus en plus utile à mesure qu'une entreprise croît. En effet, au delà d'une certaine taille, il est rare que les équipes IT aient une connaissance de tout l'historique technique. Donc, des machines, que tout le monde a oubliées, peuvent rester en service et exposer inutilement le SI.

D'autre part, le "shadow IT" est un sujet d'autant plus récurrent que la taille de l'entreprise grandit. Sans compter l'éternel poncif : *"non mais personne ne la connait cette IP, y a pas de risque"*.

Or, toute attaque ciblée commence par une phase de collecte d'informations sur la cible. Les vecteurs d'attaque qui seront privilégiés par les attaquants peuvent être anticipés en effectuant préventivement cette recherche.

Ces considérations entrainent qu'il est conseillé de mettre à jour, à intervalle régulier, la connaissance de ce qui est exposé publiquement, pour récupérer la maîtrise de l'information.

Pour qui	Les entreprises de taille conséquente ou celles dont l'activité dépend fortement de secrets industriels ou de leur réputation
Pour quoi	Contrôler le niveau d'information que peut obtenir un adversaire sur un système d'information
Quand	Tous les 2 ans environ
Tarif	900 € HT par jour

Conseil & Assistance technique

CONS-STA : StartSec

Astar a conçu cette prestation spécialement pour les Start Up. Quand vous êtes une jeune entreprise qui démarre, vous n'avez pas encore de budget dédié à la cybersécurité (car vous n'avez pas encore réellement d'activité à protéger).
La considération de la sécurité informatique est souvent repoussée à un futur où la croissance sera florissante et les marges confortables.
Mais ce sujet peut vous rattraper à tout instant, que ce soit à cause d'une attaque subie qui paralyse votre activité ou d'un client qui exige des garanties de sécurité pour contractualiser avec vous.
Dans ces cas, vous risquez d'être démuni et de devoir allouer rapidement des crédits sans avoir pu établir, en amont, une réflexion sur une stratégie globale.
Vous risquez alors de vous faire piéger par le marketing très (trop) agressif du secteur et de surinvestir dans des outils qui prétendent régler tous les problèmes ou de vous tourner vers un audit de sécurité.
Ces deux solutions sont souvent peu utiles à votre échelle. D'une part, aucun outil ne résout tous les problèmes. D'autre part, les rapports d'audit, d'entreprises qui débutent en sécurité, se ressemblent tous.

Pour vous éviter des dépenses superflues, nous avons conçu l'offre StartSec.
Il s'agit d'une prestation forfaitaire, la prestation la moins chère de notre catalogue. Il s'agit d'une journée de conseil sous la forme d'interviews et d'échanges libres :

- Astar vous posera plusieurs séries de questions pour définir votre profil d'entreprise
  - Sur quoi repose votre valeur (secrets industriels, image, rapidité d'exécution des tâches, ...)
  - Quelles sont vos menaces (pirates, concurrents, erreur interne, ...)
  - Quelle est votre tolérance aux attaques (facilité à reprendre l'activité, impacts à long terme, ...)
  - Etc...
- Vous pourrez poser toutes les questions que vous avez concernant la cybersécurité, à tout moment, dans l'ordre que vous voulez
- Astar produira ensuite une feuille de route détaillant la chronologie des sujets dont vous devez vous saisir pour les années à venir.
- Le rapport contiendra également le détail des échanges et les réponses aux questions

L'idée générale est, en quelque sorte, de disposer d'un expert en cybersécurité "as a Service", pour une journée, qui serve "d'oracle" (il répond à toutes vos questions).

Il ne s'agit pas de vous dire *"investissez tant dans tel produit"*, mais plutôt : *"quand vous aurez tant de budget à allouer à la sécurité, la meilleure façon de le dépenser sera ceci"*.
Ce qui importe c'est que vous investissiez vos ressources dans les démarches les plus **rentables** et, surtout, dans le bon ordre.
Se tromper de priorité est en effet un écueil classique des jeunes entreprises : investir dans un antivirus cher est bien moins prioritaire que de disposer d'une solution de sauvegarde performante. Investir dans un pare-feu *top tier* est bien moins prioritaire que de disposer d'un coffre-fort de mots de passe. Etc...

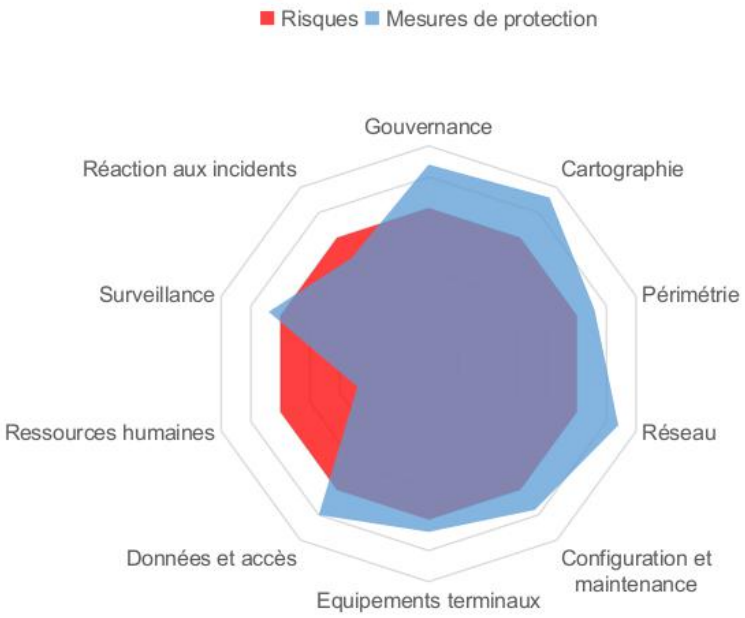
Pour qui	Les entreprises qui commencent seulement à aborder le sujet de la cybersécurité
Pour quoi	Penser sa sécurité en amont, pour suivre une feuille de route cohérente et économe
Quand	Avant d'engager vos premiers budgets en cybersécurité
Tarif	Forfait 1 000€ HT

CONS-GRC : Audit GRC

L'audit GRC (Gouvernance Risque Conformité) n'évalue pas directement votre niveau de sécurité mais plutôt les moyens que vous vous êtes donnés, pour atteindre un niveau de sécurité bien dimensionné.

L'audit est mené via des interviews des décideurs de l'entreprise et des responsables techniques, puis complété par des vérifications *in situ*. Cet audit se déroule en 3 étapes :

- Estimer votre niveau de risque "brut" (le risque inhérent, sans tenir compte des mesures de protection en place)
- Lister vos mesures de protection en place par rapport à l'état de l'art
- En déduire votre risque "net" : les domaines où vos protections sont sous-dimensionnées



L'objectif n'est pas d'implémenter toutes les mesures de sécurité de la Terre et d'avoir le niveau de sécurité de la NASA (802.1X, authentification par carte à puce, double bastion, etc.) mais d'être bien **dimensionné** face au risque inhérent.

Le rapport d'audit propose donc une liste de mesures pour combler vos faiblesses, qui dépendent de votre risque brut (les mesures ne seront pas aussi poussées si vous êtes une banque ou si vous êtes une boulangerie).

Ce type d'audit est une étape indispensable lorsque la taille de votre entreprise croit. En effet, il est quasiment impossible d'obtenir un niveau de sécurité qui progresse, au delà d'un certain nombre d'employés et de services, si vous n'avez pas une gouvernance et des procédures qui encadrent ce thème.
Les entreprises qui n'ont pas assez investi en GRC se reconnaissent au fait que les audits de vulnérabilités remontent les mêmes causes d'une année sur l'autre. Empêcher que les mêmes vulnérabilités se reproduisent, en agissant sur les causes, est le vrai signe d'une maturité en sécurité de l'information.

Pour qui	Les TPE/PME qui ont déjà mis en place certaines mesures de sécurité
Pour quoi	Connaître ses forces et dresser un plan d'action pour combler ses faiblesses
Quand	Avant de mener des audits de sécurité techniques
Tarif	Forfait 2 500 € HT

CONS-SDS : Schéma Directeur de la Sécurité

Le Schéma Directeur de la Sécurité (SDS) est la version évoluée de l'offre StartSec.

Un SDS est un document stratégique qui établit une vision globale de la sécurité informatique de l'organisation à moyen et long terme.
Contrairement au plan de sécurisation qui se concentre sur les détails opérationnels, le schéma directeur de la sécurité prend une approche plus holistique et s'intéresse aux aspects stratégiques de la sécurité informatique.
Il aborde les points suivants :

- L'alignement de la sécurité informatique avec les objectifs métier de l'organisation.
- L'évaluation des risques informatiques et la définition d'une stratégie globale de gestion des risques.
- L'identification des besoins en matière de sécurité à long terme et la planification des investissements nécessaires.
- La définition des orientations technologiques en matière de sécurité.
- L'établissement de politiques de sécurité globales et la mise en place de processus de gouvernance de la sécurité.

Pour qui	Les entreprises établies qui se lancent dans l'intégration explicite de la cybersécurité au sein de leur structure.
Pour quoi	Penser sa sécurité en amont, pour suivre une feuille de route cohérente et économe
Quand	Avant d'engager vos premiers budgets en cybersécurité
Tarif	Forfait 5 000€ HT

COND-PDS : Analyse des risques et Plan de sécurité

Un plan de sécurité est une forme plus mature et systématique de ce que propose la prestation d'Audit GRC.
L'objectif est de vous fournir une définition précise de vos risques (réutilisable pour toutes les prestations en sécurité que vous contractualiserez dans le futur) et un plan d'action pour les 4 prochaines années.

Cette prestation combine des interviews, des questionnaires et des vérifications techniques.
La démarche générale est la suivante :

- Identifier les **actifs primordiaux** de l'entreprise (au sens de l'ISO 27005)
- Cartographier les **actifs supports** associés
- Qualifier les **sources de menace** pertinentes (menaces naturelles/technologiques/humaines, intentionnelles et accidentelles, internes et externes, etc.)
- Etablir les **scénarios de menace** (source de menace -> type d'atteinte -> actif support) et leur fréquence
- Analyser les **impacts** en confidentialité, intégrité et disponibilité sur les actifs primordiaux
- Établir les **événement redoutés** (type d'atteinte -> impact -> actif primordial)
- Faire la liaison entre les scénarios de menace retenus et les événements redoutés pour déterminer les **risques**
- Déduire les **mesures de sécurité** nécessaires pour être dimensionné face à ces risques
- Comparer avec les mesures de sécurité actuellement en place, identifier les points faibles

- Proposer un plan d'action à court, moyen et long terme pour implémenter les mesures de sécurité manquantes

Cette prestation incorpore donc une analyse de risque. La méthode d'appréciation du risque utilisé par Astar repose sur les méthodes EBIOS et FAIR en y ajoutant le savoir-faire issu de notre expérience.

Ce type d'approche peut être vulgarisé par un exemple : *Si l'on établit que le scénario "un hacker compromet mon site Web via un vulnérabilité publique non corrigée" a, chez vous, une fréquence de 1 fois tous les 6 ans. Et que l'impact d'une telle compromission est estimé à 30 000 € (agrégation de la dégradation d'image de marque, des jours/homme pour décontaminer et restaurer, du manque à gagner, etc.). Alors si une mesure de sécurité réduit cette fréquence à presque 0 et coûte moins de 5 000 € par an => elle vaut le coup.*

Cette prestation vous offre également plusieurs pistes d'implémentation de la cybersécurité selon la direction dans laquelle vous voulez faire évoluer votre entreprise.
Les recommandations ne seront pas les mêmes si vous êtes dans une démarche de tout externaliser en Cloud ou inversement de tout gérer de manière souveraine. Elles varieront selon plusieurs autres critères : le nomadisme des employés, les nombre de sites physiques, le type de données amenées à être traitées dans le futur, etc.

Pour qui	Les PME/ETI/Grandes entreprises qui ont déjà mis en place certaines mesures de sécurité
Pour quoi	Disposer d'un socle qui puisse servir de prisme à tous les choix futurs en cybersécurité et d'une feuille de route pour les 4 prochaines années.
Quand	Au moment d'entamer une étape importante dans la croissance de l'entreprise
Tarif	900€ HT par jour

CONS-ORG : Audit organisationnel

La sécurité organisationnelle comprend de nombreuses sous-parties :

- L'organisation des rôles et responsabilités en cybersécurité dans l'entreprise
- L'analyse des risques (pour estimer les besoins de sécurité de l'entreprise)
- L'inventaire des mesures de sécurité en place (pour savoir si elles sont dimensionnées face aux besoins de sécurité identifiés)
- Les procédures d'exploitation du SI (mises à jour, recette, entrée d'un utilisateur, etc…)
- Les procédures de réponse à incident
- Les procédures et moyens de PCA (Plan de Continuité d'Activité) et de PRA (Plan de Reprise d'Activité)
- Les moyens de contrôle (indicateurs, mesures) du niveau de sécurité actuel
- Etc...

Chacun de ces points est généralement traité par une prestation à part entière, tant il serait volumineux de tout mener d'un seul coup.
Lorsque les points les plus importants ont été abordés, l'entreprise peut ébaucher une PSSI (Politique de Sécurité du Système d'Information).
Finalement, lorsque l'entreprise est entrée dans un processus d'enrichissement continu de cette PSSI, elle peut prétendre disposer d'un Système de Management de la Sécurité de l'Information (SMSI) sommaire et se lancer dans une procédure d'habilitation à l'ISO 270001 (qui est la principale norme de sécurité organisationnelle à laquelle vous voudrez vous conformer).

L'audit ou le conseil, en sécurité organisationnelle, interviennent à chaque étape de cette croissance vers la maturité : réaliser une analyse de risque, conseiller lors de l'élaboration de certains processus, effectuer des revues documentaires des politiques majeures, rédiger des procédures spécifiques, etc.

Pour qui	Les entreprises engagées dans des démarches de certification de leur sécurité
Pour quoi	Décrocher de nouveaux marchés, rassurer des clients, etc...
Quand	Lorsqu'un sujet nécessite ponctuellement un point de vue d'expert extérieur
Tarif	900€ HT par jour

CONS-AMO : Assistance technique

La mise en place ou l'amélioration de mesures de sécurité peut être une tâche délicate. Il arrive notamment qu'il soit nécessaire de mobiliser des compétences en cybersécurité qu'on ne possède pas parmi son personnel et qui n'auraient pas vocation à être internalisées de manière pérenne.

Dans ces cas-là, il est pertinent de recourir à une assistance technique (AMOA, AMOE) ponctuelle de quelques jours/semaines. Astar peut détacher des ingénieurs chez ses clients pour les accompagner dans la résolution des problèmes (revue des permissions, recherche des machines obsolètes, sécurisation d'une interface Web, …) ou la mise en place d'améliorations (déploiement d'un SIEM, d'un scanner de vulnérabilités, d'un outil de cartographie du SI, …).

Ce type de prestation est facturé à la demi-journée. Astar proposera un nombre de jours pertinent et le client ne paiera que les demi-journées effectivement consommées. Le client n'a pas besoin de s'engager sur un nombre de jours minimal et il peut décider à tout moment de la fin de l'assistance technique, sans préavis.

Pour qui	Les entreprises qui ont un besoin ponctuel de compétences en cybersécurité
Pour quoi	Régler des problèmes pointus sans avoir à internaliser les compétences
Quand	Après un audit pour aider à la mise en place des mesures principales
Tarif	450€ HT par demi-journée

Formations & Sensibilisations

SENS-SUA : Sensibilisation à la cybersécurité pour les StartUp et associations

Vous êtes un incubateur de StartUp, une pépinière ou un consortium d'entreprises, et vous souhaitez leur proposer une demi-journée d'animation sur le thème de la cybersécurité. Cette sensibilisation est pensée pour vous.

Astar s'engage, à son niveau, pour la protection du potentiel scientifique et technique (PPST) de la nation. Nous proposons de conseiller les jeunes entreprises innovantes pour qu'elles puissent développer tout leur potentiel en évitant l'écueil des cybermenaces (qui peut freiner, voire stopper, leur progression). C'est pour cela que cette sensibilisation est dispensée gratuitement.
Cette sensibilisation s'adresse aussi à vous si vous êtes une association à but non lucratif.

L'intitulé exact de la formation est : Approche rationnelle de la Cybersécurité
Le plan est le suivant:

- Pourquoi s'occuper de cybersécurité (*ne pas couler, décrocher des marchés, faire des économies*)
- Comment aborder la sécurité (*notions de risque, menace, vulnérabilité, traitement, dimensionnement*)
- Concepts clés de la sécurité (*défense en profondeur, notion de confiance, protection des données*)
- Conseils et ressources (*quick win, quelques bribes de sagesse, bonnes adresses*)

Pour qui	Les pépinières de Start-Up, les incubateurs, les associations, les forums, les salons professionnels, ...
Pour quoi	Sensibiliser les jeunes entreprises aux bases de la cybersécurité pour qu'elles évitent les écueils les plus évidents
Quand	Avant leur phase de "Go To Market" si possible
Tarif	GRATUIT

SENS-ADO : Sensibilisation aux risques numériques pour les adolescents

Les actuels collégiens, lycéens et étudiants sont à un carrefour générationnel : ils sont exposés à des risques que leurs parents et professeurs n'ont pas connus lorsqu'ils avaient le même âge. Et ils ne peuvent qu'imparfaitement les y préparer.

Que vous soyez un lycée, un collège, une MJC, ou toute autre structure qui accueille des adolescents, Astar peut animer une séance de sensibilisation de 2 heures ou d'une demi-journée, sur un ton informel, qui explique et éduque à propos des principaux risques numériques qui concernent la jeunesse :

- Qu'est-ce qu'un risque (*ne pas considérer un événement seulement d'après sa probabilité*)
- Internet n'oublie pas ! (*une vidéo publiée quand vous êtes ado peut vous suivre toute votre vie, les messages "éphémères" sont une illusion*)
- Le piratage peut tuer (*exemple d'Ashley Madison*)
- L'intimité en 2021 (*exemple du celebgate, des deepfake, de la "sextorsion"*)
- La vie privée (ce *qui la menace : affaire Snowden, risque des metadonnées, ... Ce qui la protège: RGPD, ...*)
- Comment les pirates nous hackent (*téléchargement illégal, "malvertising", mot de passe réutilisés, ingénierie sociale, ...*)

- Recommandations (*communiquer de manière sécurisée, choisir un mot de passe, considérations sur le matériels et les logiciels, bonnes adresses*)

Pour qui	Les collèges, lycées, MJC, Universités, les structures qui accueillent des adolescents
Pour quoi	Préparer les jeunes générations aux risques actuels et futurs qui entourent leur utilisation du numérique
Quand	Du collège à l'Université
Tarif	GRATUIT

SENS-PER : Sensibilisation du personnel au risque informatique

Aucun système informatique n'est actuellement assez perfectionné pour s'offrir le luxe de ne pas sensibiliser l'utilisateur humain à son bon usage.
Vous pouvez avoir le pare-feu le plus cher du marché, les switches Cisco les plus sophistiqués, un IPS Top Tier, si Thierry de la compta utilise le mot de passe Thierry2019!... vous avez gaspillé votre argent.

Une règle importante en sécurité informatique est que votre niveau général est égal à l'élément le plus faible de votre structure. Donc si vous laissez de côté la sensibilisation de vos utilisateurs, tout ce que vous dépensez dans d'autres chantiers est en partie gâché.
Or l'humain est aussi l'élément le plus ciblé par les pirates. La plupart des attaques informatiques d'envergure, qui font la une des médias, ont commencé par un courriel de hameçonnage.

Sensibiliser correctement ses employés aux risques informatiques et aux bonnes pratiques n'est pas trivial. C'est pourquoi Astar vous propose d'intervenir pour animer des ateliers de sensibilisation.

Les sujets abordés sont, entre autres:

- Comprendre pourquoi les pirates attaquent
  Il n'y a pas besoin d'être une banque pour intéresser les pirates, présentation de comment les pirates font leur business: botnet, minage de crypto-monnaies, revente de données personnelles, etc.
- Comprendre comment les pirates attaquent
  Vulgarisation des concepts de faille informatique, virus, trojan, phishing, ... Explication des ressorts cognitifs utilisés contre eux lors du Social Engineering, etc.
- Le choix d'un mot de passe
  Combiner la robustesse et la faculté de s'en souvenir pour ne pas l'inscrire sur un post-it, utiliser des gestionnaires de mots de passe, ...
- La sécurisation de sa session
  Démonstration en live de tout ce qu'un pirate peut extraire en 10 secondes d'une session non verrouillée: mots de passe enregistrés dans le navigateur, clés Wifi, etc.
- La vigilance physique
  Démonstration en live d'une prise de contrôle à distance d'un poste où l'on connecte une clé vérolée, ne pas tenir la porte à un inconnu lorsqu'elle nécessite un badge, ne pas laisser un externe seul dans les locaux, ne pas brancher son smartphone personnel, ...
- Etc...

Pour qui	Les employés de votre entreprise, en particulier s'ils interagissent avec l'extérieur (comptabilité, commerce, standard téléphonique, accueil, ...)

Pour quoi	Leur inculquer une culture de la sécurité afin qu'ils soient davantage des alliés actifs de la sécurité de l'entreprise plutôt que des sources de menace
Quand	Tous les deux ans environ
Tarif	1 jour - 1200€ HT par tranche de 20 personnes

SIMU-CRI : Exercice de crise cyber

L'exercice de crise cyber est une mise en situation permettant d'entraîner vos équipes aux bonnes réactions en cas de sinistre subi dans le système d'information.

En effet, sous le coup du stress, il est souvent difficile de prendre toutes les bonnes décisions et seulement les bonnes décisions. Avoir déjà rencontré une telle situation, via un exercice contrôlé, a plusieurs vertus :

- Rendre ce type d'événement plus familier, et donc moins stressant, ce qui augmentera vos facultés cognitives en cas d'incident réel ;
- Avoir pu déterminer, à froid, les meilleurs décisions à prendre, préventivement à un incident réel ;
- Réduire le nombre de décisions à prendre "à chaud" aux seules particularités d'un incident.

Selon votre niveau de maturité, l'exercice est plus ou moins immersif.
Pour les premiers exercices, il est conseillé d'opter pour un examen sur table. L'objectif est alors que chaque acteur important d'une gestion de crise se soit déjà retrouvé, à tête reposé, face à plusieurs scénarios d'incidents et qu'il ait pris le temps de réfléchir aux meilleures réponses.
De plus, ils auront bénéficié de la correction de leurs réponses. En cas de crise réelle, ils pâtiront donc moins du stress d'être face à une situation inédite et pourront mobiliser leurs souvenirs plutôt que de devoir tout inventer sur place.
Cependant, lors d'une crise réelle, l'urgence et le stress paralysent en partie l'accès de notre cerveau aux souvenirs et aux décisions rationnelles. C'est pourquoi les exercices de crise cyber ont un deuxième niveau d'immersion : la simulation réaliste : salle de gestion de crise, coups de téléphone ou courriels du personnel, de la presse, des clients, ... Tout est fait pour reproduire des conditions stressantes et voir si vous parvenez toujours à prendre les meilleures décisions.
Le stress d'un événement vécu pour la deuxième fois n'est jamais aussi intense et vous ne pourrez donc que faire mieux en cas de crise réelle.

Pour qui	Les entreprises dont l'activité est fortement dépendante du système d'information
Pour quoi	Préparer les acteurs qui devront gérer les crises futures pour que ces situations leurs soient en partie familière et qu'ils puissent mobiliser des bons réflexes.
Quand	Tous les deux ans environ
Tarif	Dépend du contexte, du nombre de services et du niveau de simulation - 900 € HT / jour

SENS-PHI : Campagne de phishing

Une campagne de hameçonnage ("phishing") est un moyen de sensibiliser vos employés aux risques d'ouvrir un courriel malveillant.

Bien que les attaques visant les équipements périmétriques (VPN, load balancer, Firewall, …) aient explosé depuis la généralisation du télétravail, le vecteur d'intrusion n°1 demeure le courriel de hameçonnage.
Il peut revêtir plusieurs formes: une pièce jointe vérolée, un lien vers un site contrefait pour voler des identifiants, une usurpation d'identité pour faire accomplir une action sensible (arnaque au président) ou obtenir une information de valeur, etc.
Il s'adapte à l'actualité et innove toujours pour être plus difficile à détecter : imitation de message de subventions COVID, utilisation d'extensions de fichier non connues pour être dangereuses, etc.

Maintenir à jour la vigilance de vos employés peut drastiquement diminuer la fréquence à laquelle vous subirez un sinistre informatique.
Les campagnes de phishing proposées par Astar répondent à ce besoin.

Astar vous présentera plusieurs scénarios de phishing crédibles (issus de cas réels), avec des niveaux de sophistication différents et vous sélectionnez celui qui vous semble le plus adapté.
Les courriels piégés sont envoyés à vos employés puis vous recevez les statistiques du nombre de personnes dupées ou sauves.
Astar fournit aussi des éléments de sensibilisation à communiquer aux employés : les règles générales mais aussi les indices qui étaient présents dans le test qu'ils ont reçu.

Mener de telles campagnes renforce la vigilance de deux façons. Directement : les employés auront été entraînés à détecter des messages frauduleux. Et indirectement : le fait de savoir que la direction mène régulièrement de tels exercices les poussent à questionner les emails de manière plus systématique.

Pour qui	Des PME aux grandes entreprises
Pour quoi	Augmenter la vigilance des utilisateurs pour réduire la fréquence des attaques réussies
Quand	Tous les 2 ans environ
Tarif	Forfait 3 000 € HT

FORM-SIA : Formation au déploiement sécurisé de l'IA

Le fort engouement pour l'IA et son adoption très rapide par les entreprises a ouvert tout un champ de nouvelles attaques pour les pirates.

- L'empoisonnement des données d'apprentissage d'un modèle peut l'amener à produire des résultats fallacieux ou à effectuer des actions illégitimes dans certaines conditions.
- L'entraînement d'un chatbot sur les documents de l'entreprise peut l'amener à révéler malgré lui des données confidentielles.
- Cacher des prompts dans des documents qui seront ingérés par une IA peut permettre une intrusion dans le système d'information d'une entreprise.
- Etc.

Or ces attaques sont encore majoritairement ignorées des utilisateurs, et même des développeurs.

Les bonnes pratiques de sécurité dans l'usage de l'IA sont en mutation constante tant le domaine évolue rapidement.
Toutefois, plusieurs réglementations existent déjà (comme l'IA Act européen) et nécessitent un minimum de maîtrise pour s'y conformer.

Que vous utilisiez une IA commerciale (ChatGPT, Gemini, ...) dans vos processus métiers, ou que vous développiez un modèle d'IA pour une tâche spécifique, il existe plusieurs écueils à éviter.

Cette formation vise à fournir les clés de compréhension des grandes familles d'attaques sur les IA (qui peuvent ensuite se décliner en une infinité de cas), à donner les bonnes pratiques de conception et de contrôle et à comprendre les exigences réglementaires et les moyens pour s'y conformer.

Pour qui	Les entreprises qui utilisent ou développent des IA pour effectuer des tâches autonomes (sans validation d'un humain)
Pour quoi	Éviter les attaques qui abusent des IA pour piéger les entreprises qui les utilisent. Éviter les sanctions pour non conformité aux règlements sur l'IA.
Quand	Lorsqu'un socle minimal de mesures et d'outils de sécurité est déjà en place
Tarif	3 jours - 4000 € HT par tranche de 10 personnes

FORM-DEV : Formation au développement sécurisé pour les développeurs

Le domaine de la cybersécurité recense plusieurs familles de bug et de mauvaises pratiques de développement (*use after free*, *race condition, session fixation, access control bypass*, ...), et a produit des référentiels pour guider les développeurs vers des pratiques sûres.
C'est ce que l'on nomme le *secure coding* (développement sécurisé).

Mais les bonnes pratiques de cybersécurité sont encore trop méconnues des développeurs et peu présentes dans les formations. Pire, elles y sont parfois abordées de manière superficielle, tout en laissant croire aux étudiants que le sujet a été couvert de manière exhaustive (créant un biais de surconfiance).
Or, en cybersécurité, les plus gros risques sont dus aux *unknown unknown* : ce qu'on ne connaît pas et dont on ignore qu'on aurait besoin de le connaître.

L'objectif profond d'une formation en développement sécurisé n'est pas de tout connaître en cybersécurité, mais avant tout d'être au courant de ce qu'il faudrait savoir (quitte à ne se pencher dessus qu'au moment où on a besoin de le mobiliser).
En somme, transformer les *unknown unknown* en *known unknown* : ce qu'on ignore encore mais dont on sait qu'on a besoin de le connaître. Il s'agit donc d'évacuer les angles morts. Et bien sûr de fournir les outils pour obtenir les connaissances nécessaires le moment venu.

À l'issue de cette formation le développeur connaît et comprend le vocabulaire associé aux vulnérabilités. Il ne confond plus des notions telles qu'impact, risque, sévérité, ... Il est capable de qualifier une vulnérabilité découverte. Il sait rechercher les vulnérabilités connues pour un produit/une dépendance et interpréter un vecteur CVSS.
Il connait les bonnes pratiques de sécurité relatives aux activités de conception de l'application et aux activités *post-release*.
Il connait les grandes familles de vulnérabilités et sait reconnaître un comportement logiciel qui mène à l'une d'elles.
Il connait les principales bonnes pratiques de développement sécurisé et comprend les risques associés à leur absence.
Il sait où trouver les ressources lui permettant d'obtenir des recommandations précises et exhaustives sur les sujets dont il ne connait que les grandes lignes. Il connait les termes consacrés (mots-clés) pour désigner les concepts sur lesquels il peut avoir besoin d'informations complémentaires.

Pour qui	Les entreprises qui développent des outils (à visée commerciale ou en interne)
Pour quoi	Éviter que les logiciels développés soient utilisables par des adversaires pour pirater l'entreprise ou ses clients
Quand	Lorsque les logiciels développés sont achetés par un nombre significatif de clients ou qu'ils sont utilisés en interne pour des processus critiques
Tarif	3 jours - 3000€ HT par tranche de 10 personnes

FORM-SAD : Formation à la sécurité d'Active Directory

Les domaines Active Directory (AD) permettent la fédération des postes et des utilisateurs Windows au sein d'une console centralisée.

Ils sont omniprésents dans les entreprises, mais pourtant mal connus.
Premièrement en raison du nombre de fonctions qu'ils assurent : annuaire d'utilisateurs, DNS, DHCP, PKI, NTP, service d'impression, partage de fichiers, déploiement de configurations, sessions à distance, accès WiFi entreprise, etc.
Deuxièmement en raison de leur complexité : ils comportent des milliers de paramètres. Certains sont interdépendants, certains sont hérités de versions obsolètes, certains sont mal documentés, etc.

Or les AD constituent de fait des « Points Uniques de Défaillance » (SPOF : *Single Point Of Failure*) : compromettre un seul compte administrateur du domaine permet souvent de prendre le contrôle (directement ou indirectement) de tout le système d'information (SI).
Ces dernières années, ils sont particulièrement ciblés par les pirates. Leur grande complexité les rend très propices aux vulnérabilités. Et identifier ces vulnérabilités peut se faire de manière discrète. L'intérêt est donc maximal : faibles chances d'être repéré et compromission intégrale du SI si la configuration AD est vulnérable.

Ces éléments font qu'il est primordial d'investir du temps et des compétences dans la sécurisation de cet outil central.
Bien qu'il ne soit pas pertinent de tenter d'apprendre exhaustivement les centaines de vulnérabilités possibles, il est utile de connaître les grands principes qui précèdent à leur existence.
La sécurisation d'un environnement Active Directory passe par trois grandes approches : diminuer la surface d'attaque (architecture et configuration), restreindre les facultés d'attaques et les impacts en cas d'attaques réussie (durcissement), identifier préventivement les angles morts pour les combler avant qu'ils ne soient utilisés par des adversaires.

Cette formation vise à transmettre, aux participants, l'état de l'art de la sécurité de Active Directory, tout en fournissant des clés opérationnelles quant à sa mise en place et aux difficultés du terrain lorsqu'on tente d'appliquer les recommandations (gestion du parc obsolètes, mots de passe codés en dur, ...).

Pour qui	Les entreprises qui ont un AD et la majorité de leurs ressources enrôlées dedans
Pour quoi	Prévenir l'introduction de vulnérabilités dans l'AD (les chances se multiplient avec la montée en complexité de celui-ci), se protéger des attaques, connaître et sanctuariser les ressources critiques, maîtriser les outils à disposition.
Quand	Lorsqu'un socle minimal de mesures et d'outils de sécurité est déjà en place
Tarif	3 jours - 3000€ HT par tranche de 10 personnes

FORM-PER : Formation sécurité offensive pour les employés

Astar propose des formations en sécurité informatique offensive destinées à votre personnel.

Vous pouvez vouloir former:

- Un DSI/RSSI pour qu'il appréhende mieux les notions techniques de la sécurité, du risque informatique, des formes de menaces, etc.
- Un technicien/ingénieur de l'équipe informatique pour qu'il soit capable d'auditer votre réseau et d'appliquer les bonnes corrections.
- Vos développeurs pour qu'ils anticipent les vulnérabilités qu'ils pourraient introduire dans le code.
- Vos pentesters en herbe, pour leur enseigner les notions de base de l'intrusion informatique: démarche, éthique, techniques, ...
- Etc...

Pour qui	Les entreprises qui ont des employés confrontés à des attaques informatiques (équipe SOC, RSSI, développeur d'un produit/site Web, administrateur réseau, ...)
Pour quoi	Améliorer leur compréhension des méthodes et moyens d'attaque employés par leurs adversaires, afin de tirer tout le profit possible des outils de sécurité à disposition
Quand	Lorsqu'un socle minimal de mesures et d'outils de sécurité est déjà en place
Tarif	5 jours - 5000€ HT par tranche de 10 personnes

FORM-RAP : Formation à la rédaction de rapport d'audit pour les pentesters

Dans une prestation de test d'intrusion, le client final juge la qualité du travail produit principalement au travers du seul matériau qui lui est livré : le rapport d'audit. Celui-ci est donc l'ambassadeur de l'entreprise. Si sa forme est négligée, le client jugera l'entreprise peu méticuleuse. Si son design est vieillissant, le client jugera l'entreprise peu innovante. Si les ingénieurs ont accompli des prouesses techniques, mais qu'ils ne savent pas correctement les restituer, le client mésestimera la qualité du service qu'il a reçu.

La profession de pentester est essentiellement composée de profils "ingénieurs" dont les qualités rédactionnelles pâtissent de plusieurs problèmes : mauvais réflexes hérités des cours de français (remplissage et paraphrase pour atteindre un nombre de pages), méconnaissance des règles de l'expertise académique (synthèse versus résumé pour décideur, constat versus hypothèse, reproductibilité des observations, ...), redondance des phases de rédaction d'une mission à l'autre, etc.
Pour autant, cet exercice peut devenir une source d'épanouissement.

La formation propose une partie théorique puis une partie pratique. Le plan couvre les grands thèmes suivants :

- Concepts, déontologie et formalisme (ton, distance professionnelle, observations, constats et hypothèses, ...)
- Caractéristiques (plan, glossaire, dimensions des vulnérabilités, transmission, ...)
- Conventions visuelles et typographiques (choix des polices, règles de lisibilité, association des couleurs, ...)
- Qualité d'expression (précision des verbes, bon usage des néologismes, marqueurs d'incertitude, ...)

- Qualité de restitution (choix des échelles, adapter son propos au lecteur, rendre le plan d'action utile, ...)

Pour qui	Les entreprises qui fournissent des services d'audit de sécurité (pentest, MSSP, ...)
Pour quoi	Améliorer la qualité des livrables
Quand	Une fois que l'on dispose d'une équipe d'audit stabilisée
Tarif	1 jour - 2 500€ HT par tranche de 5 personnes

COUR-SEC : Module d'initiation à la cybersécurité pour l'enseignement supérieur

Astar intervient dans plusieurs écoles d'ingénieurs pour assurer des cours introductifs ou avancés à la sécurité de l'information.
Le contenu est adapté en fonction des demandes spécifiques des établissements, mais la trame générale est la suivante :

- Concepts et terminologie (*confidentialité, disponibilité, intégrité, menace, vulnérabilité, impact, risque, données, ...*)
- Vulnérabilités et conséquences (*escalade de privilèges, dénis de service, exécution de commande, usurpation, ...*)
- Tactiques et techniques (*ingénierie sociale, énumération, exécution, mouvements latéraux, rebonds, exfiltration, ...*)
- Appréciation des risques (*notions d'actifs essentiels/supports, qualifier et quantifier un risque, choisir un traitement, ...*)
- Défenses (*méthodes préventives : mise à jour, segmentation, ... et palliatives : sauvegarde, détection d'intrusion, ... notion de défense en profondeur, notion de confiance, ...*)
- Focus à la carte (*virologie, cryptographie, investigation numérique, ...*)

Certains TD explorent des dimensions du cours et d'autres permettent de s'initier à des domaines particuliers :

- Weaponization (*automatisation progressive d'une attaque*)
- Fonctions de hachage (*exploration du concept cryptographique des fonctions de hachage, notamment appliqué au cracking de mots de passe*)
- OSINT (*récolte d'informations publiquement accessibles pour cibler une attaque*)
- Analyse forensic (*exploration d'un dump mémoire pour retrouver les éléments de l'attaque, dont la clé d'un ransomware*)
- Interception réseau (*ARP, DHCP, ICMP, HTTPS et réutilisation des données dérobées*)

Pour qui	Les écoles d'ingénieurs ou les formations spécialisées en cybersécurité
Pour quoi	Former les étudiants aux concepts de base de la cybersécurité et en approfondir certains
Quand	Après qu'ils aient reçu une formation minimale en informatique (réseau, programmation et administration Linux/Windows)
Tarif	10 heures CM - 15 heures TD - 35 personnes max - 5000 € HT

LIVRABLES

La majorité des prestations proposées par Astar aboutissent à la production d'un rapport. Celui-ci comprend 3 parties essentielles :

- Une **synthèse managériale** qui explique, en une page et en termes non techniques, les vulnérabilités, les préjudices à redouter et la meilleure stratégie à adopter pour les corriger. Cette synthèse est accompagnée **d'indicateurs** permettant l'aide à la décision.
- Un **plan d'action**, chiffré en jours/homme, qui récapitule les compétences à mobiliser et les actions correctrices hiérarchisées selon leur urgence et leur difficulté de mise en place
- Une **description technique**, destinée au personnel en charge des corrections/applications, qui permet notamment de comprendre, rejouer et corriger les défauts de sécurité

Les livrables sont transmis via un lien éphémère sur un service de stockage hébergé en Europe et chiffré en mode *zero knowledge*.
Par défaut, les livrables (et les éléments recueillis lors d'une prestation) sont conservés un an puis archivés. Il ne sont stockés que sur des supports chiffrés.

Options

Le livrable par défaut est un rapport PDF rédigé en français.
Par commodité, il est possible de commander des formats complémentaires/alternatifs du livrable :

- **Rapport international**
  Rédaction des livrables en anglais
- **Échelle de risque personnalisée**
  Si le client dispose de sa propre échelle de risque et qu'il veut que les résultats soient directement incorporables dans ses référentiels internes
- **Audit "live"**
  Remontée en direct des vulnérabilités dès qu'elles sont identifiées pour que les équipes puissent entamer les corrections le plus vite possible. Astar met à disposition un "pad" partagé et chiffré, disposant d'un *chat*, où les auditeurs dialoguent en direct avec les équipes du client
- **Format tableur** (Excel)
  Idéal pour un suivi opérationnel des vulnérabilités (priorisation, attribution, suivi des corrections)
- **Format présentation** (Powerpoint)
  Support de projection pour les restitutions orales à l'attention des décideurs
- **Aide aux mesures d'urgence**
  Astar peut dépêcher un ingénieur, quelques jours, afin d'aider le client à corriger les vulnérabilités les plus urgentes
- **Contre-audit** (aussi appelé "retest")
  Seconde itération de l'audit (bien plus rapide) visant à vérifier/valider la correction des vulnérabilités, quelques semaines après l'audit initial
- **Attestation d'audit**
  Pour attester que la société a bien mené un audit de sécurité et pour témoigner du résultat sans révéler les détails techniques sensibles (s'il y a contre-audit, l'attestation est produite à l'issue de ce dernier)
- **Attestation de destruction**
  Le client peut exiger qu'Astar détruise tous les éléments recueillis lors de l'audit (éventuellement après en avoir transmis une copie au client) : rapport, prise de note, captures d'écrans, sorties des outils, ...

ASTAR

contact@astar.org - 09 83 20 01 30
4 rue Alan Turing 33680 LACANAU-OCÉAN