

Audit de maturité | Outil d'automatisation Consultant Stagiaire en Cybersécurité

Rapport de stage Aéro 4



Antoine CASTEL - AERO 4 SET
Tuteur : Clément PERROD, Romain MEDIONI

Stage effectué du 3 juin
au 30 août 2024

Remerciements

Depuis longtemps, travailler dans la cybersécurité est pour moi un objectif professionnel. Ce stage m'a permis d'avoir une première expérience dans ce domaine appliqué au secteur du conseil et de l'audit. J'y ai découvert un milieu accueillant, galvanisant et passionnant.

Je souhaite remercier toutes les personnes de l'équipe cybersécurité d'Ernst & Young Advisory que j'ai eu l'occasion de rencontrer et tout particulièrement celles avec qui j'ai travaillé.

Je remercie Monsieur François REN, Consultant Senior Cybersécurité, pour son accompagnement sur la majeure partie de ce stage sur une mission d'audit.

Je remercie Monsieur Clément PERROD, Associé Cybersécurité, qui a compris mes objectifs, a veillé à me placer sur une mission en adéquation avec ceux-ci, et s'est assuré que cette expérience m'apporte une réelle valeur ajoutée.

Je tiens à remercier particulièrement Monsieur Michel RICHARD, Associé Senior, pour son suivi, son soutien et ses précieux conseils.

Merci à Ernst & Young Advisory de m'avoir donné l'opportunité d'intégrer leur entreprise et de découvrir le monde du conseil.

Avertissement

Le service de Cybersécurité d'Ernst & Young Consulting France travaille pour différents clients pour lesquels un certain niveau de discrétion, voire de confidentialité, est requis.

Afin de respecter cet engagement, le nom de l'entreprise au cœur de ma mission ne sera pas mentionné autrement que par « Entreprise hôtelière du CAC40 ».

Sommaire

Introduction.....	7
I - Ernst & Young : Un acteur mondial au cœur de la transformation numérique et de la cybersécurité.....	8
I.1 Stratégie et positionnement sur le marché du conseil	8
I.2 Innovation et développement durable : Les engagements d'EY	12
I.3 Culture d'entreprise et méthodes de travail chez EY.....	13
II - Audit de cybersécurité pour une entreprise du CAC 40 et développement d'un outil d'automatisation pour EY	14
II.1 Audit de cybersécurité pour une entreprise d'hôtellerie du CAC40	15
II.1.a Le Framework CPA	15
II.1.b Mise en place de l'Audit.....	19
II.1.c Interviews	23
II.2 Outil d'automatisation pour la génération d'un bulletin d'actualité cyber	25
II.2.a Contexte	25
II.2.b Solution Technique.....	27
II.2.b.1 Récupération des articles de la base de données	27
II.2.b.2 Mise en forme du PowerPoint avec les articles selon le modèle du CTB.....	28
II.2.b.3 Déclencheur de l'outil.....	29
II.2.b.4 Envoi du Powerpoint généré	30
II.2.c Mise en Production	31
II.2.d Livrable	32
Conclusion	34
Annexes.....	35
Bibliographie/Webographie	39
Liste des sigles et abréviations.....	40
Glossaire	41
Table des figures	43
Résumé.....	44
Abstract	44

Fiche de synthèse

Auteur : Antoine CASTEL - Aero 4 - SET

Sujet de stage	Objectifs
Participation à un audit de sécurité des systèmes d'information sous le format CPA d'EY et construction d'un outil d'automatisation pour la génération de bulletin hebdomadaire de Cybersécurité.	<ul style="list-style-type: none">Effectuer une mesure du niveau de maturité des systèmes d'information en termes de sécurité via l'exploration globale de l'entreprise d'un point de vue organisationnel.Créer un outil d'automatisation et de génération d'un bulletin hebdomadaire de cybersécurité (format PowerPoint).
Client Principal	Outils utilisés
<ul style="list-style-type: none">Un grand groupe hôtelier du CAC40 dans le cadre de la mission d'audit pilotée par Ernst & Young Advisory.L'équipe cybersécurité d'Ernst & Young Advisory pour l'outil d'automatisation.	<ul style="list-style-type: none">ExcelPowerPointWordVisual Studio Code (Python)PuTTYPowerShell & Cmd
Etudes réalisées	
<ul style="list-style-type: none">Récupération et analyse de la documentation existante.Rencontres avec les principaux intervenants de l'entreprise afin d'évaluer le niveau de maturité sous plusieurs angles (gestion, affaires, informatique, sécurité), couvrant toutes les exigences avec 2 à 3 entretiens par domaine, présent dans le Framework propre à EY, le CPA.Analyse des besoins et compréhension de l'architecture informatique d'EY pour le développement de l'outil d'automatisation.	
Résultats	Explications des écarts possibles
<ul style="list-style-type: none">Mise en place d'un fichier Excel regroupant les 515 questions propres au format CPA 2024 d'EY.Préparations des éléments nécessaires aux interviews selon les exigences du client.	<ul style="list-style-type: none">Les résultats de l'audit pourraient être influencés par une mauvaise compréhension initiale des besoins ou des exigences du

<ul style="list-style-type: none"> • Réalisation de 18 interviews des équipes du groupe hôtelier selon leur fonction puis rédaction, correction et revue de compte-rendu. • Mise en forme et structuration du compte-rendu final. • Développement et mise en production de l'outil d'automatisation du bulletin hebdomadaire de cybersécurité. 	<p>client.</p> <ul style="list-style-type: none"> • L'outil d'automatisation peut présenter des limites techniques ou des bugs non identifiés durant le développement.
Difficultés rencontrées	Travaux à poursuivre
<ul style="list-style-type: none"> • Complexité de la mise en production de l'outil d'automatisation en raison des processus mis en place pour accéder aux machines de production. • Difficulté de compréhension lors des interviews du fait de la complexité du domaine (Acronymes, Outils, Infrastructures, Organisation d'entreprise). 	<ul style="list-style-type: none"> • Finir le rapport final de l'audit de maturité. • Envoyer le rapport au client. • Prendre en compte et intégrer les retours du client. • Adapter l'outil d'automatisation en fonction des retours utilisateur.

Introduction

Fervent passionné d'informatique, j'ai fait le choix, au cours de ces deux dernières années, d'orienter mon parcours à l'IPSA vers la cybersécurité. Fils de deux ingénieurs informatiques, j'ai baigné dans le monde du numérique dès mon plus jeune âge.

A l'occasion d'un précédent stage chez Docaposte, j'ai accompagné un correspondant de la Sécurité des Systèmes d'information. C'est lors de cette expérience que j'ai pris conscience de l'ampleur et de l'importance de cette activité. La cybersécurité m'a immédiatement attiré, car, au-delà de sa nécessité cruciale, elle exige une approche holistique pour protéger l'ensemble de l'environnement numérique d'une organisation, qu'il s'agisse de multinationales, d'États ou même de particuliers.

Fort de cette passion et avec l'objectif d'orienter mon parcours vers la cybersécurité, j'ai eu l'opportunité d'effectuer un second stage dans ce domaine. J'ai ainsi pris le rôle de *consultant cybersécurité au grade de stagiaire* au sein du cabinet de conseil Ernst & Young, un cabinet internationalement reconnu pour son expertise en cybersécurité et son rôle dans la transformation numérique des entreprises et organisations.

Ce stage de 12 semaines a pris place dans le quartier d'affaires de la Défense, au 14^{ème} étage de la tour First, dans le service organisationnel de la branche cybersécurité. Mon rôle dans ce service s'est concentré sur deux missions principales.

- Une mission d'audit de maturité de la sécurité des systèmes d'information pour une entreprise du CAC40, connue pour ses services dans l'hôtellerie.
- La mise en place d'un outil d'automatisation pour la génération d'un bulletin de cybersécurité hebdomadaire à destination des clients de Ernst & Young Advisory.

Ce rapport s'articule en deux grandes parties.

En préambule, je présente l'entreprise Ernst & Young dans son ensemble.

Puis, dans le prisme du cabinet de conseil et de sa branche cybersécurité, je m'attarde sur son positionnement et sa stratégie en tant qu'acteur mondial du conseil, ses engagements en termes d'innovation et de développement durable, ainsi que sa culture d'entreprise et sa méthode de travail.

Enfin, la dernière partie détaille les différentes missions réalisées durant mon stage à savoir ma participation à l'audit de cybersécurité ainsi que la création et la mise en place de l'outil d'automatisation.

I - Ernst & Young : Un acteur mondial au cœur de la transformation numérique et de la cybersécurité

I.1 Stratégie et positionnement sur le marché du conseil

Le cabinet Ernst & Young fait partie du fameux groupe des « Big Four », regroupant les quatre plus grands cabinets d'audit et de conseil au monde.

Ce cabinet guide plus de 390 000 collaborateurs répartis dans plus de 700 bureaux à travers 148 pays.



Figure 1 - Statistique de répartition géographique d'EY dans le monde (Rapport de transparence 2023).

Avec un chiffre d'affaires de 49,4 milliards de dollars dans le monde pour 1,47 milliard d'euros en France en 2023, Ernst & Young se classe comme étant le troisième plus grand cabinet du monde au niveau du chiffre d'affaires.

Son activité est structurée autour de quatre domaines principaux :

- Audit financier
- Conseil juridique et fiscal,
- Transactions
- Consulting

Ce regroupement de services remonte à plus de 150 ans. Il est le résultat de fusions successives de plusieurs cabinets d'audit anglais et américains qui amèneront à la création d'Ernst & Young en 1989, renommé EY en 2013.

Le cabinet propose des services de conseil au niveau des systèmes d'information, des ressources humaines, de l'organisation, de la finance et de la stratégie.

Historiquement connu pour leurs prestations de commissaires au compte, la division conseil d'Ernst & Young nommée *Ernst & Young Advisory* prend aujourd'hui de la place au sein du cabinet.

Avec plus de 50% du chiffre d'affaires du groupe lié à des activités de conseil, cette branche se positionne comme étant « le leader pour accompagner la structuration et la conduite des grandes transformations business et digitales » de ses clients. La stratégie globale de cette division repose sur le besoin des entreprises et des organisations de se transformer et s'adapter à un environnement en perpétuelle évolution.

Ce contexte amène un questionnement essentiel pour anticiper ces changements :

- Comment créer une relation de proximité avec ses clients ?
- Comment intégrer les collaborateurs dans ce nouveau monde du travail ?
- Comment la technologie peut donner un avantage concurrentiel ?
- Comment placer l'innovation à la source de la croissance ? ».

C'est au travers de leur marque de fabrique « Build a better working world » que le cabinet exprime sa volonté d'aider les entreprises, les collaborateurs et plus globalement la société à se transformer et à créer de la valeur à long terme avec de nouvelles technologies et des innovations.

Ernst & Young Advisory propose différentes offres de conseil aux entreprises et organisations. Ces dernières sont structurées sous huit practices bien distincts :

- Conseil en achats, supply chain et opérations
- Conseil en analyse de données
- Conseil en expérience client
- Cybersécurité
- Diffuser l'agilité et transformer l'organisation
- Transformation des directions financières
- Transformation digitale des entreprises
- Transformation de la gestion des risques

La practice cybersécurité occupe aujourd'hui une place de plus en plus importante au sein d'*Ernst & Young Advisory*. La modernisation et la digitalisation du monde professionnel entraîne l'émergence de nouvelles technologies produisant des quantités importantes de données et révolutionnant les usages. On peut penser au Cloud il y a quelques années et aujourd'hui l'intelligence artificielle qui révolutionne le monde informatique.

Les bénéfices apportés par ces technologies entraînent malheureusement l'apparition de nouveaux risques. Avec un monde de la cybercriminalité de plus en plus

expérimenté et organisé, les structures cybercriminelles atteignent des échelles industrielles qui peuvent pour certaines, être utilisées à des fins gouvernemental. On peut penser par exemple au groupe Lazarus qui sert les intérêts financiers de la Corée du Nord depuis plus de 10 ans. Leur portfolio de victimes regroupe principalement des institutions financières et des plateformes d'échange de cryptomonnaie. Ces groupes représentent de réels dangers pour les entreprises au vu de leur force de frappe. Avec des risques de vol de données, de ransomware ou encore de piratage des systèmes financiers, la cybersécurité est devenue un sujet d'importance stratégique. Longtemps sous-estimé, du fait de la nécessité d'investissement sans retour financier, les grandes entreprises ont vite compris la puissance d'impact que pouvait avoir une attaque informatique.

La practice Cybersécurité d'EY Advisory vise à répondre aux besoins des entreprises et organisations sur les sujets de sécurité informatique. Cette branche se compose de quatre services :

- EY CSIRT
- Organisationnelle
- Laboratoire Technique
- Infrastructure

EY CSIRT (Computer Security Incident Response Team) propose l'accès à un centre d'alerte et de réactions aux attaques informatiques. Il permet d'accompagner les entreprises et organisations dans « l'anticipation, la détection et la réaction aux menaces ». La criticité de ce service fait que l'équipe responsable est regroupée dans le laboratoire « CSIRT ». L'entrée à ce laboratoire est contrôlée selon trois niveaux d'authentications répartis sur deux portes (badge, code, empreinte digitale).

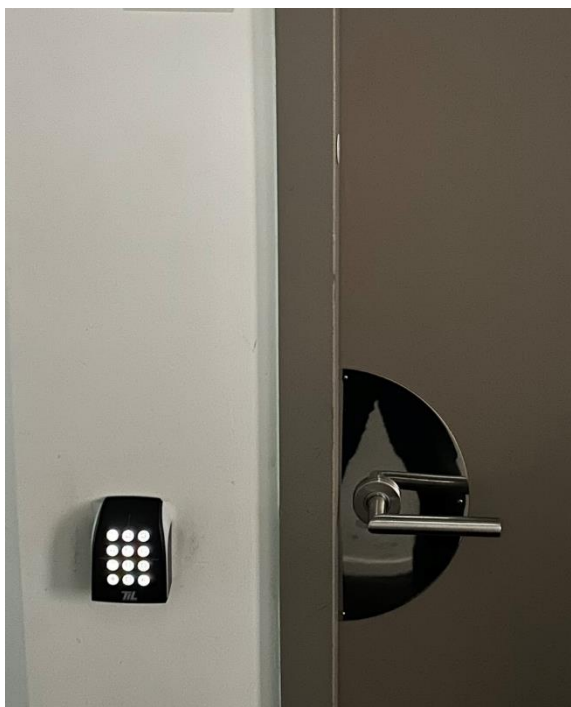


Figure 2 - Première porte du laboratoire CSIRT, double authentification nécessaire (badge, code).



Figure 2 - Seconde porte du laboratoire CSIRT, triple authentification requise (badge, empreinte, code)

Le service CSIRT d'EY, propose plusieurs offres :

- Cyber Threat Bulletin, un bulletin hebdomadaire portant sur les actualités cybersécurité à travers le monde. Il permet au client de recevoir une synthèse régulière de la veille cyber.
- CyberEYe, un outil de surveillance des actifs externes des clients, des données exposées et de l'image de l'entreprise. Cette surveillance touche à l'aspect technique et organisationnel du client.
- Réponse à incident, afin de répondre aux situations de crise faisant suite à la compromission d'un client. Des analyses forensiques sont effectuées afin d'accompagner dans la restauration des services impactés.
- Exercices de gestion de crises, le CSIRT accompagné du laboratoire technique d'EY, effectue des exercices de *purple team* en collaboration avec les équipes de défenses du client dans le but d'améliorer la détection d'intrusion.

L'équipe Organisationnelle se situe dans un open-space commun aux différentes pratiques d'EY Advisory. Cette équipe s'occupe de différents sujets liés aux aspects de gouvernance en cybersécurité :

- Gouvernance et Organisation de la sécurité
- Stratégie de la Cybersécurité
- Gestion du risque
- Elaboration de plan de reprise d'activité
- Entrainement et sensibilisation
- Conformité et respect des lois
- Audit de maturité de sécurité des systèmes d'information, de conformité aux

normes (27001, HDS...) pour homologation

- Analyse de risque (EBIOS RM) et protection des données (AIPD)
- Gestion des identités et des accès (IAM)

Le laboratoire technique, tout comme le laboratoire CSIRT, est sécurisé par une porte à triple authentification (badge, empreinte, code). Cette isolation est une condition obligatoire pour un laboratoire certifié PASSI (Prestataires d'audit de la sécurité des systèmes d'information). Les membres de cette équipe travaillent sur différents sujets opérationnels tels que des tests de pénétrations informatiques d'entreprise ou d'organisation, ils participent à des exercices de Red, de Blue voire même de Purple team en collaboration avec les équipes CSIRT.

Enfin, la dernière équipe de la practice Cybersécurité d'EY Advisory est l'équipe Infrastructure. Elle se trouve dans une salle sécurisée par une porte à double authentification, juste à côté du laboratoire CSIRT. Cette équipe est responsable de la gestion d'un datacenter situé en face de leurs bureaux. Elle gère les accès pour les flux internes et externes à ce datacenter, ainsi que les accès aux machines, les mises en production et la maintenance des différents sites et outils présents sur le datacenter. Une de leurs missions est la maintenance du matériel et le remplacement des machines arrivant en fin de vie.

I.2 Innovation et développement durable : Les engagements d'EY

Le cabinet Ernst & Young est engagé dans une démarche RSE depuis 2008. Avec leur signature « Build a better working world », EY s'engage « à prendre une part active à la construction d'un monde nouveau, et à contribuer à rendre plus équilibré le monde du travail dans lequel nous évoluons. »

D'un point de vue environnemental, EY mesure depuis 10 ans son empreinte carbone et développe des plans d'actions pour diminuer la production de carbone dans les secteurs les plus polluants auxquels l'entreprise participe.

EY possède en France une branche qui accompagne les entreprises et les organisations sur des sujets de RSE. Avec plus de 100 experts en RSE en France (sur 1200 dans le monde), cette branche propose des services de certifications financières permettant d'apporter de la transparence aux investisseurs sur les sujets environnementaux ainsi que du conseil stratégique pour l'évolution des business model en lien avec les objectifs RSE des entreprises.

Plus localement, lors de mon stage à la tour First, j'ai constaté la mise en place de certaines recommandations de politiques environnementales telles que le traitement

des déchets en fonction de leur nature ou encore la présence de machines à café utilisant le café bio d'une entreprise s'approvisionnant localement. Une autre initiative présente sur mon lieu de travail est la vente à prix réduits des invendus de la journée des différentes cafétérias et cantines de la tour.

Dans un spectre plus social, j'ai également remarqué une répartition assez égale au sujet de la parité homme-femme ce qui montre bien la présence d'une politique de parité au sein du cabinet. En effet, avec aujourd'hui en France seulement 27% de femmes travaillant dans l'IT et 11% dans la cybersécurité, le cabinet se démarque avec une note de 87/100 sur l'index d'égalité professionnelle et salariale. Les 13 points manquants sont perdus dans la proportion du sexe sous-représenté dans le TOP 10 des plus hauts salaires avec un 0/10 et dans l'écart de salaires par rang avec une note de 37/40.

I.3 Culture d'entreprise et méthodes de travail chez EY

L'intégration de nouveaux arrivants suit un processus très structuré. Une semaine avant le début du stage, j'ai reçu à domicile tous les outils (casque, ordinateur, sac, guide) nécessaires à celui-ci. Le jour de mon arrivée, stagiaires et nouveaux arrivants étaient accueillis avec une réunion d'introduction pour présenter l'entreprise, la stratégie globale du groupe, les différentes politiques internes ainsi que les outils d'administration utilisés.

Chaque nouvel arrivant se voit attribuer un « Buddy » et un « parrain/marraine ».

Le « Buddy » permet de faciliter l'intégration du nouvel arrivant dans l'équipe et sert de point d'aide pour les premières semaines.

Le parrain/marraine accompagne tout au long de son expérience chez EY, en particulier lors de son évaluation annuelle, qui permet de vérifier la cohérence de son niveau avec son rang.

EY Advisory étant un cabinet de conseil, la présence de consultant chez un client est facturée à l'heure. Un outil interne permet de pointer les heures passées chez le client. Pendant mon stage, j'ai déclaré distinctement chaque semaine les heures de travail consacrées aux clients de celles passées sur des tâches internes à EY.

II - Audit de cybersécurité pour une entreprise du CAC 40 et développement d'un outil d'automatisation pour EY

Après la présentation d'introduction à EY, mon « Buddy » m'a présenté au service de Cybersécurité d'EY Advisory. Après une journée de formalités de début de stage telles que ma présentation à toute l'équipe ou encore l'activation de tous les services internes, j'ai rencontré l'Associé en charge de l'attribution des missions, Clément PERROD.

Cette première semaine a été également l'occasion d'effectuer des formations sur différents sujets de cybersécurité via une plateforme interne à EY global et la plateforme Udemy.

J'ai suivi différents cours en ligne allant du management du risque cyber à des apprentissages plus techniques tel que le forensique, le social engineering ou encore la data protection. La validation de chaque cours dépendait du résultat à un test QCM. Je me suis donc vu remettre, après avoir suivi plus de 15h de cours, un certificat de validation de la formation appelé *EY Cybersecurity Bronze Learning*. (Voir Annexe)

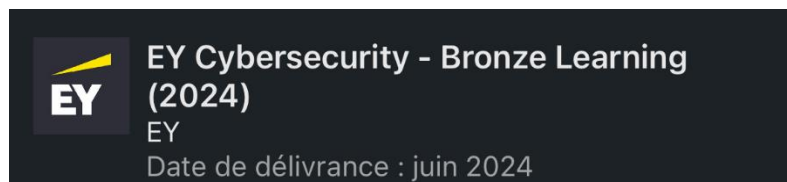


Figure 3 - Certificat - Cybersecurity Bronze Learning D'EY

Deux missions m'ont été confiées simultanément pour toute la durée de mon stage :

1. La préparation, mise en place et participation à un audit de maturité de la sécurité des systèmes d'information pour un grand groupe hôtelier du CAC40.
2. Un projet interne à la division cybersécurité d'EY Advisory, dont le but est la création d'un outil d'automatisation pour la génération d'un bulletin hebdomadaire d'informations portant sur les actualités liées à la sécurité des systèmes d'information.

II.1 Audit de cybersécurité pour une entreprise d'hôtellerie du CAC40

L'entreprise auditée est un des plus grands groupes hôteliers au monde. Sa présence internationale implique que tous les livrables de cette mission ont été réalisés en anglais.

II.1.a Le Framework CPA

Cette mission d'audit de maturité de la sécurité des systèmes d'information utilise le framework CPA d'EY.

Le Framework CPA (Cybersecurity Program Assessment) est une méthode de conseil en Stratégie, Risque, Conformité et Résilience (SRC&R). Elle permet à EY d'aider les clients à effectuer des évaluations de l'état actuel, à développer des recommandations pour l'état futur et à conseiller sur les meilleures pratiques de l'industrie.

Le cadre CPA décrit leur point de vue comme un programme de sécurité holistique à l'échelle de l'entreprise. Il se compose de plus de 26 domaines interconnectés qui sont alignés avec les normes et cadres de l'industrie de la cybersécurité, tel que l'ISO 27001/2/5/17/701, le NIST-800/NIST CSF ou encore le COBIT 5, entre autres. Ce framework est indépendant de n'importe quel cadre reconnu internationalement, mais il permet de s'y adapter et de répondre à leurs exigences.

Ce framework d'audit permet à EY d'avoir un seul outil pour auditer de multiples entreprises, chacune ayant des demandes et besoins différents. Certaines certifications ou normes sont très difficiles à obtenir et demandent une connaissance en profondeur du fonctionnement informatique de l'entreprise.

L'une des premières raisons pour laquelle une entreprise veut être auditée est pour connaître leur état d'avancement selon une norme. Par exemple, la norme HDS pour Hébergement de Données de Santé, est une norme assez compliquée à obtenir. C'est une surcouche de la certification ISO 27001, permettant de démontrer la mise en place d'un système de management de la sécurité de l'information efficace, construit selon les bases de la norme internationale de l'ISO 27001.

C'est ici que le framework d'audit CPA d'EY est performant. Il segmente les zones à étudier en fonction de l'approche demandée par le client.

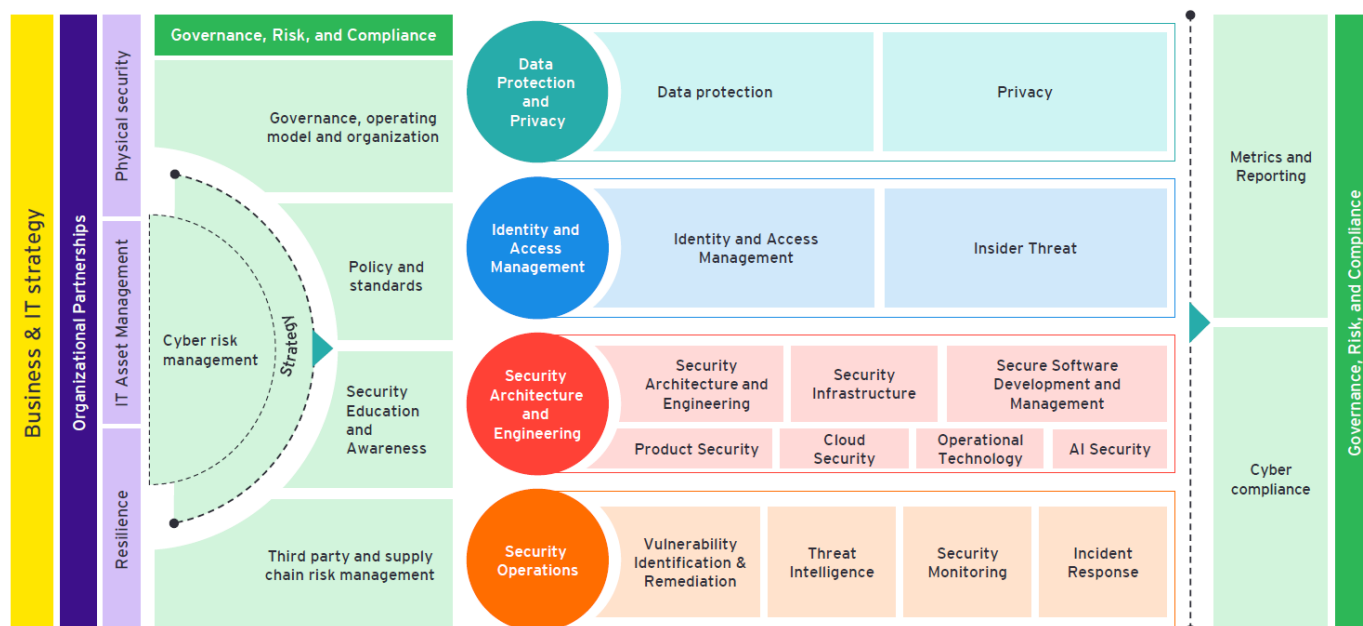


Figure 4 – Représentation graphique des différents domaines du framework CPA d'EY

Les 26 différents domaines que l'on retrouve dans le framework CPA sont les suivants :

- Strategy
- Cyber Risk Management
- Policies and Standards
- Governance, Operating Model and Organization
- Third Party and Supply Chain Security Risk Management
- Incident Response
- Cyber Compliance
- Data Protection
- IT Asset Management
- Privacy
- Metrics and Reporting
- Identity and Access Management
- Operational Technology
- Insider Threat
- Physical Security
- Cloud Security
- Resilience
- Secure Software Development and Management
- Product Security
- Security Education and Awareness
- Security Architecture and Engineering
- Security Infrastructure
- Security Monitoring
- Threat Intelligence
- Vulnerability Identification and remediation

Chacun de ces domaines comporte des thématiques techniques et méthodologiques qui leurs est propre. On y trouve aussi une dimension stratégique et business, des éléments directeurs de l'application et du développement de la cybersécurité dans les grands groupes.

Ces 26 domaines se décomposent en 169 sous-domaines pour un total de 515 questions classées. L'objectif dans un audit est de parcourir, au cours d'entretiens, un maximum de questions sous les différents axes du framework selon les besoins du client (certification/norme, maturité ...). Les réponses à ces questions sont ensuite évaluées selon des notes allant de 0 à 5 :

- 0 – Inexistant
- 1 – Initial
- 2 – Répétable
- 3 – Défini
- 4 – Géré Quantitativement
- 5 – Optimisé

Voici un exemple de question pouvant être posée au cours d'interview pendant un audit. Cette question se base sur le domaine de la *Sécurité Produit*, dans le sous-domaine du *Déploiement et Support* :

Domaine	Sous-domaine	Question
Sécurité Produit	Déploiement et Support	Comment l'organisation documente-t-elle et tire-t-elle des leçons des attaques passées ?

Et voici la grille d'évaluation permettant de mesurer le niveau de maturité par rapport à la réponse que le client va donner :

0 - Inexistant	Le processus n'existe pas ; les capacités définies n'existent pas ; les indicateurs de performance ne sont pas utilisés ; il n'y a pas de modèle de gouvernance en place pour la responsabilisation ; les indicateurs de performance n'existent pas ; aucune automatisation, outil ou technologie n'est utilisé.
1 - Initial	Les renseignements provenant des attaques passées ne sont ni collectés ni utilisés pour l'apprentissage.

2 - Répétable	Certains renseignements issus des attaques passées sont enregistrés et stockés dans des dépôts dédiés. En général, ces renseignements ne sont pas utilisés pour améliorer la conception des produits ni le processus de réponse aux incidents. L'organisation dispose de quelques indicateurs liés à la réponse aux incidents, qui sont collectés de manière ponctuelle. Des références établies pour mesurer les activités de réponse aux incidents ne sont généralement pas développées. Les indicateurs de réponse aux incidents ne sont pas intégrés dans les rapports organisationnels.
3 - Défini	Les renseignements issus des attaques passées sont enregistrés et stockés dans des dépôts dédiés. Les renseignements sont utilisés pour améliorer la conception des produits et le processus de réponse aux incidents. L'organisation dispose d'indicateurs liés à la réponse aux incidents qui sont régulièrement collectés et examinés. Des repères établis sont développés pour mesurer les activités de réponse aux incidents. Le non-respect des repères entraîne généralement une enquête supplémentaire et des mises à jour du processus. Les indicateurs de réponse aux incidents sont régulièrement intégrés dans les rapports organisationnels.
4 - Géré quantitativement	Les renseignements issus des attaques passées sont enregistrés et stockés dans des dépôts dédiés. Les renseignements sont principalement utilisés pour améliorer la conception des produits et le processus de réponse aux incidents. L'organisation dispose d'indicateurs dédiés et robustes liés à la réponse aux incidents qui sont continuellement collectés et examinés. Les indicateurs de réponse aux incidents sont intégrés dans les rapports organisationnels sur une base mensuelle.
5 - Optimisé	Les renseignements issus des attaques passées sont enregistrés et stockés dans des dépôts dédiés. Les renseignements sont utilisés pour améliorer la conception des produits et le processus de réponse aux incidents. L'organisation dispose d'indicateurs dédiés et robustes liés à la réponse aux incidents qui sont continuellement collectés et examinés. Les indicateurs de réponse aux incidents des produits sont disponibles pour les parties prenantes internes et externes via un tableau de bord interactif en temps réel.

Chaque question possède une grille de réponse unique permettant d'évaluer le niveau de maturité lié à cette dernière.

II.1.b Mise en place de l'Audit

L'audit auquel j'ai participé est une mesure du niveau de maturité globale de la sécurité des systèmes d'information pour l'un des plus grands groupes d'hôtellerie au monde. Cette mission se repose sur le framework CPA d'EY. Trois différents niveaux de prestation du service, basés sur les besoins et la portée du client sont proposés :

- Niveau 1 – Vérification rapide de l'état (« check-up » rapide).
- Niveau 2 – Évaluation globale du programme de cybersécurité.
- Niveau 3 – Évaluation complète des domaines.

Cette évaluation de la demande et des besoins du client se fait en amont de l'analyse via une RFP (Request For Proposal), l'équivalent d'un devis établi entre les deux parties, le prestataire et le client.

C'est en réponse à une demande d'audit indépendant de la maturité en cybersécurité de ce géant de l'hôtellerie qu'une proposition a été soumise. L'accent est mis sur l'importance croissante de renforcer la cybersécurité en raison de l'augmentation des cyberattaques, notamment les ransomwares.

L'objectif est d'apporter une vue externe sur la posture de cybersécurité, d'évaluer les forces et faiblesses, et d'identifier les menaces émergentes (gestion des données personnelles, shadow IT, IA générative, etc.).

Une équipe expérimentée séparée en partie technique et organisationnelle, ayant déjà travaillé sur des missions similaires pour de grandes entreprises, est proposée. EY s'appuie sur son expertise en audit et sa connaissance du marché pour fournir des analyses stratégiques et des recommandations pratiques.

Le but est de mettre en évidence les éléments à ajuster et d'accélérer les plans de cybersécurité de l'entreprise cliente tout en surmontant les vulnérabilités potentielles qui pourraient freiner son activité.

Ma première tâche dans la participation à cet audit a été de préparer les différents documents en amont de la mission. Cet audit est l'un des plus gros que la practice cybersécurité d'EY France a eu à faire. En effet, l'entreprise souhaitant une mesure totale de son niveau de cybersécurité, tous les domaines du framework CPA doivent être étudiés. L'étude devant couvrir toutes les branches de l'entreprise, certains domaines du CPA seront donc mesurés plusieurs fois en fonction des branches métiers et des divisions régionales ou globales.

Dans ce cadre, la première partie de la préparation a consisté à créer un fichier Excel regroupant l'ensemble des questions du framework CPA d'EY. La source des

questions se situe sur un site interne à EY que l'on ne peut pas extraire. J'ai donc développé un code python qui avait comme rôle de scraper ce site web afin d'en extraire les 515 questions ainsi que leurs sous-domaines et leurs domaines.

Ce script utilise les bibliothèques Selenium et Pandas. Il se connecte au site, navigue vers les pages des domaines, et extrait les questions ainsi que les niveaux de maturité associés.

Les données sont ensuite organisées en tableau et exportées dans un fichier Excel.

Domain	Sub-domain	Description	0 - Nascent	1 - Initial	2 - Repeatable	3 - Defined	4 - Routinely managed	5 - Optimized	Assessment
Cyber Risk Management	Adaptive Governance	How are the Executive Leadership Team (ELT) and Board of Directors engaged with the CSRM?	Processes does not exist; defined capabilities do not exist; performance metrics are not utilized; there is no governance model in place for accountability; performance metrics do not exist; there is no systematic, ongoing, or technology being utilized.	Cyber risk is reported to a body on the ELT and Board of Directors regularly. Cyber risk is reported to the ELT and Board of Directors periodically. Processes are formalized but are not assigned responsibility within the CSRM.	Cyber risk is reported to the ELT and Board of Directors regularly. Cyber risk is reported to the ELT and Board of Directors periodically. Processes are formalized but are not assigned responsibility within the CSRM.	Cyber risk is reported to the ELT and Board of Directors regularly. Cyber risk is reported to the ELT and Board of Directors periodically. Processes are formalized but are not assigned responsibility within the CSRM.	The ELT and Board of Directors establish a view on the top risk management's business strategy, view of cyber risk management. The ELT and Board of Directors have a good understanding of the organization's top cyber risk and how they are being managed. The ELT and Board of Directors have the top cyber risk and how they are being managed.	The ELT and Board of Directors have full visibility into the organization's cyber risk and understand how the risks are being managed. The ELT and Board of Directors have a good understanding of the organization's top cyber risk and how they are being managed. The ELT and Board of Directors have the top cyber risk and how they are being managed.	NA - Not Applicable
Cyber Risk Management	Adaptive Governance	How does management evaluate the effectiveness of the CSRM?	Processes does not exist; defined capabilities do not exist; performance metrics are not utilized; there is no governance model in place for accountability; performance metrics do not exist; there is no systematic, ongoing, or technology being utilized.	The CSRM is reviewed by the organization's internal audit function using internal/industry practices benchmark.	The CSRM is reviewed by the organization's internal audit function using internal/industry practices benchmark.	The CSRM is reviewed by an independent third party using internal/industry practices benchmark.	The CSRM is reviewed by an independent third party using internal/industry practices benchmark.	The CSRM is reviewed by an independent third party using internal/industry practices benchmark.	0 - Nascent
Cyber Risk Management	Adaptive Governance	How does the CSRM collaborate with other established risk, compliance or audit management programs and functions?	Processes does not exist; defined capabilities do not exist; performance metrics are not utilized; there is no governance model in place for accountability; performance metrics do not exist; there is no systematic, ongoing, or technology being utilized.	The CSRM is managed in a siloed manner. No formal collaboration is established with other risk, compliance or audit management programs or functions.	The CSRM only communicates with other risk, compliance or audit management programs and functions on an as-needed basis.	The CSRM only communicates with other risk, compliance or audit management programs and functions on an as-needed basis.	The CSRM only communicates with other risk, compliance or audit management programs and functions on an as-needed basis.	The CSRM only communicates with other risk, compliance or audit management programs and functions on an as-needed basis.	1 - Initial
Cyber Risk Management	Adaptive Governance	How does the Cyber Risk Management Program (CSRM) interact with business functions and units (e.g., Legal, HR and Controls, R&D, Supply Chain, Sales, Finance and Accounting, etc.)?	Processes does not exist; defined capabilities do not exist; performance metrics are not utilized; there is no governance model in place for accountability; performance metrics do not exist; there is no systematic, ongoing, or technology being utilized.	The CSRM is conducted within the context of IT organization, which has very limited interaction with the business functions and business units (BUs). The CSRM only shares cyber information with business functions and BUs per their request or as set by law.	The CSRM interacts with business functions and BUs periodically to request or share relevant cyber risks.	The CSRM interacts with business functions and BUs regularly to request or share relevant cyber risks.	A dedicated cyber risk champion or coordinator has been identified to work business functions and BUs. The risk champion is responsible for ensuring that cyber risk management is integrated into the business's overall risk management and communication plans.	The CSRM establishes a close partnership with business functions and BUs, ensuring that cyber risk management is integrated into the business's overall risk management and communication plans.	2 - Repeatable
Cyber Risk Management	Adaptive Governance	How is cyber risk managed during the organization's merger and acquisition (M&A) and divestiture activity?	Processes does not exist; defined capabilities do not exist; performance metrics are not utilized; there is no governance model in place for accountability; performance metrics do not exist; there is no systematic, ongoing, or technology being utilized.	Cyber risk is rarely considered in the organization's M&A and divestiture processes.	Cyber risk is considered after transaction. Cyber risk assessments are conducted after the core business activities have been established.	Cyber risk is considered before and after transaction. Cyber risk assessments are conducted before and after the core business activities have been established.	A formal cyber risk management M&A and divestiture process is established and deployed prior to the M&A and divestiture activities of the business.	A formal cyber risk management M&A and divestiture process is established and deployed prior to the M&A and divestiture activities of the business.	3 - Defined

Figure 5 - Extrait du fichier Excel des 515 questions du CPA

Pendant cet audit, le client reçoit différents types de livrables.

- Les comptes rendus appelés *Minutes of Meeting*. Ce sont des résumés de chaque entretien structuré selon les sous-domaines du CPA d'EY.
- Les livrables hebdomadaires appelés des *Flash Reports*. Ils ont pour objectif de résumer les différentes actions accomplies durant la semaine, celles qui sont en cours, celles qui restent à faire et l'avancement global de la mission.
- Deux versions de compte rendu final regroupant la globalité de l'étude. Une version est orientée technique, l'autre destinée aux membres exécutifs est axée business.

J'ai été chargé de créer les modèles des comptes rendus d'entretien et du flash report.

Point de vue sur les différents modèles communément appelés templates :

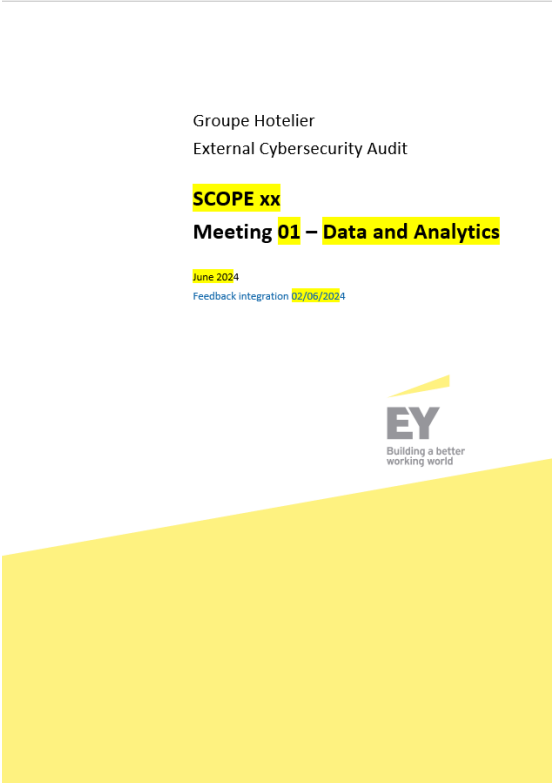


Figure 6 - Page de garde du templates du Minutes of Meeting

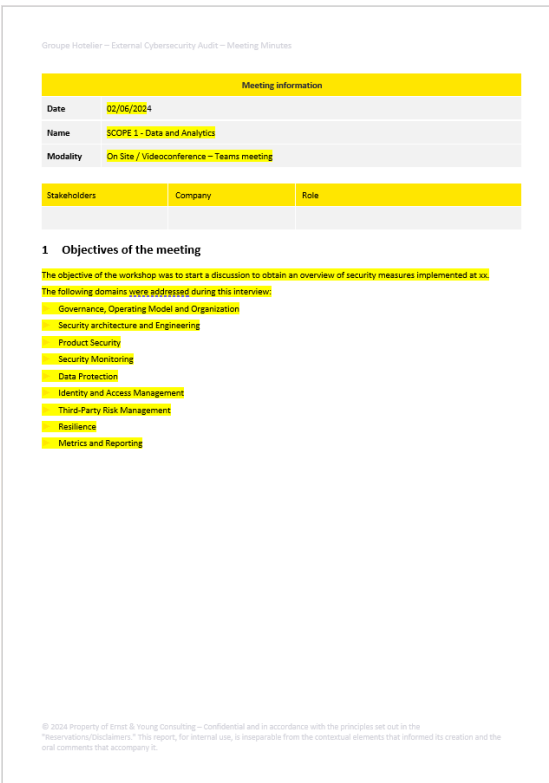


Figure 7 - Page d'introduction du templates du Minutes of Meeting

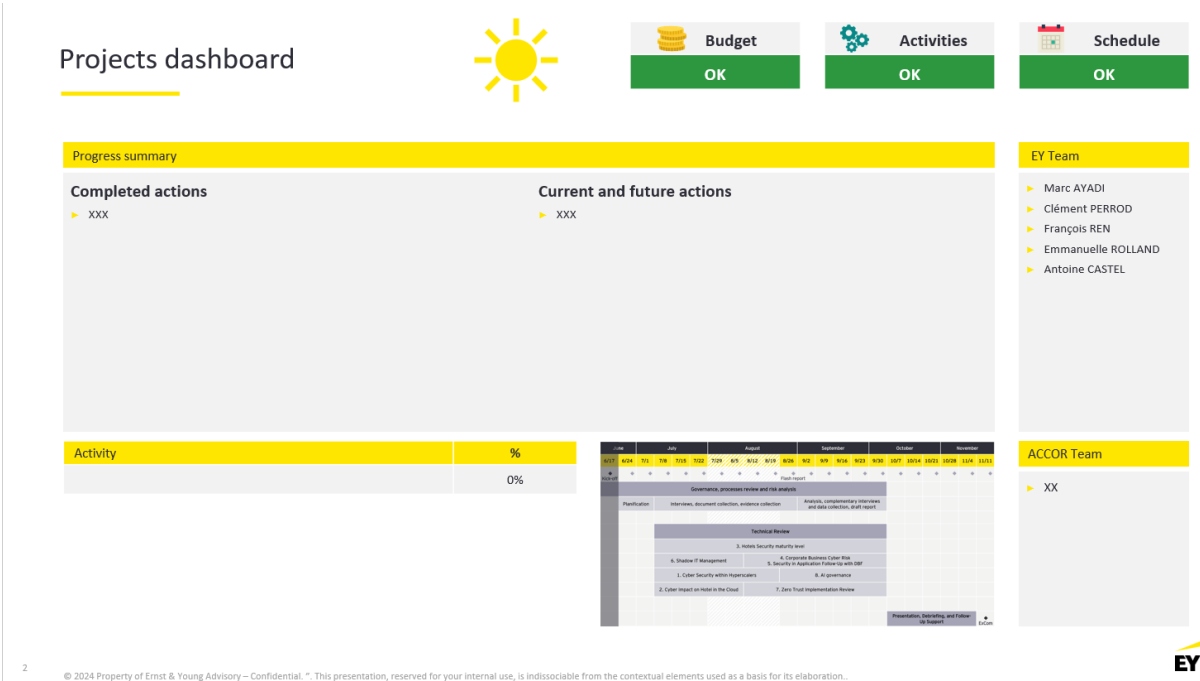
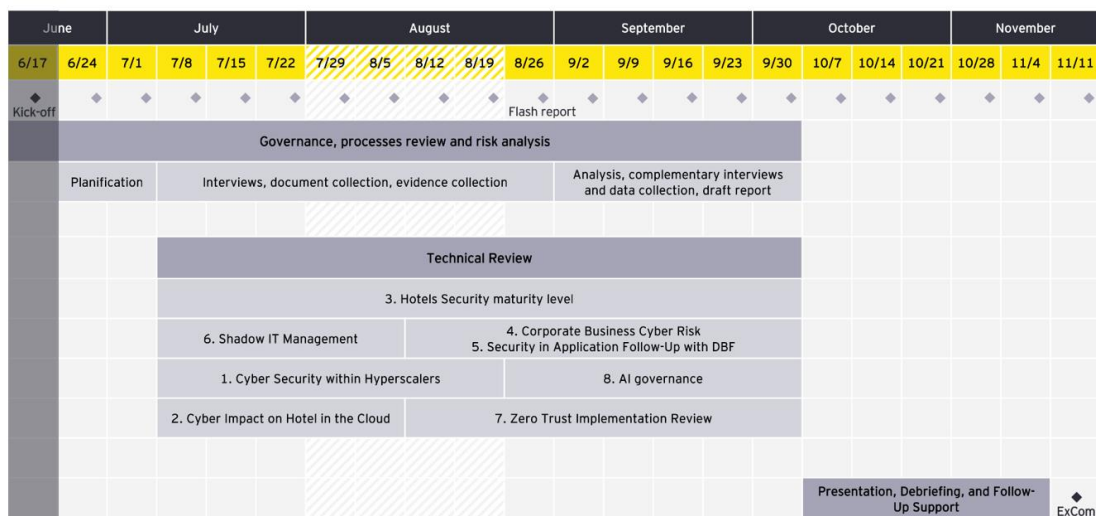


Figure 8 – Dashboard du template du Flash Report

Planning



3

© 2024 Property of Ernst & Young Advisory – Confidential. This presentation, reserved for your internal use, is indissociable from the contextual elements used as a basis for its elaboration.



Figure 9 - Suivi de l'avancement de l'audit selon le planning prévu, template du Flash Report

Une fois les templates réalisés, ma mission a consisté à créer les fichiers Powerpoint regroupant les questions à poser pendant les interviews. Ces documents s'appellent des workshops, leurs créations se basent sur le format CPA et sont couplés aux exigences du client. Le groupe hôtelier a demandé par exemple une analyse de sa migration vers les hyperscalers (le cloud). Une liste de domaine CPA est associée à cette demande et est mise en avant par les Associés afin de compléter cette mesure.

Exigence du Groupe Hôtelier	Réponse d'EY	Domaine du CPA
1. Migration vers les Hyperscalers	Comptez sur notre CPA pour examiner le modèle opérationnel, les politiques et les procédures en place chez le Groupe Hôtelier concernant l'utilisation du IaaS et du PaaS.	<ul style="list-style-type: none"> ▶ Cloud security ▶ Security Architecture and Engineering ▶ Security Infrastructure ▶ Secure Software Development and Management

Figure 10 - Exemple de domaine CPA associé à une demande client

En suivant cette liste mise en avant, je mets en forme un fichier PowerPoint regroupant l'ensemble des questions de ces domaines. J'ai fait un total de vingt workshops différents suivant les exigences du client et aussi des particuliers par exemple pour l'entretien du responsable de la sécurité des systèmes d'information (RSSI).

Protect

Which actions have been taken to mitigate these threats?

Identity and Access Management	Identity and Access Management can be described by defining its core components, identity management and access management. Identity Management refers to the processes associated with managing the entire lifecycle of digital identities and profiles for people, processes, and technology.
Questions <ul style="list-style-type: none">▶ Access management<ul style="list-style-type: none">▶ Credential and Key Management<ul style="list-style-type: none">▶ How are password resets enabled? Are recipients authenticated prior to resetting an authenticator?▶ How are privileged access passwords managed (e.g., password vaulting)?▶ How are recipients authenticated prior to distribution?▶ Federation and Single Sign-On<ul style="list-style-type: none">▶ Are identity federation services in use in the enterprise? Is federated authentication in use?▶ What is the rate of adoption for single sign-on across the organization (e.g., specific businesses, specific platform environment (Windows/AD), etc.)?▶ What solution is used for single sign-on? Is single sign-on fully automated across channels?▶ Multi-Factor Authentication<ul style="list-style-type: none">▶ Is multi-factor authentication in use? What forms? Where? Is use of stronger forms of authentication mandated based on policy, risk, or other criteria?▶ Administration & Intelligence<ul style="list-style-type: none">▶ Architecture and infrastructure<ul style="list-style-type: none">▶ How many domains are in your environment and how is group membership managed? Is there governance around AD group management?▶ Authoritative sources<ul style="list-style-type: none">▶ Entitlement Data<ul style="list-style-type: none">▶ How many applications are connected to your IAM solution and for how many are pulling in entitlement data?▶ Identity Data<ul style="list-style-type: none">▶ What are the authoritative sources for identity data? Who owns the data sources?▶ Governance<ul style="list-style-type: none">▶ Compliance<ul style="list-style-type: none">▶ How does the organization monitor compliance with the IAM program?	Documentation/Evidences <ul style="list-style-type: none">▶ IAM policy, IAM strategy document▶ Third party access processes / Third party onboarding processes▶ Access Management Procedure (Network, physical sites and application accesses)▶ Remote Access Management Policy▶ Procedure for each type of authenticator request▶ RFP related to IAM

28 © 2024 Property of Ernst & Young Advisory – Confidential. This proposal for services, reserved for your internal use, is indissociable from the contextual elements used as a basis for its elaboration EY

Figure 11 - Exemple d'une slide présente dans le workshop deck pour le RSSI

II.1.c Interviews

Une fois les préparatifs terminés, l'audit a démarré. Cette mission est scindée en deux parties bien distinctes. L'audit demandé par le client exige une analyse en profondeur du niveau de maturité de l'entreprise. Pour remplir cette mission, la practice Cybersécurité d'EY doit s'organiser de manière à explorer la gouvernance de l'entreprise et la solidité technique des hôtels.

Dans ce cadre-là, l'équipe organisationnelle d'EY va analyser la dimension de gouvernance du global au régional tandis que l'équipe du laboratoire technique, effectuera des tests de pénétrations techniques et physiques dans 5 hôtels sélectionnés au hasard parmi les différentes branches du groupe hôtelier.

J'ai fait partie de l'équipe organisationnelle pendant cette mission. Cette équipe se composait :

- D'un associé, Clément PERROD, en charge de la gestion de la relation avec le client en direct et de mener les interviews.
- D'un senior consultant, François REN. Il fait office de manager et vérifie les livrables tout en intervenant pendant les échanges avec les clients
- De deux consultants, Emmanuelle ROLLAND et moi-même. Nous étions chargés de la rédaction des différents livrables et de l'interprétation des réponses lors des entretiens.

Cet audit a démarré par une réunion d'ouverture au siège de l'entreprise hôtelière. Elle a permis de réévaluer les objectifs, de présenter la méthode de travail, de comprendre les attentes du RSSI et des différents responsables IT, et d'organiser les premières interviews.

J'ai participé à 18 différentes interviews dont deux dans les locaux de l'entreprise et le

reste sur Teams. Ces entretiens durent entre 30 minutes et deux heures. Voici une liste des différentes personnes qui ont été interviewés :

- Le RSSI Groupe
- Le responsable Conformité IT Groupe
- Le responsable de l'IT Hôtels et des hubs au niveau Groupe
- Le responsable ainsi que deux responsables techniques de la division Infrastructure Sécurité
- L'équipe du SOCVOC (Security and Vulnerability Operation Center)
- L'équipe en charge de la division Sécurité des Applications
- Le RSSI de la région Europe et Moyen Orient Atlantique
- Le responsable du centre de Support Global IT
- La responsable du contrôle interne
- Le responsable de la gestion des données
- Le RSSI de la région Moyen Orient, Asie, Pacifique
- Le vice-président en charge de la conformité globale du Groupe
- Le CEO Amériques
- Le responsable IT Amériques

Chacune de ces interviews a entraîné la rédaction d'un compte rendu faisant le constat des éléments cités et organisés selon les domaines CPA. Je me suis occupé avec Emmanuelle ROLLAND de rédiger chacun de ces comptes rendus.

Une réunion se déroule classiquement selon ce schéma :

- L'associé se présente puis présente l'objectif de la mission, les raisons pour lesquelles cet audit est réalisé, l'expertise qu'EY apporte.
- Nous nous présentons ensuite l'un après l'autre en expliquant notre rôle dans cette mission.
- La personne interviewée se présente, expose son rôle dans l'entreprise et explique de son point de vue ce que fait son service.
- S'en suit un échange d'environ une heure entre l'associé, le senior consultant et le client. L'objectif est de capter le plus d'informations possible, que la personne nous remonte les points techniques ou non qu'il considère important à soulever.
- Pendant cette discussion, notre rôle à Emmanuelle ROLLAND et moi est de prendre en note les éléments importants mais aussi les détails qui peuvent être énoncés.

Une fois la réunion terminée, nous nous répartissons le travail avec Emmanuelle ROLLAND quant à la rédaction du compte rendu (*Minute of Meeting*). J'ai personnellement rédigé 11 comptes rendus sur les 18 réunions auxquelles nous avons participé.

J'ai également réalisé 2 comptes rendus hebdomadaires (*Flash Reports*) sur 7.

Mon stage s'est terminé avant la fin de l'audit, je n'ai donc pu ni participer à la fin des entretiens ni à la rédaction du compte rendu final de la mission. Cependant je me suis occupé de préparer la structure du compte rendu final avant mon départ.

II.2 Outil d'automatisation pour la génération d'un bulletin d'actualité cyber

II.2.a Contexte

Au sein du département de cybersécurité, les équipes d'EY proposent une solution de cyber-veille à ses clients et collaborateurs. Un bulletin intitulé "Cyber Threat Bulletin" (CTB) est publié chaque semaine et deux équipes différentes se partagent son élaboration. Une équipe a en charge de la rédaction des articles hebdomadaires, et l'autre équipe supervise la mise en forme du bulletin avant son envoi. Pour assurer un travail collaboratif efficace, une plateforme de rédaction a été mise en place afin que les deux équipes puissent travailler sur un espace partagé.

Les rédacteurs se composent principalement de consultants juniors tandis que l'équipe des relecteurs se compose de quatre consultants seniors.

Les rédacteurs ont accès à un fil d'informations sur une plateforme d'agrégation de l'actualité liés au monde de la cybersécurité. Chaque rédacteur choisit un article par semaine et en fait une synthèse. Cette synthèse est ensuite postée sur la plateforme de rédaction (un site Wiki.js). Le relecteur en charge du CTB va passer au travers des articles rédigés, les corriger si besoin. Il récupère le texte et les images de chaque article sur chaque page du site, pour les intégrer dans un PowerPoint qu'il va ensuite mettre en forme selon le modèle du CTB. C'est seulement après ces différentes étapes manuelles qu'il l'envoie par mail au client.

J'ai rédigé plusieurs articles pour le CTB durant mon stage.

Le processus des relecteurs est un travail fastidieux et répétitif.

Clément PERROD, Associé Cybersécurité, m'a chargé de reprendre la main sur un projet de création d'un outil pour faciliter le travail des relecteurs en automatisant la génération du PowerPoint selon le templates du CTB et récupérant tous les articles corrigés de la plateforme de rédaction.

La personne ayant initié cet outil m'a transmis son travail et décrit son avancement ainsi que l'architecture du projet. Le travail pour cet outil venait à peine d'être commencé, on ne m'a donc transmis que très peu d'informations.

Le site d'écriture se base sur un serveur en production placé dans le datacenter d'EY. 2 serveurs ont été créés :

- Le serveur de maquette, utilisé pour les tests. Il n'est pas accessible depuis l'extérieur.
- Le serveur de production sur lequel les équipes du CTB travaillent toutes les semaines.

Les deux serveurs se basent sur la distribution Linux Ubuntu 22.04.2 LTS.

L'application du site tourne de façon conteneurisée grâce à un Docker version 24.04.4, déployé avec docker-compose version 1.29.2.

En plus de faire tourner l'application, ce serveur fait aussi tourner une base de données, d'où le docker-compose qui permet de déployer deux conteneurs différents,

un pour le site wiki.js et un pour la base de données PostgreSQL liée au site.

```
services:
  db:
    image: postgres:15.1
    environment:
      POSTGRES_DB: wiki
      POSTGRES_PASSWORD: aLNF.....d4S
      POSTGRES_USER: wikijs
    logging:
      driver: "none"
    restart: always
    volumes:
      - ./db-data:/var/lib/postgresql/data
  wiki:
    image: ghcr.io/requarks/wiki:latest
    depends_on:
      - db
    environment:
      DB_TYPE: postgres
      DB_HOST: db
      DB_PORT: 5432
      DB_USER: wikijs
      DB_PASS: aLNF.....d4S
      DB_NAME: wiki
    restart: always
    volumes:
      - ./config.yml:/wiki/config.yml
      - ./certs:/wiki/certs
    ports:
      - "80:3000"
      - "443:3443"
volumes:
  db-data:
  config.yml:
  certs:
networks:
  default:
    external:
      name: wikinet
```

Figure 12 - Extrait du docker-compose de la plateforme d'écriture

La base de données stocke toute l'architecture du site Wiki.js (page, arborescence, etc.) ainsi que tous les documents présents sur le site (articles, images).

II.2.b Solution Technique

Afin de développer cet outil, on m'a donné accès au laboratoire CSIRT qui a des machines pouvant se connecter aux serveurs du datacenter. On m'a attribué une machine NUC (Next Unit of Computing) d'Intel à laquelle a été lié un compte linux sur la machine de maquette du site de rédaction.

La solution technique s'articule en quatre parties distinctes, toutes développées en Python3 :

1. La récupération des articles de la base de données.
2. La mise en forme du PowerPoint avec les articles selon le modèle du CTB.
3. Le déclencheur de l'outil.
4. L'envoi du Powerpoint généré.

II.2.b.1 Récupération des articles de la base de données

Pour récupérer les articles de la base de données, il faut s'y connecter. C'est avec un simple script utilisant une chaîne de connexion que l'on y parvient :

```
1. def connect_db():
2.     try:
3.         # Créez une URL de connexion correcte pour SQLAlchemy
4.         connection_string = os.getenv('DB_CONNECTION_STRING')
5.
6.         # Créez une instance de l'engine
7.         engine = sqlalchemy.create_engine(connection_string)
8.
9.         # Établir la connexion
10.        conn = engine.connect()
11.
12.        # Retourne l'objet de connexion
13.        return conn
14.    except Exception as e:
15.        print(f"Error connecting to the database: {e}")
16.        exit(1)
17.
```

La ligne de connexion se compose de la sorte :

```
1. DB_CONNECTION_STRING = postgresql://<username>:<password>@127.0.0.1:5432/wiki
```

Une fois connecté, on doit extraire tous les articles corrigés de la semaine. Pour cela une requête SQL est envoyée à la base de données :

```
query = sqlalchemy.text("""SELECT pages.id, pages.title, pages.content, pages.path, tags.title
FROM (pages JOIN "pageTags" on pages.id="pageTags"."pageId") JOIN tags ON
tags.id="pageTags"."tagId" WHERE SUBSTRING(pages.path, 0, 22) = 'CurrentWeek/Validated' ORDER BY
tags.title;""")
```

Ce résultat retourne un texte balisé sous le format HTML.

La bibliothèque BeautifulSoup permet de traiter les différents éléments de l'articles (id, titre, texte, source). Les balises images sont extraites de ce texte. Elles renvoient un nom de fichier en .jpg ou .png récupéré plus tard dans la base de données avec la valeur brute des images. Les balises image et table sont remplacées par des balises

personnalisées permettant de savoir où les positionner dans le traitement pour la création du Powerpoint (Voir annexe).
La sortie finale est un objet Article.

II.2.b.2 Mise en forme du PowerPoint avec les articles selon le modèle du CTB.

Cette partie de code a été la plus complexe. L'objectif est de créer un PowerPoint qui intégrant tous les articles avec leurs images et leurs tableaux en respectant le format du CTB. Chaque article se voit attribuer un label correspondant à l'un des 7 thèmes du modèle :

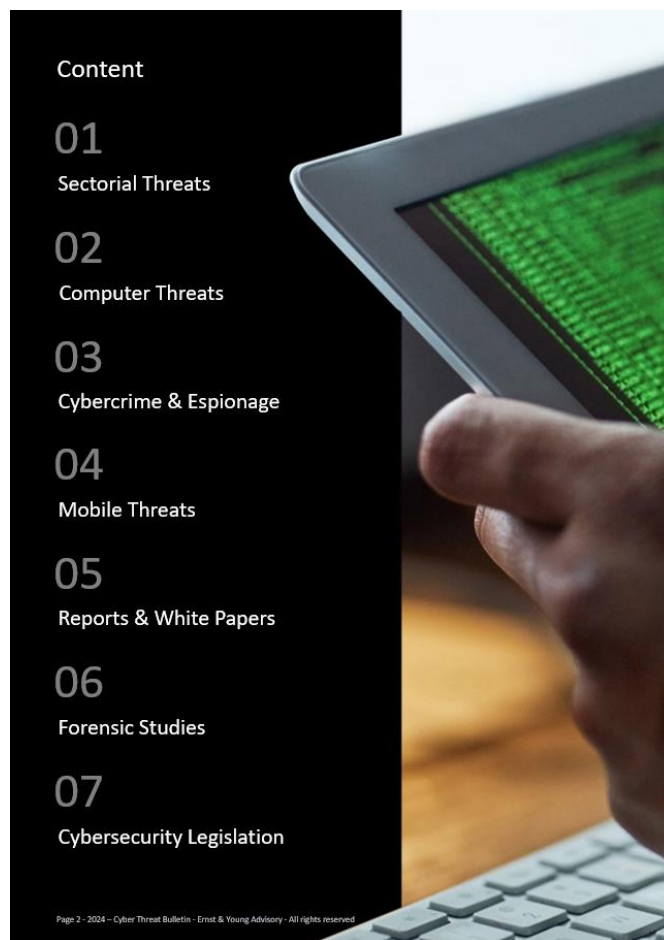


Figure 13 - Extrait de la liste des labels du template du CTB

Les articles doivent apparaitre dans l'ordre suivant ce modèle.
La bibliothèque Python en interaction avec le fichier PowerPoint ne possède que très peu de fonctionnalités. La gestion de l'ordre des pages n'en fait pas partie par exemple. Il a été nécessaire de créer mon propre organisateur de page en utilisant différents dictionnaires couplés à des listes.

La gestion du positionnement des différents éléments dans les articles (titres, corps du texte, images) soulève une nouvelle difficulté.

La bibliothèque ne permet pas la gestion dynamique des éléments présents sur une slide PowerPoint. J'ai ainsi créé une méthode pour adapter la position des éléments sur la slide de sorte qu'ils apparaissent de la même façon que sur le site d'écriture.

La complexité de ce morceau code, qui semble pourtant être une tâche plutôt facile dans ce projet, se traduit en un fichier appelé *powerpoint.py* de plus de 500 lignes.

Ce script génère en sortie un fichier PowerPoint nommé *ctb.pptx*

II.2.b.3 Déclencheur de l'outil.

Le moyen de déclenchement de l'outil est une problématique à part entière.

L'idée de base est de créer un bouton à cliquer dans une page spéciale sur le site de rédaction pour envoyer une requête d'exécution à la machine. Cependant, il n'est pas possible de créer un bouton sur ce site.

Le site de rédaction Wiki.js n'a pas de structure de dossiers au sens traditionnel du terme. Il n'y a pas besoin de créer des dossiers pour créer des nouvelles pages. Elles sont toutes positionnées sur la même racine et se différencient par leur chemin d'accès.

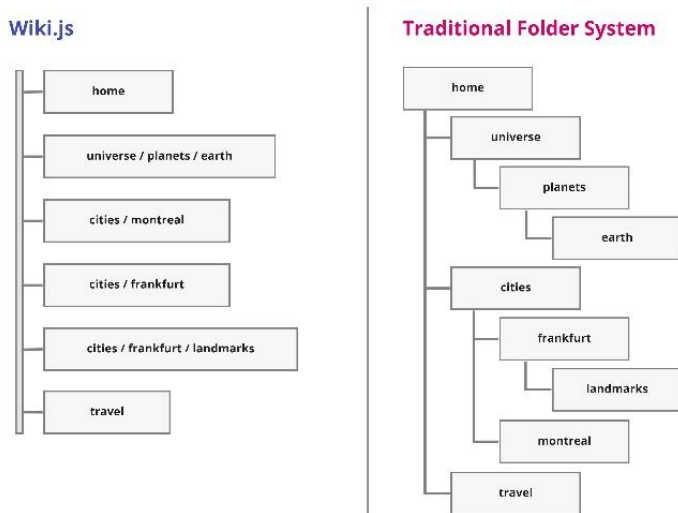


Figure 14 - Structure des dossiers d'un Wiki.js par rapport à un système normal

La structure des dossiers est toujours disponible lors de la création et le déplacement des pages. Les dossiers sont déduits automatiquement des chemins d'accès aux pages.

En conclusion, pour créer un dossier il faut créer une page.

Sur la plateforme CTB, chaque dossier repose sur une page avec des droits d'accès limités aux administrateurs. Ces pages ne sont utiles que pour créer les dossiers et y ajouter des informations importantes.

Chacune page possède un champ commentaire en bas de page. Ces commentaires sont comme tous les éléments du site, stockés dans la base de données.

Par conséquent, j'ai créé une page spéciale pour mon outil appelé CTB Generator. J'ai intégré à la base de données une fonction de déclencheur et de notification qui s'exécute lorsqu'un nouveau commentaire est posté sur la page CTB Generator. Le fichier *listener_server.py* (Voir annexe) est responsable d'intercepter ce déclencheur *new_comment* et de lancer la génération de la présentation PowerPoint.

Generate a Cyber Threat Bulletin

[USAGE RESERVED TO ADMINISTRATORS]

To generate a Cyber Threat Bulletin, you will need to comment under this page any content and then follow the Mandatory part.

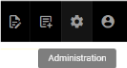
The Cyber Threat Bulletin will be generated using all the articles contained in the Validated folder and will be sent by email to the address linked to the account that published the comment. The email will be sent by cyberthreatbulletin@freylab.fr and you will find the PowerPoint file attached. All the file contained in the validated folder will be moved to the folder corresponding to the actual week.

Before generating it, you must verify the following points:

- The Cyber Threat Bulletin contains a maximum of 7 different topics.
- Each article has only one tag.

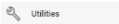
MANDATORY. After publishing the comment:

1. Go to the administration area by clicking on the setting wheel.




Administration

2. On the left side of the page scroll down and then click on the utilities button



Utilities

3. Then go on the Contents tools page



Content
Various tools for pages

4. Use the Rebuild Page Tree tool

Rebuild Page Tree

The virtual structure of your wiki is automatically inferred from all page paths. You can trigger a full rebuild of the tree if some virtual folders are missing or not valid anymore.

[PROCEED](#)

Please note:

- The email might take more than 10 minutes to arrive
- The generated powerpoint might have some difference from the original articles (format, image and table position, bulleted point).
- No colors or text styles are transferred from the Writing Platform to the PowerPoint file
- Feel free to clean the comment section after using it !

Comments

No comments yet.

Figure 15 - Page d'accueil de l'outil d'automatisation du CTB

II.2.b.4 Envoi du Powerpoint généré

Une fois le PowerPoint généré, il est stocké sur la machine. Cependant personne n'y a accès. Pour résoudre ce problème, j'ai écrit un script qui utilise un serveur SMTP, hébergé sur le datacenter d'EY, afin d'envoyer automatiquement le fichier généré par mail à la personne ayant posté le commentaire (Voir annexe).

Pour résumer, voici un schéma de l'architecture applicative du projet :

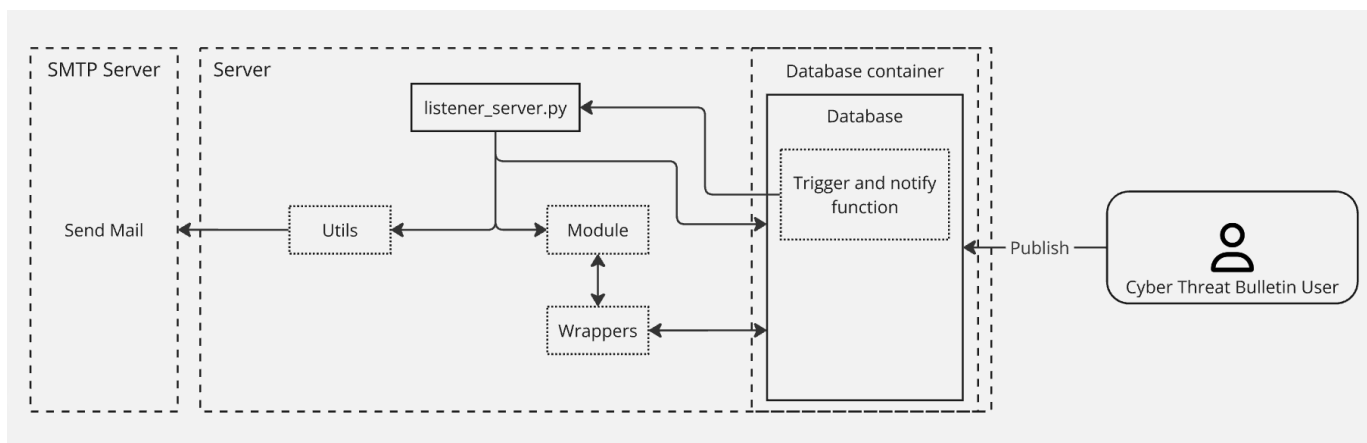


Figure 16 - Schéma d'architecture applicative de l'outil d'automatisation du CTB

- La base de données a une fonction de déclencheur et de notification, un trigger. Il s'exécute lorsqu'un nouveau commentaire est posté sur la page CTB Generator.
- Le fichier *listener_server.py* est responsable d'intercepter ce déclencheur *new_comment*, de lancer la génération de la présentation PowerPoint. Une fois la génération terminée, il envoie le fichier par e-mail et déplace les fichiers dans le dossier de la semaine en cours.
- **Module** implémente la logique de génération PowerPoint.
- **Wrappers** regroupe le code Python et SQL qui gèrent les connexions et interactions avec la base de données.
- **Utils** contient le fichier *mail_sender.py* qui est responsable de la connexion avec le serveur SMTP et de la fonction *sendmail*.

II.2.c Mise en Production

Une fois que l'outil est fonctionnel sur la machine maquette, il est nécessaire de le mettre sur la machine de production.

Ne connaissant pas les différentes règles nécessaires quant à l'ouverture de flux, à la demande d'accès à la machine, ce processus a été long et fastidieux.

Chaque action sur la machine est contrôlée par l'équipe infrastructure.

Chaque ouverture de flux, chaque demande d'accès doit être envoyée avec une justification par mail.

J'ai dû notamment demander une ouverture de flux détaillée pour l'installation des différentes bibliothèques python requises pour le fonctionnement de l'outil.

Bibliothèque	Source
python-pptx	https://files.pythonhosted.org/packages/72/49/6eee83072983473e9905ffddd5c2032b9a0ca4616425560d6d582287b467/python_pptx-0.6.23-py3-none-any.whl
sqlalchemy	https://files.pythonhosted.org/packages/f3/89/ff21b6c7ccdb254fba5444d15afe193d9a71f4fa054b4823d4384d10718e/SQLAlchemy-2.0.31-py3-none-any.whl
python-dotenv	https://files.pythonhosted.org/packages/6a/3e/b68c118422ec867fa7ab88444e1274aa40681c606d59ac27de5a5588f082/python_dotenv-1.0.1-py3-none-any.whl
beautifulsoup4	https://files.pythonhosted.org/packages/b1/fe/e8c672695b37eccc5cbf43e1d0638d88d66ba3a44c4d321c796f4e59167f/beautifulsoup4-4.12.3-py3-none-any.whl
psycpg2-binary	https://files.pythonhosted.org/packages/56/a2/7851c68fe8768f3c9c246198b6356ee3e4a8a7f6820cc798443faada3400/psycpg2_binary-2.9.9-cp312-cp312-muslinux_1_1_x86_64.whl

Figure 17 - Liste des bibliothèques demandées ainsi que leurs sources pour une ouverture de flux pour l'installation sur la machine de production.

Afin que l'outil ait un fonctionnement opérationnel continu, il a été nécessaire de mettre en place lors du déploiement un fichier superviseur. Son rôle est de maintenir l'exécution constante du fichier *listener_server.py*.

```
[program:listener_server]
command=python3 /path/to/listener_server.py
autostart=true
autorestart=true
startsecs=5
stderr_logfile=/var/log/listener_server.err.log
stdout_logfile=/var/log/listener_server.out.log
directory=/path/to/ctb_auto/folder
```

Dans l'exemple ci-dessus, le superviseur déclenche automatiquement le démarrage ou le redémarrage du fichier *listener_server.py* après 5 secondes d'arrêt.

La commande suivante permet de lancer l'outil :

```
sudo supervisorctl start listener_server
```

Elle démarre le superviseur qui va déclencher ensuite l'exécution du fichier *listener_server.py*

II.2.d Livrable

L'outil maintenant terminé, des éléments de documentation sont à rédiger.

- Un document d'architecture technique (DAT)
- Une procédure d'installation technique (PTI)

Le DAT décrit l'architecture nécessaire au projet, le nombre de serveur requis, les

flux entre machines, la structure applicative du code.

Le PTI décrit la procédure d'installation nécessaire au fonctionnement de l'outil, les bibliothèques à installer, la connexion à la base de données, la création d'un superviseur.

Conclusion

Ce stage chez EY Advisory, au sein de la division Cybersécurité, a été une expérience enrichissante et formatrice tant sur le plan technique que professionnel. En intégrant le troisième plus grand cabinet au monde, j'ai découvert une application concrète de la cybersécurité au sein de grandes entreprises. J'ai constaté l'importance accordée au monde de la cybersécurité et c'est en plongeant dans une mission d'audit pour une entreprise hôtelière que j'ai pu apprécier le fonctionnement stratégique et technique tentaculaire d'un aussi grand groupe.

Pendant deux mois, la mission d'audit à laquelle j'ai participé m'a permis de découvrir le fonctionnement informatique d'une entreprise, depuis une vue globale jusqu'à des niveaux techniques détaillés.

Cette expérience m'a permis de repenser mes objectifs professionnels. Souhaitant initialement me diriger vers la cybersécurité, j'ai constaté au cours de ce stage mon attirance pour le monde de l'informatique d'un point de vue global. La cybersécurité est le domaine que je privilégiais car il nécessite une vue holistique du fonctionnement informatique d'une entreprise. Cette approche globale m'attire bien au-delà de la sécurité informatique en elle-même. Bien qu'ayant une aisance pour l'opérationnel, mes préférences tendent vers le décisionnel ou la stratégie.

Fort de cette passion pour l'informatique et malgré l'idée de départ d'orienter mon parcours vers la cybersécurité, je souhaite donner un nouvel axe à mes objectifs et m'orienter vers la stratégie informatique et l'architecture d'entreprise.

L'aspect prestigieux de travailler pour un cabinet de conseil de grande renommée a été pour moi un catalyseur. Le conseil est sans aucun doute une porte d'entrée pour un apprentissage accéléré du monde de l'entreprise. Un des points forts réside dans le fait d'accumuler de nombreuses expériences dans des structures qui peuvent être très différentes en un laps de temps assez court.

Les deux missions auxquelles j'ai participé m'ont permis d'apprendre à m'adapter à un environnement rigoureux et exigeant couplé à une charge de travail importante. J'ai dû apprendre à sortir de ma zone de confort, bien éloigné, de celle d'un étudiant. Cela a donné une nouvelle perspective à mes objectifs de carrière tout en consolidant mon intérêt pour le monde de l'informatique.

Annexes

[Certification d'obtention du badge Cybersecurity Bronze Learning](#)

Code de traitement des articles (article_wrapper.py) :

```
1. from wrappers.basic import connect_db
2. from entities.article import Article
3. from bs4 import BeautifulSoup
4. import os, sqlalchemy
5. from dotenv import load_dotenv
6.
7. # Charger les variables d'environnement depuis le fichier .env
8. load_dotenv()
9.
10. # CLASS POUR LA PROD (BDD)
11. class Article_wrapper:
12.     def __init__(self) -> None:
13.         pass
14.
15.     def get(self):
16.         try:
17.             conn = connect_db()
18.             # PROD
19.             query = sqlalchemy.text("""SELECT pages.id, pages.title, pages.content,
pages.path, tags.title FROM (pages JOIN "pageTags" on pages.id="pageTags"."pageId") JOIN tags ON
tags.id="pageTags"."tagId" WHERE SUBSTRING(pages.path, 0, 22) = 'CurrentWeek/Validated' ORDER BY
tags.title;""")
20.             article_datas = conn.execute(query).fetchall()
21.
22.             # Requête pour récupérer les images
23.             image_query = sqlalchemy.text("SELECT filename FROM assets")
24.             image_datas = conn.execute(image_query).fetchall()
25.             image_dict = {image[0]: image[0] for image in image_datas}
26.
27.             article_list = []
28.             for article in article_datas:
29.                 id = article[0]
30.                 title = article[1]
31.                 text = article[2]
32.                 path = article[3]
33.                 chapter = article[4]
34.                 soup = BeautifulSoup(text, from_encoding="utf-8", features='lxml')
35.
36.                 links = [a['href'] for a in soup.find_all('a', href=True)]
37.                 for a in soup.find_all('a'):
38.                     a.decompose()
39.
40.                 # Récupération des chemins d'image
41.                 images = [os.path.basename(img['src'].strip('/')) for img in
soup.find_all('img') if os.path.basename(img['src'].strip('/')) in image_dict]
42.
43.                 # Remplacer les balises d'image et table par des marqueurs de position
44.                 for img in soup.find_all('img'):
45.                     img.replace_with(f'IMGFLAG:IMAGE:{os.path.basename(img["src"].strip("/"))
}}')
46.
47.                 for table in soup.find_all('table'):
48.                     table.replace_with(f'TBLFLAG:TABLE:{str(table)}')
49.
50.                 text = soup.get_text()
51.                 article_list.append(Article(id=id, title=title, body=text, links=links,
path=path, chapter=chapter, images=images))
52.                 conn.close()
53.
54.             return article_list
55.
56.         except Exception as e:
```

```

57.         conn.close()
58.         print(f"Error: {e}")
59.         return 1, e
60.

```

Code du listener (listener_server.py) :

```

1. import datetime, json, os, select, sqlalchemy, logging, time
2. from dotenv import load_dotenv
3. from sqlalchemy.orm import sessionmaker
4. from module.powerpoint import Module
5. from utils.mail_sender import Mail_sender
6. from wrappers.basic import connect_listener_db, connect_db
7.
8. # Configure logging
9. logging.basicConfig(level=logging.INFO, format='%(asctime)s - %(levelname)s - %(message)s')
10.
11. # Charger les variables d'environnement depuis le fichier .env
12. load_dotenv()
13.
14. def get_current_week_number():
15.     return datetime.datetime.now().isocalendar()[1]
16.
17. def update():
18.     weeknumber = get_current_week_number()
19.     session = None
20.     try:
21.         engine = connect_db()
22.         Session = sessionmaker(bind=engine)
23.         session = Session()
24.
25.         query_path = f"""
26.             UPDATE pages
27.             SET path = REPLACE(path, 'CurrentWeek/Validated/', 'Week{weeknumber}/')
28.             WHERE path LIKE 'CurrentWeek/Validated/%'
29.             AND path != 'CurrentWeek/Validated/00';
30.         """
31.         query_tree = f"""
32.             UPDATE "pageTree"
33.             SET path = REPLACE(path, 'CurrentWeek/Validated/', 'Week{weeknumber}/')
34.             WHERE path LIKE 'CurrentWeek/Validated/%'
35.             AND path != 'CurrentWeek/Validated/00';
36.         """
37.
38.         session.execute(sqlalchemy.text(query_path))
39.         session.execute(sqlalchemy.text(query_tree))
40.         session.commit() # Commit both updates in a single transaction
41.         session.close()
42.         logging.info(f'Articles déplacés en Week{weeknumber}')
43.         return None
44.
45.     except Exception as e:
46.         logging.error(f"Error during SQL execution: {e}")
47.         if session:
48.             session.rollback() # Rollback in case of error
49.             session.close()
50.         return 1, e
51.
52. def send_mail(email):
53.     ctb_file_path = os.getenv('CTB_FILE_PATH')
54.     if not ctb_file_path:
55.         logging.error("CTB_FILE_PATH environment variable not set.")
56.         return
57.     Mail_sender(email, ctb_file_path)
58.
59. def generate_ppt(comment_id, email):
60.     logging.info(f"Generating PPT for comment ID: {comment_id}, Email: {email}")
61.     try:
62.         createReport()

```

```

63.     except Exception as e:
64.         logging.error(f"Error generating PPT: {e}")
65.     try:
66.         send_mail(email)
67.     except Exception as e:
68.         logging.error(f"Error sending mail: {e}")
69.     try:
70.         update()
71.     except Exception as e:
72.         logging.error(f"Error while moving the articles: {e}")
73.     return
74.
75. def createReport():
76.     m = Module()
77.     status, list_id = m.run()
78.     return status, list_id
79.
80. def listen_notifications():
81.     conn = connect_listener_db()
82.     conn.set_isolation_level(0)
83.     cur = conn.cursor()
84.     cur.execute("LISTEN new_comment;")
85.
86.     logging.info("Waiting for notifications on channel 'new_comment'")
87.     while True:
88.         try:
89.             if select.select([conn], [], [], 5) == ([], [], []):
90.                 logging.info(".")
91.             else:
92.                 conn.poll()
93.                 while conn.notifies:
94.                     notify = conn.notifies.pop(0)
95.                     notify_data = json.loads(notify.payload)
96.                     comment_id = notify_data['id']
97.                     email = notify_data['email']
98.                     logging.info(f"Got NOTIFY: {notify.payload}")
99.                     generate_ppt(comment_id, email)
100.        except Exception as e:
101.            logging.error(f"Error in notification loop: {e}")
102.            time.sleep(5)
103.
104. if __name__ == '__main__':
105.     listen_notifications()
106.

```

Script pour l'envoi de mail :

```

1. import datetime, smtplib, os
2. from email.mime.multipart import MIMEMultipart
3. from email.mime.text import MIMEText
4. from email.mime.base import MIMEBase
5. from email import encoders
6. from dotenv import load_dotenv
7.
8. # Charger les variables d'environnement depuis le fichier .env
9. load_dotenv()
10.
11. def Mail_sender(receiver, file_path):
12.
13.     smtp_server = os.getenv('SMTP_SERVER')
14.     smtp_port = os.getenv('SMTP_PORT')
15.     sender_email = os.getenv('SENDER_EMAIL')
16.
17.     # Informations de l'email
18.     date = datetime.datetime.now().strftime("%B %d, %Y")
19.     subject = f'Generated CTB of {date}'
20.     body = f'You can find attached to this e-mail the automatically generated Cyber Threat
Bulletin of {date}'

```

```

21.
22. message = MIMEMultipart()
23. message['From'] = sender_email
24. message['To'] = receiver
25. message['Subject'] = subject
26.
27. # Attacher le corps de l'email
28. message.attach(MIMEText(body, 'plain'))
29.
30. # Attacher le fichier
31. try:
32.     attachment = open(file_path, "rb")
33.     mime_base = MIMEBase('application', 'octet-stream')
34.     mime_base.set_payload(attachment.read())
35.     encoders.encode_base64(mime_base)
36.     mime_base.add_header('Content-Disposition', f'attachment;
filename={file_path.split("/")[-1]}')
37.     message.attach(mime_base)
38.     attachment.close()
39. except Exception as e:
40.     print(f'Erreur lors de l\'ouverture du fichier : {e}')
41.     return
42.
43. try:
44.     # Connexion au serveur SMTP
45.     server = smtplib.SMTP(smtp_server, smtp_port)
46.
47.     text = message.as_string()
48.     server.sendmail(sender_email, receiver, text)
49.     print('Email envoyé avec succès !')
50.
51. except Exception as e:
52.     print(f'Erreur lors de l\'envoi de l\'email: {e}')
53.
54. finally:
55.     server.quit()
56.

```

Bibliographie/Webographie

EY, Rapport de transparence d'EY 2023, consulté le 10/09/2024,
https://www.ey.com/fr_fr/rapport-de-transparence

EY, Site de façade de la branche consulting d'EY, consulté le 10/09/2024,
https://www.ey.com/fr_fr/consulting

EY, Rapport RSE EY 2023, consulté le 11/09/2024,
https://www.ey.com/fr_fr/engagement-rse-mecenat-et-fondation/rapport-rse

EY, Egalité professionnelle femmes-hommes à EY, consulté le 11/09/2024,
https://www.ey.com/fr_fr/careers/egalite-professionnelle-femmes-hommes

Liste des sigles et abréviations

- AIPD : Analyse d'Impact sur la Protection des Données.
- CAC 40 : Cotation Assistée en Continu de 40 valeurs françaises
- CEO : Chief Executive Officer.
- COBIT : Control Objectives for Information and related Technology
- CPA : Cybersecurity Program Assessment
- CSIRT : Computer Security Incident Response Team
- EBIOS RM : Expression des Besoins et Identification des Objectifs de Sécurité, RM pour Risk Manager
- EY : Ernst & Young
- HDS : Hébergeurs de Données de Santé
- IAM : Identity and Access Management
- ISO : International Organization for Standardization
- NIST : National Institute of Standards and Technology
- CSF : Cyber Security Framework
- PASSI : Prestataires d'Audit de la Sécurité des Systèmes d'Information
- RFP : Request For Proposal.
- RSE : Responsabilité Sociétale des Entreprises
- RSSI : Responsable Sécurité des Systèmes d'Information
- SI : Système d'Information

Glossaire

- AIPD : Analyse d'Impact sur la Protection des Données. C'est une étude qui doit être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.
- Blue team – équipe bleu : Dans l'arc-en-ciel des équipes sécurité (rouge, bleu, violet), la *blue team* représente les défenseurs. Lors des exercices, elle lutte contre la *red team*.
- CAC 40 : Cotation Assistée en Continu de 40 valeurs parmi les 100 premières capitalisations françaises
- CEO : Chief Executive Officer. C'est le terme employé pour désigner le président-Directeur Général (PDG) ou encore le Directeur Général (DG) d'une entreprise
- COBIT : le terme signifiait initialement Control Objectives for Information and related Technology ou objectifs de contrôle pour l'information et les technologies afférentes. Avec le temps seul l'acronyme est resté. Il s'agit du référentiel principal de gouvernance des SI. Il est fondé sur les bonnes pratiques collectées auprès d'experts des SI.
- CPA : Cybersecurity Program Assessment : framework d'EY
- CSIRT : Computer Security Incident Response Team
- EBIOS RM : Expression des Besoins et Identification des Objectifs de Sécurité, RM pour Risk Manager. Cela désigne une politique d'administration des risques destinée à accompagner les entreprises et organisations à identifier, évaluer et gérer les risques liés à leur activité.
- EY : Ernst & Young a été renommé EY en 2013
- HDS : Hébergeurs de Données de Santé. La certification réglementaire HDS est basée sur la norme ISO/IEC 27001. Elle permet de démontrer l'engagement en matière de protection des données de santé à caractère personnel.
- IAM : Identity and Access Management – Gestion des identités et des accès
- ISO : International Organization for Standardization – Organisation internationale de normalisation
- NIST : *National Institute of Standards and Technology* du département du commerce américain. En français, il s'agit de l'*Institut national des normes et de la technologie*. Son "cybersecurity framework" se définit comme un ensemble de normes, de lignes directrices et de bonnes pratiques destinées à gérer les risques informatiques
- NIST (National Institute of Standards and Technology) CSF (CyberSecurity Framework) : c'est un ensemble de normes, de directives et de bonnes pratiques pour gérer les risques liés à la cybersécurité.
- Purple team – équipe violette : en cybersécurité, la *purple team* n'est pas permanente. Elle a pour fonction transitoire de superviser et optimiser l'exercice des *red team* et *blue team*.
- Red team – équipe rouge : Il s'agit d'une équipe de hackers éthiques, experts dans la cybersécurité et les méthodes d'attaques des pirates malveillants. Ce

groupe intervient en toute légalité auprès d'une entreprise ou une organisation pour tester la sécurité globale.

- RFP : Request For Proposal. Il s'agit d'un appel à propositions (ou Appel d'Offres - AO) au sens technique et commercial (et non juridique). Une RFP est un processus formel utilisé par les entreprises pour solliciter des offres de fournisseurs potentiels pour un service ou un produit spécifique. Ce mécanisme permet aux acheteurs de comparer différentes propositions selon des critères établis, tels que la qualité, le coût et la durabilité, afin de choisir la meilleure option pour répondre à leurs besoins.
- RSE : Responsabilité Sociétale des Entreprises également appelé responsabilité sociale des entreprises. Cette responsabilité est définie par la commission européenne comme la responsabilité des entreprises vis-à-vis des effets qu'elles exercent sur la société

Table des figures

Figure 1 - Statistique de répartition géographique d'EY dans le monde (Rapport de transparence 2023).	8
Figure 2 - Seconde porte du laboratoire CSIRT, triple authentification requise (badge, empreinte, code).....	11
Figure 3 - Certificat - Cybersecurity Bronze Learning D'EY	14
Figure 4 – Représentation graphique des différents domaines du framework CPA d'EY	16
Figure 5 - Extrait du fichier Excel des 515 questions du CPA.....	20
Figure 6 - Page de garde du templates du Minutes of Meeting	21
Figure 7 - Page d'introduction du templates du Minutes of Meeting	21
Figure 8 – Dashboard du template du Flash Report.....	21
Figure 9 - Suivi de l'avancement de l'audit selon le planning prévu, template du Flash Report.....	22
Figure 10 - Exemple de domaine CPA associé à une demande client	22
Figure 11 - Exemple d'une slide présente dans le workshop deck pour le RSSI.....	23
Figure 12 - Extrait du docker-compose de la plateforme d'écriture.....	26
Figure 13 - Extrait de la liste des labels du template du CTB	28
Figure 14 - Structure des dossiers d'un Wiki.js par rapport à un système normal	29
Figure 15 - Page d'accueil de l'outil d'automatisation du CTB	30
Figure 16 - Schéma d'architecture applicative de l'outil d'automatisation du CTB	31
Figure 17 - Liste des bibliothèques demandées ainsi que leurs sources pour une ouverture de flux pour l'installation sur la machine de production.	32

Résumé

Pendant mon stage chez Ernst & Young Advisory, au sein de la division **cybersécurité**, j'ai eu l'opportunité de travailler sur deux missions différentes.

La première a consisté en la préparation puis la mise en place et enfin la participation à un **audit** de maturité de la sécurité des **systèmes d'information** pour un groupe hôtelier présent au CAC40.

La seconde a porté sur la création d'un outil interne d'**automatisation** de la génération d'un PowerPoint pour un bulletin hebdomadaire d'actualités en cybersécurité.

Ces missions m'ont montré la rigueur attendue dans les grands cabinets de **conseil** et m'ont apporté une vision éclairée du fonctionnement global d'un système informatique dans une entreprise à l'échelle internationale.

Ce stage a été une expérience enrichissante et formatrice tant sur le plan technique que professionnel. EY, troisième plus grand cabinet au monde, m'a exposé à des experts dans le domaine. J'ai acquis de nombreuses compétences en développement, en architecture informatique et en gestion de projet, j'ai aussi compris l'importance de l'intégration des processus au sein d'un environnement informatique et me suis adapté à un mode de travail exigeant nécessitant une rigueur importante.

Abstract

During my internship at Ernst & Young Advisory, in the **cybersecurity** division, I had the opportunity to work on two different projects.

The first mission was to prepare, implement, and ultimately participate in a security maturity **audit** of **information systems** for a CAC40-listed hotel group.

The second focused on creating an internal tool to **automate** the generation of a PowerPoint document for a weekly cybersecurity news bulletin.

These projects demonstrated the level of rigor expected in large **consulting** firms and gave me a comprehensive understanding of how an IT system operates within a global company.

This internship was both an enriching and formative experience, technically and professionally. EY, the third-largest firm in the world, gave me exposure to experts in the field. I gained numerous skills in development, IT architecture, project management, and I also understood the importance of process integration within an IT environment. I adapted to a demanding work style that requires significant attention to detail.