CESI FISA3 INFO 24-27

Mémoire Technique

Assistant RSSI - VISIATIV

Alban CALVO
01/07/2025

Sommaire

1. Présentation de l'entreprise

1.1 Historique

- **Création et évolution** : Visiativ a été fondée en 1987. Depuis sa création, l'entreprise a connu une croissance significative, passant d'une petite entreprise locale à un acteur majeur dans le secteur des technologies de l'information et de la communication.
- **Dates clés** :
  - **1987 – 1997 :** Création d'une structure de distribution de la solution SOLIDWORKS
  - **1997 – 2007 :** Création d'écosystèmes partenaires
  - **2007 – 2017 :** Implantation à l'international et introduction en bourse
  - **2017 – 2023 :** Migration Cloud des solution métiers
  - **2025 :** Rachat par le groupe SNEF

1.2 Secteur d'activité

- **Domaine d'activité** : Visiativ opère dans le domaine des technologies de l'information et de la communication (TIC). L'entreprise se spécialise dans la transformation numérique des entreprises, offrant des solutions logicielles et des services de conseil.
- **Expertise** : Visiativ est reconnue pour son expertise dans les solutions de gestion de l'information, l'industrie 4.0, et les services cloud.

1.3 Produits et services

- **Solutions logicielles** : Visiativ propose une gamme de solutions logicielles pour la gestion de l'information, la collaboration, et la transformation numérique. Parmi ses produits phares, on trouve des solutions de gestion électronique de documents (GED), de gestion de la relation client (CRM), et de planification des ressources d'entreprise (ERP).
- **Services de conseil** : En plus des solutions logicielles, Visiativ offre des services de conseil pour aider les entreprises à optimiser leurs processus et à adopter les nouvelles technologies.
- **Formations** : Visiativ propose également des programmes de formation pour aider les utilisateurs à tirer le meilleur parti de ses solutions logicielles.

Son cœur d'activité historique est la vente de produits Dassault Systèmes. Visiativ assure le conseil, l'intégration et les formations sur ces produits.

Visiativ à su également capitaliser sur la récolte des données du bureau d'études en proposant deux solutions :

- Visiativ PLM : Solution qui permet d'optimiser les échanges en phase de conception d'un produit. Il centralise les informations et permet de structurer les rapports entre les équipes via des processus
- Service Client : Solution qui propose 4 modules pour les relations entre client et fournisseur.

1.4 Organisation

À la suite du rachat par le groupe SNEF, l'organisation des activités de Visiativ est découpée de la manière suivante :

- **Intégration (VAR)** : déployer les logiciels tiers (Dassault) et Visiativ chez les clients en France et à l'international, apporter du service, du conseil et de la formation autour de ces solutions.
- **Edition (vSOFT)** : développement de logiciels métiers dans les domaines du PLM, du service client, de la gestion documentaire et logiciels métiers au support des RH (PROCESS)
- **Conseil (ABGI)** : conseil en financement de l'innovation, en pilotage de projet d'innovation et en pilotage de projets RSE

- **Structure organisationnelle** : Visiativ est une entreprise internationale avec des bureaux dans plusieurs pays. Elle est organisée en différentes divisions, chacune spécialisée dans un domaine spécifique des TIC.
- **Effectifs** : L'entreprise emploie plus de 1600 personnes, réparties dans ses différents bureaux et centres de développement.
- **Culture d'entreprise** : Visiativ met l'accent sur l'innovation, la collaboration, et la satisfaction client. L'entreprise encourage une culture d'entreprise ouverte et collaborative, où les idées nouvelles sont toujours les bienvenues.

1.5 Positionnement sur le marché

- **Clients cibles** : Visiativ cible principalement les entreprises de taille moyenne et grande, dans divers secteurs d'activité tels que l'industrie, les services, et la santé.
- **Stratégie de croissance** : Visiativ poursuit une stratégie de croissance basée sur l'innovation, l'acquisition de nouvelles technologies, et l'expansion internationale.

2. Présentation du sujet et des objectifs

2.1 Contexte

Dans un environnement numérique en constante évolution, la cybersécurité est devenue une préoccupation majeure pour les entreprises de toutes tailles et de tous secteurs. Les cyberattaques sont de plus en plus sophistiquées et fréquentes, ciblant les vulnérabilités des systèmes et des applications. Ces attaques peuvent avoir des conséquences dévastatrices, allant de la perte de données sensibles à des perturbations majeures des opérations commerciales.

Pour Visiativ, il est crucial de garantir la sécurité de ses produits et services afin de protéger les données de ses clients et de maintenir leur confiance. Cette confiance est assurée par le respect de la norme ISO 27001 de la part de Visiativ. Cette norme s'adresse à tous les types d'organismes. Elle définit les exigences pour la mise en place en place d'un Système de Management de la Sécurité de l'Information **(SMSI).** Cela permet d'évaluer les risques liés à la sécurité et élaborer la politique adéquate. Pour conserver cette certification, Visiativ doit obligatoirement réaliser la veille en vulnérabilité.

Visiativ est également soumise à la directive NIS2. Cette directive à pour objectifs de :

- Renforcer la résillience face aux cybermenaces
- Harmoniser les exigences de cybersécurité
- Elargir la portée des secteurs concernés par NIS

Les exigences principales de cette directive sont :

- La mise en œuvre de mesures de sécurité techniques et organisationnelles
- L'obligation de notifier un incident majeur sous 24 heures
- La mise en place d'une gouvernance
- L'évaluation régulière des risques

L'entreprise respecte également le RGPD (Règlement Général sur la Protection des Données à caractère personnel).

La surveillance de la surface d'attaque et la mise en conformité des produits sont des éléments clés pour assurer cette sécurité. En identifiant et en corrigeant les vulnérabilités, Visiativ peut ainsi se protéger contre les cybermenaces.

La surface d'attaque d'une entreprise comprend tous les points d'entrée possibles par lesquels un attaquant pourrait tenter d'accéder à ses systèmes. Cela inclut les applications web, les réseaux, les serveurs, les appareils mobiles, et même les employés. Une surveillance efficace de cette surface permet de détecter les vulnérabilités et de prendre des mesures correctives avant qu'elles ne soient exploitées par des cybercriminels.

2.2 Problématique

Malgré les efforts déployés pour sécuriser ses produits, Visiativ fait face à plusieurs défis en matière de cybersécurité. L'un des principaux problèmes est l'identification des vulnérabilités (CVE) au sein de ses produits et services exposés. Les CVE, ou Common Vulnerabilities and Exposures, sont des failles de sécurité connues et répertoriées qui peuvent être exploitées par des cybercriminels pour accéder aux systèmes, voler des données sensibles ou perturber les opérations.

Les cybercriminels utilisent une variété de techniques pour exploiter ces vulnérabilités, telles que les attaques par injection SQL, les attaques par déni de service (DDoS), et les attaques de phishing. Ces attaques peuvent avoir des conséquences graves, notamment la perte de données, des temps d'arrêt coûteux, et des dommages à la réputation de l'entreprise.

De plus, la mise en conformité des produits avec les normes et réglementations de sécurité est un processus complexe et continu. Les réglementations en matière de cybersécurité évoluent constamment, et les entreprises doivent s'adapter rapidement pour rester conformes. Les non-conformités peuvent entraîner des sanctions financières, une perte de réputation, et une diminution de la confiance des clients.

Par exemple, le RGPD impose des exigences strictes en matière de protection des données personnelles et de notification des violations de données. Les entreprises qui ne se conforment pas à ces exigences peuvent être soumises à des amendes pouvant atteindre 4 % de leur chiffre d'affaires mondial annuel. De même, la directive NIS2 exige que les entreprises des secteurs critiques, tels que l'énergie, les transports, et la santé, mettent en place des mesures de sécurité robustes pour protéger leurs systèmes et leurs données.

2.3 Objectifs

- L'objectif principal de ma mission est d'identifier les vulnérabilités (CVE) présentes au sein des produits Visiativ et de leurs services exposés publiquement, et de proposer des solutions pour les corriger. Pour atteindre cet objectif, plusieurs étapes clés seront réalisées :
- **Audit de sécurité** : Réaliser un audit de sécurité complet des produits Visiativ pour identifier les vulnérabilités potentielles. Cet audit inclura une revue des configurations de sécurité, des tests de pénétration, et une analyse des vulnérabilités connues. L'audit sera réalisé en collaboration avec les équipes de développement et de sécurité de Visiativ pour garantir une couverture complète de tous les produits et services.

- **Utilisation d'outils de scan** : Utiliser des outils comme EASM (External Attack Surface Management) et ZAP (Zed Attack Proxy) pour scanner et identifier les vulnérabilités. EASM permet de surveiller en continu la surface d'attaque externe de l'entreprise, tandis que ZAP est un outil de scan open source qui permet de détecter les vulnérabilités dans les applications web. Ces outils seront utilisés régulièrement pour surveiller les systèmes et les applications de Visiativ et générer des rapports détaillés sur les vulnérabilités identifiées.
- **Proposition de mesures correctives** : Proposer des mesures correctives pour mettre en conformité les produits et réduire les risques de sécurité. Ces mesures peuvent inclure des correctifs de sécurité, des mises à jour de configuration, des formations pour les employés, et des modifications des processus de développement. Les mesures correctives seront priorisées en fonction de leur impact potentiel sur la sécurité et de la facilité de leur mise en œuvre.
- **Validation des mesures** : Valider l'efficacité des mesures mises en place pour garantir la sécurité et la conformité des produits. Cette validation inclura des tests de pénétration supplémentaires, des audits de sécurité, et des revues de conformité. Les résultats de ces tests seront documentés et utilisés pour améliorer continuellement les processus de sécurité de Visiativ.
- En atteignant ces objectifs, cette mission contribuera à renforcer la sécurité des produits Visiativ et à assurer leur conformité avec la politique de sécurité de l'entreprise. Les résultats obtenus seront bénéfiques pour l'entreprise, ses clients, et ses partenaires, en garantissant un environnement numérique plus sûr et plus fiable.

3. Logigramme des étapes de la mission

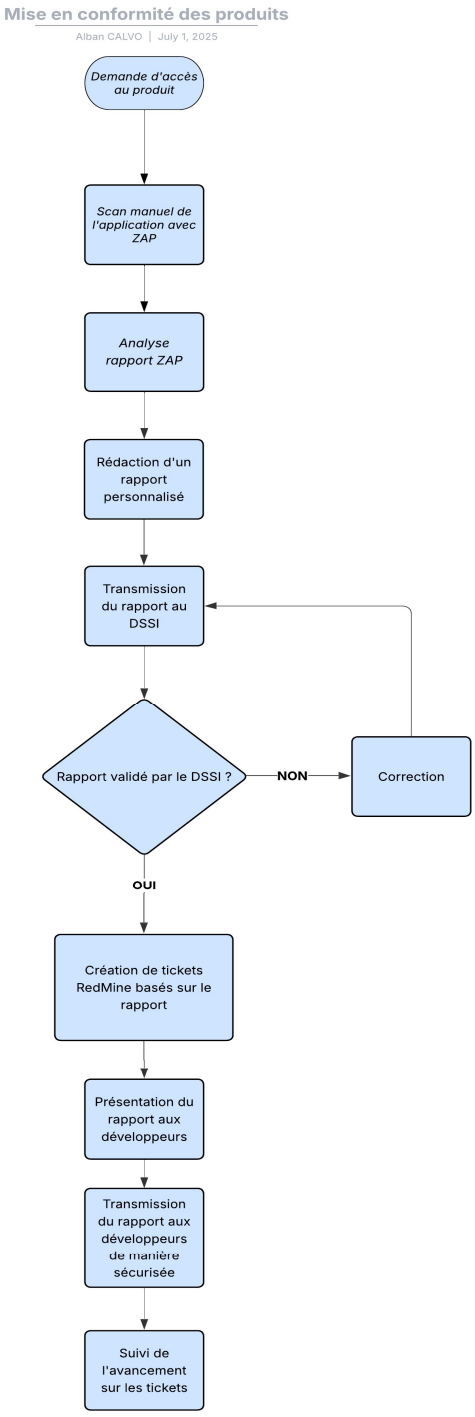


Figure 1 : Logigramme de mise en conformité avec un scan ZAP

La demande d'accès au produit se fait par des échanges avec les TeamLeaders. Je leur demande un accès à la plateforme par le biais d'un environnement de tests dédiés pour ne pas mettre en danger la version du produit en production. Quand cela n'est pas possible, je dois m'assurer de réaliser uniquement des scans passifs (pas de manipulation des données).

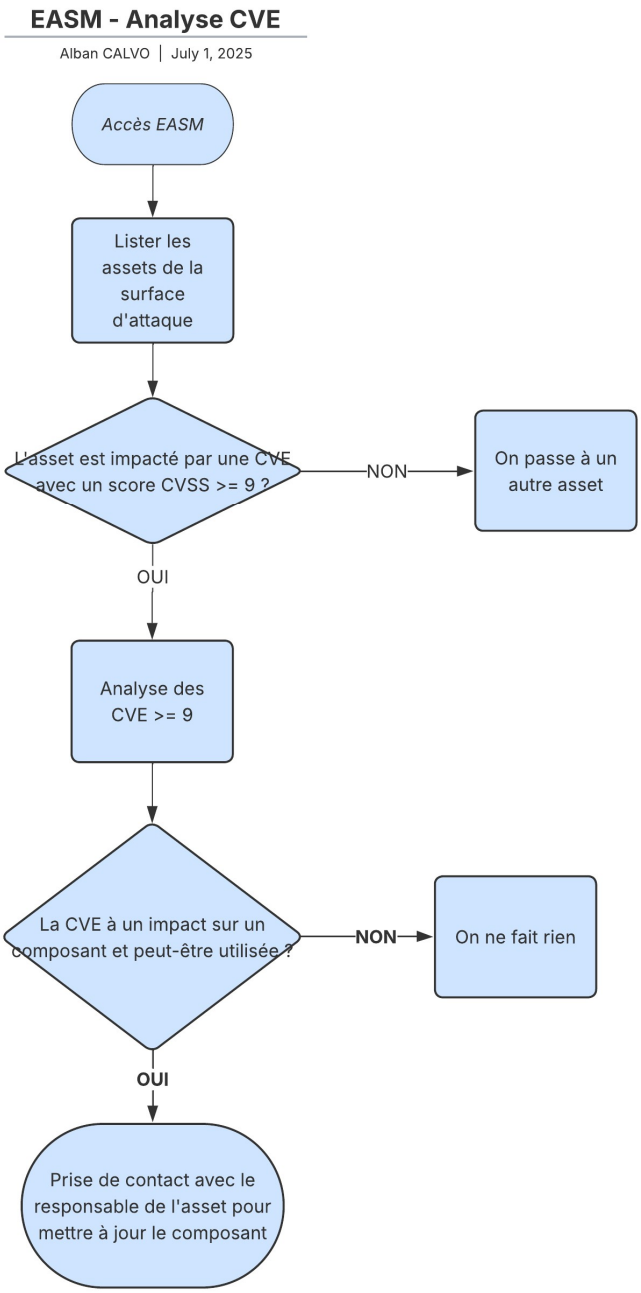


Figure 2 : Surveillance des CVE sur la surface d'attaque

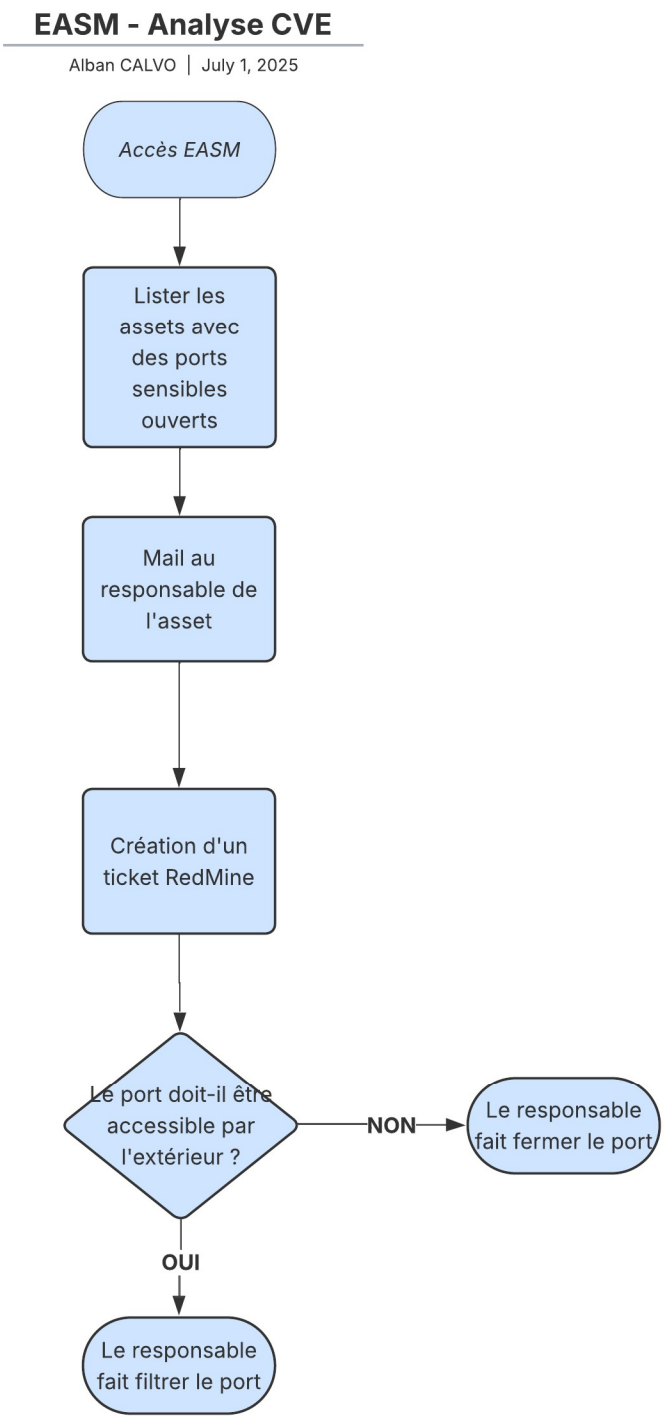


Figure 3 : Surveillance des ports exposés sur la surface d'attaque

4. Développement de la mission

4.1 Recherche et Planification

Description des activités réalisées :

Une des premières étapes de ma mission a été de me renseigner sur les bonnes pratiques en matière de cybersécurité. Cette phase de recherche était cruciale pour comprendre les enjeux et les défis spécifiques liés à la surveillance de la surface d'attaque et à la mise en conformité des produits. J'ai lu de la documentation sur les différents outils utilisés dans le cadre de cette mission, notamment ZAP (Zed Attack Proxy) et EASM (External Attack Surface Management). Ces outils sont essentiels pour identifier et corriger les vulnérabilités dans les systèmes et les applications web.

En plus de la lecture de documentation, j'ai assisté à des présentations de ces outils par le DSSI. Ces présentations m'ont permis de mieux comprendre les fonctionnalités et les capacités de chaque outil, ainsi que les meilleures pratiques pour leur utilisation. Les documentations internes de Visiativ, mises en place par la DSSI, m'ont également fourni des informations précieuses sur les politiques de sécurité de l'entreprise et les procédures à suivre pour identifier et corriger les vulnérabilités.

Outils et méthodes utilisés :

Pour planifier efficacement la mission, j'ai élaboré un plan d'action détaillé. Ce plan incluait les étapes suivantes :

- **EASM :** EASM a été configuré pour surveiller en continu la surface d'attaque externe de Visiativ. Un schéma détaillé, présent en annexe, a permis à l'équipe de définir un plan d'action pour identifier les CVE (Common Vulnerabilities and Exposures) et les ports ouverts sur EASM, ainsi que la démarche à suivre pour traiter ces vulnérabilités. Ce schéma a été un outil précieux pour visualiser les différentes étapes du processus et pour s'assurer que rien n'était omis.
- **ZAP :** J'ai défini une marche à suivre claire pour l'utilisation de ZAP, ainsi que le format des rapports à fournir aux développeurs. Ces rapports incluent des détails sur les vulnérabilités identifiées, leur niveau de criticité, et des recommandations pour les corriger. La standardisation des rapports a permis de s'assurer que les développeurs recevaient des informations cohérentes et complètes pour traiter les vulnérabilités.

4.2 Identification des Vulnérabilités

La deuxième étape de la mission a été consacrée à l'identification des vulnérabilités au sein des produits Visiativ. Cette étape était cruciale pour comprendre les points faibles

des systèmes et des applications de l'entreprise et pour proposer des mesures correctives efficaces.

Description des activités réalisées :

J'ai réalisé un audit de sécurité complet, qui a inclus plusieurs phases clés :

- **Collecte d'informations :** Cette phase a consisté à recueillir des informations détaillées sur les systèmes et les applications de Visiativ. Cela incluait des informations sur les configurations de sécurité, les versions des logiciels utilisés, et les politiques de sécurité en place. La collecte d'informations a été effectuée en collaboration avec les équipes de développement et de sécurité pour garantir une couverture complète de tous les produits et services.
- **Analyse des vulnérabilités :** Utilisant les informations collectées, j'ai effectué une analyse approfondie pour identifier les vulnérabilités potentielles. Cette analyse a inclus des scans de vulnérabilités. Les outils EASM et ZAP ont été particulièrement utiles pour cette phase, car ils permettent de détecter automatiquement les vulnérabilités connues et de générer des rapports détaillés.
- **Documentation des résultats :** Les résultats de l'analyse des vulnérabilités ont été documentés de manière détaillée. Cela incluait des descriptions des vulnérabilités identifiées, leur niveau de criticité, et des recommandations pour les corriger. La documentation des résultats a été essentielle pour communiquer efficacement les découvertes aux équipes et responsables et pour s'assurer que les mesures correctives étaient mises en place.

Outils et méthodes utilisés :

Pour identifier les vulnérabilités, j'ai utilisé des outils spécialisés comme EASM et ZAP. Ces outils ont été choisis pour leur efficacité et leur capacité à fournir des résultats détaillés et précis.

- **EASM :** EASM permet de scanner les systèmes pour identifier les points d'entrée potentiels pour les cyberattaques. Cet outil est particulièrement utile pour surveiller en continu la surface d'attaque externe de l'entreprise et pour détecter les vulnérabilités connues. EASM a été configuré pour scanner régulièrement les systèmes et les applications de Visiativ et pour générer des rapports détaillés sur les vulnérabilités identifiées.
- **ZAP :** ZAP est un outil de test de pénétration open source qui permet de détecter les vulnérabilités dans les applications web. Cet outil a été utilisé pour effectuer des tests de pénétration approfondis sur les applications web de Visiativ et pour identifier les vulnérabilités potentielles. ZAP a été configuré pour générer des rapports détaillés sur les vulnérabilités identifiées, incluant des recommandations pour les corriger.

4.3 Mise en Conformité des Produits

La troisième étape de la mission a consisté à proposer et à mettre en œuvre des mesures correctives pour corriger les vulnérabilités identifiées. Cette étape était cruciale pour s'assurer que les produits de Visiativ étaient sécurisés et conformes aux normes et réglementations de sécurité.

Description des activités réalisées :

J'ai priorisé les mesures correctives en fonction de leur impact potentiel sur la sécurité des produits et de la facilité de leur mise en œuvre. Cela a inclus une évaluation détaillée de chaque vulnérabilité identifiée, de son niveau de criticité, et des ressources nécessaires pour la corriger. Les mesures correctives ont été classées par ordre de priorité, en s'assurant que les vulnérabilités les plus critiques étaient traitées en premier.

Pour ce qui est de la surface d'attaque, j'ai pris contact par email avec les responsables des assets en leur expliquant que certains composants étaient vulnérables à des CVE. Ces communications ont été essentielles pour s'assurer que les responsables étaient informés des vulnérabilités et des mesures correctives nécessaires. Suite à ces contacts, les responsables ont mis à jour leurs composants pour corriger les vulnérabilités identifiées.

Outils et méthodes utilisés :

Pour appliquer les mesures correctives, j'ai utilisé une variété d'outils et de méthodes, incluant des logiciels de gestion de la configuration, des procédures de test, et des revues de code. Ces outils et méthodes ont été essentiels pour s'assurer que les mesures correctives étaient mises en place de manière efficace et pour valider leur efficacité.

4.4 Validation

La quatrième et dernière étape de la mission a été consacrée à la validation des mesures mises en place. Cette étape était cruciale pour s'assurer que les mesures correctives étaient efficaces et pour garantir la sécurité et la conformité des produits de Visiativ.

Description des activités réalisées :

Suite aux échanges avec les responsables des assets, j'ai créé des tickets pour suivre l'avancement des correctifs de sécurité. Ces tickets incluaient des détails sur les vulnérabilités identifiées, les mesures correctives proposées, et les responsables de la mise en œuvre de ces mesures. Le suivi des tickets a permis de s'assurer que les correctifs étaient appliqués de manière efficace.

J'ai suivi l'avancement des correctifs de sécurité et j'ai redemandé des accès aux plateformes de tests pour vérifier que les mesures de sécurité avaient été appliquées. Pour EASM, j'ai refait un scan des CVE présentes et des ports ouverts pour s'assurer que

les vulnérabilités avaient été corrigées et que les systèmes étaient sécurisés. Ces scans de validation ont été essentiels pour confirmer l'efficacité des mesures correctives et pour garantir la conformité des produits avec les normes et réglementations de sécurité.

En conclusion, la mission de surveillance de la surface d'attaque et de mise en conformité des produits Visiativ a permis de progresser. Grâce à une planification rigoureuse, à l'utilisation d'outils de scan et de test efficaces, et à une collaboration étroite avec les équipes de développement et de sécurité, nous avons pu identifier et corriger certaines vulnérabilités critiques. Cependant, l'avancement dans cette tâche reste fastidieux. Certains produits étant trop anciens, il est difficile de les mettre à jour et il faut faire des compromis. Parfois, c'est la communication qui est en jeu, car malgré des efforts de la part de tous, certaines réponses se font parfois attendre car les responsables d'assets ou de produits ont leurs propres occupations qui passent en priorité.

Néanmoins, l'objectif à long terme de corriger ces vulnérabilité étant clair, il reste atteignable, et pour cela, il faut persévérer dans cette démarche.

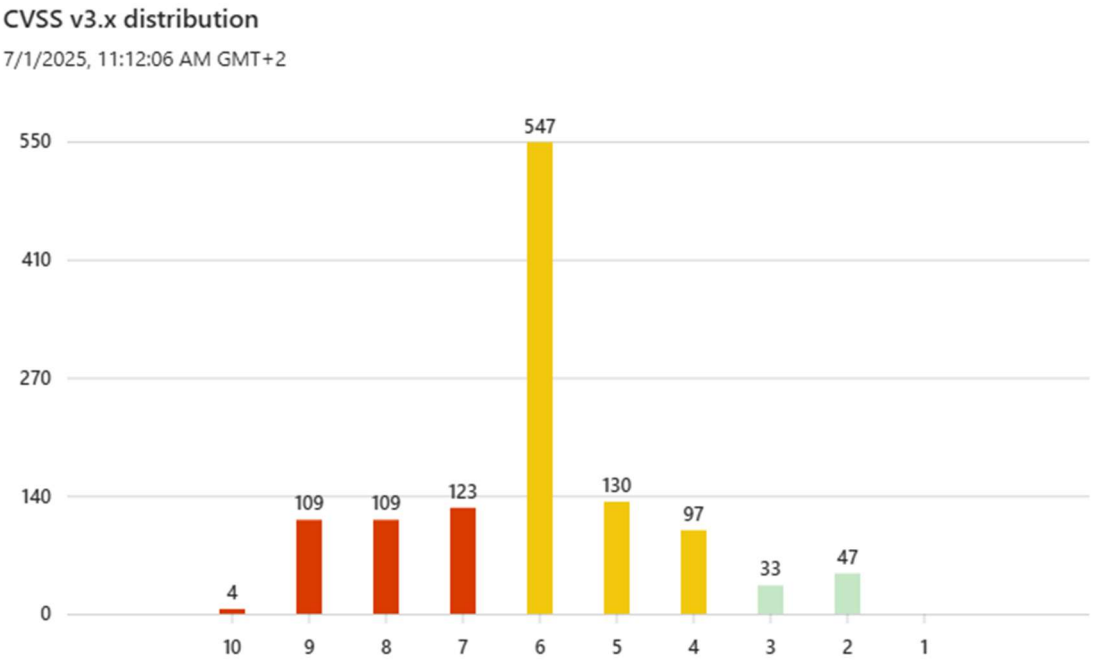
5. Bilan

5.1 Résultats Obtenus

La mission de surveillance de la surface d'attaque et de mise en conformité des produits Visiativ a permis d'identifier un certain nombre de vulnérabilités (CVE) au sein des produits et services exposés. Les vulnérabilités les plus critiques ont été adressées dans le cadre d'un plan de correction à court/moyen terme.

Grâce à l'utilisation d'outils comme EASM et ZAP, nous avons pu scanner efficacement les systèmes et les applications pour identifier les points faibles. Les mesures correctives mises en place ont permis de réduire significativement les risques de sécurité identifiés initialement.

Les indicateurs de performance montrent une amélioration de la sécurité des produits. Ces améliorations ont été rendues possibles grâce à une meilleure planification et à l'utilisation d'outils de gestion de projet efficaces.



5.2 Écarts par Rapport aux Objectifs

Bien que la mission ait atteint certains de ses objectifs, plusieurs écarts ont été observés. Par exemple, l'objectif initial était d'identifier et de corriger l'intégralité des vulnérabilités critiques dans un délai minimum. Cependant, en raison de la complexité de certaines vulnérabilités et des ressources limitées, toutes les vulnérabilités critiques n'ont pas pu être traitées.

Les facteurs de succès de cette mission incluent une planification rigoureuse, l'utilisation d'outils de scan et de test efficaces, et une collaboration étroite avec les équipes de développement et de sécurité de Visiativ. Les défis rencontrés comprenaient des contraintes de temps et de ressources, ainsi que des difficultés techniques liées à la correction de certaines vulnérabilités.

En conclusion, cette mission permet de renforcer sur le long terme la sécurité des produits Visiativ et de les mettre en conformité avec la politique de sécurité de l'entrprise. Les résultats obtenus sont encourageants et montrent l'importance de la surveillance continue de la surface d'attaque ainsi que des applications pour garantir la sécurité des systèmes et des données.

6. Conclusion

6.1 Résumé des Résultats

En conclusion, cette mission de surveillance de la surface d'attaque et de mise en conformité des produits Visiativ a permis d'identifier et de corriger un nombre significatif de vulnérabilités critiques. Grâce à l'utilisation d'outils comme EASM et ZAP, nous avons pu améliorer de manière substantielle la sécurité des produits et services de l'entreprise. Les résultats obtenus montrent une réduction notable des risques de sécurité et une conformité accrue avec la politique de sécurité de Visiativ.

6.2 Impact de la Mission

L'impact de cette mission est encourageant. En renforçant la sécurité de ses produits, l'entreprise peut non seulement protéger ses systèmes et ses données contre les cybermenaces, mais aussi maintenir la confiance de ses clients et partenaires. Les bénéfices pour les parties prenantes sont multiples : les clients bénéficient de produits plus sûrs et plus fiables, les équipes internes peuvent travailler dans un environnement plus sécurisé, et les partenaires peuvent avoir une plus grande confiance dans les solutions proposées par Visiativ.

6.3 Perspectives Futures

Pour continuer à améliorer la sécurité de ses produits, Visiativ devrait envisager plusieurs actions futures. Tout d'abord, il est essentiel de maintenir une surveillance continue de la surface d'attaque pour détecter et corriger rapidement les nouvelles vulnérabilités. Ensuite, il serait bénéfique de continuer à adopter les meilleures pratiques et les normes de sécurité les plus récentes pour rester à la pointe de la protection contre les cybermenaces.

En conclusion, cette mission est un début prometteur et a permis de poser des bases solides pour une amélioration continue de la sécurité des produits Visiativ. Les résultats obtenus sont encourageants et montrent l'importance de la vigilance et de l'innovation en matière de cybersécurité.

7. Annexes

2 SCORE GLOBAL

2.1 NOMBRE DE VULNERABILITES

Le niveau de risque est celui fourni par ZAP

Niveau de risque	Nombre d'alertes
Haut	1
Moyen	4
Faible	10
Pour information	8

2.2 CALCUL DU NIVEAU DE SECURITE

Nombre de points	Niveau de sécurité
0 – 20	Satisfaisant
21 – 50	Perfectible
51 – 100	Insatisfaisant

Le niveau de sécurité est calculé selon le nombre de vulnérabilités par catégories :

- Haut = 10 points
- Moyen = 5 points
- Faible = 2 points
- Pour information = 0 points

La formule du score est donc : S = (nHaut * 10) + (nMoyen * 5) + (nFaible * 2)

Score attribué = Perfectible (50 / 100)

Figure 4 : Score de sécurité calculé pour une application après scan ZAP

3.1 TABLE DES VULNERABILITES

N°	Nom	Niveau de Risque	Avis DSSI
1	Vulnerable JS Library	Haut	A traiter avant la prochaine version
2	Absence de Jetons Anti-CSRF	Moyen	A étudier
3	Content Security Policy (CSP) Header Not Set	Moyen	A étudier
4	Missing Anti-clickjacking Header	Moyen	A étudier
5	Vulnerable JS Library	Moyen	A étudier
6	Big Redirect Detected (Potential Sensitive Information Leak)	Faible	Risque accepté
7	Cookie No HttpOnly Flag	Faible	A traiter avant la prochaine version
8	Cookie with SameSite Attribute None	Faible	A traiter avant la prochaine version
9	Cross-Domain JavaScript Source File Inclusion	Faible	Risque accepté
10	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Faible	A traiter avant la prochaine version
11	Server Leaks Version Information via "Server" HTTP Response Header Field	Faible	A traiter avant la prochaine version
12	Strict-Transport-Security Header Not Set	Faible	A traiter avant la prochaine version
13	Timestamp Disclosure - Unix	Faible	Risque accepté
14	X-AspNet-Version Response Header	Faible	A traiter avant la prochaine version
15	X-Content-Type-Options Header Missing	Faible	A étudier

Figure 5 : Tableau des vulnérabilités présentes

3.2.4 *Vulnérabilité n°5 :*

Moyen	Vulnerable JS Library
Description	La librairie Bootstrap v3.3.7 est vulnérable
Evidence	`* Bootstrap v3.3.7`
Vulnérabilités	CVE-2024-6485 : score CVSS3 = 5.9 CVE-2024-6484 : score CVSS3 = 5.9 CVE-2019-8331 : score CVSS3 = 6.5 CVE-2018-20677 : score CVSS3 = 6.5 CVE-2018-20676 : score CVSS3 = 6.5 CVE-2016-10735 : score CVSS3 = 6.5

Solution : Mettre à jour vers Bootstrap v5.3

Avis DSSI : A étudier

Difficulté : Moyenne

Figure 6 : Exemple d'une vulnérabilité identifiée

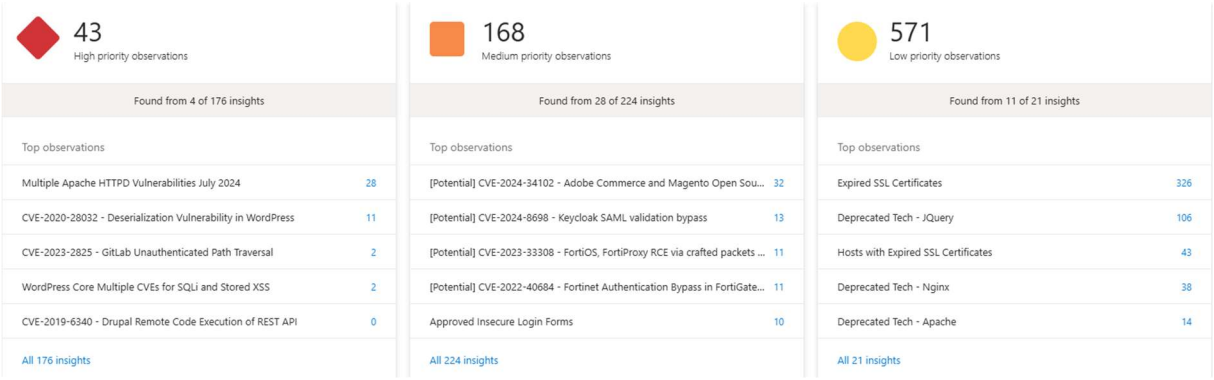


Figure 7 : Vulnérabilités par catégories de criticité sur EASM

7.1 Glossaire

RSSI : Responsable de la Sécurité des Systèmes d'Information.

CVE : Common Vulnerabilities and Exposures, liste publique de vulnérabilités de sécurité.

RGPD : Règlement Général sur la Protection des Données, réglementation européenne sur la protection des données personnelles.

NIS : Network and Information Security, directive européenne sur la sécurité des réseaux et des systèmes d'information.

Surface d'attaque : Ensemble des points d'entrée potentiels par lesquels un attaquant pourrait accéder à un système.

EASM : External Attack Surface Management, outil de gestion de la surface d'attaque externe.

ZAP : Zed Attack Proxy, outil de test de pénétration pour les applications web.

DSSI : Directeur/Direction de la Sécurité des Systèmes d'Information.

GED : Gestion Électronique de Documents, système de gestion des documents électroniques.

CRM : Customer Relationship Management, gestion de la relation client.

ERP : Enterprise Resource Planning, planification des ressources d'entreprise.

Injection SQL : Type d'attaque où des commandes SQL malveillantes sont insérées dans une requête.

DDoS : Distributed Denial of Service, attaque visant à rendre un service indisponible en le surchargeant de requêtes.

Phishing : Technique de fraude où un attaquant se fait passer pour une entité de confiance pour obtenir des informations sensibles.

CVSS : Common Vulnerability Scoring System, système de notation des vulnérabilités de sécurité.

RedMine : Outil de gestion de projets.

SSI : Sécurité des Systèmes d'Information.

MITRE : Organisation à but non lucratif qui gère une base de données CVE.

Header HTTP Strict Transport Security (HSTS) : En-tête HTTP qui force les connexions sécurisées via HTTPS.

Header Content Security Policy (CSP) : En-tête HTTP qui aide à prévenir les attaques de type Cross-Site Scripting (XSS).

Header X-Frame-Options : En-tête HTTP qui contrôle si une page peut être affichée dans un cadre ou une iframe.

HTTP Only Secure : Attribut de cookie qui empêche l'accès via JavaScript et limite la transmission aux connexions sécurisées.

7.2 Bibliographie

7.2.1 Documentation interne

- Header http Strict Transport Security
- Header Content Security Policy
- Header X-Frame-Options
- HTTP Only Secure

7.2.2 Documentation ZAP

- **Installation :** https://www.zaproxy.org/getting-started/
- **Automatisation :** https://www.zaproxy.org/docs/automate/
- **Rapports :** https://www.zaproxy.org/docs/alerts/

7.2.3 Documentation Microsoft EASM

- **Vue d'ensemble :** https://learn.microsoft.com/fr-fr/azure/external-attack-surface-management/overview
- **Ressources & inventaire :** https://learn.microsoft.com/fr-fr/azure/external-attack-surface-management/understanding-inventory-assets
- **Découverte :** https://learn.microsoft.com/fr-fr/azure/external-attack-surface-management/what-is-discovery
- **Déploiement :** https://learn.microsoft.com/fr-fr/azure/external-attack-surface-management/deploying-the-defender-easm-azure-resource
- **Tutoriel :** https://learn.microsoft.com/fr-fr/azure/external-attack-surface-management/discovering-your-attack-surface

7.2.4 CVE

- **MITRE :** https://attack.mitre.org/
- **ANSSI :** https://cert.ssi.gouv.fr/alerte/