Compte Rendu Détaillé du Projet : Veille Technologique Collaborative

Date de rendu : 04/04/2025

Durée du projet :

**1. Contexte et Objectifs**

Objectif principal : Mettre en place un système de veille technologique collaboratif pour surveiller les vulnérabilités Zero-Day, partager les connaissances en temps réel, et améliorer la réactivité de l’équipe face aux menaces émergentes.

Livrables attendus :

- Environnement de veille opérationnel (Feedly pour l’agrégation de flux, Discord pour la collaboration).

- Fiches techniques détaillées sur les vulnérabilités critiques (analyse CVSS, correctifs, impact).

- Synthèses des webinaires suivis et diffusion des connaissances en interne.

Contraintes :

- Centraliser les informations pour éviter la dispersion des données.

- Assurer une mise à jour régulière des fiches techniques (réactivité face aux Zero-Day).

**2. Méthodologie et Organisation**

Rôles de l’équipe :

- Coordinateur de la veille : Gestion des outils (Feedly, Discord), validation des sources.

- Rédacteur technique : Analyse des vulnérabilités et rédaction des fiches.

- Animateur de communauté : Organisation des échanges sur Discord, planification des webinaires.

- Documentaliste : Archivage des ressources et vérification des références.

Outils utilisés :

- Feedly : Agrégation de flux RSS (CVE, blogs spécialisés, comptes Twitter d’experts).

- Discord : Création de salons dédiés (#zero-day, #webinaires, #alertes).

- Notion/Google Docs : Stockage des fiches techniques et des comptes rendus.

- Zoom/Teams : Participation aux webinaires et enregistrement des sessions.

**3. Phases du Projet**

**Phase 1 : Configuration de l’environnement de veille (2h)**

- Configuration de Feedly :

- Création de collections thématiques : "Zero-Day", "Menaces Récentes", "Outils de Sécurité".

- Ajout de sources : Flux RSS du MITRE CVE, Krebs on Security, Palo Alto Networks Blog.

- Mise en place de Discord :

- Création de salons :

- #alertes-en-direct : Notifications des nouvelles vulnérabilités.

- #fiches-techniques : Partage des analyses.

- #replay-webinaires : Accès aux enregistrements.

- Intégration de bots :

- RSS Bot : Synchronisation des flux Feedly vers Discord.

- GitHub Bot : Suivi des mises à jour des projets open source.

**Phase 2 : Rédaction des fiches techniques (6h)**

- Structure type d’une fiche :

- Titre : Nom de la vulnérabilité (exemple : "CVE-2023-XXXX : Vulnérabilité RCE dans Apache Tomcat").

- CVSS Score : Indice de gravité (exemple : 9.8/10).

- Impact : Scénarios d’exploitation (exemple : Exécution de code à distance).

- Correctifs : Versions patchées, solutions temporaires.

- Références : Liens vers les advisories officiels.

- Processus de validation :

- Revue par un expert avant publication.

- Ajout de tags dans Notion pour un filtrage rapide (exemple : #Windows, #RCE).

**Phase 3 : Participation aux webinaires et partage interne (4h)**

- Sélection des webinaires :

- Critères : Pertinence (Zero-Day, bonnes pratiques), intervenants reconnus.

- Exemples : Webinaires Black Hat, OWASP, SANS Institute.

- Synthèse des apprentissages :

- Format : Fiche résumée en 5 points clés.

- Diffusion : Partage dans le salon #replay-webinaires sur Discord et sur Notion.

- Exemple de synthèse :

"Webinaire : Tendances des attaques Zero-Day en 2024

- Augmentation de 40 % des exploitations de vulnérabilités non patchées.

- Secteurs les plus ciblés : Santé, Énergie.

- Recommandation : Mettre en place un double système de sauvegarde."\*

**Phase 4 : Collaboration et amélioration continue (2h)**

- Retours d’expérience :

- Enquête anonyme auprès de l’équipe pour évaluer l’utilité des outils.

- Points forts : Réactivité sur les Zero-Day, accessibilité des fiches.

- Axes d’amélioration : Réduire le bruit dans les alertes Feedly.

- Optimisation des flux :

- Filtrage des sources peu pertinentes dans Feedly.

- Ajout de mots-clés pour prioriser les alertes (exemple : "critical", "exploit").

**4. Résultats et Livrables**

Environnement de veille opérationnel :

- 15 sources de flux RSS actives dans Feedly.

- 3 salons Discord actifs avec 95 % de participation de l’équipe.

Fiches techniques produites :

- 10 fiches sur des Zero-Day critiques (exemple : CVE-2023-1234, CVE-2023-5678).

- Temps moyen de rédaction : 1h par fiche (incluant la validation).

Webinaires et partage :

- Participation à 5 webinaires en 1 mois.

- 100 % des synthèses partagées dans les 24h suivant l’événement.

5. Défis Rencontrés et Solutions

Problème 1 : Surcharge d’informations dans Feedly

- Solution : Utilisation de filtres par mots-clés (exemple : "zero-day", "critical").

Problème 2 : Retard dans la rédaction des fiches techniques

- Solution : Création d’un modèle prédéfini pour standardiser le processus.

Problème 3 : Engagement variable sur Discord\*

- Solution : Organisation de sessions de questions-réponses hebdomadaires pour stimuler les échanges.

6. Bilan et Perspectives

Points forts :

- Centralisation efficace des informations critiques.

- Amélioration de la réactivité face aux menaces Zero-Day.

Améliorations futures :

- Automatiser la génération de fiches techniques via IA (exemple : ChatGPT pour les résumés).

- Intégrer un système de scoring des vulnérabilités basées sur l’impact métier.

**Annexes**

Annexe 1 : Exemple de fiche technique

Titre : CVE-2023-XXXX – Vulnérabilité RCE dans Microsoft Exchange

- CVSS : 9.1 (Critique)

- Impact : Permet une exécution de code à distance via une requête non authentifiée.

- Correctifs : Appliquer le correctif KB1234567.

- Références : Lien vers l’advisory Microsoft.

Annexe 2 : Capture d’écran du salon Discord

[Description : Salon #alertes-en-direct avec des notifications de nouvelles vulnérabilités.]

Annexe 3 : Modèle de synthèse de webinaire

Titre : Résumé du webinaire "Détection des attaques Zero-Day"

- Date : 15/10/2024

- Intervenant : John Doe (Expert en cybersécurité)

- Points clés :

1. Utiliser les outils EDR pour une détection en temps réel.

2. Mettre à jour les systèmes dans les 72h après la publication d’un correctif.

Équipe Projet

- Coordinateur de la veille : Axel

- Rédacteur technique : Axel

- Animateur de communauté : Axel

- Documentaliste : Axel