w	**BTS Services Informatiques aux Organisations Opt SISR**	**Gabriel Pilarski** SIO 26

Projet Personnel Encadré

Numéro 2

05/02/2026

Présentation du projet

1. Contexte de l'entreprise

L'entreprise fictive **TechSolutions** est une PME spécialisée dans le développement d'applications web. Elle compte une vingtaine d'employés et manipule des données sensibles liées à ses clients (identifiants, projets, documents internes).

Jusqu'à présent, l'infrastructure informatique de l'entreprise était fonctionnelle mais peu sécurisée. Aucune solution de supervision ni de centralisation des journaux n'était en place, et les politiques de sécurité étaient limitées.

---

2. Incident de sécurité

L'entreprise a récemment été victime d'une cyberattaque ayant entraîné une compromission partielle de son système d'information.

2.1 Origine de l'attaque

Un employé a reçu un email de phishing imitant un service interne. En cliquant sur un lien frauduleux, il a saisi ses identifiants professionnels, qui ont été récupérés par un attaquant.

2.2 Déroulement de l'attaque

Grâce aux identifiants compromis, l'attaquant a pu :

- Accéder au réseau interne de l'entreprise
- Effectuer une reconnaissance du réseau (scan des machines et des services)
- Identifier les serveurs critiques, notamment :
    - le contrôleur de domaine (Active Directory)
    - le serveur de fichiers
    - le serveur web

L'attaquant a ensuite tenté plusieurs actions malveillantes :

- Accès à des partages de fichiers contenant des documents sensibles
- Tentatives d'élévation de privilèges
- Multiples connexions suspectes sur le domaine

L’absence de supervision n’a pas permis de détecter rapidement ces activités. Suite à cet incident, la direction a décidé de renforcer la sécurité de son infrastructure.

L’entreprise TechSolutions a fait appel à une société spécialisée en cybersécurité nommée **Securos**. Cette entreprise externe a pour mission d’accompagner TechSolutions dans la sécurisation de son système d’information.

Dans ce cadre, Securos réalise un audit de l’infrastructure existante afin d’identifier les vulnérabilités exploitées lors de l’attaque. À la suite de cette analyse, elle met en place des solutions adaptées, notamment l’implémentation d’outils de supervision et de centralisation des logs tels que Zabbix et Graylog, ainsi que l’application de bonnes pratiques de sécurité.

Securos assure également un suivi continu de l’infrastructure, permettant de détecter rapidement toute activité suspecte et de garantir une meilleure protection contre de futures attaques.

3. Objectifs du projet

L’objectif de ce projet est de :

- Reconcevoir une infrastructure sécurisée
- Mettre en place des outils de supervision et de journalisation
- Détecter les comportements anormaux
- Réagir efficacement en cas d’incident
- Prévenir de futures attaques

---

4. Infrastructure de l’entreprise

4.1 Équipements réseau

- Un switch
- Un poste client

4.2 Serveurs

Contrôleur de domaine

Un serveur Windows Server avec les rôles suivants :

- Active Directory : gestion centralisée des utilisateurs et des droits
- DNS : résolution de noms interne

Serveur Web + zabbix

Un serveur Linux (Ubuntu) héberge le site web de l'entreprise et sert également de poste Zabbix.

Serveur Graylog

Un serveur Linux (Ubuntu) héberge le logiciel Graylog de l'entreprise.

---

5. Mise en place de la supervision

Afin de détecter rapidement toute activité suspecte, des outils de supervision ont été déployés.

5.1 Supervision des équipements

L'outil Zabbix a été mis en place pour surveiller :

- L'utilisation CPU et mémoire des serveurs
- L'état des services
- La disponibilité des machines

Des alertes sont générées en cas de comportement anormal.

5.2 Centralisation des logs

L'outil Graylog a été installé pour :

- Collecter les journaux des serveurs.
- Analyser les connexions
- Détecter des tentatives d'intrusion

Grâce à cet outil, il est possible d'identifier :

- Des connexions échouées répétées
- Des accès inhabituels
- Des comportements suspects

---

8. Conclusion

Ce projet a permis de mettre en évidence l'importance de la cybersécurité au sein d'une entreprise.

La mise en place d'une infrastructure sécurisée, associée à des outils de supervision comme Zabbix et Graylog, permet :

- Une meilleure visibilité sur le système d'information
- Une détection rapide des incidents
- Une réaction efficace face aux menaces

Ce PPE illustre les bonnes pratiques en matière de sécurisation des systèmes et des réseaux dans un contexte professionnel réel.

ANNEXE :

Zabbix :