Standard Operating Procedure

Cette procédure, appelé SOP (Standard Operating Procedure) en anglais comporte plusieurs défis.

Cette page vous présente notre méthodologie en ce qui a trait aux faux positifs que vous observez sur votre site web.
Cet article s'adresse donc seulement aux situations de sites web qui affichent des "faux positifs". Nous ne touchons pas le sujet des filières.

SOP Client - Faux positif sur un site web

Version: 1.0

Public cible: OBNL, PME, équipes non techniques
Objectif: Retirer un blocage injustifié et rétablir la réputation d'un site web, sans prendre de risques.

Contexte

Un **faux positif** survient quand un service de sécurité (antivirus, filtre web, navigateur, fournisseur de réputation) classe votre site comme **malveillant/phishing** alors qu'il est légitime.

Résultat attendu

- Le site n'est plus bloqué par les principaux outils et listes de réputation.
- Vous avez des preuves de nettoyage, un plan de prévention et un dossier de support complet.

---

1) Mesures immédiates (0-30 minutes)

- **Ne paniquez pas et ne faites pas de changement au hasard.**
- Activer un mode maintenance si vous le pouvez.
- Notez
    - Date/heure du premier signalement
    - Outils qui bloquent (navigateur, antivirus, réseau d'entreprise, etc.)
    - URL exacte signalée (page précise, pas juste le domaine)
- Faire des captures d'écran des avertissements.

---

2) Vérification de base (30-90 minutes)

- Vérifier vos accès admin:
    - Liste des comptes administrateurs
    - Recherchez tout compte inconnu
- Mettez a jour:

    - Votre CMS
    - Vos plugins/modules
    - Vos .css de thèmes/skins
- Cherchez des signes d'injection:
    - redirections étranges
    - scripts inconnus
    - popups inhabituels

Si vous voyez un de ces signes, traitez-le comme une vraie de compromission et passez au point 3.

---

3) Nettoyage minimal recommande (si doute)

- Changez tous vos mots de passe:
    - admin CMS
    - FTP/SFTP
    - hébergeur
    - base de données
- Activez la double authentification (2FA) si disponible.
- Supprimez:
    - plugins non utilisés
    - thèmes non utilisés
- Vérifier que le site force HTTPS

---

4) Tests croisés de réputation

- Testez le domaine et l'URL exact avec:
    - un scanner multi-moteurs
    - un scanner web
- Notez les résultats et les moteurs qui déclenchent l'alerte.

But: identifier **qui bloque quoi** pour demander une correction ciblée.

---

5) Demandez une reclassification (la clé du faux positif)

- Soumettez une demande de faux positif à
    - L'éditeur AV / réputation qui bloque
    - Google Safe Browsing si le navigateur montre une alerte "site dangereux"
- Fournir un dossier clair:
    - Domaine + URL précise
    - Description de votre organisation et du site

- Preuves de mises a jour/nettoyage
- Date du début du problème
- Captures d'écrans des alertes

---

6) Vérification post-correction

- Attendre la mise a jour des listes (peut être progressive selon les fournisseurs)
- Re-tester sur:
  - un autre réseau, un autre appareil
  - un autre navigateur
- Confirmez que l'alerte est levée.

---

7) Prevention (a conserver)

- Activez:
  - sauvegardes quotidiennes
  - WAF si possible
  - surveillance d'integrité des fichiers
- Mettre un calendrier:
  - mises a jour mensuelles mini
  - audit trimestriel

---

8) Quand escalader

Contactez-nous si:

- l'alerte persiste après vos demandes de reclassification
- vous suspectez une injection ou une redirection
- vous ne connaissez pas l'origine du blocage
- votre site est lié a une collecte de dons, boutique ou base membres

---

Modèle de message court a copier-coller

si vous avez besoin de nous

Primo, préparez un dossier qui nous explique qui, quoi, quand, comment. utilisez ce modèle ci-dessous.

```
Bonjour,
Notre site [DOMAINE] semble être bloqué comme phishing/malware.
Nous croyons qu'il s'agit d'un faux positif.
URL signalé: [URL]
Date du début: [DATE]
Actions à effectuer: mises a jour CMS/plugins, vérification des comptes admin, changement
des mots de passe, activation HTTPS.
Pouvez-vous réanalyser et corriger la classification si confirme légitime?
Merci.
```

Liens intéressants

- Vous êtes ici
- Vérifiez votre site

Questions

Contactez votre humble serviteur par email via cette adresse: daniel@telepartout.com avec le titre: J'ai besoin d'aide

TelePartout.org - Cybersécurite accessible, humaine et utile