MODÈLE DE CONFORMITÉ GRC

Intégration de la Data-Shield IPv4 Blocklist

1. PRÉSENTATION DU DISPOSITIF

1.1 Nature et fonctionnement de la blocklist

La Data-Shield IPv4 Blocklist, développée et maintenue par Duggy Tuxy (Laurent Minne), constitue une source de renseignement sur les menaces cyber mise à jour quotidiennement. Cette liste recense jusqu'à 110 000 adresses IPv4 identifiées comme sources d'activités malveillantes, collectées via des sondes de sécurité déployées mondialement et centralisées sur une plateforme HIDS/SIEM auto-hébergée et sécurisée.

La méthodologie repose sur la discipline de la Deceptive Security basée sur une analyse comportementale intelligente des activités malveillantes liées à la cybercriminalité. Les adresses IP correspondent à des infrastructures d'attaque actives : scanners de vulnérabilités, tentatives de brute-force, serveurs de commande de botnets, exploits connus. L'intégration de cette liste dans vos équipements de filtrage réseau (pare-feux, WAF) permet un blocage automatisé et proactif de ces menaces avant qu'elles n'atteignent votre infrastructure interne.

1.2 Bénéfices opérationnels

Réduction mesurable de la surface d'attaque : Le blocage automatique de dizaines de milliers d'adresses IP malveillantes réduit le bruit opérationnel jusqu'à 50 pour cent, libère jusqu'à 90 pour cent des ressources consacrées à la gestion du trafic malveillant des bots, et diminue significativement la consommation de ressources serveur (CPU, RAM).

Conformité réglementaire facilitée : L'utilisation documentée d'une source externe de threat intelligence de haute qualité répond directement aux exigences de la Directive NIS2 (applicable aux entités essentielles et importantes) et de la norme ISO 27001 pour les organisations certifiées ou en cours de certification.

Transparence et maîtrise totale : La solution est open-source sous licence GNU GPLv3, auditable, et ne génère aucune dépendance commerciale. Vous conservez un contrôle total via votre whitelist locale pour autoriser spécifiquement les adresses IP légitimes nécessaires à votre activité.

Fiabilité et minimisation des faux positifs : Data-Shield IPv4 Blocklist fournit des données de haute qualité avec un taux de faux positifs minimal pour éviter de bloquer des instances légitimes exposées. La rétention des données est limitée à 15 jours maximum, période optimisée pour surveiller les activités des adresses IP à durée de vie courte mais susceptibles de réapparaître.

2. PRINCIPES DE GOUVERNANCE

2.1 Règles d'utilisation impératives

Configuration obligatoire WAN vers LAN uniquement : Le blocage doit être appliqué EXCLUSIVEMENT dans le sens Internet vers réseau interne (WAN to LAN). Cette configuration est impérative pour garantir l'efficacité du dispositif et exclure tout traitement de données personnelles au sens du RGPD. Ne jamais implémenter ces règles de flux dans la direction LAN vers WAN.

Mise à jour quotidienne automatisée : La blocklist doit être synchronisée toutes les 24 heures pour maintenir une protection adaptée aux menaces émergentes. Plusieurs sources de téléchargement sont disponibles (GitHub, JSdelivr CDN, GitLab) pour garantir la disponibilité.

Choix de la liste adaptée à votre équipement : Certains équipements limitent le nombre d'adresses IPv4 par liste pour éviter la surconsommation de ressources. Data-Shield propose 5 listes officielles : une liste complète (110 000 IP max) et 4 listes fractionnées de 30 000 IP chacune (prod_aa, prod_ab, prod_ac, prod_ad) pour s'adapter aux limitations constructeurs.

Documentation des exceptions : Toute adresse IP légitime ajoutée à votre whitelist locale doit faire l'objet d'une justification métier documentée, avec révision trimestrielle de sa pertinence.

Signalement communautaire des erreurs : Lorsqu'une adresse IP légitime est incorrectement bloquée (faux positif avéré), vous devez la signaler via GitHub Issues dans les 48 heures pour contribuer à l'amélioration collective de la blocklist et bénéficier d'un retrait rapide.

Conservation maîtrisée des logs : Les logs de blocage sont conservés pendant 60 jours maximum, durée strictement nécessaire aux investigations de sécurité et à la conformité réglementaire.

2.2 Responsabilités organisationnelles

Dans les structures de taille réduite, plusieurs fonctions peuvent être assumées par une même personne. La répartition suivante doit être adaptée à votre organisation :

Responsable technique (administrateur système/réseau) : Exécute les opérations de déploiement, configure les équipements de filtrage, assure la synchronisation quotidienne, traite les incidents techniques, gère la whitelist locale, valide la configuration WAN vers LAN exclusive.

Responsable sécurité (RSSI ou équivalent) : Valide la politique d'utilisation, approuve les modifications substantielles de configuration, supervise les indicateurs de sécurité, assure la liaison avec la direction, vérifie trimestriellement la conformité de la configuration.

Direction : Valide l'acceptation du risque résiduel après application des mesures de protection, alloue les ressources nécessaires, approuve les arbitrages en cas de conflit entre sécurité et continuité d'activité.

3. ANALYSE DES RISQUES OPÉRATIONNELS

3.1 Risque de faux positifs

Nature du risque : Une adresse IP légitime (fournisseur SaaS, partenaire commercial, serveur de mise à jour éditeur) est incorrectement présente dans la blocklist, entraînant le blocage automatique de connexions nécessaires au fonctionnement de votre activité.

Probabilité : Faible à Moyenne. Data-Shield IPv4 Blocklist minimise activement les faux positifs grâce à une méthodologie d'analyse comportementale rigoureuse. Quelques occurrences par an restent possibles selon votre écosystème numérique.

Impact : Perturbation de service, perte de productivité temporaire, nécessité d'intervention technique urgente

Mesures de protection :

- Période d'observation initiale de 7 jours en mode journalisation uniquement avant activation du blocage effectif

- Constitution préventive d'une whitelist locale recensant vos partenaires critiques identifiés lors de la phase d'observation
- Procédure de déblocage rapide documentée avec objectif de rétablissement sous 30 minutes
- Surveillance quotidienne des alertes de blocage pour détection rapide des anomalies
- Signalement systématique des faux positifs avérés via GitHub Issues pour retrait rapide de la liste

3.2 Risque d'indisponibilité du flux de mise à jour

Nature du risque : Le flux de mise à jour devient temporairement indisponible (incident hébergeur, problème de connectivité de votre organisation) ou potentiellement altéré, empêchant la synchronisation quotidienne.

Probabilité : Très Faible. Data-Shield IPv4 Blocklist est disponible via 4 sources indépendantes (GitHub, JSdelivr CDN, GitLab) garantissant une haute disponibilité. Disponibilité historique des plateformes supérieure à 99,9 pour cent.

Impact : Protection dégradée face aux menaces les plus récentes pendant la période d'indisponibilité, exposition aux nouvelles adresses IP malveillantes non bloquées

Mesures de protection :

- Mécanisme de failover automatique : configuration de sources de téléchargement multiples (GitHub primaire, JSdelivr CDN ou GitLab en secours)
- Mécanisme de retry automatique : 3 tentatives de récupération espacées de 4 heures en cas d'échec sur la source primaire
- Conservation de la dernière version valide pendant minimum 7 jours pour maintien de la protection
- Alerte automatique vers votre système de supervision en cas d'échec de mise à jour persistant sur toutes les sources
- Maintien opérationnel de la protection avec la dernière version disponible

3.3 Risque de configuration incorrecte

Nature du risque : Application erronée du blocage dans le sens réseau interne vers Internet (LAN to WAN) au lieu de la configuration impérative Internet vers réseau interne (WAN to LAN) uniquement.

Probabilité : Faible si les procédures de déploiement sont suivies rigoureusement et que la documentation technique est respectée

Impact : CRITIQUE

- Blocage massif des connexions sortantes légitimes de vos collaborateurs (navigation web, accès aux services cloud, VPN)
- Dysfonctionnement majeur de l'activité nécessitant une intervention d'urgence
- Obligation réglementaire de documentation RGPD exhaustive rétroactive (traitement d'adresses IP de vos collaborateurs)
- Risque de non-conformité réglementaire significatif

Mesures de protection :

- Documentation technique explicite soulignant la configuration impérative WAN vers LAN uniquement (WAN to LAN)
- Validation obligatoire par le responsable sécurité avant mise en production
- Tests fonctionnels post-déploiement vérifiant que les connexions sortantes ne sont pas impactées
- Revue trimestrielle de la configuration effective lors de l'audit de conformité
- Formation du personnel technique sur les implications de chaque sens de blocage et consultation des tutoriels d'intégration officiels

4. CONFORMITÉ RÉGLEMENTAIRE

4.1 Application de la norme ISO 27001:2022

Pour les organisations certifiées ou en cours de certification ISO 27001, l'intégration de la Data-Shield IPv4 Blocklist répond directement aux mesures de sécurité suivantes de l'Annexe A :

Mesure A.5.28 (Collecte de preuves lors d'incidents de sécurité de l'information) : La blocklist constitue une source structurée de renseignement sur les menaces (threat intelligence), collectée quotidiennement via des sondes de sécurité déployées mondialement et centralisées sur une plateforme HIDS/SIEM auto-hébergée.

Mesure A.8.20 (Sécurité des réseaux) : Le filtrage automatisé basé sur la réputation IP renforce la défense périmétrique contre les attaques automatisées connues (scans, brute-force, exploits), réduisant mécaniquement la surface d'attaque exposée et la phase de reconnaissance sur des plateformes comme Shodan.

Mesure A.8.21 (Sécurité des services réseau) : La synchronisation quotidienne garantit une protection adaptative face aux nouvelles campagnes d'attaque, avec un délai maximum de 24 heures entre l'identification d'une menace et son blocage effectif. La rétention limitée à 15 jours optimise la surveillance des menaces à durée de vie courte.

Mesure A.5.7 (Threat intelligence) : Utilisation d'indicateurs de compromission externes de haute qualité validés par la communauté pour enrichir votre posture défensive. La source Data-Shield est open-source sous licence GNU GPLv3, auditable et maintenue activement par Duggy Tuxy (Laurent Minne).

Documentation pour audit : Présentez ce document comme preuve formelle de maîtrise lors de vos audits de certification. Les logs de synchronisation quotidienne et votre registre d'exceptions (whitelist) constituent des preuves d'application opérationnelle complémentaires.

4.2 Conformité Directive NIS2

Pour les entités essentielles et importantes soumises à la Directive NIS2 (en cours de transposition dans certains pays européens), l'intégration de la Data-Shield IPv4 Blocklist répond aux exigences suivantes de l'article 21 :

Gestion des risques de cybersécurité (article 21.2.a) : Ce document démontre une approche structurée d'identification, d'analyse et de traitement des risques opérationnels liés à l'utilisation d'une source externe de threat intelligence de haute qualité. La documentation des responsabilités et des mesures de protection répond à l'obligation de formalisation.

Sécurité des réseaux et des systèmes (article 21.2.d) : Le filtrage automatisé des adresses IP malveillantes constitue une mesure technique de défense périmétrique proportionnée aux menaces actuelles, contribuant directement à la résilience de vos services critiques. Les performances mesurables (réduction du bruit jusqu'à 50 pour cent, blocage de 90 pour cent du trafic malveillant de bots) démontrent l'efficacité du dispositif.

Gestion des incidents de sécurité (article 21.2.b) : Les logs de blocage conservés pendant 60 jours facilitent les investigations post-incident et la déclaration réglementaire aux autorités compétentes (ANSSI) dans les délais imposés (24 heures pour incidents significatifs).

Utilisation de solutions appropriées (article 21.2.e) : La blocklist Data-Shield représente une solution éprouvée (jusqu'à 110 000 adresses IPv4, mise à jour quotidienne), maintenue de façon continue, open-source sous licence GNU GPLv3 (transparence et auditabilité), et largement utilisée par la communauté de cybersécurité internationale.

Conservation documentaire : Les organisations soumises à NIS2 doivent impérativement référencer ce document dans leur dossier de conformité et le présenter lors des inspections de l'ANSSI. L'absence de documentation des mesures techniques peut entraîner des sanctions administratives allant jusqu'à 10 millions d'euros ou 2 pour cent du chiffre d'affaires mondial pour les entités essentielles.

4.3 Exclusion du périmètre RGPD

Conclusion juridique : HORS CHAMP D'APPLICATION DU RGPD

Lorsque la Data-Shield IPv4 Blocklist est correctement configurée (blocage WAN to LAN EXCLUSIVEMENT), le dispositif est hors du champ d'application du RGPD. Aucune documentation RGPD (registre des traitements, analyse d'impact, mentions d'information) n'est requise.

Fondements de l'exclusion :

Absence de traitement de données personnelles : Les adresses IP bloquées appartiennent à des acteurs malveillants externes (cybercriminels, botnets, scanners automatisés) qui n'ont aucune relation contractuelle, professionnelle ou personnelle avec votre organisation. Ce sont des attaquants anonymes cherchant à exploiter des vulnérabilités de votre infrastructure.

Impossibilité d'identification raisonnable : Votre organisation n'a aucun moyen raisonnable d'identifier les personnes physiques derrière ces adresses IP malveillantes. Vous ne disposez ni des logs d'attribution du fournisseur d'accès Internet, ni de relation contractuelle permettant une quelconque identification. Il ne s'agit pas de clients, partenaires ou employés de votre structure.

Contexte juridique spécifique : La jurisprudence Breyer (CJUE, C-582/14, 19 octobre 2016) concernait un site web disposant de moyens légaux pour obtenir l'identité des visiteurs via leur FAI. Dans le cas Data-Shield, vous ne fournissez aucun service à ces adresses IP, vous bloquez simplement des tentatives d'attaque en amont. Le contexte juridique est fondamentalement différent.

ATTENTION CRITIQUE : Si par erreur de configuration le blocage était appliqué dans le sens LAN to WAN (connexions sortantes de vos collaborateurs vers Internet), alors le RGPD deviendrait pleinement applicable. Les adresses IP bloquées seraient celles de vos collaborateurs, pour lesquels vous disposez de moyens raisonnables d'identification. Cette configuration INCORRECTE nécessiterait une documentation RGPD exhaustive. La configuration WAN to LAN EXCLUSIVEMENT est donc obligatoire pour garantir l'exclusion du RGPD et la simplicité de gouvernance.

5. PROCÉDURES OPÉRATIONNELLES

5.1 Déploiement initial

Le déploiement suit une approche progressive garantissant la sécurité et la maîtrise du dispositif :

Phase 1 - Validation (1 semaine avant activation)

- Approbation formelle de votre responsable sécurité
- Identification des équipements de filtrage réseau concernés (pare-feux, WAF)
- Vérification de la compatibilité technique et des limitations constructeur (liste complète ou fractionnée)
- Consultation des tutoriels d'intégration officiels pour votre équipement (Fortinet, Checkpoint, Palo Alto, OPNsense, Stormshield, F5, etc.)
- Revue du présent document par les parties prenantes

Phase 2 - Observation (7 jours minimum)

- Téléchargement initial de la blocklist depuis la source choisie (GitHub primaire recommandé)
- Configuration en mode journalisation uniquement (blocage désactivé)
- Analyse quotidienne des logs pour identifier les faux positifs potentiels
- Documentation des flux légitimes détectés

Phase 3 - Constitution whitelist (3 jours avant activation)

- Documentation des adresses IP légitimes identifiées lors de la phase d'observation
- Validation métier des flux critiques nécessitant une exclusion
- Création du fichier whitelist versionné
- Tests de non-régression sur les services critiques

Phase 4 - Activation (jour J)

- Activation de la configuration WAN to LAN EXCLUSIVEMENT (Internet vers réseau interne)
- Vérification impérative : NE PAS configurer en LAN to WAN
- Tests fonctionnels post-activation vérifiant que les connexions sortantes de vos collaborateurs ne sont pas impactées
- Surveillance renforcée pendant 72 heures
- Communication interne auprès de vos équipes support et utilisateurs

Phase 5 - Stabilisation (30 jours)

- Surveillance quotidienne des alertes de blocage
- Ajustements de la whitelist si nécessaire
- Collecte des retours utilisateurs
- Documentation des incidents et résolutions
- Revue bilan après 30 jours d'exploitation

5.2 Choix et mise à jour de la blocklist

Sélection de la liste appropriée :

Data-Shield IPv4 Blocklist propose 5 listes officielles mises à jour quotidiennement :

- **Liste complète :** prod_data-shield_ipv4_blocklist.txt (jusqu'à 110 000 adresses IPv4) - pour équipements sans limitation
- **Listes fractionnées :** prod_aa, prod_ab, prod_ac, prod_ad (30 000 adresses IPv4 chacune) - pour équipements avec limitations constructeur. Ces listes peuvent être utilisées individuellement ou combinées selon vos besoins et capacités.

Sources de téléchargement disponibles :

- **GitHub (source primaire recommandée) :** https://raw.githubusercontent.com/duggytuxy/Data-Shield_IPv4_Blocklist/refs/heads/main/prod_data-shield_ipv4_blocklist.txt
- **JSdelivr CDN (miroir) :** https://cdn.jsdelivr.net/gh/duggytuxy/Data-Shield_IPv4_Blocklist@refs/heads/main/prod_data-shield_ipv4_blocklist.txt
- **GitLab (miroir) :** https://gitlab.com/duggytuxy/Data-Shield-IPv4-Blocklist/-/raw/main/prod_data-shield_ipv4_blocklist.txt?ref_type=heads

Configuration de la mise à jour automatique :

- Configurer votre équipement pour télécharger automatiquement la liste depuis l'URL choisie
- Fréquence : synchronisation toutes les 24 heures (recommandation : entre 2h et 4h du matin)

- Configurer une source secondaire en failover (ex : GitHub primaire, JSdelivr CDN en secours)
- Mécanisme de retry : 3 tentatives espacées de 4 heures en cas d'échec
- Alerte automatique en cas d'échec persistant sur toutes les sources
- Conservation de la dernière version valide pendant minimum 7 jours

5.3 Gestion des faux positifs

Un faux positif survient lorsqu'une adresse IP légitime est incorrectement présente dans la blocklist, entraînant le blocage de services légitimes nécessaires à votre activité.

Procédure de traitement immédiat :

- **Détection :** Surveillance proactive quotidienne des alertes de blocage ou signalement par vos utilisateurs
- **Analyse rapide :** Vérification du contexte métier (nature du service impacté, criticité pour l'activité)
- **Déblocage immédiat :** Ajout de l'adresse IP à votre whitelist locale (objectif : rétablissement sous 30 minutes)
- **Documentation :** Consignation formelle de l'adresse IP, date de détection, service impacté, justification métier
- **Notification :** Information de votre responsable sécurité pour traçabilité

Procédure de signalement communautaire :

Dans les 48 heures suivant la confirmation d'un faux positif, vous devez signaler l'adresse IP via GitHub Issues pour contribuer à l'amélioration collective de la blocklist et bénéficier d'un retrait rapide :

- Accéder à : https://github.com/duggytuxy/Data-Shield_IPv4_Blocklist/issues
- Créer une nouvelle issue avec titre explicite, description du service légitime impacté, contexte métier et date de détection
- Suivre la résolution par le mainteneur (Duggy Tuxy - Laurent Minne)
- Mettre à jour votre registre interne des faux positifs avec référence de l'issue GitHub

6. INDICATEURS DE PILOTAGE

6.1 Indicateurs opérationnels

Les indicateurs suivants permettent de piloter l'efficacité du dispositif et de mesurer les bénéfices attendus :

Nombre de tentatives de connexion bloquées quotidiennement : Mesure l'exposition réelle aux menaces. Un volume significatif justifie le maintien du dispositif. Objectif de réduction du bruit opérationnel : jusqu'à 50 pour cent.

Taux de blocage du trafic malveillant de bots : Pourcentage du trafic malveillant automatisé bloqué avec succès. Objectif : 90 pour cent du trafic malveillant de bots bloqué, libérant significativement les ressources serveur.

Réduction de consommation des ressources serveur : Mesure de la diminution de charge CPU, RAM et autres ressources suite au blocage du trafic malveillant. Indicateur de performance économique du dispositif.

Taux de mise à jour réussie : Pourcentage de synchronisations quotidiennes réussies sur le mois. Objectif : supérieur à 98 pour cent (haute disponibilité multi-sources). Un taux inférieur nécessite une investigation.

Nombre de faux positifs détectés mensuellement : Objectif de stabilisation : moins de 2 faux positifs par mois après la période de stabilisation initiale de 30 jours, grâce à la méthodologie rigoureuse de Data-Shield minimisant les faux positifs.

Délai moyen de traitement des faux positifs : Temps écoulé entre la détection d'un faux positif et le rétablissement du service. Objectif : inférieur à 30 minutes pendant les heures ouvrées.

Taille de la whitelist locale : Nombre d'adresses IP légitimes exclues du blocage. Une croissance continue peut indiquer des besoins spécifiques de votre activité nécessitant une analyse.

6.2 Indicateurs de conformité

Conformité de configuration WAN to LAN : Vérification trimestrielle obligatoire via tests fonctionnels que le blocage est bien appliqué dans le sens Internet vers réseau interne uniquement. Toute déviation constitue un risque RGPD majeur.

Taux de révision de la whitelist : 100 pour cent des adresses IP en whitelist doivent faire l'objet d'une révision trimestrielle avec justification métier actualisée. Les exclusions devenues obsolètes doivent être supprimées.

Exhaustivité du registre des faux positifs : 100 pour cent des faux positifs traités doivent être documentés avec date, adresse IP, justification, et référence de l'issue GitHub associée.

Réactivité des signalements GitHub : Objectif : 100 pour cent des faux positifs avérés signalés sous 48 heures maximum pour contribution à l'amélioration collective et bénéfice d'un retrait rapide.

7. RESSOURCES ET RÉFÉRENCES

7.1 Projet Data-Shield IPv4 Blocklist

Dépôt GitHub principal : https://github.com/duggytuxy/Data-Shield_IPv4_Blocklist

Dépôt GitLab : https://gitlab.com/duggytuxy/Data-Shield-IPv4-Blocklist

Signalement des faux positifs : https://github.com/duggytuxy/Data-Shield_IPv4_Blocklist/issues

Tutoriels d'intégration : Consultez le README du dépôt GitHub pour les guides d'intégration officiels par constructeur (Fortinet, Checkpoint, Palo Alto, OPNsense, Stormshield, F5, etc.)

Mainteneur : Duggy Tuxy (Laurent Minne) - Expert cybersécurité reconnu

Licence : GNU GPLv3 (2023-2025)

Support du projet : Ko-Fi (https://ko-fi.com/laurentmduggytuxy)

7.2 Références réglementaires

ISO/IEC 27001:2022 : Systèmes de management de la sécurité de l'information - https://www.iso.org/standard/27001

CCB : Centre For Cybersecurity Belgium

https://ccb.belgium.be/fr

Directive NIS2 (UE 2022/2555) : Sécurité des réseaux et des systèmes d'information - https://eur-lex.europa.eu/eli/dir/2022/2555

Règlement RGPD (UE 2016/679) : Protection des données personnelles - https://eur-lex.europa.eu/eli/reg/2016/679

ANSSI : Agence nationale de la sécurité des systèmes d'information - https://www.ssi.gouv.fr/

7.3 Glossaire technique

Blocklist : Liste d'adresses IP identifiées comme sources de menaces cyber, utilisée pour bloquer automatiquement les connexions provenant de ces adresses.

Deceptive Security : Discipline de sécurité basée sur l'utilisation de leurres et l'analyse comportementale des activités malveillantes.

HIDS/SIEM : Host-based Intrusion Detection System / Security Information and Event Management. Plateformes de détection d'intrusion et de gestion centralisée des événements de sécurité.

WAN to LAN : Direction de flux réseau depuis Internet (WAN - Wide Area Network) vers le réseau local interne (LAN - Local Area Network). Configuration impérative pour Data-Shield.

LAN to WAN : Direction de flux réseau depuis le réseau local interne vers Internet. Configuration à ne JAMAIS utiliser pour Data-Shield (risque RGPD).

WAF : Web Application Firewall. Pare-feu applicatif protégeant spécifiquement les applications web.

Faux positif : Erreur de classification où une adresse IP légitime est incorrectement identifiée comme malveillante.

Whitelist : Liste d'exceptions contenant les adresses IP légitimes à exclure du blocage automatique pour préserver les flux nécessaires à votre activité.

IOC : Indicator of Compromise. Indicateur de compromission, ici une adresse IP associée à une activité malveillante avérée.

Threat intelligence : Renseignement sur les menaces cyber, collecte et analyse structurées des indicateurs d'attaque pour améliorer la détection et la prévention.