GRC COMPLIANCE MODEL

Data-Shield IPv4 Blocklist Integration

1. PRESENTATION OF THE SYSTEM

1.1 Nature and operation of the blocklist

The IPv4 Data-Shield Blocklist, developed and maintained by Duggy Tuxy (Laurent Minne), is a daily updated source of cyber threat intelligence. This list lists up to 120,000 IPv4 addresses identified as sources of malicious activity, collected through globally deployed security probes and centralized on a secure, self-hosted HIDS/SIEM platform.

The methodology is based on the discipline of Deceptive Security based on intelligent behavioral analysis of malicious activities related to cybercrime. IP addresses correspond to active attack infrastructures: vulnerability scanners, brute-force attempts, botnet command servers, known exploits. Integrating this list into your network filtering equipment (firewalls, WAF) allows for automated and proactive blocking of these threats before they reach your internal infrastructure.

1.2 Operational benefits

Measurable attack surface reduction: Auto-blocking tens of thousands of malicious IP addresses reduces operational noise by up to 50 percent, frees up to 90 percent of resources spent on managing malicious bot traffic, and significantly decreases server resource consumption (CPU, RAM).

Facilitated regulatory compliance: The documented use of a high-quality external source of threat intelligence directly meets the requirements of the NIS2 Directive (applicable to essential and important entities) and the ISO 27001 standard for organizations certified or in the process of certification.

Transparency and total control: The solution is open-source under the GNU GPLv3 license, auditable, and does not generate any commercial dependency. You retain full control through your local whitelist to specifically authorize legitimate IP addresses needed for your business.

Reliability and minimization of false positives: Data-Shield IPv4 Blocklist provides high-quality data with a minimal false positive rate to avoid blocking legitimate instances exposed. Data retention is limited to a maximum of 15 days, which is optimized to monitor the activities of IP addresses that are short-lived but likely to reappear.

2. GOVERNANCE PRINCIPLES

2.1 Mandatory rules of use

Mandatory WAN to LAN configuration only: Blocking must be applied EXCLUSIVELY in the Internet-to-internal network (WAN to LAN) direction. This configuration is imperative to guarantee the effectiveness of the system and to exclude any processing of personal data within the meaning of the GDPR. Never implement these flow rules in the LAN-to-WAN direction.

Automated daily update: The blocklist should be synchronized every 24 hours to maintain adequate protection for emerging threats. Several download sources are available (GitHub, JSdelivr CDN, GitLab) to ensure availability.

Choosing the right list for your device: Some devices limit the number of IPv4 addresses per list to avoid overconsumption of resources. Data-Shield offers 5 official lists: a complete list (120,000 IPs max) and 4 split lists of 30,000 IPs each (prod_aa, prod_ab, prod_ac, prod_ad) to adapt to manufacturers' limitations.

Exception documentation: Any legitimate IP address added to your local whitelist must have a documented business justification, with a quarterly review of its relevance.

Community error reporting: When a legitimate IP address is incorrectly blocked (proven false positive), you should report it through GitHub Issues within 48 hours to help collectively improve the blocklist and benefit from a quick removal.

Controlled log retention: Blocking logs are retained for up to 60 days, which is strictly necessary for security investigations and regulatory compliance.

2.2 Organizational Responsibilities

In small structures, several functions can be performed by the same person. The following breakdown should be appropriate for your organization:

Technical manager (system/network administrator): Executes deployment operations, configures filtering equipment, ensures daily synchronization, handles technical incidents, manages the local whitelist, validates the exclusive WAN-to-LAN configuration.

Security Officer (CISO or equivalent): Validates the usage policy, approves substantial configuration changes, oversees security indicators, liaises with management, verifies configuration compliance on a quarterly basis.

Management: Validates the acceptance of the residual risk after application of the protective measures, allocates the necessary resources, approves arbitrations in the event of a conflict between security and business continuity.

3. OPERATIONAL RISK ANALYSIS

3.1 Risk of false positives

Nature of the risk: A legitimate IP address (SaaS provider, business partner, update server, publisher) is incorrectly present in the blocklist, causing connections necessary for the operation of your business to be automatically blocked.

Probability: Low to Medium. Data-Shield IPv4 Blocklist actively minimizes false positives through a rigorous behavioral analysis methodology. A few occurrences per year are still possible depending on your digital ecosystem.

Impact: Service disruption, temporary loss of productivity, need for urgent technical intervention

Protective measures:

- Initial 7-day observation period in logging-only mode before effective blocking is enabled
- Preventive constitution of a local whitelist listing your critical partners identified during the observation phase
- Documented quick release procedure with 30-minute recovery goal
- Daily monitoring of blocking alerts for rapid detection of anomalies
- Systematically report proven false positives via GitHub Issues for quick delisting

3.2 Risk of unavailability of the update feed

Nature of the risk: The update flow becomes temporarily unavailable (host incident, connectivity issue of your organization) or potentially corrupted, preventing daily synchronization.

Probability: Very low. Data-Shield IPv4 Blocklist is available via 4 independent sources (GitHub, JSdelivr CDN, GitLab) guaranteeing high availability. Historical platform availability greater than 99.9 percent.

Impact: Degraded protection against the latest threats during the downtime period, exposure to new malicious IP addresses not blocked

Protective measures:

- Automatic failover mechanism: configuration of multiple download sources (GitHub primary, JSdelivr CDN or GitLab as a fallback)
- Automatic retry mechanism: 3 retrieval attempts spaced 4 hours apart in case of failure on primary source
- Retention of the latest version valid for a minimum of 7 days to maintain protection
- Automatic alert to your monitoring system in the event of persistent update failure on all sources
- Keeping protection up and running with the latest version available

3.3 Risk of Misconfiguration

Nature of risk: Incorrect application of blocking in the internal network to the Internet (LAN to WAN) direction instead of the mandatory Internet-to-internal network (WAN to LAN) configuration only.

Likelihood: Low if deployment procedures are rigorously followed and technical documentation is adhered to

Impact: CRITICAL

- Massive blocking of legitimate outbound connections of your employees (web browsing, access to cloud services, VPN)
- Major malfunction of the activity requiring emergency intervention
- Regulatory obligation of retroactive comprehensive GDPR documentation (processing of your employees' IP addresses)
- Significant regulatory non-compliance risk

Protective measures:

- Explicit technical documentation highlighting the imperative WAN to LAN configuration (WAN to LAN)
- Mandatory validation by the safety manager before production is put into production
- Post-deployment functional testing verifying that outbound connections are not impacted
- Quarterly review of the effective configuration during the compliance audit
- Training of technical staff on the implications of each blocking direction and consultation of official integration tutorials

4. REGULATORY COMPLIANCE

4.1 Application of ISO 27001:2022

For organizations that are ISO 27001 certified or in the process of certification, the integration of the IPv4 Blocklist Data-Shield directly addresses the following security measures in Appendix A:

Action A.5.28 (Evidence collection during information security incidents): The blocklist is a structured source of threat intelligence, collected daily via globally deployed security probes and centralized on a self-hosted HIDS/SIEM platform.

Action A.8.20 (Network Security): Automated IP reputation-based filtering strengthens perimeter defense against known automated attacks (scans, brute-force, exploits), mechanically reducing the exposed attack surface and reconnaissance phase on platforms like Shodan.

Measure A.8.21 (Network Services Security): Daily synchronization provides adaptive protection against new attack campaigns, with a maximum delay of 24 hours between the identification of a threat and its effective blocking. The 15-day retention optimizes monitoring for short-lived threats.

Measure A.5.7 (Threat intelligence): Use of high-quality, community-validated external indicators of compromise to enrich your defensive posture. The Data-Shield source is open-source under the GNU GPLv3 license, auditable and actively maintained by Duggy Tuxy (Laurent Minne).

Audit documentation: Present this document as formal proof of proficiency during your certification audits. Daily synchronization logs and your whitelist provide additional evidence of operational application.

4.2 NIS2 Compliance

For essential and important entities subject to the NIS2 Directive (currently being transposed in some European countries), the integration of the IPv4 Blocklist Data-Shield meets the following requirements of Article 21:

Cybersecurity Risk Management (Article 21.2.a): This document demonstrates a structured approach to identifying, analyzing, and addressing operational risks related to the use of a high-quality external source of threat intelligence. The documentation of responsibilities and protective measures meets the formalization obligation.

Network and system security (Article 21.2.d): Automated filtering of malicious IP addresses is a technical perimeter defense measure proportionate to current threats, directly contributing to the resilience of your critical services. Measurable performance (up to 50 percent noise reduction, 90 percent blocking of malicious bot traffic) demonstrates the effectiveness of the device.

Security incident management (Article 21.2.b): Blocking logs kept for 60 days facilitate post-incident investigations and regulatory reporting to the competent authorities (ANSSI) within the imposed deadlines (24 hours for significant incidents).

Use of appropriate solutions (Article 21.2.e): The Data-Shield blocklist represents a proven solution (up to 120,000 IPv4 addresses, updated daily), continuously maintained, open-source under the GNU GPLv3 (transparency and auditability) license, and widely used by the international cybersecurity community.

Document retention: Organizations subject to NIS2 must imperatively reference this document in their compliance file and present it during ANSSI inspections. Failure to document technical measures can result in administrative penalties of up to €10 million or 2 per cent of global turnover for essential entities.

4.3 Exclusion from the GDPR scope

Legal conclusion: OUTSIDE THE SCOPE OF THE GDPR

When the IPv4 Blocklist Data-Shield is correctly configured (WAN-to-LAN blocking ONLY), the device is outside the scope of the GDPR. No GDPR documentation (processing register, impact assessment, information notices) is required.

Grounds for exclusion:

Lack of processing of personal data: Blocked IP addresses belong to external malicious actors (cybercriminals, botnets, automated scanners) who have no contractual, business, or personal relationship with your organization. They are anonymous attackers looking to exploit vulnerabilities in your infrastructure.

Lack of Reasonable Identification: Your organization has no reasonable way to identify the natural persons behind these malicious IP addresses. You do not have the Internet service provider's attribution logs or a contractual relationship that allows any kind of identification. These are not customers, partners or employees of your structure.

Specific legal context: The Breyer case law (CJEU, C-582/14, 19 October 2016) concerned a website with legal means to obtain the identity of visitors via their ISP. In the case of Data-Shield, you do not provide any service to these IP addresses, you simply block upstream attack attempts. The legal context is fundamentally different.

CRITICAL ATTENTION: If the blocking is applied in the LAN to WAN direction (outgoing connections of your employees to the Internet) by a configuration error, then the GDPR would become fully applicable. The blocked IP addresses would be those of your employees, for whom you have reasonable means of identification. This INCORRECT configuration would require exhaustive GDPR documentation. The WAN to LAN EXCLUSIVE configuration is therefore mandatory to ensure the exclusion of the GDPR and the simplicity of governance.

5. OPERATIONAL PROCEDURES

5.1 Initial Deployment

The deployment follows a progressive approach guaranteeing security and control of the system:

Phase 1 - Validation (1 week before activation)

- Formal approval from your security manager
- Identification of the network filtering devices concerned (firewalls, WAF)
- Verification of technical compatibility and manufacturer limitations (full or split list)
- Consult the official integration tutorials for your equipment (Fortinet, Checkpoint, Palo Alto, OPNsense, Stormshield, F5, etc.)
- Stakeholder review of this document

Phase 2 - Observation (7 days minimum)

- Initial download of the blocklist from the chosen source (primary GitHub recommended)
- Configuration in journal-only mode (blocking disabled)
- Daily log analysis to identify potential false positives
- Documentation of legitimate flows detected

Phase 3 - Constitution whitelist (3 days before activation)

- Documentation of legitimate IP addresses identified during the observation phase
- Business validation of critical flows requiring exclusion
- Creating the versioned whitelist file
- Non-regression testing on critical services

Phase 4 - Activation (D-Day)

- Enabling WAN to LAN Configuration EXCLUSIVELY (Internet to Internal Network)
- Imperative check: DO NOT configure in LAN to WAN
- Post-activation functional tests to ensure that your employees' outgoing connections are not impacted

- Enhanced surveillance for 72 hours
- Internal communication with your support teams and users

Phase 5 - Stabilization (30 days)

- Daily monitoring of blocking alerts
- Whitelist adjustments if necessary
- Collecting user feedback
- Incident documentation and resolutions
- Review of the results after 30 days of operation

5.2 Choosing and Updating the Blocklist

Selecting the appropriate list:

Data-Shield IPv4 Blocklist offers 5 official lists updated daily:

- **Full list:** prod_data-shield_ipv4_blocklist.txt (up to 120,000 IPv4 addresses) - for devices without limitation
- **Split lists:** prod_aa, prod_ab, prod_ac, prod_ad (30,000 IPv4 addresses each) - for equipment with manufacturer limitations. These lists can be used individually or combined according to your needs and abilities.

Available download sources:

- **GitHub (recommended primary source):** https://raw.githubusercontent.com/duggytuxy/Data-Shield_IPv4_Blocklist/refs/heads/main/prod_data-shield_ipv4_blocklist.txt
- **JSdelivr CDN (mirror):** https://cdn.jsdelivr.net/gh/duggytuxy/Data-Shield_IPv4_Blocklist@refs/heads/main/prod_data-shield_ipv4_blocklist.txt
- **GitLab (mirror):** https://gitlab.com/duggytuxy/Data-Shield-IPv4-Blocklist/-/raw/main/prod_data-shield_ipv4_blocklist.txt?ref_type=heads
- BitBucket (Mirror) : https://bitbucket.org/duggytuxy/data-shield-ipv4-blocklist/raw/99c4b9fd8aa92f0e7d0f7b76cd465d130d752f5d/prod_data-shield_ipv4_blocklist.txt
- Codeberg (Mirror) : https://codeberg.org/duggytuxy21/Data-Shield_IPv4_Blocklist/raw/branch/main/prod_data-shield_ipv4_blocklist.txt

Configuring automatic update:

- Configure your device to automatically download the list from the chosen URL
- Frequency: synchronization every 24 hours (recommendation: between 2 a.m. and 4 a.m.)
- Configure a secondary source as a failover (e.g. GitHub primary, JSdelivr CDN as a backup)
- Retry mechanism: 3 attempts spaced 4 hours apart if they fail
- Automatic alert in case of persistent failure on all sources
- Retention of the latest valid version for a minimum of 7 days

5.3 Handling false positives

A false positive occurs when a legitimate IP address is incorrectly present in the blocklist, causing legitimate services necessary for your business to be blocked.

Immediate Processing Procedure:

- **Detection:** Daily proactive monitoring of blocking alerts or reports by your users
- **Quick analysis:** Verification of the business context (nature of the service impacted, criticality for the business)
- **Immediate unblock:** Add the IP address to your local whitelist (goal: restore within 30 minutes)

- **Documentation:** Formal logging of IP address, date of detection, impacted service, business justification
- **Notification:** Informing your safety manager for traceability

Community reporting procedure:

Within 48 hours of a false positive being confirmed, you must report the IP address via GitHub Issues to help collectively improve the blocklist and receive a quick removal:

- Jump to: https://github.com/duggytuxy/Data-Shield_IPv4_Blocklist/issues
- Create a new issue with an explicit title, description of the legitimate service impacted, business context, and detection date
- Monitoring the resolution by the maintainer (Duggy Tuxy - Laurent Minne)
- Update your internal false positive registry with GitHub issue reference

6. STEERING INDICATORS

6.1 Operational Indicators

The following indicators make it possible to manage the effectiveness of the system and to measure the expected benefits:

Number of login attempts blocked daily: Measures the actual exposure to threats. A significant volume justifies the maintenance of the system. Operational noise reduction target: up to 50 percent.

Bot Malicious Traffic Blocking Rate: The percentage of automated malicious traffic that has been successfully blocked. Goal: 90 percent of malicious bot traffic blocked, significantly freeing up server resources.

Server Resource Consumption Reduction: Measure of the decrease in CPU, RAM, and other resource load as a result of blocking malicious traffic. Economic performance indicator of the scheme.

Update Success Rate: The percentage of successful daily syncs over the month. Target: Greater than 98 percent (multi-source high availability). A lower level requires investigation.

Number of false positives detected monthly: Stabilization goal: Less than 2 false positives per month after the initial 30-day stabilization period, thanks to Data-Shield's rigorous methodology minimizing false positives.

Mean time to handle false positives: The time between the detection of a false positive and the restoration of service. Goal: Less than 30 minutes during business hours.

Local whitelist size: The number of legitimate IP addresses that are excluded from blocking. Continued growth may indicate specific needs in your business that require analysis.

6.2 Compliance Indicators

WAN to LAN configuration compliance: Mandatory quarterly verification via functional tests that the blocking is applied in the Internet-to-internal network direction only. Any deviation is a major GDPR risk.

Whitelist review rate: 100 percent of whitelist IP addresses should be reviewed quarterly with updated business justification. Exclusions that have become obsolete must be removed.

Completeness of the false positive registry: 100 percent of the false positives processed should be documented with date, IP address, justification, and reference of the associated GitHub outcome.

GitHub report responsiveness: Goal: 100 percent of proven false positives reported within 48 hours for collective improvement and rapid removal.

7. RESOURCES AND REFERENCES

7.1 IPv4 Data-Shield Project Blocklist

Core GitHub repository: https://github.com/duggytuxy/Data-Shield_IPv4_Blocklist

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

Reporting false positives: https://github.com/duggytuxy/Data-Shield_IPv4_Blocklist/issues

Integration tutorials: Check out the GitHub repository README for official integration guides by manufacturer (Fortinet, Checkpoint, Palo Alto, OPNsense, Stormshield, F5, etc.)

Maintainer: Duggy Tuxy (Laurent Minne) - Recognized cybersecurity expert

License: GNU GPLv3 (2023-2025)

Project support: Ko-Fi (https://ko-fi.com/laurentmduggytuxy)

7.2 Regulatory References

ISO/IEC 27001:2022: Information Security Management Systems - https://www.iso.org/standard/27001

CCB : Centre For Cybersecurity Belgium

https://ccb.belgium.be/fr

NIS2 Directive (EU 2022/2555): Security of network and information systems - https://eur-lex.europa.eu/eli/dir/2022/2555

GDPR Regulation (EU 2016/679): Protection of personal data - https://eur-lex.europa.eu/eli/reg/2016/679

ANSSI: French National Agency for the Security of Information Systems - https://www.ssi.gouv.fr/

7.3 Technical Glossary

Blocklist: A list of IP addresses identified as sources of cyber threats, used to automatically block connections from those addresses.

Deceptive Security: Security discipline based on the use of decoys and behavioral analysis of malicious activity.

HIDS/SIEM: Host-based Intrusion Detection System / Security Information and Event Management. Intrusion detection and centralized security event management platforms.

WAN to LAN: The direction of network flows from the Internet (WAN) to the Local Area Network (LAN). Data-Shield is a must.

LAN to WAN: Directing network flow from the internal LAN to the Internet. Configuration to NEVER use for Data-Shield (GDPR risk).

WAF: Web Application Firewall. Application firewall specifically protecting web applications.

False positive: A misclassification where a legitimate IP address is incorrectly identified as malicious.

Whitelist: A list of exceptions containing legitimate IP addresses to exclude from automatic blocking to preserve the flows necessary for your business.

IOC : Indicator of Compromise. Indicator of compromise, in this case an IP address associated with proven malicious activity.

Threat intelligence: Cyber threat intelligence, structured collection and analysis of indicators of attack to improve detection and prevention.