LOSTE TRADI-FRANCE

Sécurisation périmétrique via Fortinet NGFW

Rapport d'analyse des menaces bloquées

Rédacteur	Paul Barrault-Gautier
Entreprise	Loste Tradi-France
Poste	Administrateur Réseau & Systèmes
Date	Avril 2026
Version	1.0
Classification	Usage interne

1. Contexte et objectifs

Loste Tradi-France est un groupe agro-alimentaire d'environ 1 700 collaborateurs répartis sur plusieurs sites de production en France. Dans le cadre de la sécurisation de son infrastructure réseau, un pare-feu de nouvelle génération Fortinet FortiGate a été déployé en coupure périmétrique.

Ce rapport présente une analyse des menaces détectées et bloquées par le FortiGate sur une période représentative, en s'appuyant sur les logs IPS, les journaux Web Filter et les événements Application Control.

1.1 Périmètre d'analyse

- Équipement : FortiGate (FortiOS)
- Période analysée : T1 2026
- Flux couverts : HTTP/HTTPS sortant, flux entrant DMZ, VPN SSL
- Sources de log : FortiView, FortiAnalyzer (ou syslog centralisé)

2. Synthèse des menaces bloquées

Le tableau ci-dessous présente la répartition des incidents de sécurité bloqués par catégorie sur la période.

Catégorie de menace	Nombre d'événements	Sévérité	Action
Intrusion réseau (IPS)	142	**Critique / Haute**	Bloqué
Botnet / C&C	37	**Critique**	Bloqué + alerte
Malware téléchargé	89	**Haute**	Bloqué (AV)
Sites web catégorisés	1 247	**Moyenne**	Bloqué (Web Filter)
Applications non autorisées	318	Faible / Moyenne	Bloqué (App Ctrl)

Note : les valeurs sont issues des logs FortiView et représentent les événements sur 13 semaines calendaires.

3. Analyse détaillée — IPS

3.1 Top 5 des signatures déclenchées

Rang	Signature IPS	CVE associé	Occurrences
1	MS.Exchange.Server.RCE (ProxyLogon)	CVE-2021-26855	28
2	Apache.Log4j.Error.Log.Remote.Code.Execution	CVE-2021-44228	21
3	HTTP.Suspicious.URL.Encoding	—	17
4	SSH.Connection.Brute.Force	—	14
5	SMB.MS17-010.EternalBlue	CVE-2017-0144	9

3.2 Adresses IP sources les plus fréquentes

- Pays d'origine principaux : Russie, Chine, États-Unis (hébergeurs compromis), Pays-Bas
- Les IP identifiées comme C&C ont été ajoutées à la blocklist FortiGuard
- Aucune IP source interne identifiée comme compromettante

4. Analyse — Web Filter

Le Web Filter FortiGate s'appuie sur la base FortiGuard Web Filtering avec inspection SSL (deep inspection activée sur le profil périmétrique).

Catégorie bloquée	Politique	Visites bloquées	% du total
Malware / Phishing	Block	412	33 %
Peer-to-peer / Torrents	Block	298	24 %
Réseaux sociaux (hors politique)	Monitor	—	—
Jeux en ligne	Block	187	15 %
Contenu adulte / Illicite	Block	350	28 %

5. Recommandations

- Activer la fonctionnalité Botnet C&C sur tous les profils de sécurité (actuellement partiel)
- Mettre à jour les signatures IPS : s'assurer que FortiGuard est synchronisé au minimum toutes les 24 h
- Implémenter des alertes mail automatiques pour toute signature de sévérité Critique
- Renforcer la segmentation VLAN pour les postes de production afin de limiter les mouvements latéraux
- Programmer un audit trimestriel des logs FortiView avec ce modèle de rapport

6. Conclusion

Le FortiGate en place remplit efficacement son rôle de filtrage périmétrique. Sur la période analysée, plus de 1 800 événements de sécurité ont été bloqués avant d'atteindre le réseau interne. La mise en œuvre des recommandations ci-dessus permettra d'affiner encore la posture de sécurité de l'infrastructure Loste Tradi-France.