Checklist opérationnelle de cybersécurité proactive

1. Surveillance continue

- Mettre en place un SIEM/XDR (ex. Wazuh, ELK, Splunk).
- Configurer des alertes en temps réel sur les comportements suspects.
- Centraliser les logs (serveurs, firewalls, applications).

2. Tests et audits réguliers

- Réaliser des tests d'intrusion trimestriels (Metasploit, OWASP ZAP).
- Auditer les configurations réseau et systèmes.
- Vérifier la conformité aux normes (ISO 27001, RGPD, loi 09-08).

3. Formation et sensibilisation

- Organiser des sessions de sensibilisation au phishing et ingénierie sociale.

- Diffuser des guides internes de bonnes pratiques (mots de passe, VPN, usage cloud).
- Simuler des campagnes de phishing pour tester la vigilance.

Checklist opérationnelle de cybersécurité proactive

Catégorie	Actions clés
Surveillance continue	• Mettre en place un SIEM/XDR (ex. Wazuh, ELK, Splunk.). • Configurer des alertes en temps réel sur ces comportements suspects. • Centraliser les logs (serveurs, firewalls, applications).
Tests et audits réguliers	• Réaliser des tests d'intrusion trimestriels (Métasploit. OWASP ZAP). • Auditer lés configurations réseau et systémes. • Vérifier la conformité aux normes (I5O 27001, RGPD, loi 09-08).
Formation et sensibilisation	• Organiser des sessions de sensibilisation au phishing et ingénierle sociale. • Diftuser des guides internes de bonnes pratiques (mots de passe, VPN, usage cloud). • Simuler des campagnes de phishing pour tester la vigilance.
Automatisation et IA	• Déployer des scripts pour le patch management (PowerShell, Bash). • Utiliser l'IA pour détecter les anomailes dans les flux réseau. • Automatiser la classification et la réponse aux incidents.
Mesures complémeentalres	• Activer l'authentification multi-facteurs (MFA). • Appliquer le principe du moindre privilege. • Surveiller les vulnérabilites via des bases conmme CVE/NVD.

4. Automatisation et IA

- Déployer des scripts pour le patch management (PowerShell, Bash).
- Utiliser l'IA pour détecter les anomalies dans les flux réseau.
- Automatiser la classification et la réponse aux incidents.

5. Plan de continuité et résilience

- Documenter un PCA/PRA (Plan de Continuité / Reprise d'Activité).
- Tester régulièrement les sauvegardes (Veeam, TrueNAS, Commvault).
- Prévoir des scénarios de bascule (cloud, site secondaire).

6. Gestion des accès et identités

- Activer l'authentification multi-facteurs (MFA).
- Appliquer le principe du moindre privilège.

- Revoir régulièrement les droits d’accès.

7. Mesures complémentaires

- Cartographier la surface d’attaque (Shadow IT, SaaS).
- Mettre en place un threat hunting proactif.
- Surveiller les vulnérabilités via des bases comme CVE/NVD.

Exemple de routine mensuelle

- Mise à jour des systèmes et applications.
- Vérification des journaux SIEM.
- Mini-test d’intrusion interne.
- Session de sensibilisation rapide (15 min).
- Test de restauration de sauvegarde.