# Checklist de préparation CISO Mythos

Les correctifs arrivent. Avant leur déploiement, vos dirigeants, votre service juridique et les régulateurs auront des questions.

## 1 Exposition et visibilité des actifs

*« Quelle est notre exposition, et disposons nous d'un inventaire précis de nos actifs ? »*

- [ ] Mettez à jour votre inventaire des actifs afin qu'il reflète votre environnement de production actuel.
- [ ] Vérifiez qu'une analyse continue est bien active sur l'ensemble de vos environnements de production.
- [ ] Reclassez les vulnérabilités selon une hiérarchisation fondée sur le risque, et non sur le simple nombre de CVE.
- [ ] Préparez une synthèse d'exposition d'une page, prête à être présentée à la direction sur demande.

## 2 Rapidité de déploiement des correctifs et sécurité de la production

*« Pouvons-nous appliquer les correctifs assez vite, à grande échelle, sans perturber la production ? »*

- [ ] Évaluez la cadence actuelle de votre cycle de correctifs au regard de la fenêtre entre la divulgation d'une faille et son exploitation active.
- [ ] Classez vos actifs par criticité avant que les attaques n'arrivent, et non lorsqu'elle survient.
- [ ] Formalisez un protocole de gestion des changements, avec des responsables désignés et des procédures de retour arrière.
- [ ] Organisez un exercice de simulation autour d'un scénario de déploiement rapide de correctifs, afin de mettre à l'épreuve vos circuits de décision et votre préparation au retour arrière.

## 3 Chaîne d'approvisionnement et exposition à l'open source

*« Que se cache-t-il dans nos logiciels open source et tiers ? »*

- [ ] Générez ou mettez à jour votre nomenclature logicielle (SBOM).
- [ ] Recensez les intégrations tierces héritées de vos acquisitions.
- [ ] Mettez en place une analyse continue des dépendances issues de bibliothèques open source.
- [ ] Identifiez les engagements de délai de correction de vos fournisseurs ainsi que leurs points de contact, avant toute divulgation de faille.

## 4 Capacité d'ingénierie

*« Disposons-nous de la capacité d'ingénierie nécessaire pour traiter notre propre Backlog de remédiation ? »*

- [ ] Estimez le nombre d'heures de remédiation au regard des engagements actuels de votre équipe.
- [ ] Priorisez le backlog afin de concentrer vos équipes internes uniquement sur les éléments présentant le plus grand risque.
- [ ] Mobilisez des ressources d'ingénierie externes avant d'en avoir besoin.
- [ ] Intégrez dès maintenant des pratiques de sécurité par défaut dans vos développements en cours.

## 5 Détection et confinement

*« Si un correctif tarde, sommes-nouscapables de détecter et de contenir l'exploitation de la faille ? »*

- [ ] Vérifiez qu'une surveillance SOC 24h/24 et 7j/7 est active sur l'ensemble de vos environnements critiques.
- [ ] Définissez un temps moyen pour trier et isoler les menaces (en minutes, pas en heures).
- [ ] Lancer des chasses aux menaces anticipatives, axées sur les points d'exposition liés à Mythos.
- [ ] Validez votre playbook « assume breach » au moyen d'un exercice ou d'une simulation récente.

## Évaluation de la préparation des dirigeants

*Avant de présenter la situation à votre direction :*

- [ ] Identifiez clairement quelles réponses peuvent être soutenues et justifiées en l'état actuel, et lesquelles nécessitent un alignement formel avec le niveau exécutif ou un sponsoring décisionnel.

## Si vous réfléchissez à la manière de combler ces lacunes :

Certaines organisations développent ces capacités en interne. D'autres s'appuient sur des partenaires pour accélérer leur couverture ou renforcer des équipes aux ressources limitées.

**Insight Managed Exposure Defence** propose une approche intégrée couvrant les cinq domaines ci-dessus, d'abord conçue et exploitée en interne, puis étendue aux clients confrontés aux mêmes questions.

Pour en savoir plus, rendez-vous sur fr.insight.com