Programme de sécurité et opérations

Comment Cyber Crucible gère son programme de sécurité — gestion des changements, gestion des correctifs et des vulnérabilités, reprise après sinistre et continuité d'activité, réponse aux incidents et aux violations de données, et contrôle des terminaux — décrit à l'intention des évaluateurs du risque fournisseur. Précise clairement ce qui est documenté et ce qui est fourni sous accord de confidentialité (NDA), et ne revendique aucune certification.

Cyber Crucible dispose-t-il d'un processus de gestion des changements ?

Réponse courte : Oui. Les changements en production suivent un processus documenté de gestion des changements comprenant une revue, des tests et une approbation. Étant donné que le produit fonctionne au niveau du noyau, la discipline en matière de changements est considérée comme un contrôle de sécurité plutôt que comme une simple pratique d'ingénierie.

Ce que couvre le processus

Les modifications apportées au code applicatif, aux pilotes du noyau, aux configurations des serveurs et à l'infrastructure sous-jacente passent par des étapes de cycle de vie définies : les exigences de sécurité sont établies dès la conception ; le code source est géré par contrôle de version et les secrets ne sont jamais intégrés en clair ; des tests automatisés valident les changements avant leur mise en production ; et les changements en production font l'objet d'une revue et d'une approbation formelles. La séparation des tâches est maintenue, de sorte que l'auteur d'un changement n'en est pas le seul approbateur. Les bases de référence des serveurs suivent des guides de configuration approuvés, et les services inutilisés sont désactivés lorsque cela est possible.

Changements d'urgence et changements de pilotes

Les changements d'urgence suivent une voie accélérée qui exige néanmoins une autorisation, des tests ciblés et une revue post-implémentation. Les pilotes du noyau Windows font l'objet d'une assurance qualité interne et sont soumis à la certification du programme de compatibilité matérielle Windows (WHCP) de Microsoft avant leur publication — un contrôle externe indépendant du composant le plus privilégié.

Alignement avec les référentiels et limites en toute transparence

Le processus s'aligne sur la norme NIST SP 800-53 (famille CM) et sur la norme ISO/IEC 27001:2022 A.8.32. Cyber Crucible ne revendique aucune certification. La procédure détaillée de gestion des changements ainsi que les éléments justificatifs correspondants sont fournis aux évaluateurs dans le cadre d'un accord de confidentialité (NDA).

Cyber Crucible dispose-t-il d'un programme de gestion des correctifs ?

Réponse courte : Oui. Un programme de gestion des correctifs et des vulnérabilités fondé sur les risques permet de maintenir à jour les logiciels, les pilotes de noyau, les serveurs et les postes de travail, et les constats sont suivis jusqu'à leur résolution.

Fonctionnement

Des tests de sécurité automatisés continus s'exécutent au sein du pipeline de développement, des tests d'intrusion manuels fondés sur les risques sont réalisés avec un minimum annuel, et des tests déclenchés par événement sont exécutés à chaque modification significative, couvrant à la fois les réseaux internes et externes. Les correctifs de sécurité et les correctifs à chaud sont appliqués conformément aux recommandations des fournisseurs, et les groupes propriétaires sont responsables de rester à jour sur les correctifs applicables. Les supports amovibles et portables sont soumis à la même protection et au même contrôle par analyse que les supports fixes.

Priorisation et déploiement

Les constats sont priorisés selon la gravité et l'exploitabilité, les vulnérabilités activement exploitées étant traitées via un parcours accéléré, hors bande. Les correctifs suivent le processus de gestion des changements — validés avant leur passage en production — et les mises à jour des pilotes de noyau sont revalidées via Microsoft WHCP avant leur publication.

Alignement avec les référentiels et limite de transparence

Le programme s'aligne sur les normes NIST SP 800-40, NIST SP 800-53 (SI-2, RA-5), CIS Control 7 et ISO/IEC 27001:2022 A.8.8. Aucune certification n'est revendiquée. Les délais de remédiation cibles spécifiques et les preuves de remédiation sont fournis aux évaluateurs sous accord de confidentialité (NDA).

Cyber Crucible dispose-t-il d'un plan de reprise après sinistre et de continuité d'activité ?

Réponse brève : Oui. Cyber Crucible maintient un plan de reprise après sinistre testé, dont la responsabilité incombe à la direction informatique, ainsi qu'une architecture conçue pour une haute disponibilité. Étant donné que la prévention des menaces s'exécute localement sur le poste, la protection du poste continue même en cas d'interruption du backend de gestion.

Résilience par l'architecture

Le backend de gestion est construit avec un stockage redondant et répliqué afin que la perte d'un nœud individuel n'entraîne ni perte de données ni interruption de service. L'accord de niveau de service (SLA) publié garantit une disponibilité mensuelle de 99,9 % pour le backend de gestion et de reporting, à l'exclusion de la maintenance planifiée et des causes échappant à un contrôle raisonnable. La protection du poste elle-même n'est pas affectée par une interruption du backend.

Sauvegardes et planification de contingence

Les données sont répliquées et sauvegardées en continu vers un stockage sécurisé hors site à l'aide d'identifiants privilégiés distincts, les sauvegardes étant protégées contre les rançongiciels grâce à une gestion hors ligne ou immuable, et testées régulièrement. Le plan comprend un plan d'intervention en cas d'urgence informatique, un plan de succession, une étude de criticité des données et une liste de criticité des services, et intègre une analyse d'impact sur l'activité, des stratégies de reprise, un plan de communication incluant la notification des clients, ainsi que des objectifs de reprise définis. Les tests comprennent des exercices de simulation sur table et des exercices de reprise.

Alignement avec les référentiels et limite en toute transparence

Le plan s'aligne sur la norme NIST SP 800-34 et sur les normes ISO/IEC 27001:2022 A.5.29–A.5.30. Cyber Crucible définit des objectifs de point de reprise (RPO) et de temps de reprise (RTO) pour le backend ; les valeurs cibles spécifiques, ainsi que le plan lui-même, sont communiqués aux évaluateurs sous accord de confidentialité (NDA). Étant donné que la protection s'exécute localement, la défense du poste se poursuit sans écart de temps de reprise significatif, que ce soit lors d'une interruption du backend ou dans un déploiement isolé du réseau (air-gapped).

Cyber Crucible dispose-t-elle d'un processus de réponse aux incidents et de notification des violations de données ?

Réponse courte : Oui. Un processus documenté de réponse aux violations de données définit les rôles et les étapes à suivre en cas de suspicion de vol, de violation ou d'exposition de données protégées, y compris la notification aux clients. Un délai de notification engagé peut être fixé par contrat pour les clients soumis à réglementation.

Le processus de réponse

Tout incident suspecté est signalé immédiatement via les canaux internes surveillés par la fonction Sécurité de l'information. Dès son identification, l'accès à la ressource concernée est supprimé et une équipe de réponse aux incidents, présidée par la direction générale, est réunie. Des enquêteurs et experts en criminalistique numérique, fournis dans le cadre de l'assurance cyber et technologique de Cyber Crucible, déterminent comment l'incident s'est produit, les données concernées, les parties affectées et la cause première. Un plan de communication est élaboré avec les services Juridique, Communication et Ressources humaines afin d'informer le personnel, le public et les parties concernées, selon le cas — y compris la notification aux clients via un canal convenu d'un commun accord — suivi d'un examen post-incident.

Réponse du support et notification

Les incidents affectant les clients sont suivis selon les niveaux de gravité définis dans le SLA publié (SEV1 à SEV4), et un délai de notification en cas de violation ou d'incident peut être engagé contractuellement pour les clients soumis à réglementation.

Alignement sur les référentiels et limites en toute transparence

Ce processus est aligné sur la norme NIST SP 800-61 et sur les clauses A.5.24 à A.5.26 de la norme ISO/IEC 27001:2022. Aucune certification n'est revendiquée. La procédure complète de réponse aux incidents et de notification des violations est communiquée aux évaluateurs sous accord de confidentialité (NDA).

Comment Cyber Crucible sécurise-t-il et contrôle-t-il les terminaux ?

Réponse courte : De deux manières. Le produit lui-même constitue une solution de prévention autonome des terminaux fonctionnant au niveau du noyau, et Cyber Crucible contrôle ses propres terminaux d'entreprise et d'ingénierie dans le cadre d'un programme formel. Les deux reposent sur le développement en interne du code le plus privilégié.

Protection des terminaux du produit

Le produit assure une prévention autonome contre les rançongiciels, les attaques en mémoire (sans fichier) et l'injection de processus, appliquée au niveau du noyau. Il est délibérément découplé des bibliothèques du système d'exploitation, de sorte que lorsque des attaquants compromettent ou détournent ces bibliothèques en mémoire, le produit continue de fonctionner, d'appliquer les protections et de générer des rapports. Étant donné que la détection et la réponse s'exécutent localement, la protection se poursuit lors d'une interruption du backend de gestion ou dans un déploiement délibérément isolé du réseau (air-gapped).

Intégrité de la chaîne d'approvisionnement et validation indépendante

Les algorithmes de détection, les heuristiques du noyau, les capteurs et les pilotes sont conçus et maintenus en interne ; aucune bibliothèque tierce non vérifiée ni aucun mécanisme de télémétrie caché n'est intégré au logiciel. Étant donné que le composant disposant des privilèges les plus élevés est propriétaire, toute une catégorie d'exposition liée à la chaîne d'approvisionnement des tiers est éliminée plutôt que simplement gérée. Tous les pilotes de noyau Windows sont validés et signés dans le cadre du Windows Hardware Compatibility Program (WHCP) de Microsoft.

Contrôles des terminaux d'entreprise

Les terminaux gérés suivent des configurations de référence sécurisées approuvées, exécutent une protection et une analyse des terminaux, et appliquent les mêmes contrôles aux supports amovibles et portables qu'aux supports fixes, l'utilisation non autorisée de supports étant restreinte. L'installation de logiciels est régie par une politique, les données au repos sur les terminaux sont chiffrées, et les terminaux sont maintenus à jour dans le cadre du programme de gestion des correctifs.

Alignement avec les référentiels et limites assumées

Les contrôles des terminaux s'alignent sur les CIS Critical Security Controls (v8) et le NIST SP 800-53 (SI-3, CM-2, MP-7). Aucune certification n'est revendiquée. Des normes de configuration détaillées et des preuves sont fournies aux évaluateurs sous accord de confidentialité (NDA).

Quelles politiques de sécurité Cyber Crucible maintient-elle, et comment puis-je les demander ?

Réponse brève : Cyber Crucible maintient un ensemble complet de politiques de sécurité de l'information — couvrant l'utilisation acceptable, l'accès et l'authentification, le chiffrement, la gestion des changements, la reprise après sinistre, la réponse aux incidents et aux violations, la rétention et la destruction des données, et bien plus encore. Les politiques et les preuves à l'appui sont mises à disposition des évaluateurs sous accord de non-divulgation (NDA).

Domaines de politique représentatifs

L'ensemble des politiques couvre l'utilisation acceptable et l'éthique ; l'accès, l'authentification et l'accès à distance ; le chiffrement et la protection des clés ; le développement sécurisé et la gestion des changements ; la sécurité des serveurs et des terminaux ; la reprise après sinistre et la continuité des activités ; la réponse aux incidents et aux violations ; ainsi que la rétention, la destruction des données et la rétention des e-mails. Des résumés de programme relatifs à la conformité, à l'audit et à la gouvernance IA/SDLC sont maintenus aux côtés de ces politiques.

Ce qui est public et ce qui relève du NDA

Les pages publiques de la base de connaissances décrivent l'existence, les principes et l'alignement sur les référentiels de chaque programme, de sorte qu'un évaluateur puisse comprendre la posture à un niveau général. Les documents de politique spécifiques, les normes de configuration, les chiffres exacts (tels que les calendriers de rétention et les objectifs de reprise) ainsi que les preuves d'audit sont confidentiels et fournis dans le cadre d'un accord de non-divulgation mutuel (NDA), accompagnés du dossier de diligence raisonnable fournisseur préparé.

Comment les demander

Les évaluateurs peuvent demander l'ensemble des politiques de sécurité, le dossier fournisseur préparé et les preuves à l'appui auprès de **dpo@cybercrucible.com**. L'accord de non-divulgation mutuel standard de Cyber Crucible est disponible si un tel accord n'est pas déjà en place. Aucune

certification n'est revendiquée pour un quelconque référentiel ; la documentation explique comment l'architecture et les contrôles répondent à chaque obligation.