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).

Revision #1
Created 2026-07-24 23:43:48 UTC by Dennis Underwood
Updated 2026-07-24 23:43:48 UTC by Dennis Underwood