Analyse et Surveillance Sécurité

GROUPE BRETAGNE PAYS DE LA LOIRE
UGECAM
Soigner, rééduquer, réinsérer : la santé sans préjugés

Accompagner et soigner en Bretagne et Pays de la Loire

UN GROUPE DE l'Assurance Maladie
Agir ensemble, protéger chacun

Dans le cadre de mes missions au sein de mon entreprise, j’ai pris en charge une partie de l’analyse et de la surveillance de la sécurité du système d’information, avec une approche clairement proactive. Concrètement, je surveille l’état du matériel et des postes de travail à l’aide de l’outil de supervision Nexthink, qui permet d’analyser en temps réel la conformité, la santé et l’usage des postes utilisateurs. L’objectif est de détecter en amont les machines qui ne sont pas au niveau attendu en matière de sécurité ou de standardisation, afin de réduire les risques et les interventions d’urgence.

Grâce aux tableaux de bord et aux packs “Security & Compliance” de Nexthink, je suis notamment les postes qui ne respectent pas les règles définies par la DSI : chiffrement du disque non activé, mises à jour système ou applicatives en retard, présence de comptes administrateur locaux non conformes, ou encore machines qui n’ont pas encore été migrées vers Windows 11 et Office 2024. J’utilise également les filtres et segments de Nexthink pour distinguer, par exemple, les postes utilisateurs standard, les machines sensibles (administratif, médical, etc.) et les équipements critiques, ce qui permet de prioriser les actions correctives sur les environnements les plus exposés.

Chaque mois, je consulte les rapports et indicateurs de conformité générés par la plateforme afin d’obtenir une vision globale des anomalies, de leur évolution et du taux de postes conformes par rapport aux objectifs fixés par la DSI. À partir de ces informations, je prépare un suivi structuré : listes de postes non conformes, type de problème rencontré (chiffrement, mises à jour, droits locaux, version de l’OS ou de la suite Office), et proposition de priorité de traitement. Ces éléments sont ensuite partagés avec le service support et les équipes concernées, qui prennent en charge les actions de remédiation (planification des mises à jour, corrections de configuration, retrait de comptes locaux, accompagnement des utilisateurs pour la migration, etc.).

Dans certains cas, je suis également le traitement de bout en bout : vérification que les actions ont bien été réalisées, contrôle sur Nexthink que les postes sont repassés au vert, et mise à jour du suivi pour éviter que les mêmes anomalies réapparaissent les mois suivants. Ce travail régulier de surveillance, d’alerte et de suivi m’a permis de contribuer à l’amélioration continue du niveau de sécurité et de conformité du parc postes de travail, tout en donnant à la DSI une visibilité plus fine sur la réalité terrain, les écarts persistants et les efforts restant à fournir.