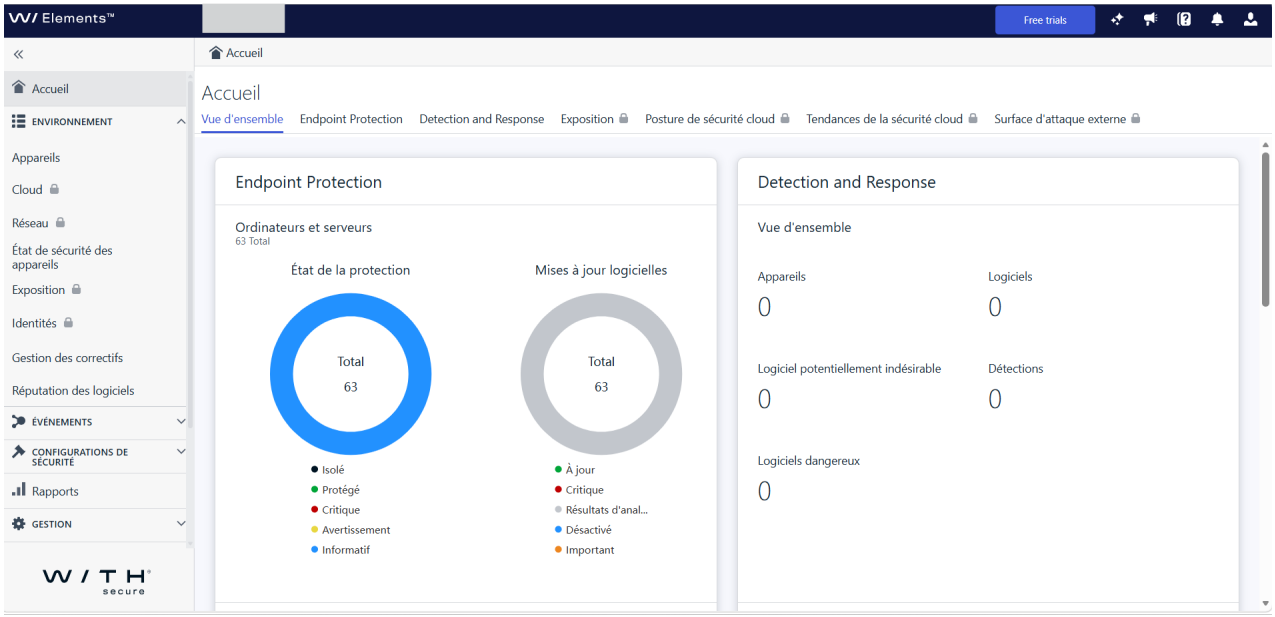
1. Introduction

1.1 Contexte de la mission

Dans le cadre de l'alternance en tant qu'apprenti administrateur systèmes et réseaux, cette mission portait sur la maintenance préventive et corrective du parc informatique de l'entreprise. L'objectif principal était d'assurer un niveau de sécurité satisfaisant tout en maintenant la disponibilité des postes de travail et des serveurs.

La solution retenue pour centraliser la supervision de la sécurité est **WithSecure Elements**, anciennement connue sous le nom de F-Secure. Cette plateforme permet de piloter la protection du parc depuis une interface web unique et d'assurer un suivi régulier de l'état de santé des équipements .



L'abonnement WithSecure a expiré, par conséquent les captures d'écran seront spéciales.

1.2 Objectifs de la mission

Les objectifs définis dans le cadre de cette activité étaient les suivants :

- Maintenir à jour les systèmes d'exploitation des postes clients et des serveurs .
- Assurer le suivi des mises à jour applicatives sur l'ensemble du parc .
- Superviser les alertes de sécurité depuis la console WithSecure .

- Détecter puis traiter les incidents de sécurité, comme les malwares ou les comportements anormaux .
- Garantir la conformité et l'intégrité de l'environnement informatique .

1.3 Périmètre d'intervention

Composant	Quantité	Type
Postes clients	Environ 50	Windows 11
Serveurs Windows	Environ 20	Windows Server 2022
Console d'administration	1	WithSecure Elements Portal

Le périmètre d'intervention couvrait à la fois les postes utilisateurs, les serveurs Windows et la console de supervision de sécurité .

2. Présentation de WithSecure Elements

2.1 Présentation générale

WithSecure est une solution de cybersécurité orientée entreprise. La suite Elements regroupe plusieurs briques de sécurité permettant de protéger les terminaux, de détecter les menaces avancées et de suivre les vulnérabilités du parc .

2.2 Architecture fonctionnelle

Module	Rôle
Elements EPP	Antivirus, antimalware et protection web des postes
Elements EDR	Détection avancée des menaces et réponse aux incidents
Vulnerability Management	Identification des vulnérabilités et aide à la remédiation
Security Cloud	Analyse comportementale en temps réel via le cloud
WithSecure Portal	Console web centralisée d'administration

Cette architecture permet de disposer d'une vue unifiée sur la sécurité du parc tout en facilitant le traitement des incidents.

2.3 Accès à la console d'administration

La console WithSecure Elements est accessible via un navigateur web et protégée par une authentification multifacteur. Depuis cette interface, il est possible de visualiser l'état de protection des équipements, de consulter les alertes, de lancer des analyses, de configurer des politiques et de produire des rapports .

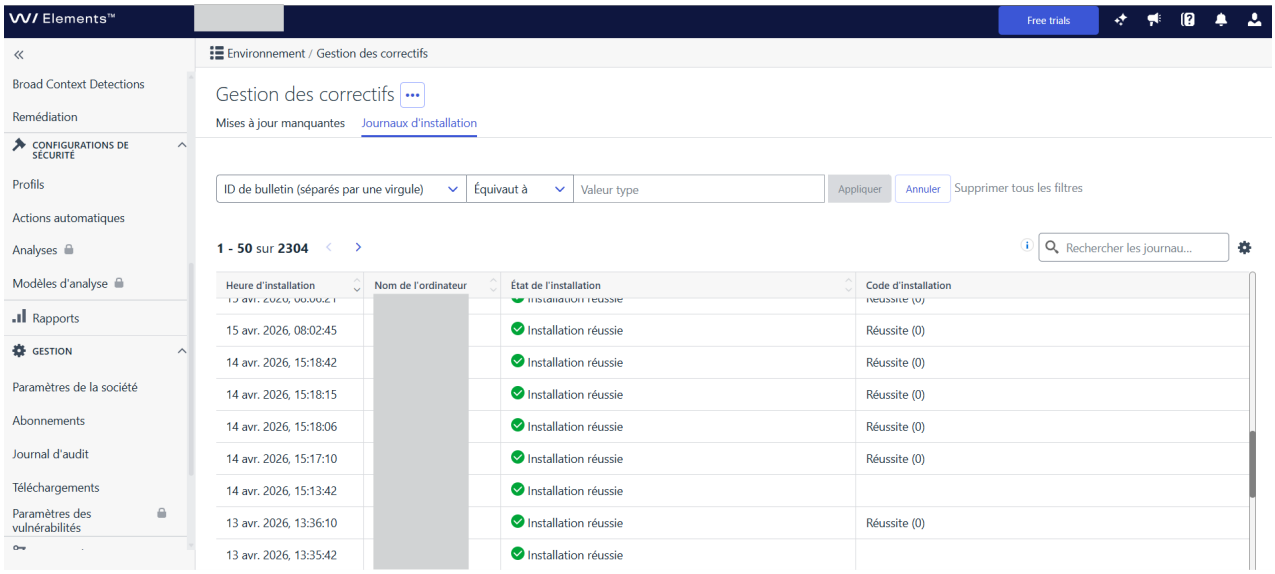
3. Gestion des mises à jour du parc

3.1 Mise à jour des postes clients

Les mises à jour des postes Windows sont gérées à l'aide de WSUS, avec un contrôle complémentaire réalisé dans WithSecure pour vérifier la conformité des équipements .

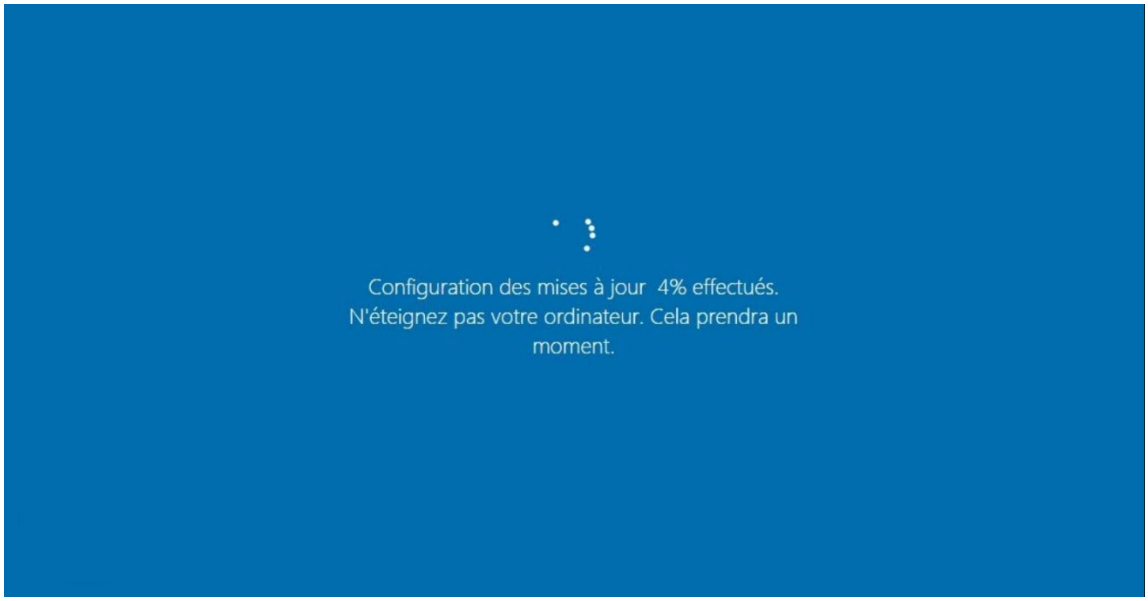
Étape	Action	Détail
1	Vérification des mises à jour disponibles	Consultation régulière du Patch Tuesday Microsoft et du portail WithSecure
2	Test sur poste pilote	Validation préalable sur une machine de test
3	Approbation et déploiement	Validation dans WSUS puis déploiement sur le parc
4	Suivi et vérification	Contrôle de la bonne application des mises à jour
5	Rapport d'intervention	Rédaction d'un compte-rendu des actions réalisées

Les mises à jour traitées concernent notamment les correctifs de sécurité, les mises à jour cumulatives Windows, les signatures antivirus WithSecure ainsi que, si nécessaire, les montées de version du système .



3.2 Mise à jour des serveurs

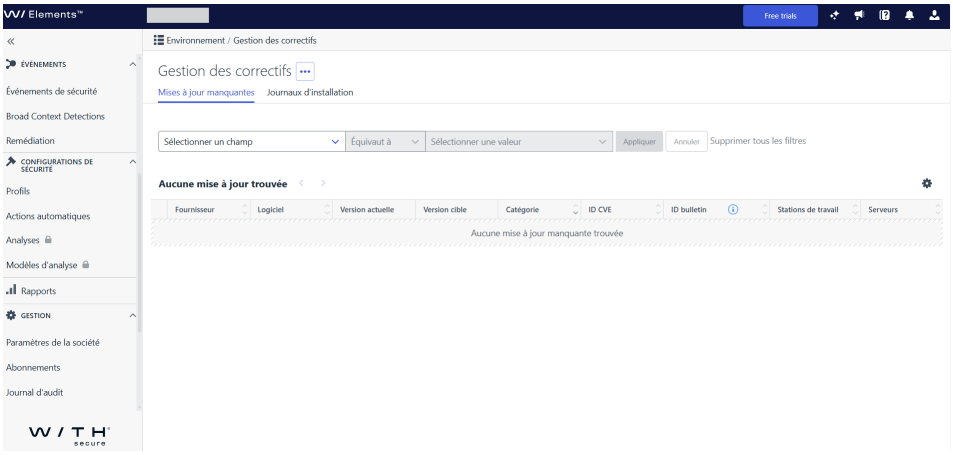
Les serveurs Windows font l'objet d'un traitement spécifique afin de préserver la continuité de service. Les interventions sont planifiées hors production, avec sauvegarde ou snapshot préalable, application des correctifs, redémarrage contrôlé puis vérification des services critiques comme AD DS, DNS ou DHCP .



3.3 Mise à jour des applications

Les applications installées sur le parc doivent également être maintenues à jour. WithSecure permet d'identifier les logiciels obsolètes, ce qui facilite la planification des actions correctives .

Application	Méthode de mise à jour	Fréquence
Microsoft Office 365	Microsoft Update / Intune	Mensuelle
Google Chrome / Firefox	Mise à jour automatique + contrôle manuel	Hebdomadaire
Adobe Reader / Acrobat	Adobe Update Manager	Mensuelle
Logiciels métier	Déploiement manuel ou via script	À la demande
Agent WithSecure	Déploiement depuis le portail Elements	Automatique

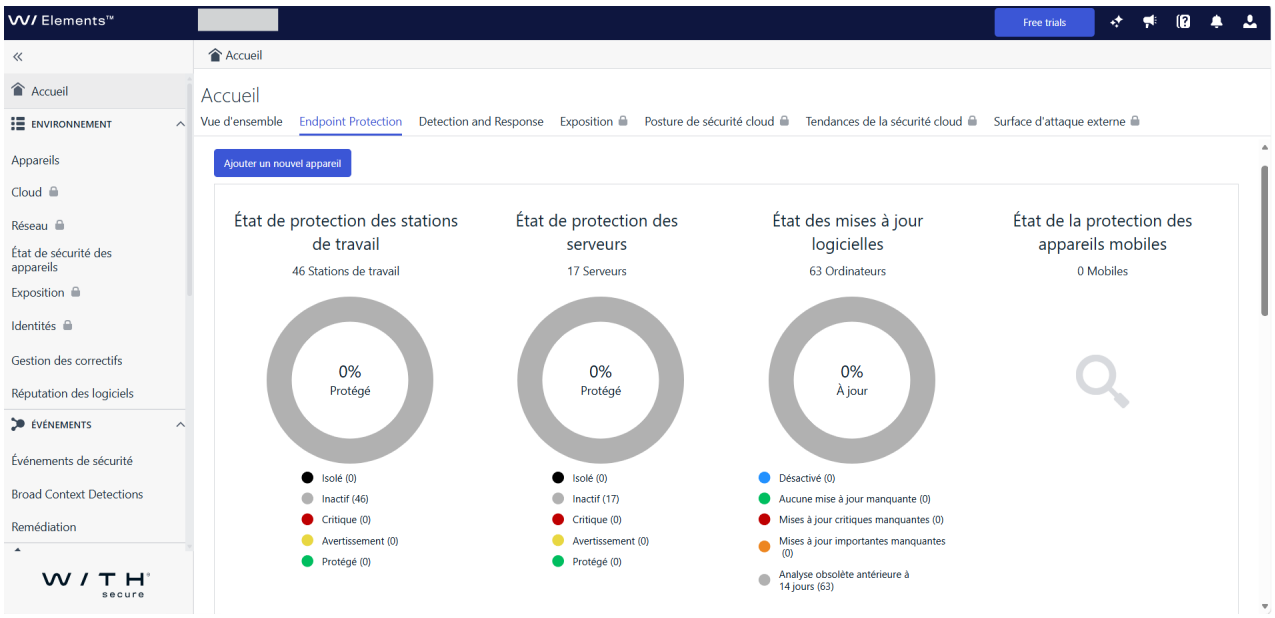


Aucune information n'est affiché car l'abonnement a expiré

4. Gestion des alertes de sécurité

4.1 Tableau de bord de supervision

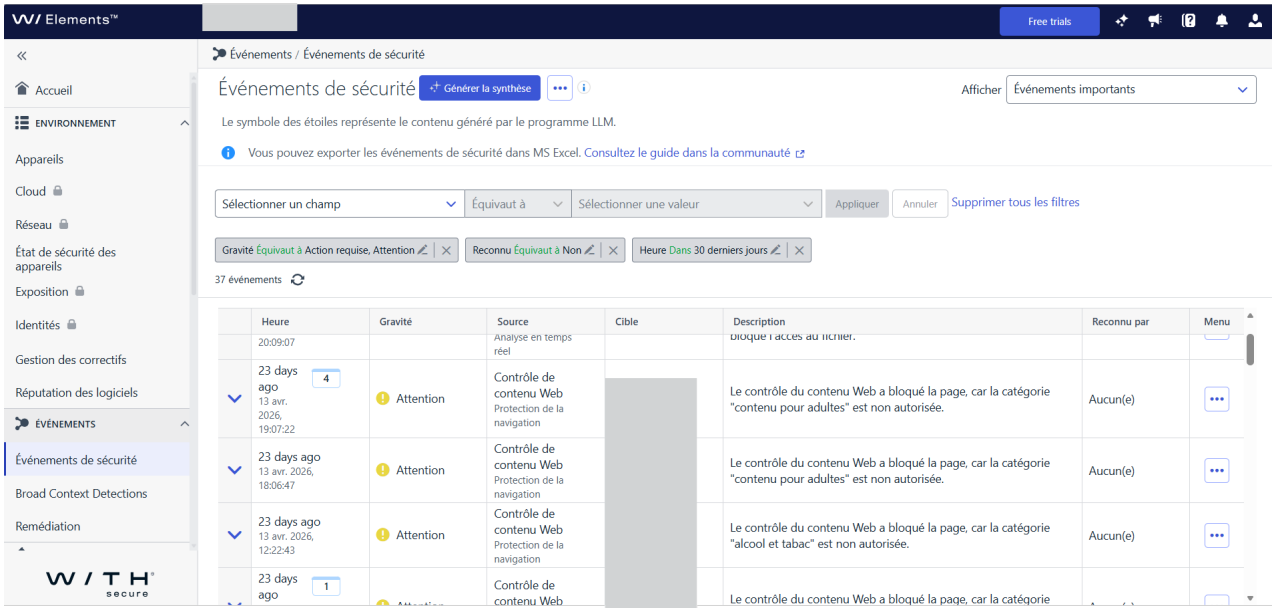
Le portail WithSecure offre un tableau de bord centralisé qui permet de suivre l'état global de la sécurité du parc. Les éléments surveillés au quotidien incluent le nombre d'alertes actives, leur niveau de criticité, l'état de protection des endpoints, les agents obsolètes et les événements récents .



4.2 Alertes de navigation non autorisée

WithSecure intègre un module de protection web capable de bloquer et journaliser l'accès à des sites dangereux ou non autorisés. L'analyse de ces alertes permet d'identifier les postes concernés, de comprendre la nature du blocage et, si besoin, d'adapter les politiques de filtrage .

Catégorie bloquée	Niveau de risque	Action à mener
Sites de phishing	Critique	Vérification immédiate du poste et scan antivirus
Commandes et contrôle (C&C)	Critique	Isolation du poste et investigation approfondie
Téléchargements non autorisés	Élevé	Avertissement utilisateur et remontée hiérarchique
Réseaux sociaux hors politique	Moyen	Rapport statistique et rappel des règles
Publicités / tracking	Faible	Journalisation sans action immédiate



4.3 Alertes de détection de malwares

La détection de malwares représente l'un des incidents les plus critiques à traiter. Lorsqu'une menace est remontée par la plateforme, une procédure structurée est appliquée afin d'identifier l'incident, d'évaluer sa gravité, d'isoler si besoin la machine concernée, de lancer une analyse complète, de supprimer ou mettre en quarantaine le fichier, puis de vérifier le retour à un état sain .

Étape	Action	Détail
1	Identification	Analyse du nom de la menace, du poste concerné, du chemin et de l'horodatage
2	Évaluation	Détermination du niveau de gravité
3	Confinement	Isolation du poste en cas de menace critique
4	Analyse	Scan complet et étude des détails de détection
5	Nettoyage	Quarantaine ou suppression du fichier malveillant
6	Vérification	Nouveau contrôle après remédiation
7	Rapport	Création d'un rapport d'incident et ticket GLPI

Heure	Gravité	Source	Cible	Description	Reconnu par	Menu
22 days ago 14 avr. 2026, 20:09:16	Attention	Analyse de fichier Analyse en temps réel		Le produit a détecté « riskware » dans « WCInstaller.exe » et a bloqué l'accès au fichier.	Aucun(e)	•••
22 days ago 14 avr. 2026, 20:09:07	Attention	Analyse de fichier Analyse en temps réel		Le produit a détecté « riskware » dans « WebCompanion.exe » et a bloqué l'accès au fichier.	Aucun(e)	•••

4.4 Autres alertes surveillées

D'autres alertes sont également suivies, notamment les vulnérabilités connues, les non-conformités à la politique de sécurité, les comportements suspects remontés par l'EDR et les défauts de communication de l'agent WithSecure .

4.5 Priorisation du traitement

Le traitement des alertes repose sur une matrice de criticité afin d'assurer une prise en charge adaptée à l'impact potentiel sur le système d'information .

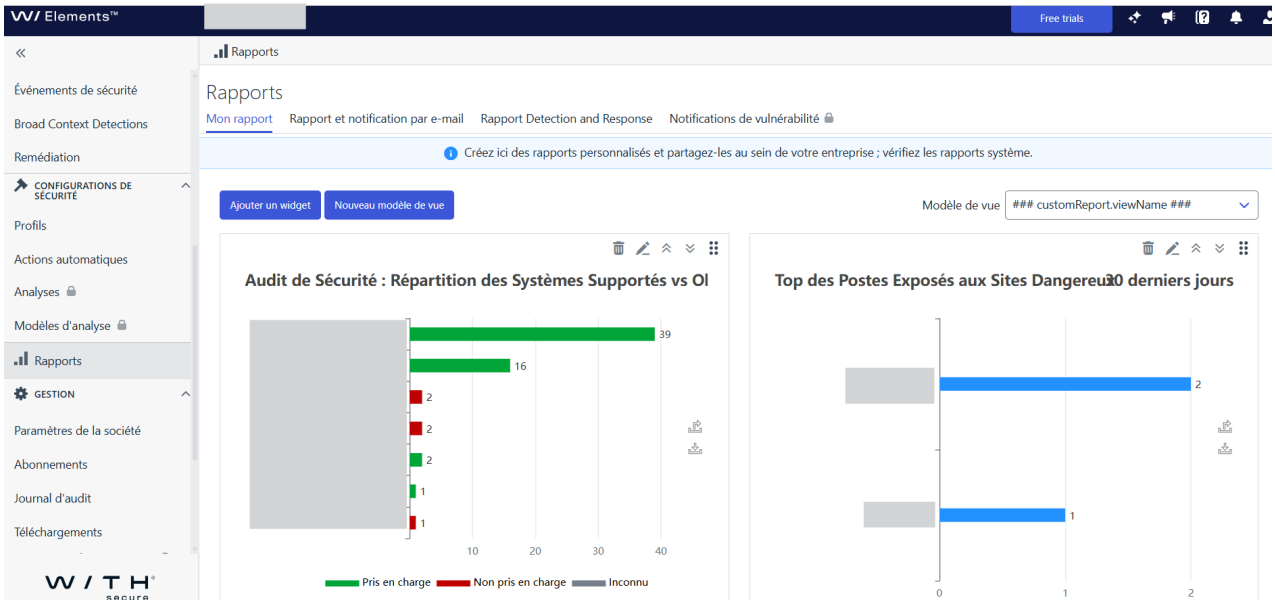
Criticité	Délai de traitement	Exemple	Responsable
Critique	Immédiat (< 1h)	Ransomware, C&C actif	Administrateur systèmes
Élevé	Dans la journée	Trojan, phishing actif	Administrateur systèmes
Moyen	Sous 48h	PUP, site suspect	Technicien support
Faible	Hebdomadaire	Adware, tracking	Rapport mensuel

5. Procédures opérationnelles

5.1 Routine de surveillance

La maintenance du parc s'appuie sur une routine de surveillance régulière afin d'anticiper les incidents et de conserver une visibilité complète sur l'environnement .

Fréquence	Tâche
Quotidien	Consultation du tableau de bord et vérification des alertes critiques et élevées
Quotidien	Contrôle de la connectivité des agents
Hebdomadaire	Revue complète des alertes de la semaine
Hebdomadaire	Vérification et approbation des mises à jour WSUS
Mensuel	Mise à jour des serveurs hors heures ouvrables
Mensuel	Génération d'un rapport de sécurité et analyse des tendances
Mensuel	Vérification des applications tierces



6. Bilan et compétences mobilisées

6.1 Compétences techniques développées

Cette mission a permis de renforcer plusieurs compétences opérationnelles, en particulier l'administration d'une solution EDR/EPP, la gestion du patching, la réponse à incident et l'analyse des journaux de sécurité .

Compétence	Mise en œuvre concrète
Administration EDR/EPP	Gestion quotidienne de la console WithSecure Elements
Gestion du patching	Déploiement via WSUS et mises à jour manuelles ciblées
Réponse aux incidents	Traitement des alertes malware selon une procédure définie
Analyse des logs	Exploitation des journaux de navigation et de sécurité

6.2 Compétences BTS SIO mobilisées

Cette activité couvre plusieurs compétences du référentiel BTS SIO, notamment le recensement des infrastructures, la sécurisation du SI, la participation à la continuité de service, le traitement des incidents et la documentation des interventions .

- B1.1 – Recenser et caractériser les infrastructures physiques et virtuelles d'un SI .
- B1.2 – Recenser et caractériser les services attendus et les ressources associées .
- B2.2 – Assurer la sécurité de l'infrastructure .
- B2.3 – Participer à la continuité de service .
- B3.1 – Traiter des situations d'incident .
- B4 – Travailler en mode projet et documenter les interventions .

6.3 Apport de la mission

Cette mission illustre concrètement l'importance de la maintenance en condition opérationnelle et de la supervision sécurité dans un environnement professionnel. Elle montre également comment une solution comme WithSecure Elements peut servir à la fois d'outil de protection, d'aide à la décision et de support à la gestion des incidents .