ENSEIGNEMENT CATHOLIQUE
URADEL Pays de la Loire

Webinaire offre régionale Antivirus – With Secure

Contexte

- Jusqu'alors (+15 ans), les établissements d'enseignement catholique bénéficiaient de **licences antivirus fournies gratuitement par le rectorat** dans le cadre d'un marché passé par le ministère de l'éducation nationale auprès de Trend Micro.
- **Nombre d'établissements catholiques couverts en Pays de la Loire** :
  - ***34*** *collèges*
  - ***44*** *lycées*
  - ***45*** *ensembles scolaires*

  + instances enseignement catholique (DDEC, etc.)
- **Estimatif du nombre postes informatiques couverts** : environ **35 000** postes

- Début 2024 : Annonce de **désengagement du ministère** à partir d'octobre 2024

→ **Elaboration d'une offre régionale** par le pôle numérique de l'URADEL

Pourquoi WithSecure ?

- ✓ **Une solution plus simple et moins contraignante pour les établissements :**
  Gestion en Cloud, administration et interface simplifiées
- ✓ **Une solution plus complète et sécurisée** :
  Fonctionnalités complémentaires nécessaires pour la sécurisation des établissements (mises à jour du parc logiciel, EDR, etc.)
- ✓ **Une solution européenne également sélectionnée par l'EC Bretagne :**
  Déjà proposée aux collèges, lycées et DDEC. Déploiement dans toutes les écoles au cours de l'année scolaire 2024-2025
- ✓ **Un accompagnement technique de la société With Secure :**
  Ateliers techniques, documentations, etc.
- ✓ **Conserver l'homogénéité des solutions de sécurisation dans nos établissements**
  Continuité dans l'entraide entre pairs au niveau régional
- ✓ **Des tarifs abordables et acceptables pour les établissements**

Pourquoi choisir une solution antivirus Client-Serveur?

1. Gestion Centralisée

- ✓ **Simplicité** : gestion de tous les postes depuis un seul point central.
- ✓ **Efficacité** : déploiement rapide des mises à jour et configurations.
- ✓ **Moins de Temps Perdu** : permet de se concentrer sur d'autres tâches

2. Sécurité Renforcée

- ✓ **Protection Complète** : couverture des postes de travail, serveurs et mobiles.
- ✓ **Détection Avancée** : fonctionnalités comme la détection en temps réel et l'analyse comportementale.
- ✓ **Suivi en Temps Réel** : rapports détaillés sur l'état de la sécurité.

3. Réduction des Risques

- ✓ **Réduction des risques** de points de défaillance individuels.
- ✓ **Réponse Rapide** : Réaction rapide et efficace en cas d'incident,

WithSecure Elements EPP et EDR

CLIENT RESTRICTED

+ de 30 ans
d'expertise

1988

30 Pays

1 300 employés

5 a 10 000 utilisateurs

Spécialiste
Endpoint & cloud





Protection
&
confidentialité

co-sécurité

Face aux défis de la cybersécurité, agir seul est sans effet.

WITH secure

CLIENT RESTRICTED



Computers

Windows, Mac, Linux



Server

Windows, Linux



Email

Microsoft Outlook



Cloud collaboration apps

Microsoft Teams, SharePoint, OneDrive



Networks

Vulnerability scans

Elements™

Un agent unique
EPP + EDR + Vuln

Threat Intelligence

Un centre de sécurité



WITH secure

CLIENT RESTRICTED

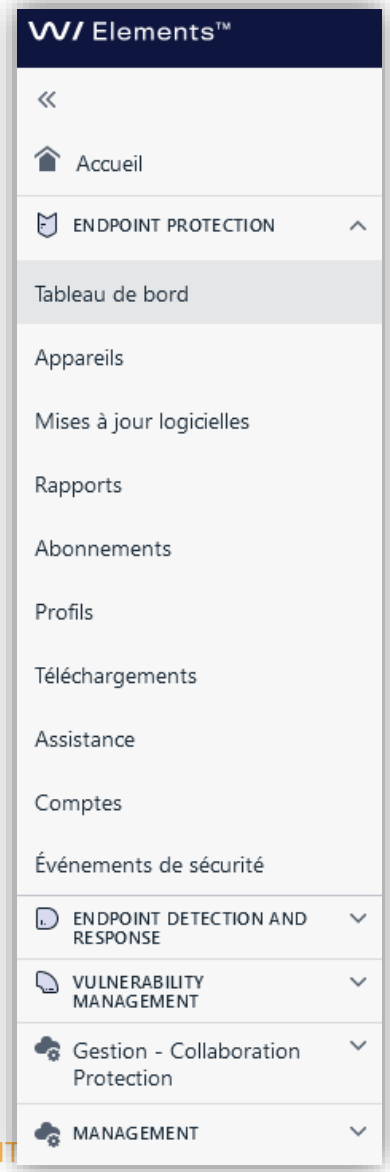
Elements EPP : fonctionnalités

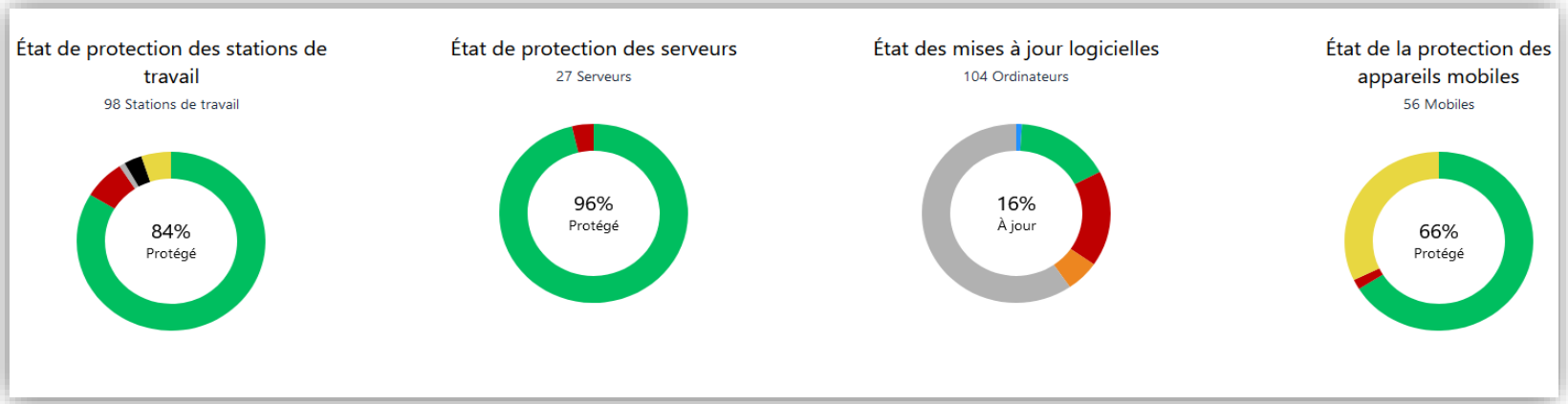
Anti-Virus

	Elements EPP for Windows	Elements EPP for Windows Servers	Elements EPP for macOS	Elements EPP for Linux
Multi-Engine malware protection				
Cloud analysis				
Advanced & Behavioral Protection	 DeepGuard	 DeepGuard	 XFence	-
Firewall Management				
Patch Management				-
Browsing Protection / Web Content Control				-
Device Control			-	-
Application Control			 XFence	-
Data Protection	 DataGuard	 DataGuard	-	 File Integrity Control
System Event Detection			-	-
Server Share Protection	-		-	-

CLIENT RESTRICTED

Accès rapide aux informations

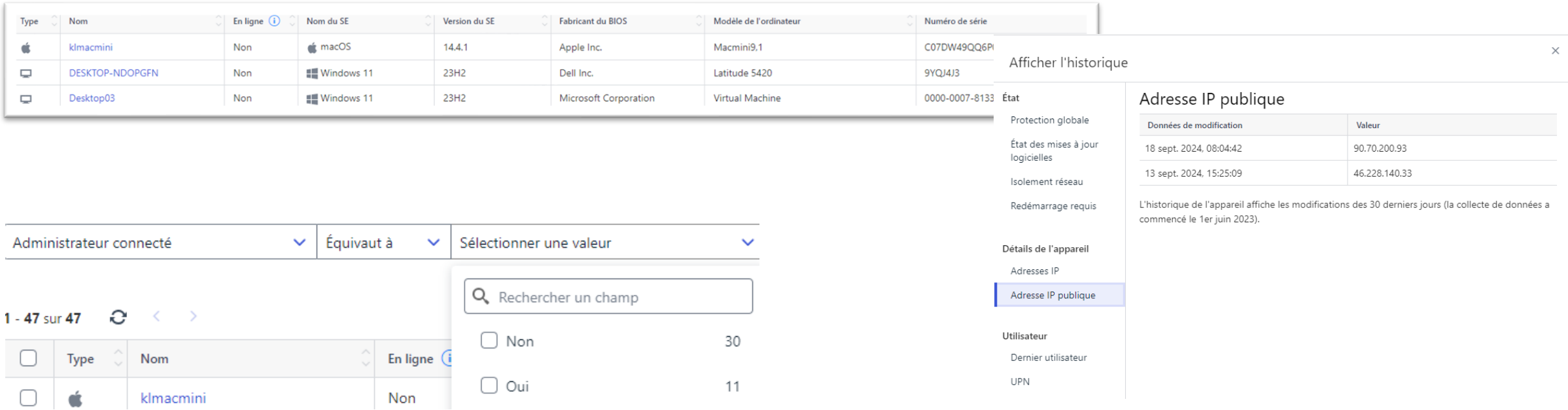


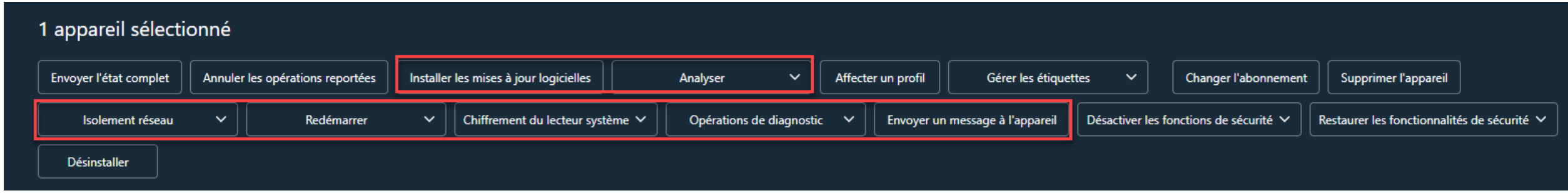


Problèmes

Type d'éléments	Gravité	Appareils concernés
Mises à jour logicielles critiques manquantes Utilisez Software Updater pour appliquer les mises à jour critiques. Utilisez « Tâches automatisées » dans le profil pour automatiser l'installation des mises à jour logicielles. Vérifiez 18 appareils Des mises à jour critiques sont manquantes dans le logiciel tiers de l'appareil. Ces mises à jour peuvent être installées via la page « Software Updater » ou automatisées sous l'onglet « Automatisation » du profil. Les mises à jour critiques doivent toujours être effectuées et automatisées, car elles comprennent des correctifs qui peuvent réduire considérablement la surface d'attaque pour les cybercriminels ou même corriger les vulnérabilités zero-day.	Critique	18
Analyse en temps réel désactivée Vérifiez que l'analyse en temps réel est activée sur le profil. Si ce n'est pas le cas, activez le paramètre. Verrouillez-le afin que les utilisateurs ne puissent pas le désactiver. Vérifiez 9 appareils	Critique	9
Problème lors de l'analyse en temps réel Vérifiez la version du client. Assurez-vous que le lecteur système de l'appareil contient suffisamment d'espace disque disponible (plus de 5 Go). Redémarrez l'appareil. Vérifiez 4 appareils	Critique	4
Appareils avec des incidents EDR graves ouverts Résoudre les incidents sur les appareils. Vérifiez 3 appareils	Critique	3
Définitions de programme malveillant obsolètes Envoyer la mise à jour complète de l'état à l'appareil. Démarrer l'appareil. Vérifiez 2 appareils	Critique	2
Le pare-feu est désactivé Verrouillez le paramètre de pare-feu sur le profil afin que les utilisateurs ne puissent pas le désactiver. Vérifiez 1 appareils	Critique	1
Exclusions dangereuses Vérifiez et gérez les exclusions dans le profil. Assurez-vous qu'il ne contient aucune exclusion dangereuse. Vérifiez 1 appareils	Critique	1
Clients en fin de vie Mettez à jour le logiciel client. Si des produits en fin de vie (EOL) sont utilisés, remplacez-les par des produits actuels (sidegrade). Vérifiez 26 appareils	Important	26

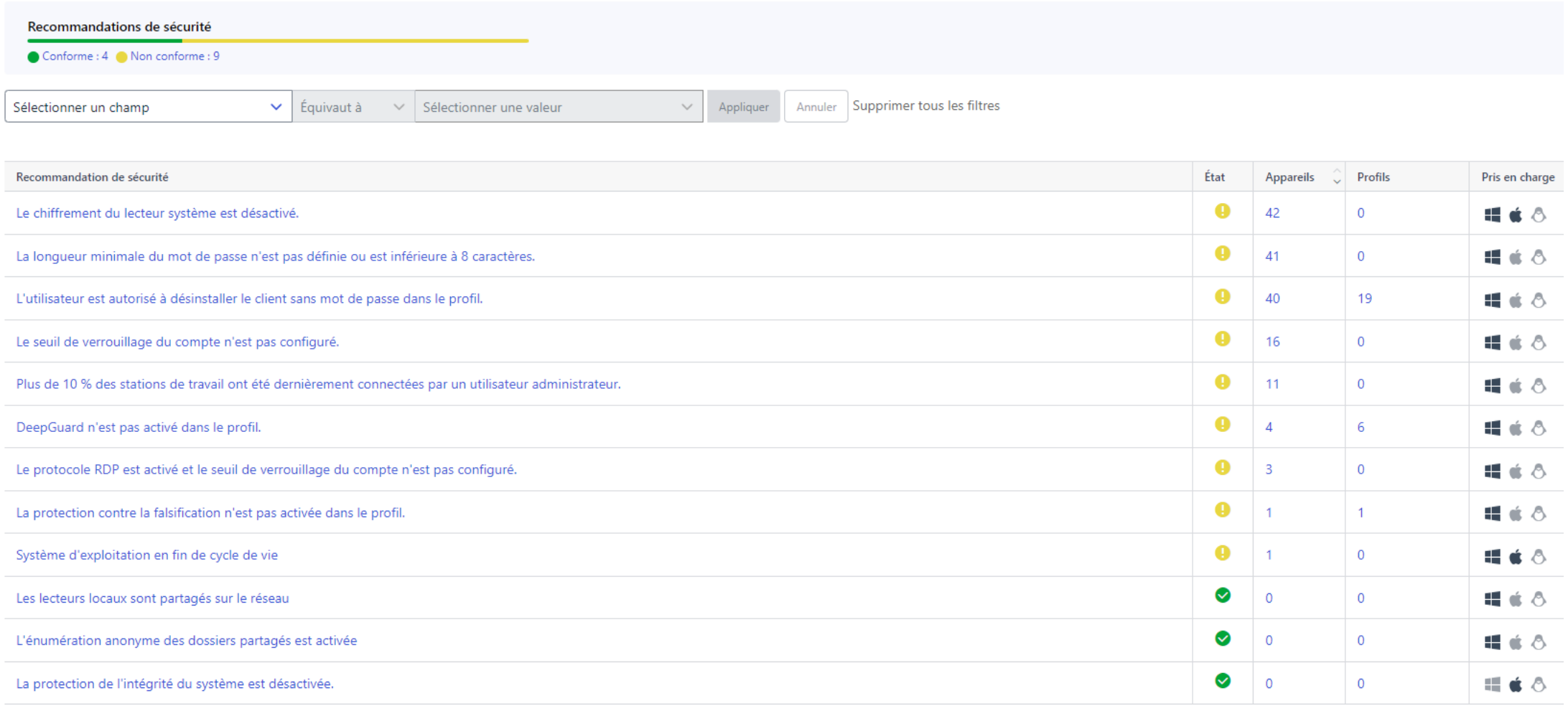
Améliorer sa productivité





CLIENT RESTRICTED

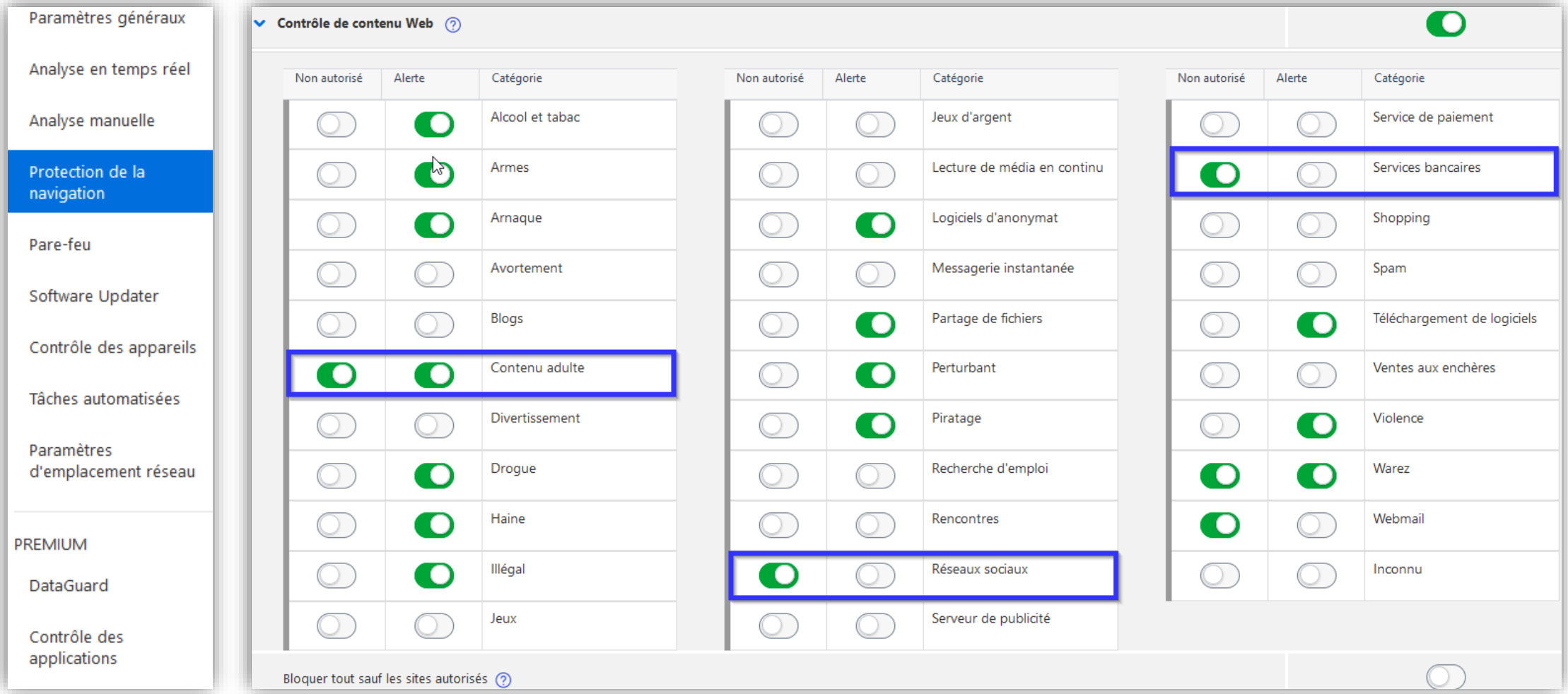
Diminuer le risque / améliorer la posture



Recommandation de sécurité	État	Appareils	Profils	Pris en charge
Le chiffrement du lecteur système est désactivé.	!	42	0	
La longueur minimale du mot de passe n'est pas définie ou est inférieure à 8 caractères.	!	41	0	
L'utilisateur est autorisé à désinstaller le client sans mot de passe dans le profil.	!	40	19	
Le seuil de verrouillage du compte n'est pas configuré.	!	16	0	
Plus de 10 % des stations de travail ont été dernièrement connectées par un utilisateur administrateur.	!	11	0	
DeepGuard n'est pas activé dans le profil.	!	4	6	
Le protocole RDP est activé et le seuil de verrouillage du compte n'est pas configuré.	!	3	0	
La protection contre la falsification n'est pas activée dans le profil.	!	1	1	
Système d'exploitation en fin de cycle de vie	!	1	0	
Les lecteurs locaux sont partagés sur le réseau	✓	0	0	
L'énumération anonyme des dossiers partagés est activée	✓	0	0	
La protection de l'intégrité du système est désactivée.	✓	0	0	

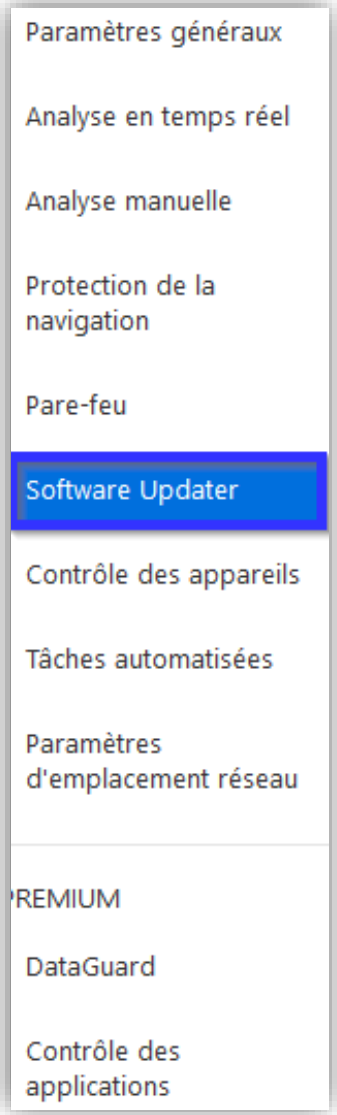
CLIENT RESTRICTED

Protection Web par catégories



CLIENT RESTRICTED

Correction automatique des vulnérabilités



Mises à jour logicielles

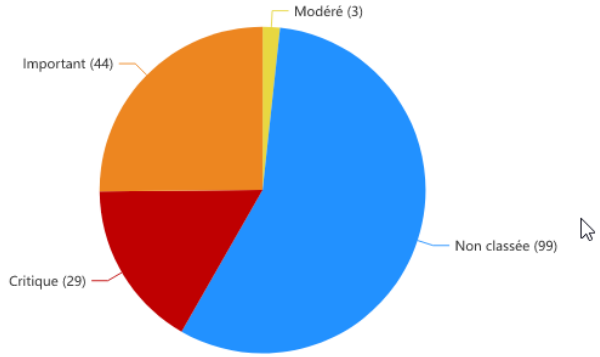
Mises à jour manquantes | Résumé de l'installation | Historique des installations

Catégorie Toutes les mises à jour | Fournisseur Tous les fournisseurs | Logiciel Tous les logiciels | Type de plate-forme Toutes les plateformes

Fournisseur	Logiciel	Version actuelle	Version cible	Catégorie	ID CVE	ID bulletin	Ordinateurs	Serveurs
Microsoft Corporation	Microsoft Edge 107.0.1418.35	N/D	N/D	Sécurité importante	7.1 CVE-2022-3723	FSPM-3103-37031-183/x64	1	0
Google Inc.	Google Chrome	106.0.5249.119	107.0.5304.88	Sécurité importante	8.8 CVE-2022-3652	FSPM-41-3794-4/x64	3	0
Adobe Systems Inc.	Adobe Acrobat Reader DC Continuous	22.002.20212	22.003.20263	Sécurité modérée	7.8 CVE-2022-42339	FSPM-2819-50065-1/x86	1	0
Spencer Kimball, Peter Mattis and the GIMP Development Team	GIMP	2.10.30	2.10.32	Sécurité modérée	5.5 CVE-2022-30067	FSPM-708-16875-35/x64	1	0
Igor Pavlov	7-Zip (x64)	21.06	22.01	Sécurité importante	7.8 CVE-2022-29072	FSPM-200-64642-82/x64	1	0

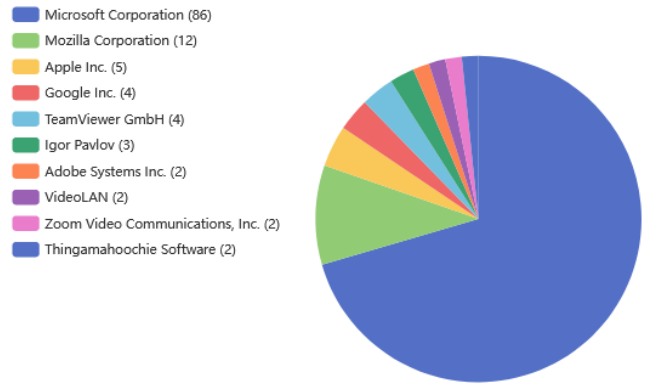
Statistiques de gravité des patchs

Toutes les plateformes



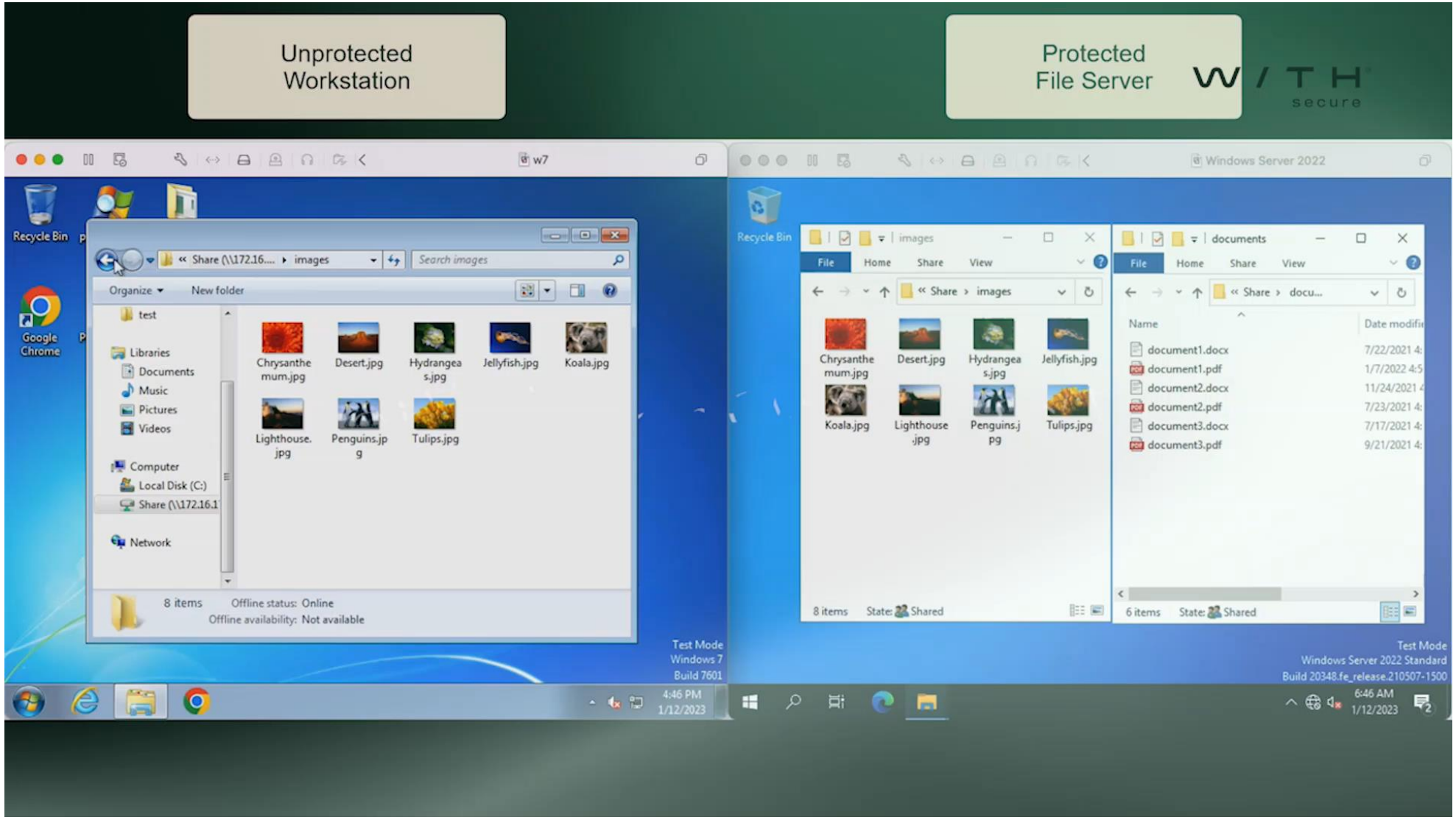
Principaux fournisseurs par nombre de patchs

Toutes les plateformes



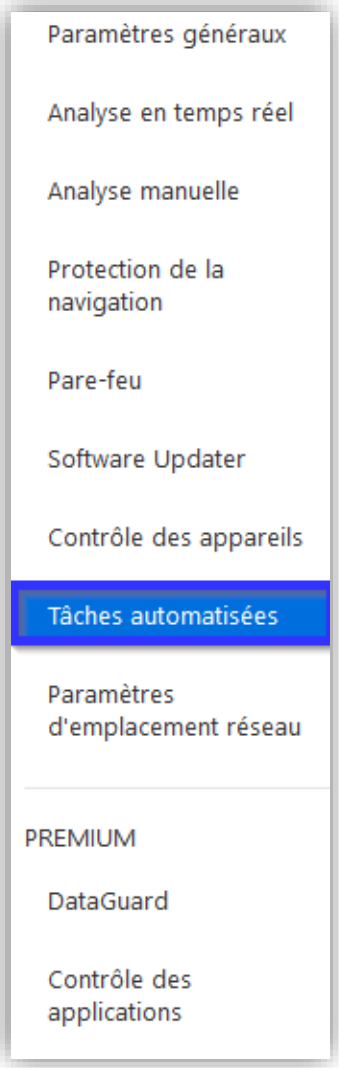
CLIENT RESTRICTED

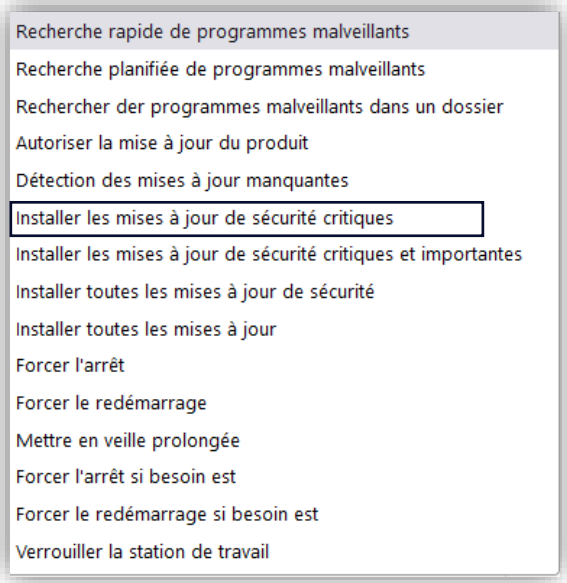
Rollback et protection des serveurs de fichiers

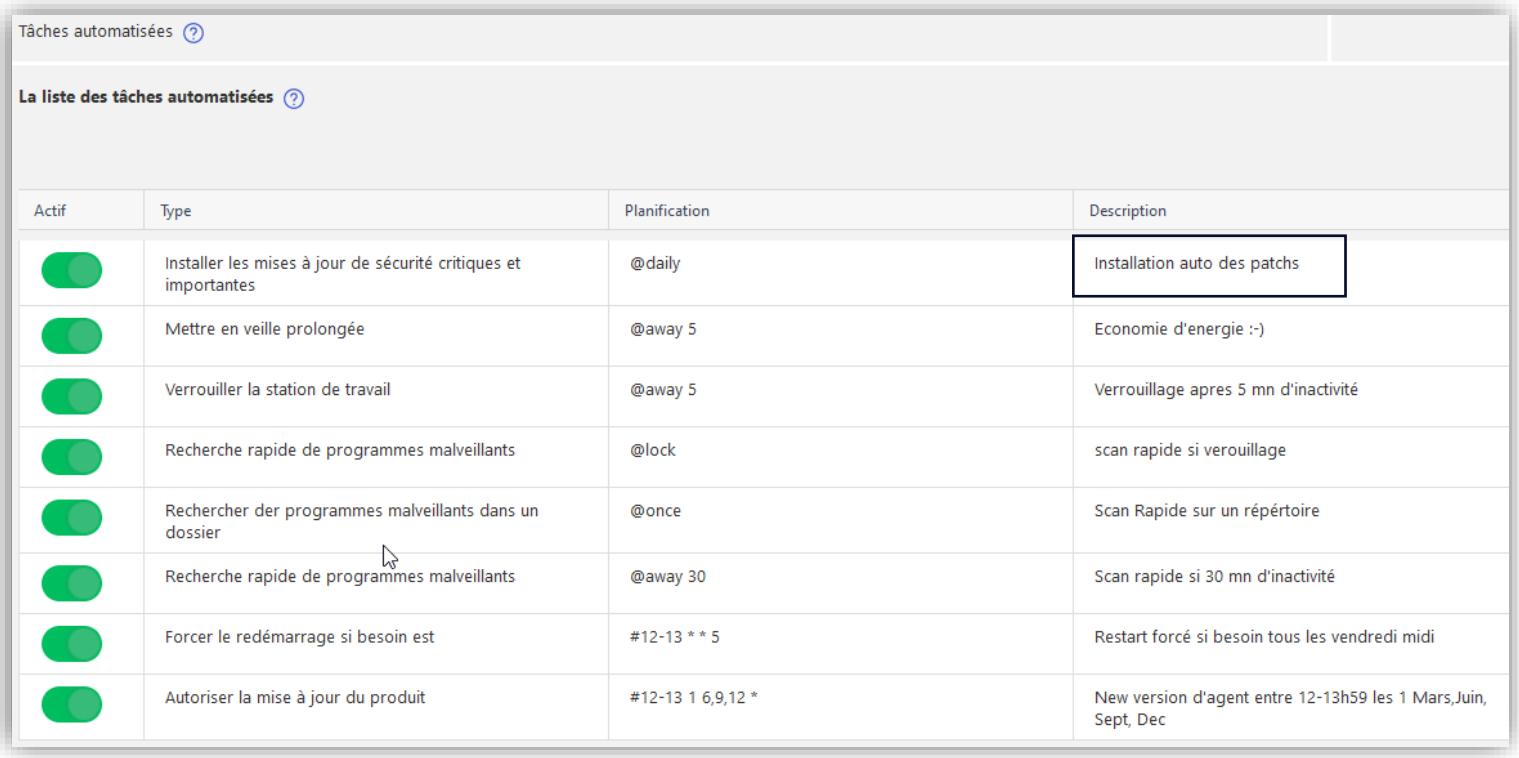


CLIENT RESTRICTED

Automatisation des tâches



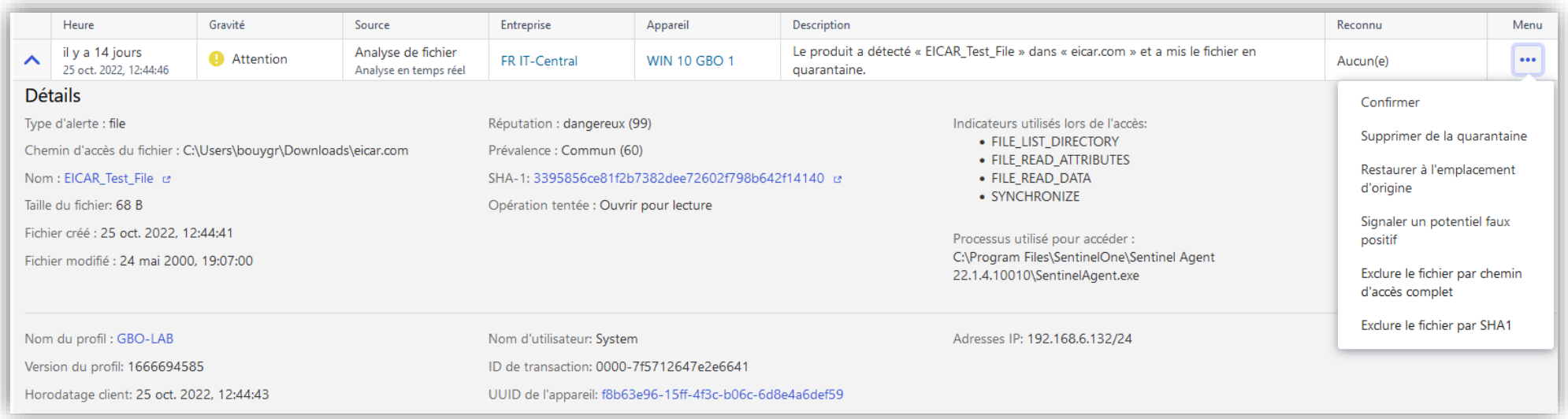




Actif	Type	Planification	Description
	Installer les mises à jour de sécurité critiques et importantes	@daily	Installation auto des patchs
	Mettre en veille prolongée	@away 5	Economie d'energie :-)
	Verrouiller la station de travail	@away 5	Verrouillage apres 5 mn d'inactivité
	Recherche rapide de programmes malveillants	@lock	scan rapide si verouillage
	Rechercher der programmes malveillants dans un dossier	@once	Scan Rapide sur un répértoire
	Recherche rapide de programmes malveillants	@away 30	Scan rapide si 30 mn d'inactivité
	Forcer le redémarrage si besoin est	#12-13 * * 5	Restart forcé si besoin tous les vendredi midi
	Autoriser la mise à jour du produit	#12-13 1 6,9,12 *	New version d'agent entre 12-13h59 les 1 Mars,Juin, Sept, Dec

CLIENT RESTRICTED

Exploitation simple, intuitive



	Heure	Gravité	Source	Entreprise	Appareil	Description	Reconnu	Menu
^	il y a 14 jours 25 oct. 2022, 12:44:46	Attention	Analyse de fichier Analyse en temps réel	FR IT-Central	WIN 10 GBO 1	Le produit a détecté « EICAR_Test_File » dans « eicar.com » et a mis le fichier en quarantaine.	Aucun(e)	•••

Détails

Type d'alerte : file
Chemin d'accès du fichier : C:\Users\bouygr\Downloads\eicar.com
Nom : EICAR_Test_File
Taille du fichier: 68 B
Fichier créé : 25 oct. 2022, 12:44:41
Fichier modifié : 24 mai 2000, 19:07:00

Réputation : dangereux (99)
Prévalence : Commun (60)
SHA-1: 3395856ce81f2b7382dee72602f798b642f14140
Opération tentée : Ouvrir pour lecture

Indicateurs utilisés lors de l'accès:
- FILE_LIST_DIRECTORY
- FILE_READ_ATTRIBUTES
- FILE_READ_DATA
- SYNCHRONIZE

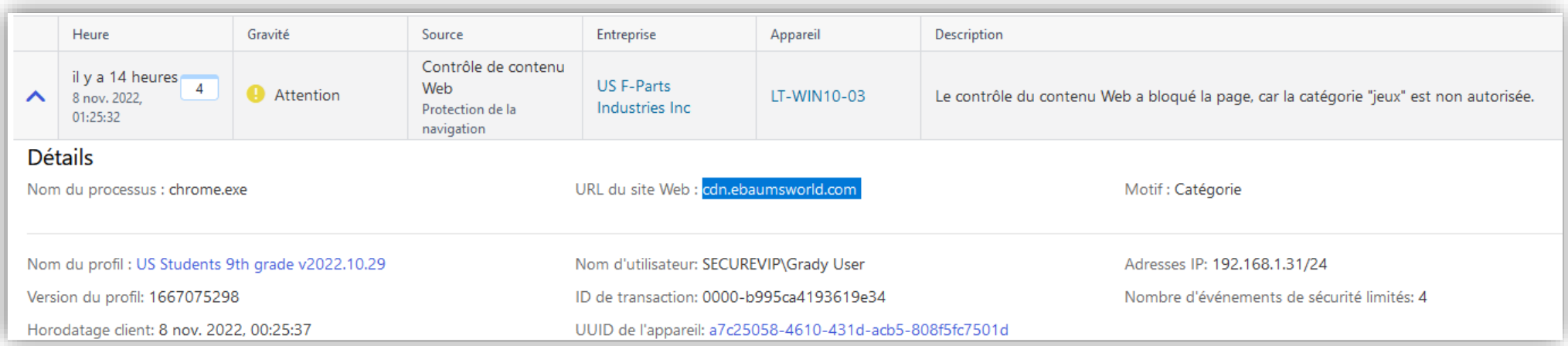
Processus utilisé pour accéder :
C:\Program Files\SentinelOne\Sentinel Agent 22.1.4.10010\SentinelAgent.exe

Nom du profil : GBO-LAB
Version du profil: 1666694585
Horodatage client: 25 oct. 2022, 12:44:43

Nom d'utilisateur: System
ID de transaction: 0000-7f5712647e2e6641
UUID de l'appareil: f8b63e96-15ff-4f3c-b06c-6d8e4a6def59

Adresses IP: 192.168.6.132/24

Confirmer
Supprimer de la quarantaine
Restaurer à l'emplacement d'origine
Signaler un potentiel faux positif
Exclure le fichier par chemin d'accès complet
Exclure le fichier par SHA1



	Heure	Gravité	Source	Entreprise	Appareil	Description
^	il y a 14 heures 4 8 nov. 2022, 01:25:32	Attention	Contrôle de contenu Web Protection de la navigation	US F-Parts Industries Inc	LT-WIN10-03	Le contrôle du contenu Web a bloqué la page, car la catégorie "jeux" est non autorisée.

Détails

Nom du processus : chrome.exe
URL du site Web : cdn.ebaumsworld.com
Motif : Catégorie

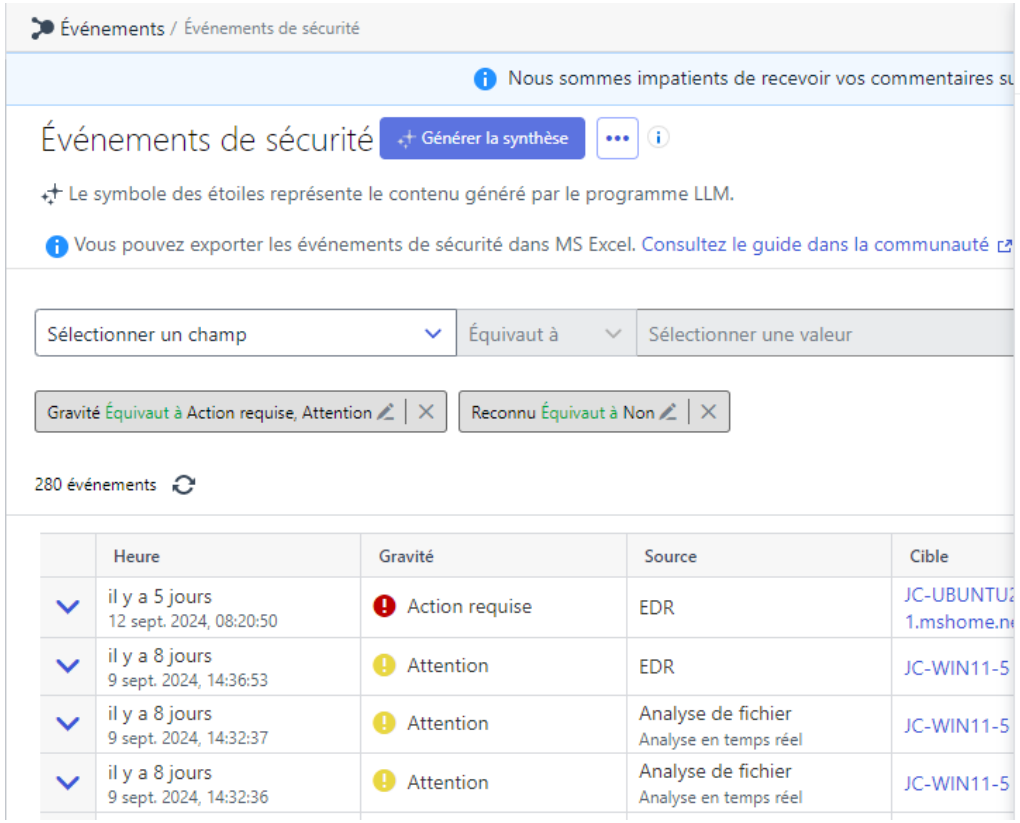
Nom du profil : US Students 9th grade v2022.10.29
Version du profil: 1667075298
Horodatage client: 8 nov. 2022, 00:25:37

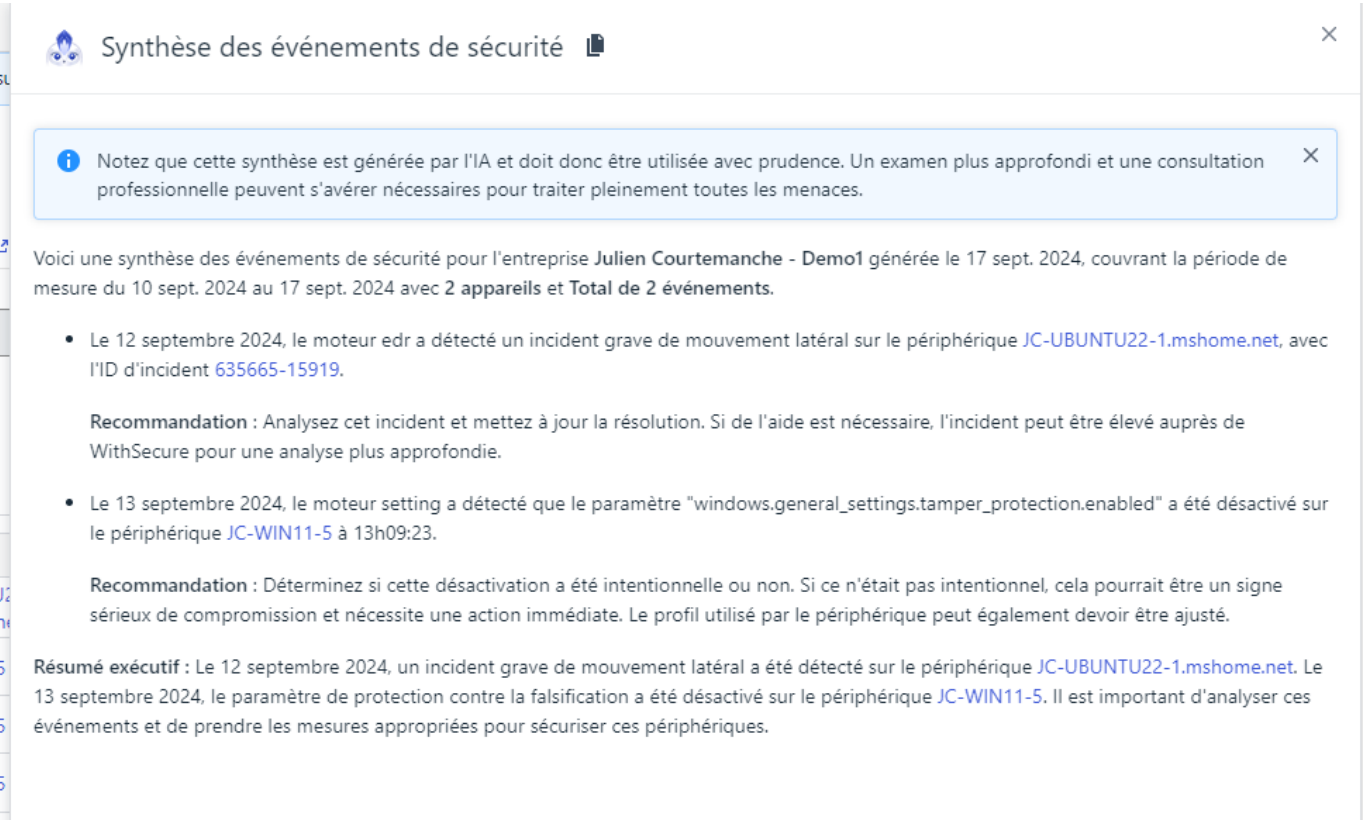
Nom d'utilisateur: SECUREVIP\Grady User
ID de transaction: 0000-b995ca4193619e34
UUID de l'appareil: a7c25058-4610-431d-acb5-808f5fc7501d

Adresses IP: 192.168.1.31/24
Nombre d'événements de sécurité limités: 4

CLIENT RESTRICTED

Et assistée par notre IA Luminem





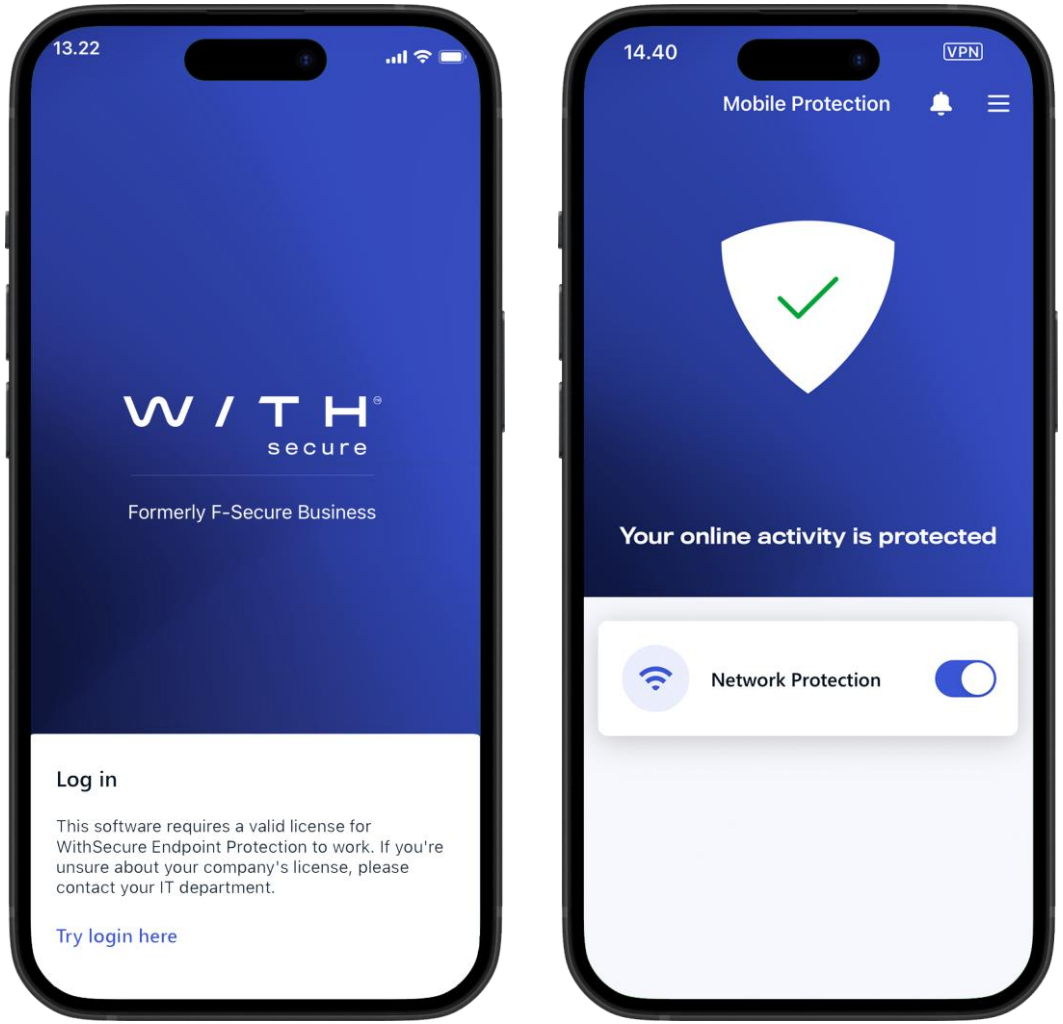
CLIENT RESTRICTED

Protection des smartphones



CLIENT RESTRICTED

WithSecure™ Elements Mobile Protection



- Naviguez en toute sécurité
- Protection contre les logiciels malveillants
- Bloquer les URL dangereuses
- Scanner les applications
- Prise en charge de MDM tiers

Download on the App Store

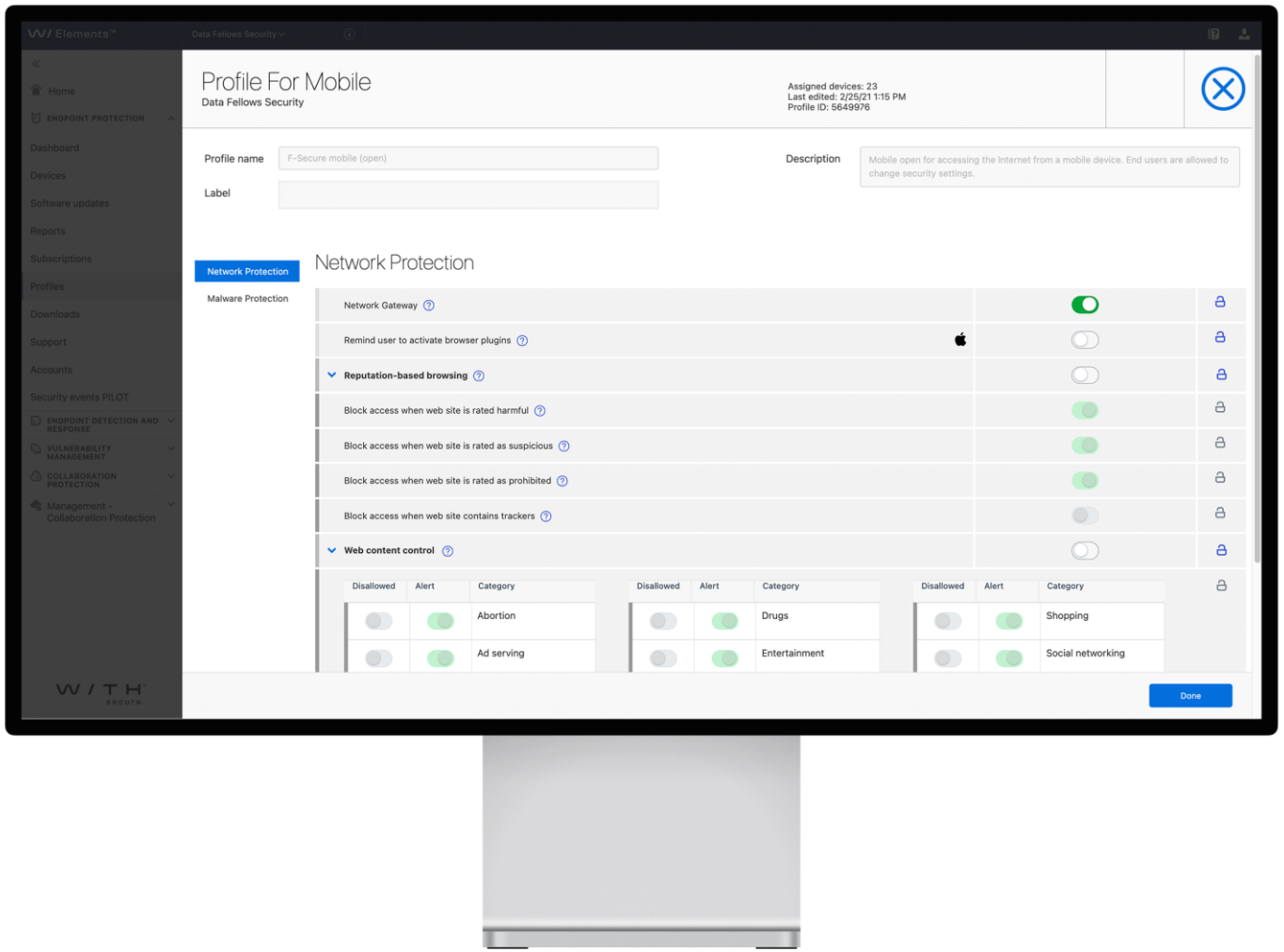
GET IT ON Google Play

* for Android only

** the Network Gateway functionality is only available in selected countries due to local regulations

W / T H secure

CLIENT RESTRICTED



S’intègre à Elements Security Center pour une visibilité et un contrôle sur l’ensemble de votre environnement

Gérez votre sécurité mobile à partir d’une console unique

Gestion des politiques de sécurité

Les profils de sécurité mis à jour sont rapidement appliqués sur tous les appareils concernés

Étroitement intégré à notre sécurité unifiée des endpoints native du cloud

CLIENT RESTRICTED

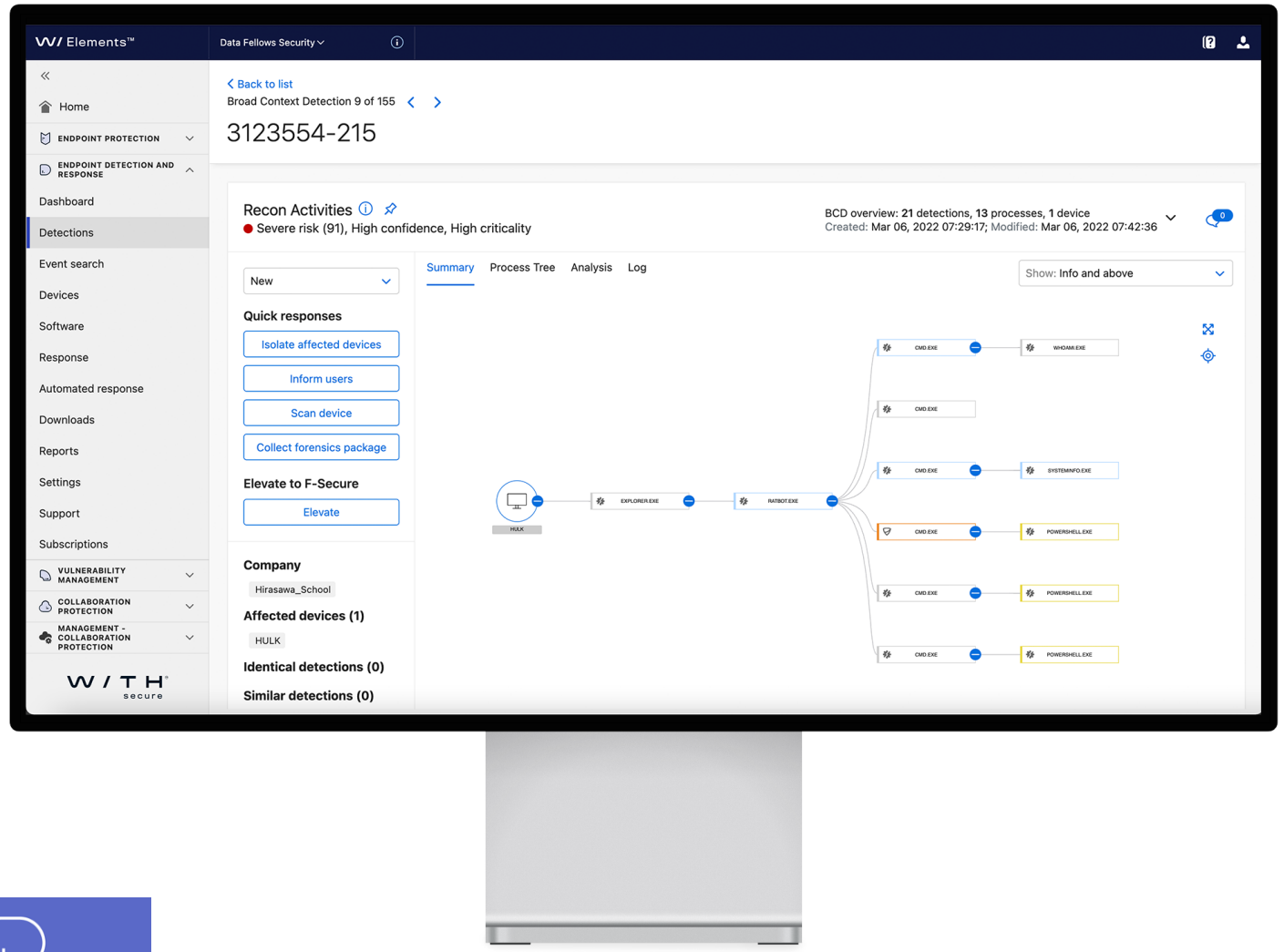
Démo

CLIENT RESTRICTED



WITH secure

Un EDR, c’est quoi ?



- EDR = Endpoint Detection and Response
- **Surveille et collecte les données** d'activité des terminaux
- **La visibilité est primordiale.** Sans visibilité, il n'y a aucun moyen de comprendre ce qui ce passe ?
- **La « machine » est là pour pondérer et contextualiser le risque**
- EDR nécessite toujours une **interaction humaine** pour rechercher, enquêter, trier et répondre à une menace émergente
- EDR ne remplace pas EPP : me doter d’une capacité **à détecter l’intrus** ne doit pas pour autant m’inciter à lui ouvrir la porte.

Endpoint Detection and Response

CTED



OCI INFORMATIQUE & DIGITAL

DEPLOIEMENT SOLUTION EPP/EDR

DE L'INFORMATIQUE AU DIGITAL

Accélérateur de la transformation digitale des entreprises

Votre interlocuteur commercial

Sébastien Pressé : spresse@oci.fr / 0698461571

ZOOM sur la Région OUEST



7
Agences

220 Collaborateurs

77 M€ de CA consolidé 2023

2500 Clients

PME/ETI/Collectivités locales

Les Expertises de Proximité

Ensemble pour construire l'IT de demain



Espaces de travail modernes

Distribution informatique, Déploiements volumiques orchestrés et automatisés avec mise en service des appareils, Déploiements Intune/Autopilot, Impression



Infrastructure hybride & hébergement de donnés

Cloud de proximité privé, IAAS et SAAS, Infrastructure hybride et hébergement de données



Cybersécurité & réseaux

Pares-feux nouvelles générations, protection end-points et SOC, supervision, patch management

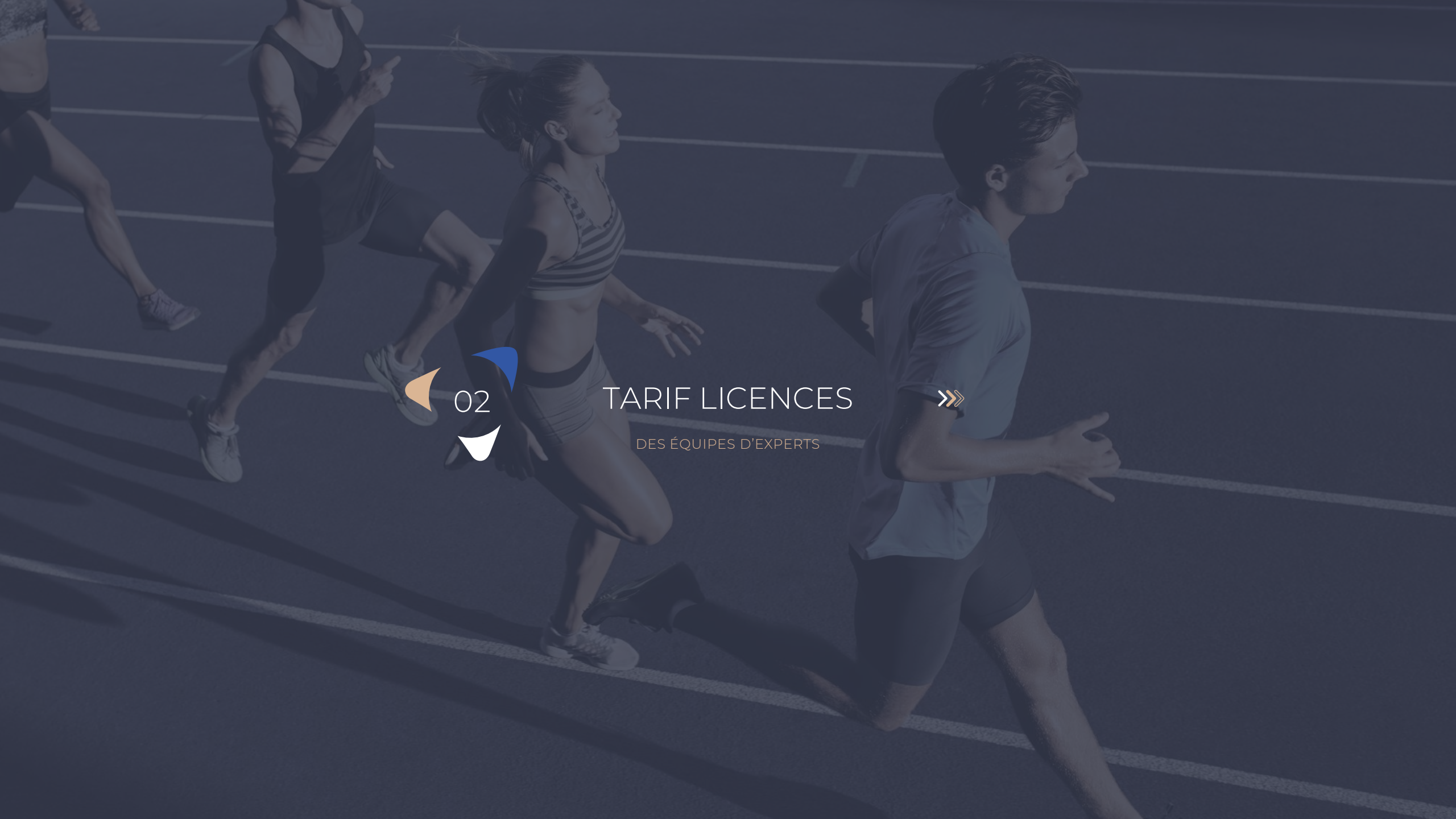
Expert de proximité des Pays de la Loire, Bretagne, Centre Val de Loire

Partenaire des PME / Grands Comptes / Collectivités / Education

NOTRE REPONSE AVEC WITH SECURE

NOS ATOUTS

- Expérience de plus de 15 ans de nos équipes techniques, administration des ventes et commerciales.
- Références clients de déploiement d'envergure de la solution.
  - NANTES METROPOLE
  - UNIVERSITE D'ANGERS
- Solution éprouvée par les établissements de Bretagne
- Certification WithSecure PLATINIUM
- Solution de Services Managés sur mesure
- Flexibilité de la gestion des consoles



02

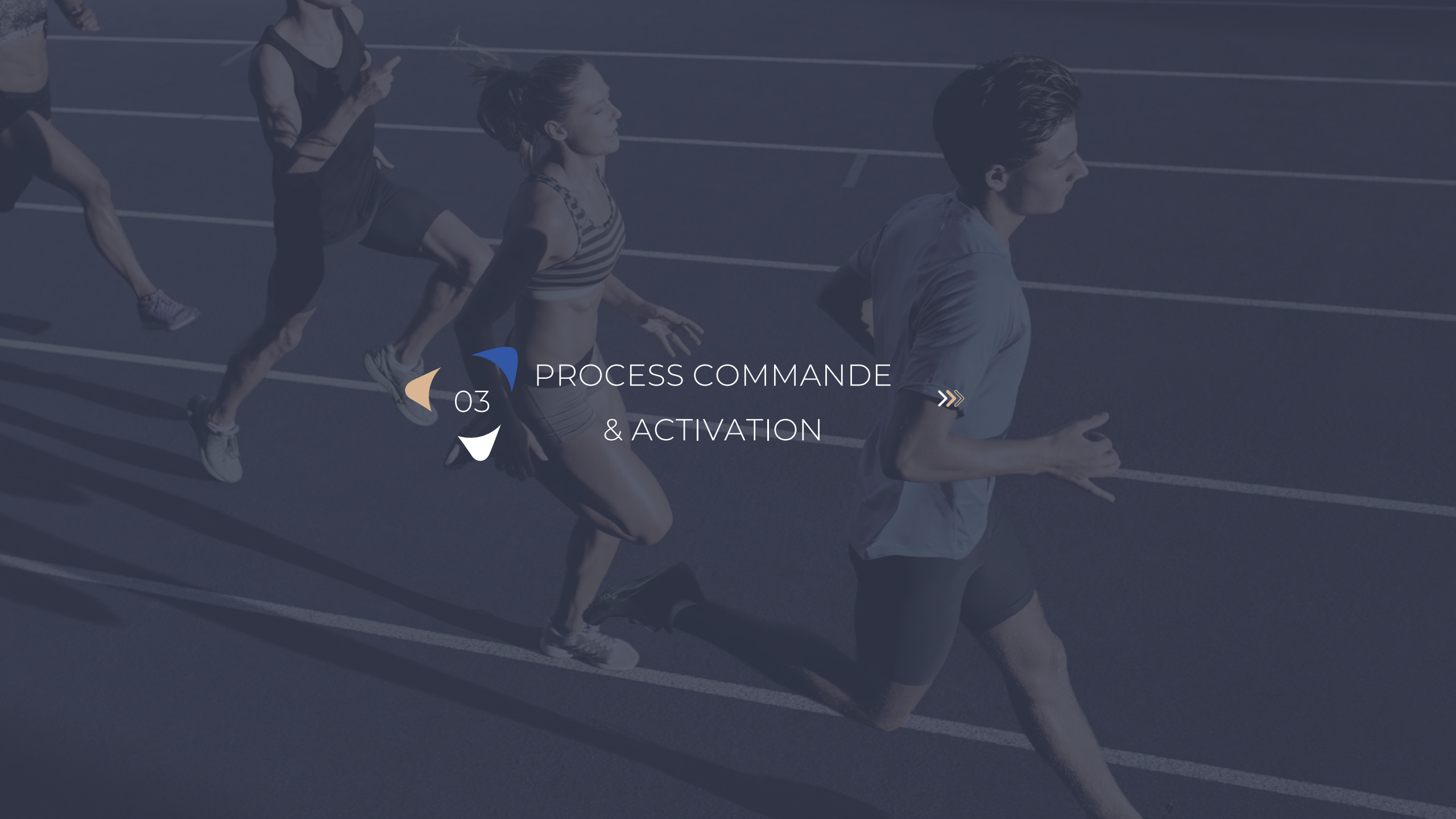
TARIF LICENCES

DES ÉQUIPES D'EXPERTS

TARIFS LICENCES

DESIGNATION	EPP Cloud Saas 1 an	EPP Cloud Saas 3 ans	EPP Cloud Saas 5 ans	EPP + EDR Saas 1 an	EPP + EDR Saas 3 ans	EPP + EDR Saas 5 ans	MDR-SOC With secure 1 an 25 licences minimum	SOC OCI 1 an
Postes de travail (Windows, MacOS)	FCYBSN1EVXGQQ	FCYBSN3EVXGQQ	FCYBSN5EVXGQQ	FCEGSN1NVXEQQ	FCEGSR3NVXEQQ	FCEGSR5NVXEQQ	FCVZSN1NVXGQQ	SOC OCI
Serveur + tout OS Linux	FCRESN1EVXGQQ	FCRESN3EVXGQQ	FCRESN5EVXGQQ	FCRASN1NVXEQQ	FCRASR3NVXEQQ	FCRASR5NVXEQQ	FCVZSN1NVXGQQ	
Mobile	FCDCSN1NVXGQQ	FCDCSN3NVXGQQ	FCDCSN5NVXGQQ	-	-	-	-	
Tarif € HT	1,31 €	3,81 €	6,35 €	9,19 €	26,49 €	44,15 €	35,20 €	24 €
Tarif € TTC	**1,57 €**	**4,57 €**	**7,62 €**	**11,03 €**	**31,78 €**	**52,98 €**	**42,24 €**	**28,8 €**

A noter : des frais administratifs de 36€ TTC pour la création de l'espace et du compte client seront facturés uniquement pour la 1e commande et si le montant de celle-ci dépasse 96€ TTC afin de ne pas pénaliser les petits établissements.



03

PROCESS COMMANDE & ACTIVATION

FAIRE DU DIGITAL LE LEVIER DE VOTRE CROISSANCE

PROCESSUS DE COMMANDE

01

Envoi du bordereau de pré-commande par l'établissement par mail à une adresse générique OCI commandepdl@oci.fr.

02

Pour les licences : Envoi du devis correspondant par OCI à l'établissement

Pour les prestations : Echange avec notre avant-vente pour définir le périmètre de la prestation et envoi du devis correspondant

03

A réception des devis signés :
Création du compte dans la console dans le cas d'un nouveau contrat.
En cas de prestation :
Création du projet de prestation

04

Activation des licences et rattachement au compte de l'établissement sous **72 heures** maximum

En cas de prestation OCI : activation des licences synchronisée à la date de la prestation

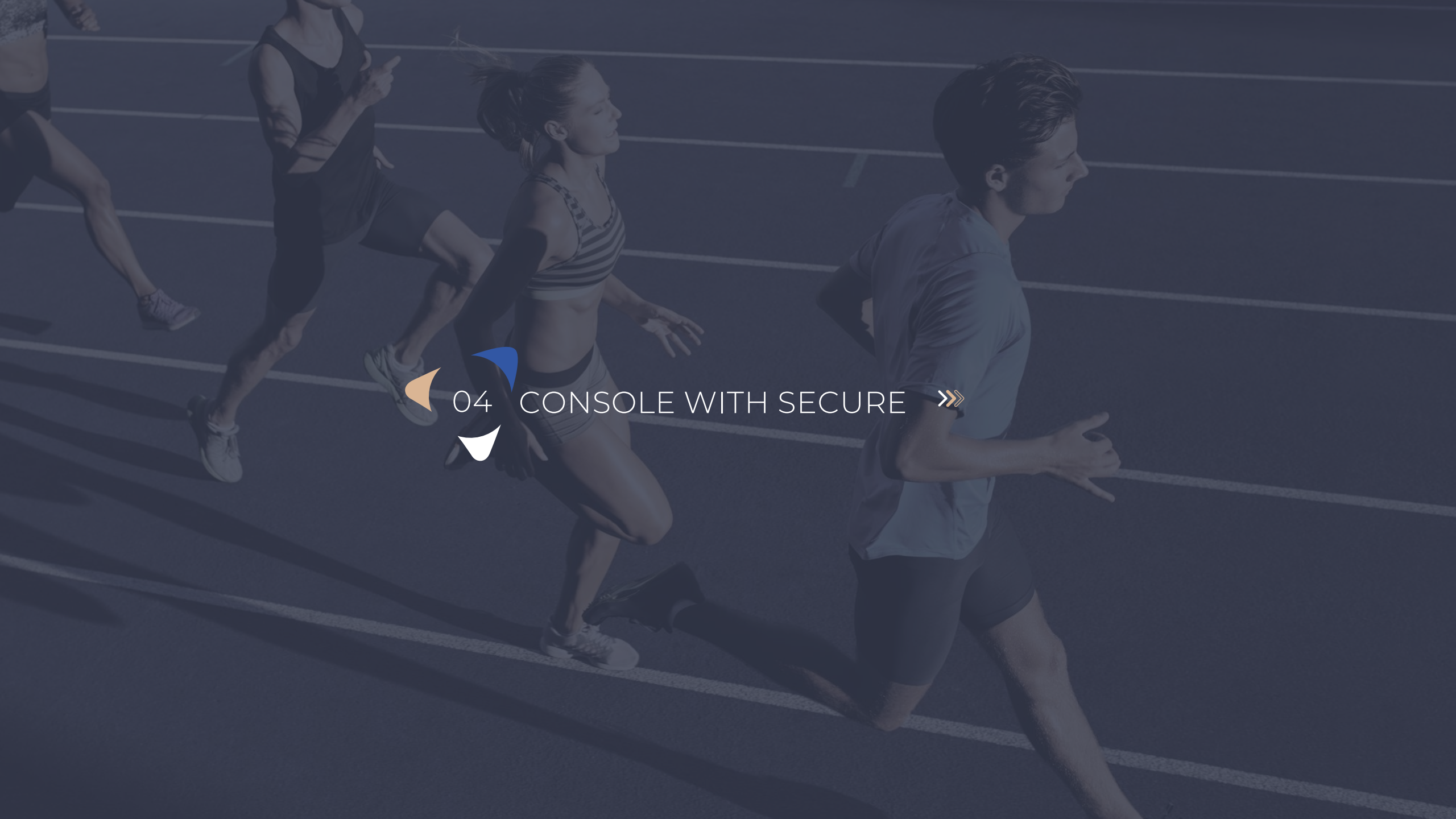
05

Confirmation par mail à l'établissement

Facturation des licences one shot sur la durée de l'engagement.

06

Alerte de renouvellement à date anniversaire transmis à l'établissement **30 jours avant l'échéance**

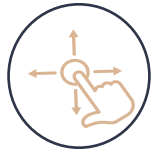


04 CONSOLE WITH SECURE

DES ATOUTS POUR VOUS

CONSOLE ADMINISTRATION DES LICENCES

CADRE DE REPONSE

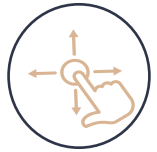


- Les établissements ont un accès en lecture seule à leur nombre de licences et date anniversaire du contrat.
- Le Pôle Numérique de l'URADEL aura une visibilité régionale (lecture seule) permettant un suivi statistique de l'offre régionale et donc une potentielle renégociation à échéance
- En cas d'ajout de licences , un calcul au prorata temporis sera effectué sans changement de la date anniversaire du contrat.

DES ATOUTS POUR VOUS

CONSOLE TECHNIQUE

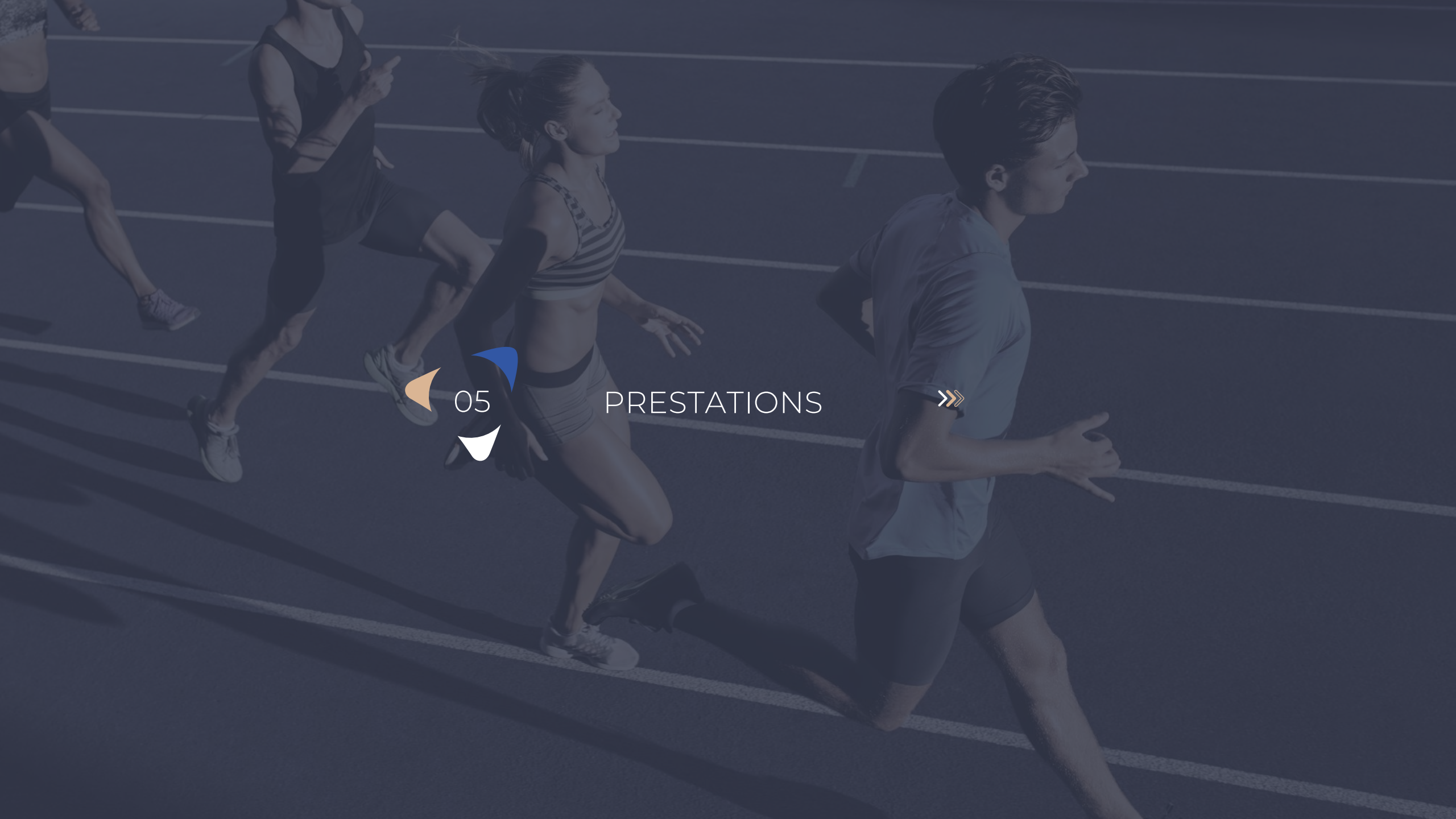
CADRE DE REPONSE



- Les établissements auront la main sur leur console technique

- Si vous l'acceptez, l'URADEL disposera d'un accès en lecture seule permettant :
  - Une veille sur les potentielles infections à l'échelle régionale permettant d'alerter l'ensemble des établissements
  - De connaitre l'état global de sécurité du parc

  → Les **établissements pourront refuser cette visibilité** régionale en le signalant sur le bon de commande,



05 PRESTATIONS



5-1

DESINSTALLATION DE L'ANTIVIRUS EN PLACE
INSTALLATION DE WITHSECURE

EXEMPLE DE PRESTATION

PRESTATION COMPLETE SUR LA BASE

6 VMS / 150 POSTES

POC DE DEPLOIEMENT

DESINSTALLATION DE L'ANTIVIRUS EN PLACE

INSTALLATION ET PARAMETRAGE DE WITHSECURE

+

TRANSFERT DE COMPETENCE

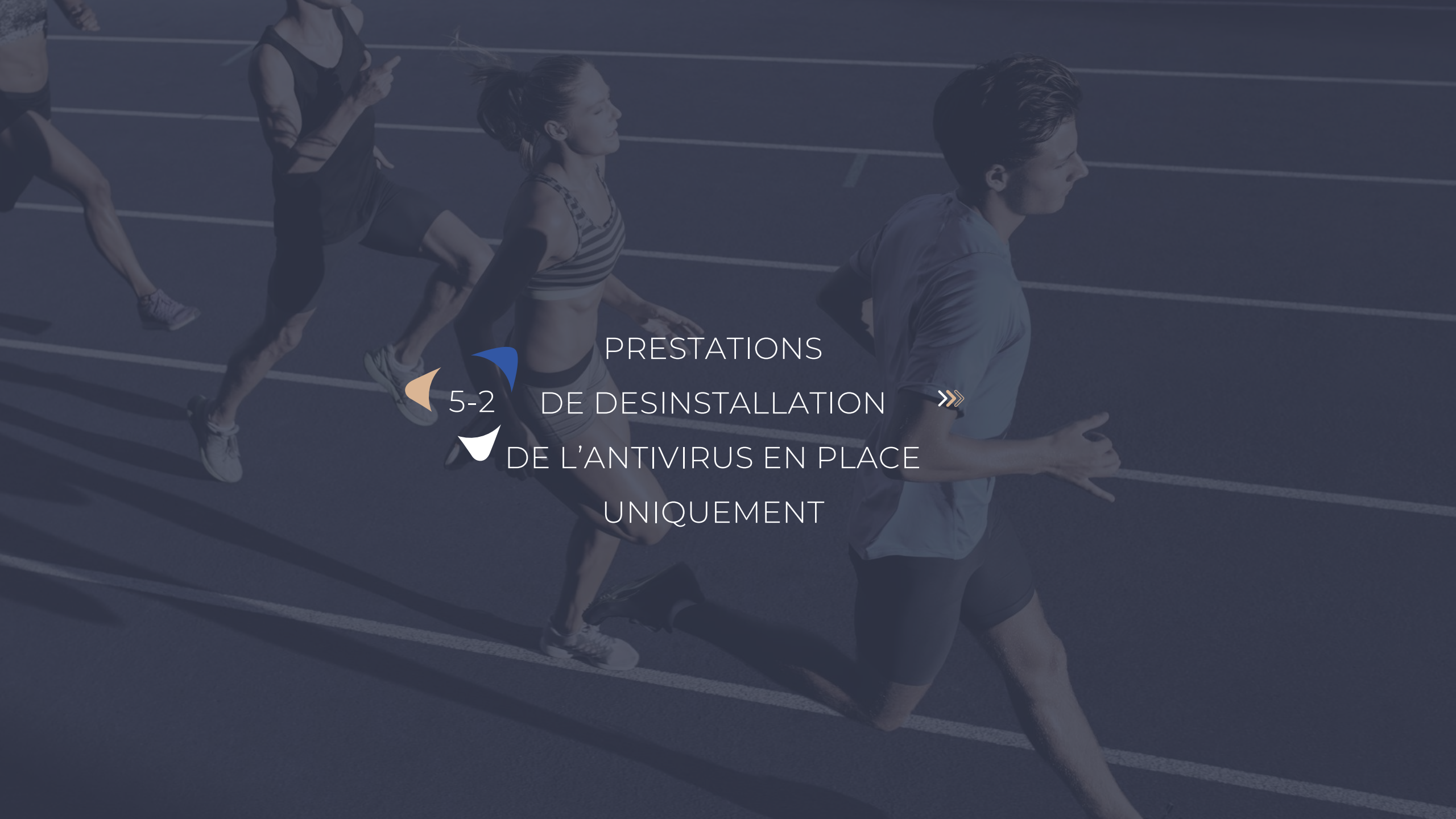
TARIF DE LA PRESTATION AVEC OPTION HNO

5 276,4 € TTC

PRESTATION SUR DEVIS

PREREQUIS ET PERIMETRE

1 site géographique
6 VMs Windows
1 SEUL AD
Les GPO sont fonctionnelles sur les postes
Version de poste W10 21H2 22H2



5-2 PRESTATIONS DE DESINSTALLATION DE L'ANTIVIRUS EN PLACE UNIQUEMENT

EXEMPLE DE PRESTATION CORRESPONDANT

PRESTATION SUR LA BASE

6 VMS / 150 POSTES

POC DE DEPLOIEMENT

DESINSTALLATION DE L'ANTIVIRUS EN PLACE

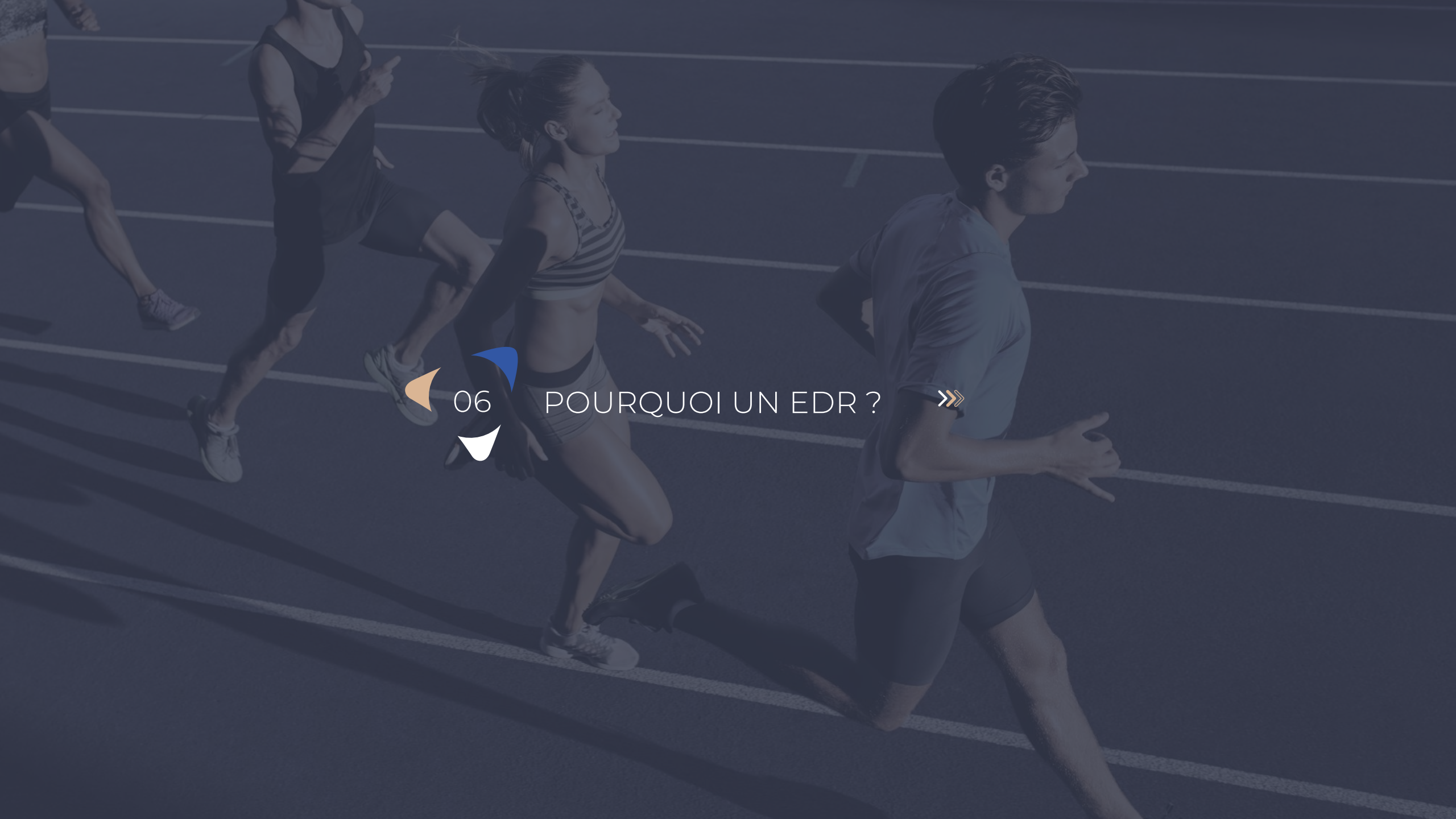
TARIF DE LA PRESTATION AVEC HNO

3 343,2 € TTC

PRESTATION SUR DEVIS

PREREQUIS ET PERIMETRE

1 site géographique
6 VMs Windows
1 SEUL AD
Les GPO sont fonctionnelles sur les postes
Version de poste W10 21H2 22H2



06 POURQUOI UN EDR ?

RESILIENCE – PLUS QUE RÉAGIR

LE RÔLE DE L'EDR

La sécurité continue

Antivirus	EDR
• **Bloque un spectre de menaces connues** sur la base de signatures, et dans certains cas sur la base de comportements • **Première ligne de défense** scanne, détecte et bloque • **Protection passive** contre les menaces dont la détection est triviale • **Protège les terminaux** sans fournir de données approfondies sur leurs comportements et les menaces	• **Répond aux menaces** avérées sur les terminaux • **Deuxième ligne de défense** contient une attaque, permet l'investigation et la réponse sur incident • **Protection active** contre les menaces même lorsqu'elles utilisent les techniques d'évasion des antivirus • Permet d'agréger des données avancées sur les terminaux du périmètre pour **faciliter la détection, l'investigation et la réponse sur incident**



5-3

POURQUOI UN SOC ?

RESILIENCE – PLUS QUE RÉAGIR

SOC OCI 8/5

Caractéristiques

- EDR :détection et réponse sur poste de travail / serveur
- Détection comportementale : détection de comportement suspect
- Isolation de la machine – blocage de la menace
- Intelligence artificielle : détection de menaces avancées

-

Suppléments

- Surveillance 24/7 : surveillance la nuit et le week-end sur astreinte
- Gestion des vulnérabilités continue : détection des failles de sécurité sur les équipements

Solution

- With Secure

SOC MDR (WithSecure) : Support en anglais 24/7

25 licences minimum

DÉLAI MAXIMUM DE PRISE EN COMPTE DES ALERTES HO/HNO PAR UN N1

La sécurité continue

Critique (Niveau 4) 10 minutes	Haute (Niveau 3) 30 minutes
Moyenne (Niveau 2) 45 minutes	Basse (Niveau 1) 60 minutes



5-3 DEPLOIEMENT DU SOC

PROCESSUS ORGANISATIONNEL

La sécurité continue

CONSTRUCTION DE SERVICE

Intégration	Déploiement	Contextualisation de la détection
- Définition du périmètre et des prés-requis - Définition du plan de communication	- Mise en service des outils et solutions - Paramétrage et optimisation	- Optimisation des règles de détection

EXEMPLE DE PRESTATION DE DEPLOIEMENT DU SERVICE SOC :
2990,4 € TTC - BASE 5 vms 10 Postes

Et maintenant ?

Processus de commande disponible sur l'intranet de l'URADEL

https://intranet.uradel.org

Documentation technique disponible sur le bloc-notes régional

Rubrique « *Sécurité du SI / Antivirus / WithSecure* »

- ✓ Désinstallation de Trend Micro APEX ONE
  - → À minima prévoir suppression du mot de passe de désinstallation **avant le 30 septembre**
- ✓ Déploiement automatisé du client WithSecure
- ✓ Bonnes pratiques EPP et EDR With Secure

Ateliers techniques WithSecure

- ✓ Vendredi **4 octobre** 10h à 12h – lien d'inscription
- ✓ Vendredi **11 octobre** à 10h à 12h – lien d'inscription
- ✓ Mardi **15 octobre** à 10h à 12h – lien d'inscription

35 personnes maximum par atelier