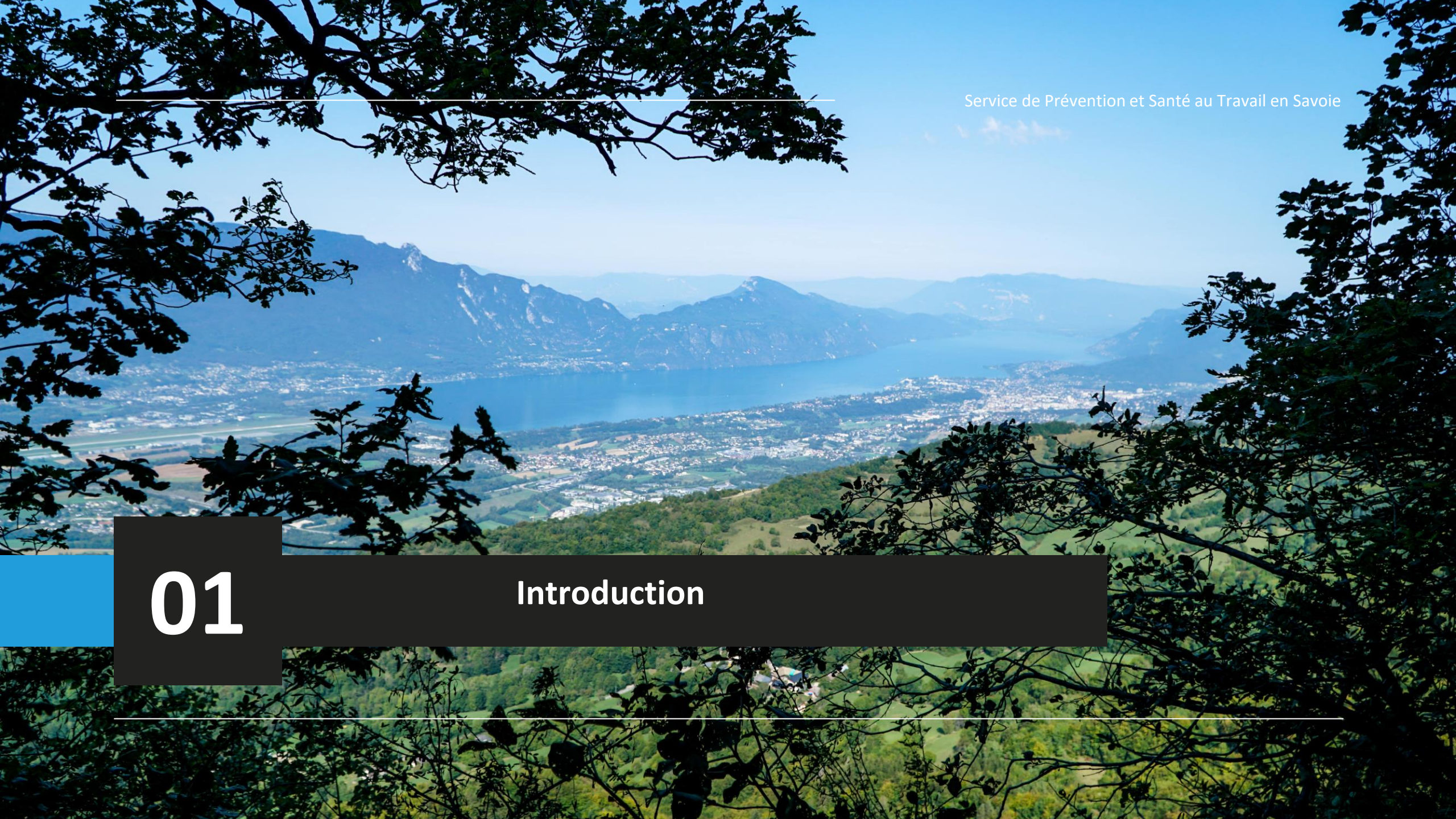
Intervention de
M . Thomas RIVIERE
Directeur du Système d'Information du Service SPST73

La Cybersécurité

27/09/2023

Table des matières



01 Introduction

Définition

ensemble des technologies, processus et pratiques visant à protéger les réseaux, les appareils, les programmes informatiques ou les données **contre les cyberattaques**

Enjeux

- **l'informatique occupe désormais une place majeure**
- une large partie des **informations sont sensibles**
- Au fil des années, **le volume des cyberattaques augmente** à un rythme effréné
- Ces dernières années, de grandes organisations ont subi **des fuites de données** extrêmement confidentielles

Composantes

- **Protection des réseaux informatiques**
- **Protection des systèmes informatiques**
- Les **bases de données, données** et **les infrastructures** doivent être défendues
- Les **applications** doivent aussi être défendues
- La **restauration** des données en cas de désastre doit également être protégée
- La **formation et sensibilisation** des salariés à la cybersécurité

Et la santé dans tout ca?

TECHTOMED

Santé et cyber-sécurité

ÉTAT DES LIEUX

+13%
de cyberattaques en entreprises en 2021 (1)

730
incidents déclarés en 2021 par l'Agence du numérique en santé (ANS) (2)

500 000 personnes
personnes concernées par la fuite de données de santé en 2021 (2)

34
incidents ont mis en danger la vie de patients en 2020 (2)

x2
dans les établissements de santé (2)

27
attaques majeures sur des hôpitaux en **2020** et **une** par semaine en **2021** (2)

70%
des professionnels de santé interrogés se disent également concernés par les questions de cybersécurité (3)

54 milliards €
investis en cybersécurité entre 2017 et 2021 (1)

Sources:
(1) Orange Cyberdefense Security Report
(2) Agence du numérique en santé
(3) https://www.apssis.com/
(4) https://www.ssi.gouv.fr/
(5) https://www.cybermalveillance.gouv.fr/

LEXIQUE

Cyberattaque :
Acte de piratage informatique sur Internet.

Cybersécurité :
désigne l'ensemble des outils et des processus de sécurité utilisés pour la protection de l'environnement numérique (le cyber-environnement). La cyber sécurité protège à la fois les personnes, les idées et les données.

5 types de cyberattaques

Écoute:
Espionnage via les **microphones** pour collecter des informations sensibles.

Attaque par déni de service:
Saturation d'un **réseau** afin de le rendre indisponible.

Logiciel malveillant ou malware:
Programme développé dans le but de **nuire à un système informatique**, sans le consentement de l'utilisateur dont l'ordinateur est infecté.

Hameçonnage ou Phishing:
technique frauduleuse destinée à leurrer l'internaute pour **l'inciter à communiquer des données personnelles et/ou bancaires** en se faisant passer pour un tiers de confiance.

Rançongiciel ou Ramsomware:
est un **logiciel malveillant** qui prend en otage des **données personnelles**.

LES RÉGLEMENTATIONS

Scannez-moi!

- Le Règlement Général sur la Protection des Données
- La loi Informatique et Libertés (section 3)
- Le Code de Santé Publique

LES BONNES PRATIQUES À APPLIQUER (4)(5)

Sauvegarder régulièrement les données de valeur	Limiter au maximum l'utilisation de **clé usb**	**Séparer** l'activité professionnelle des usages personnels
Opter pour des **logiciels certifiés HDS***	Utiliser des **mots de passe** complexes et robustes	Utiliser un **antivirus**
Ne pas ouvrir les messages suspects, leurs pièces jointes et ne pas cliquer sur les liens	**Sécuriser** l'accès de mes appareils mobiles par des mots de passe	**Mettre à jour** les appareils et applications régulièrement
Fermer la session en cas d'absence et **éteindre** l'ordinateur lorsqu'il n'est pas utilisé	Ne pas se connecter aux réseaux **wifi publics**	

*Hébergeur Données de Santé

02 Sécurisation de l’Active Directory

Les outils

Utilisation de deux logiciels complémentaires et gratuits

- PING CASTLE
- PURPLE KNIGHT

Pourquoi?

- Générer un état des lieux du niveau de sécurité de votre annuaire Active Directory
- détecter les problèmes de sécurité critiques le tout classés par priorité
- obtenir une vue d'ensemble de la situation à l’instant T
- établir un plan de remédiation des risques principaux permettant d’améliorer le niveau de sécurité global

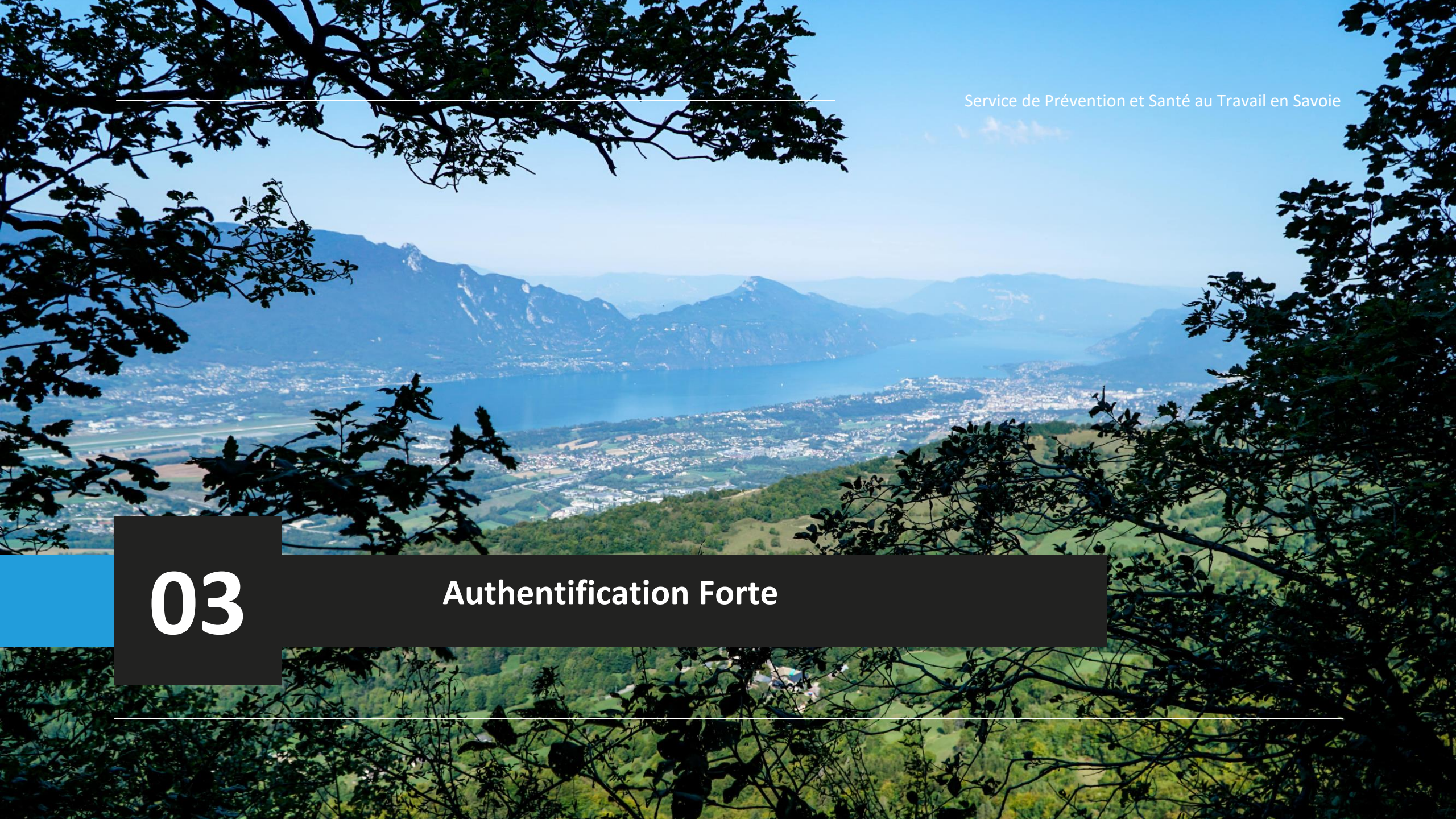
0%

Méthodologie

Comment remédier aux problèmes?

- Se rapprocher de son prestataire de service(ex Access Group)
- On peut organiser un atelier mensuel afin d'avancer sur le sujet

- Dresser l'état des lieux
- Réaliser un plan d'action selon les priorités et le risque associé
- Traitement des risques identifiés
- Réduction de la surface d'attaque
- Planifier cet audit de manière annuelle



03 Authentification Forte

Définition

L'authentification multifacteur (MFA) est une méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource.

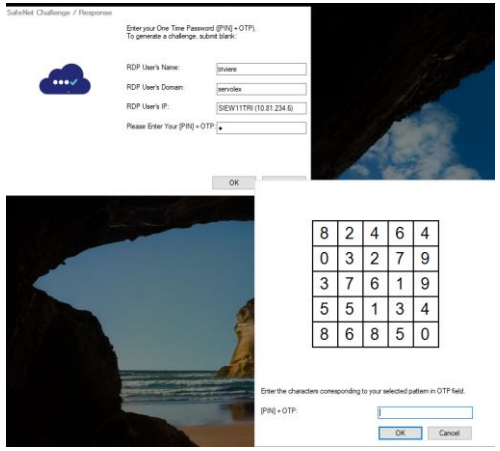
Les outils

- Voici une liste de logiciels :

10 Best Single Sign-On Solutions (SSO) Providers - 2023 (cybersecuritynews.com)
Top 11 Multi-Factor Authentication (MFA) Solutions for Business In 2023 (expertinsights.com)
7 Best Multi-Factor Authentication (MFA) Solutions in 2023 (guru99.com)

Pourquoi?

- Renforcer le niveau de sécurité côté utilisateurs
- Renforcer le niveau de sécurité côté administration des serveurs
- Le système d'authentification à deux facteurs doit pouvoir s'interfacer avec un maximum de vos logiciels ou équipements
- C'est encore mieux s'il permet de faire du Single Sign On (SSO) ce qui permet de s'authentifier une seule fois



Choix du SPST73

- Le choix de SPST73 s'est porté sur Thales SafeNet Trusted Access .

L'objectif est de coupler l'authentification forte avec les équipements suivants :

- Serveurs RDS
- Ensemble des serveurs Windows
- Authentification VPN SSL Fortigate
- Authentification Azure AD
- Authentification Radius/NPS
- Authentification EDR SentinelOne

Méthodologie

- Le seul verrouillage par un mot de passe n'est pas suffisant pour assurer la sécurité des comptes face à des pirates toujours plus performants et ingénieux. Pour contrer leurs attaques, l'authentification double facteur a été mise en place et se généralise.

- En général, on retrouve trois méthodes d'authentification forte : token physique, application mobile et schéma mental

04 EPP vs EDR

Définition

L'Endpoint Detect & Response (EDR) est une solution de sécurité combinant une surveillance en temps réel, une collecte continue des données avec une capacité de réponse et d'analyse comportementale automatisée basée sur des règles (Intelligence artificielle).

Les solutions

Voici une liste des EDR les plus performants actuellement sur le marché, d'après mes analyses:

- SentinelOne
- Huntress
- Crowdstrike

Pourquoi?

- Les nouvelles menaces persistantes avancées (APT) sont un nouveau type de piratage de haut niveau, furtif et capable de se maintenir dans le SI pendant une longue période pour y agir sans se faire repérer.
- Ces nouvelles menaces permettent exfiltration, modification, destruction et chiffrement des données
- Il faut donc éviter la compromission du Système d'Information à travers des postes de travail ou serveurs
- L'EDR permet de Détecter et Répondre aux menaces qui ont contourné votre première ligne de défense(= EPP) , permet une analyse complète post attaque et fournit des informations précises sur le scénario de l'attaque, les mouvements du programme malveillant et leurs conséquences.

Choix du SPST73

- Le choix de SPST73 s'est porté sur SentinelOne.

Il est installé sur l'ensemble des postes de travail, serveurs Windows et Linux.

- SentinelOne protège également les identités et le cloud (fonctionnalités étendues XDR)

Méthodologie

- Désinstallation de l'antivirus
- Déploiement et paramétrage du nouveau EDR
- Traitement des faux positifs
- Tuning et transfert de compétences « correspondant sécurité »

05 Sécurisation des systèmes d’exploitation

Définition

La sécurisation des postes de travail consiste à protéger les ordinateurs et les données des utilisateurs contre les menaces informatiques telles que les virus, les logiciels malveillants, les attaques par phishing, les ransomwares…

Pour répondre aux besoins des collaborateurs en situation de mobilité, de télétravail… l'entreprise doit garantir un niveau de sécurité élevé aussi bien « dans ses murs » qu'en situation de nomadisme.

Pourquoi?

Plus exposés que les serveurs, les postes de travail peuvent constituer un point d'entrée permettant l'accès au SI (Système d'Information) de l'entreprise et leur compromission peut avoir un impact très fort sur celui-ci.

Les éléments clés sont :

- Un paramétrage initial maîtrisé (lors du déploiement)
- Un maintien en conditions sécurisée (mises à jour)
- Une surveillance des nouvelles vulnérabilités
- L'adaptation de la configuration des postes de travail.

La protection des postes de travail constitue par conséquent un enjeu essentiel dans la sécurisation de l'infrastructure globale du SI.

Gestion des vulnérabilités :Choix du SPST73

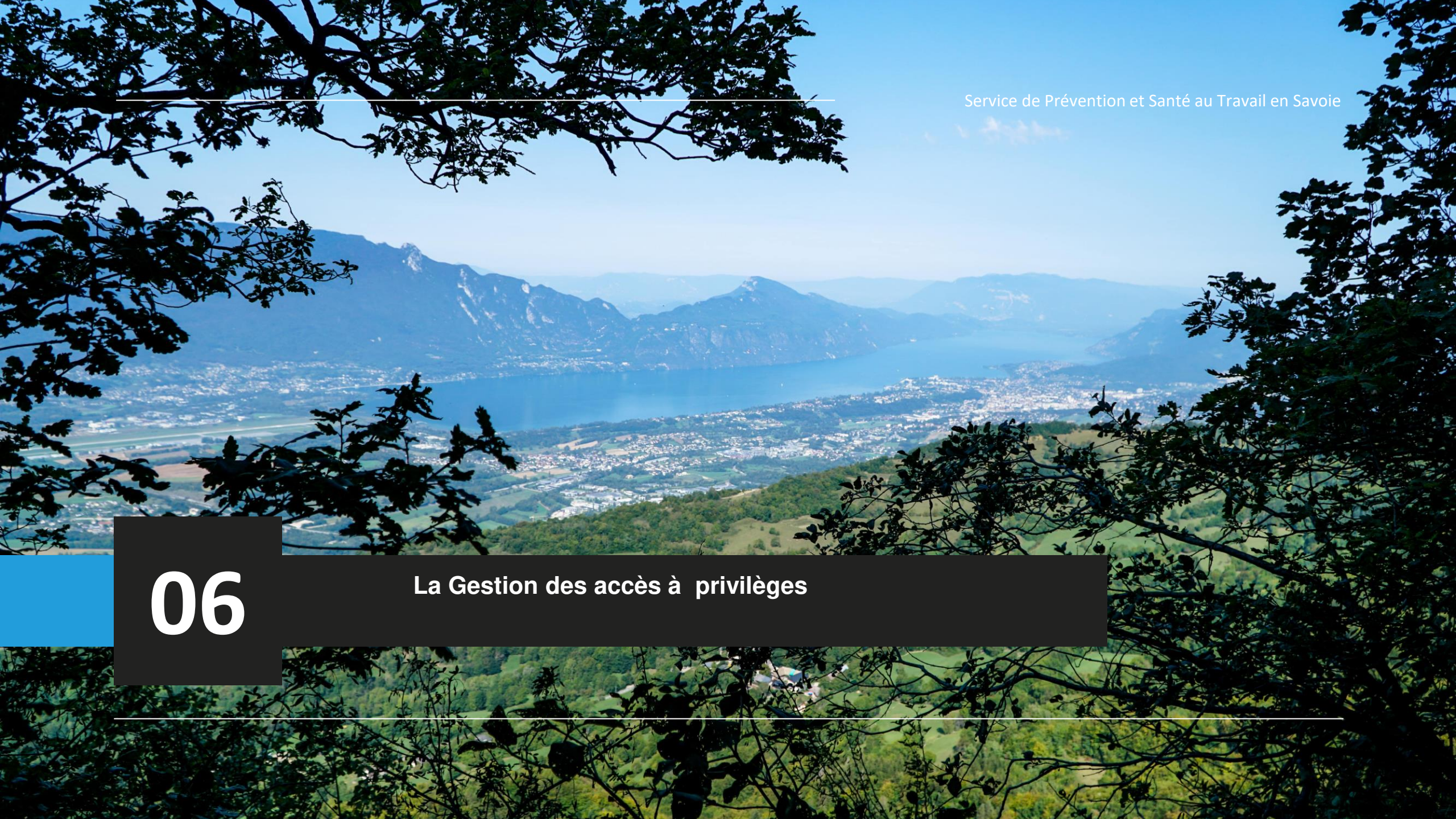
Le choix de SPST73 s'est porté sur PDQ Deploy & Inventory.

Ce logiciel permet l'inventaire et la mise à jour automatique des postes de travail et serveurs, concernant:

- Les applications
- Les runtimes
- Les mises à jour Microsoft

Méthodologie et solutions

- Réduction des privilèges (l'utilisateur n'est jamais administrateur local) ➔ GPO (gratuit)
- Le mot de passe du compte administrateur local est différent sur chacun des postes ➔ LAPS (gratuit)
- Chiffrement du disque dur ➔ Bitlocker (gratuit)
- Chiffrement des disques amovibles ➔ Bitlocker (gratuit)
- Activation du pare-feu ➔ Windows (gratuit) ou EDR
- détecter les problèmes de sécurité critiques (vulnérabilités connues, mises à jour Windows…) et déployer les mises à jour automatiquement ➔ RMM ou Patch Management
- Protection de l'accès au BIOS et au menu d'amorçage ➔ selon constructeur (gratuit)
- Durcissement des systèmes d'exploitation ➔ GPO (gratuit)



06

La Gestion des accès à privilèges

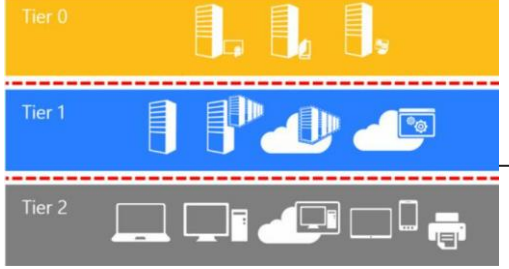
Définition

Les organisations mettent en œuvre la gestion des accès à privilèges (PAM) pour se protéger contre les menaces que constituent le vol d'identifiants et l'utilisation mal intentionnée des privilèges.

Les solutions de gestion des accès à privilèges (PAM) sont des solutions visant à gérer et protéger les comptes utilisateurs possédant de forts privilèges (administrateurs internes et prestataires) et à gérer les accès d'administration aux équipements d'un SI.

Pourquoi?

- Les humains sont le maillon faible. Il faut éviter la compromission de compte et donc l'usurpation d'identité
- Dans les entreprises numériques, les privilèges sont omniprésents
- Les cybercriminels ciblent les terminaux et les stations de travail et il faut donc les empêcher de prendre le contrôle du Système et bloquer les mouvements latéraux
- La gestion des accès à privilèges est essentielle pour atteindre la conformité



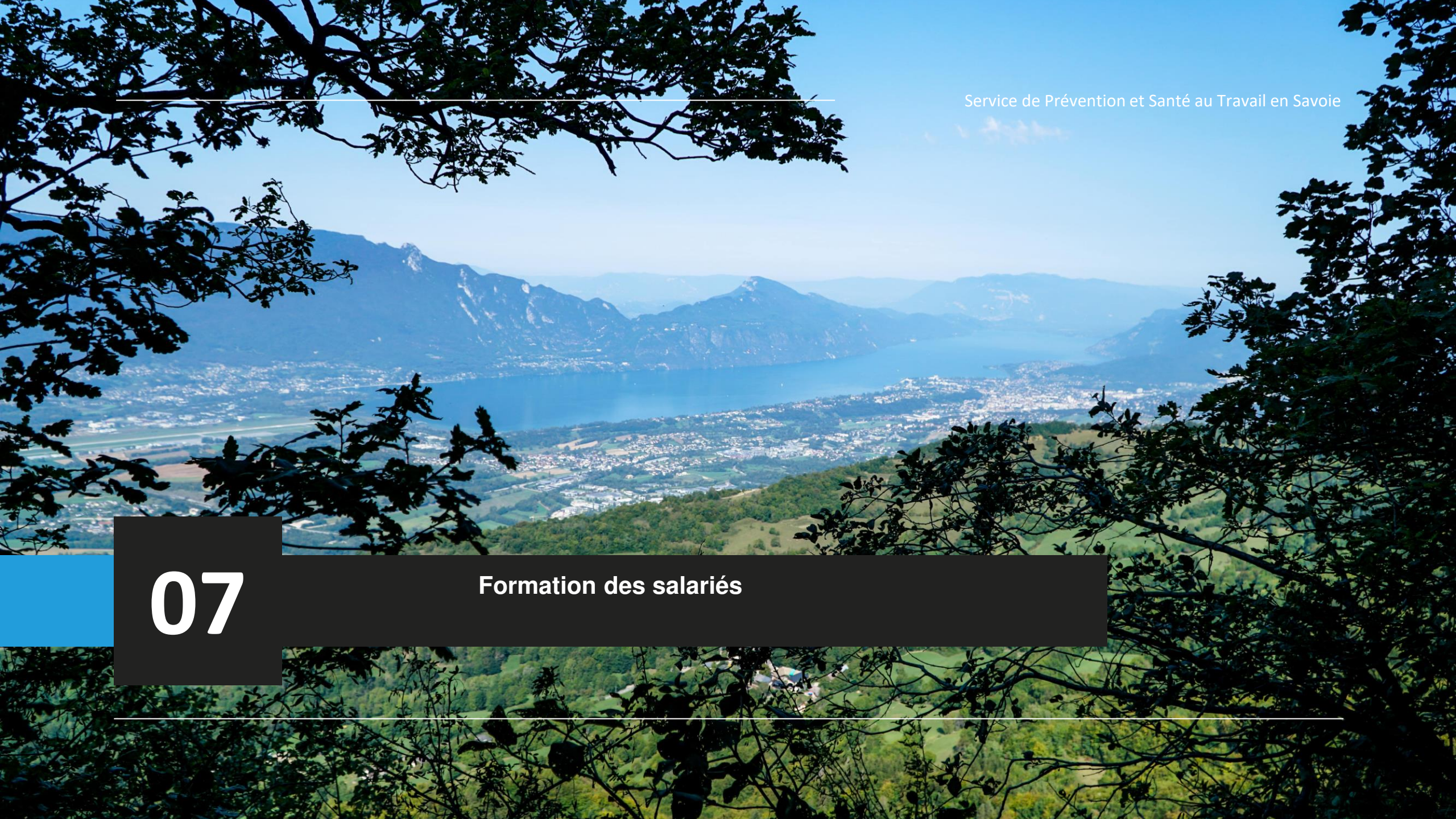
La Gestion et réduction des accès à privilèges :Choix du SPST73

Les choix logiciels de SPST73 se sont portés:

- Mise en place de l'AD Tiers
- Remplacement des comptes de service par des comptes gmsa dans la mesure du possible
- Principe de moindre privilège par défaut sur les postes et serveurs
- Authentification Forte Thales
- SIEM Wazuh pour Logger et générer des rapports concernant l'authentification sur l'ensemble des serveurs, équipements actifs et Office365
- Administration Juste à temps en interne sur les serveurs (Lithnet)
- Bastion Guacamole

Méthodologie et solutions

- Limiter les déplacement latéraux en supprimant les utilisateurs des groupes à privilèges locaux sur les ordinateurs
- Limiter les privilèges des comptes de services et d'administration sur les serveurs (remplacement par des comptes gMSA, administration Juste à temps)
- Authentification Multi-Facteurs dès que l'on peut
- politique de changement des mots de passe de tous les comptes (entre 16 et 20 caractères, c'est bien) et coffre fort de mot de passe
- Logging et reporting sur les comptes à privilèges (SIEM, notifications par mail)
- Mise en place du modèle de sécurité AD Tiers afin d'isoler les comptes à privilèges
- Revue bi-annuelles des habilitations
- Mise en place d'un Bastion qui servira d'intermédiaire entre un administrateur et une ressource



07

Formation des salariés

Définition

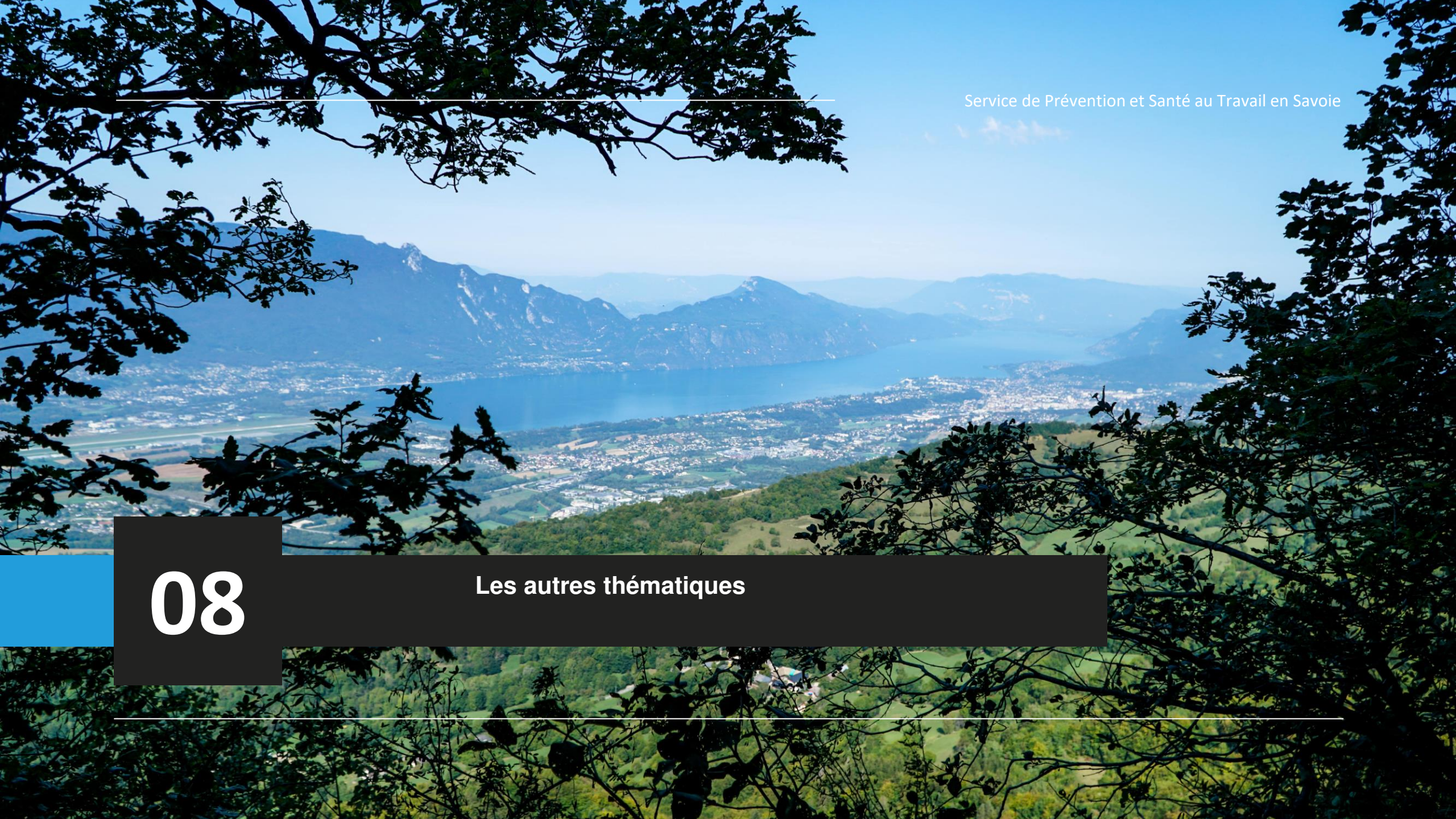
Spearphishing, ransomware, téléchargement de logiciels malveillants… Ces menaces de cybersécurité touchent les salariés de toutes entreprises, notamment en télétravail. La sensibilisation à la cybersécurité est aujourd'hui indispensable.

Méthodologie

- Sensibiliser les utilisateurs par des jeux (quizz) gcs ara
- Former les utilisateurs régulièrement (MOOC SecNumAcadémie, Les 4 films de la Hack Academy CIGREF)
- Renforcer la communication en interne
- Campagnes de phishing (GOPHISH, Microsoft 365), bouton d'alerte Phishing dans Outlook, Inspection de mot de passe, simulateur de ransomware

Pourquoi?

Les collaborateurs d'une organisation sont en première ligne face à ces risques de cybersécurité qui se multiplient. La sensibilisation à la cybersécurité est ainsi indispensable pour qu'ils puissent en prendre conscience et réagir en conséquence.



08 Les autres thématiques

Les autres thématiques

- Alertes emails déclenchées sur des indices de compromission
- Amélioration protocoles et authentifications(Kerberos, Ntlm, Smb, Ldaps,...)
- Sécurisation du transport des données (chiffrement des communications RDP,HTTPS,SSH)
- Supervision du Système d'Information
- Centralisation et corrélation des évènements (SIEM)
- Orchestration, automatisation et réponse en sécurité (SOAR)
- Réagir (procédures et playbook en cas d'incident SSI)
- Revue des habilitations et contrôle hebdomadaire de la sécurité

- Cloisonnement du réseau
- PareFeu en cœur de réseau
- Contrôle d'accès au réseau sur le périmètre via 802.1x ou par adresse MAC (filaire et wifi)
- Règles de filtrage de parefeu stricte afin de limiter l'accès aux diverses ressources informatiques sensibles
- N'autoriser que le trafic sortant authentifié
- Mise en place de solution Network Detect & Response (NDR)

Merci pour votre attention !

info@santetravail73.org | 04 79 60 76 76 |
www.santetravail73.fr

N’hésitez pas à me contacter en cas de questions.