ivanti

Le « Shift Left » de la sécurité

Comment favoriser des environnements de sécurité réactifs avec les outils IT d'aujourd'hui

Sommaire :

ivanti

01

À la croisée des chemins

Comment trouver le juste équilibre entre la nécessité d'une cybersécurité proactive et la pression pour une consolidation des technologies

Dans cette section :

1. Créer un écosystème de cybersécurité réactive...
2. ... ou consolider votre pile technologique ?
3. Comment l'équipe Sécurité peut faire les deux à la fois !

ivanti

Des exigences contradictoires

Votre équipe de cybersécurité doit être proactive pour contrer les futures cyberattaques, tout en parant en continu aux urgences de sécurité… une mission complexe, même dans les entreprises riches en ressources ! En parallèle, elle doit réduire l'empreinte de sa pile technologique : il faut « faire autant avec moins » pour répondre aux pressions budgétaires qui pèsent sur tous les départements.

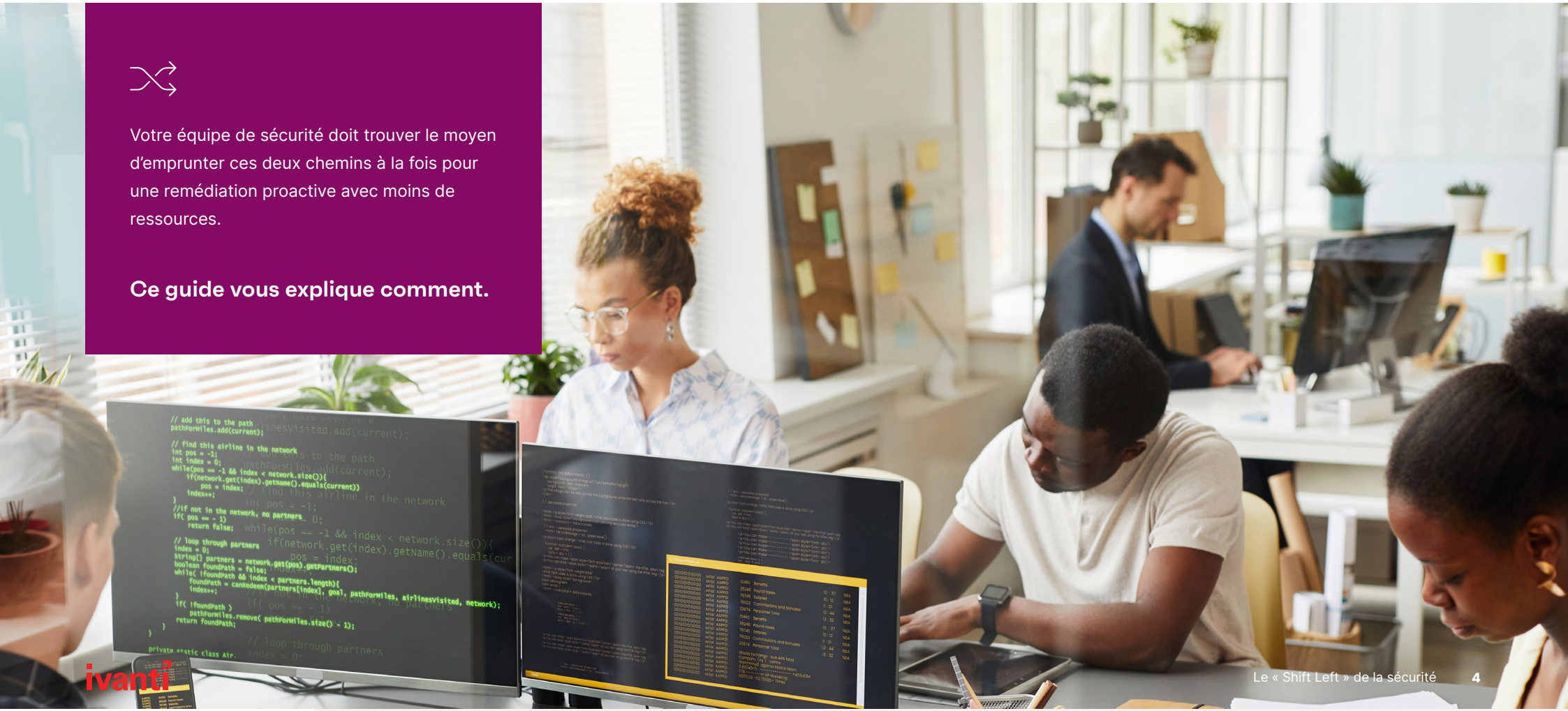
Mais comment relever les deux défis ?

Bien entendu, c'est exactement pour le savoir que vous lisez ce guide. Alors, examinons ces deux exigences à l'échelle de l'entreprise.

À cette croisée des chemins, vous ne pouvez pas faire un choix en ignorant l'autre.

Votre équipe de sécurité doit trouver le moyen d'emprunter ces deux chemins à la fois pour une remédiation proactive avec moins de ressources.

Ce guide vous explique comment.



Exigence n°1 des équipes de sécurité :

Créer des « cyberécosystèmes réactifs » pour une remédiation proactive

Dans un récent rapport de Gartner, les analystes décrivent la nécessité pour les équipes de sécurité modernes de développer ce qu'ils appellent un « cyberécosystème réactif ».

Ces écosystèmes réactifs doivent :

Scanner en continu l'environnement

Identifier les risques existants et potentiels

Tenter de réagir avant qu'un problème ne survienne

Pour atteindre ces objectifs, vous devez gérer en continu l'exposition aux menaces, effectuer une vérification des utilisateurs et des accès, et créer un « système immunitaire numérique » qui détecte et réduit les lacunes de votre sécurité.

Ces initiatives peuvent paraître ambitieuses pour n'importe quelle équipe de sécurité, et particulièrement difficiles à réaliser dans l'environnement actuel compte tenu des incitations à réduire les outils de sécurité (comme nous allons le voir plus loin).

ivanti

En appliquant une **approche continue de la gestion des menaces et de la vérification de la cybersécurité, ces initiatives confortent les efforts de remédiation des risques. Elles permettent d'améliorer la détection et les capacités de réponse, et de mettre en place des écosystèmes dotés d'une meilleure immunité numérique.**

- Gartner
« Top Strategic Cybersecurity Trends for 2023 »

Gartner

Exigence n°2 des équipes de sécurité :

Consolider la pile technologique pour réduire les coûts

En parallèle, la deuxième exigence, qui consiste à consolider et à restructurer les outils de sécurité, montre que les départements Sécurité et IT sont eux aussi soumis à des pressions financières.

Après tout, même si elles sont importantes pour la sécurité et le bon fonctionnement de l'entreprise, ces deux équipes ne génèrent pas directement de revenus.

Cette perception de l'équipe Sécurité en tant que centre de coûts a conduit à une pression croissante sur les CSO et les CISO. On leur demande de réduire les frais généraux de ces départements, notamment via la consolidation technologique et l'intégration accrue de leurs outils actuels. C'est ce que révèlent des représentants du secteur dans des entretiens publiés dans le Wall Street Journal.

De plus, d'après une récente étude réalisée par ESG et ISSA, les professionnels de la cybersécurité interrogés tiennent davantage compte du coût, des capacités d'intégration des produits et de la facilité d'utilisation que des tests réalisés par de tierces parties ou des recommandations des analystes du secteur.

Ces pressions ont poussé les entreprises à consolider leurs piles technologiques, en recherchant des plateformes multifonctionnelles plutôt que des technologies de niche ou de pointe.

Quels sont parmi ces critères les plus importants lors de vos achats de technologies de sécurité ?

(En pourcentage des réponses sur N=280, trois réponses acceptées) Source : ESG, division de TechTarget, Inc.

Une troisième voie existe : des outils transverses pour les cas d'usage de sécurité proactive

Devant ces deux exigences qui s'opposent (non seulement intervenir en urgence sur les problèmes actuels mais aussi parer ceux à venir, et avec un budget de plus en plus limité, sans aucune place pour les outils à usage unique), les équipes de sécurité sont confrontées à une décision impossible..

Quelle voie faut-il suivre ?
Quelle est la priorité ?

Et s'il existait pourtant un moyen d'ouvrir une nouvelle voie : une troisième voie encore inconnue, qui permettrait aux équipes de sécurité de satisfaire ces deux exigences ?

Cette troisième option doit fournir les résultats des deux exigences, à savoir la remédiation proactive et la réduction du nombre d'outils coûteux. Mais il ne faut pas se perdre dans son implémentation, provoquer le burnout des équipes, ou gaspiller du temps et des ressources..

Il n'est possible de suivre cette voie que si l'équipe Sécurité parvient à utiliser et « recycler » les outils et solutions des autres équipes pour son propre usage.

Par quoi commencer ? Les architectures et les outils actuels de l'équipe IT.

En les utilisant, l'équipe Sécurité peut créer un environnement de cybersécurité réactif tout en réduisant les coûts grâce au « recyclage » des plateformes IT déjà budgétées et utilisées.

D'autre part, les avantages de la réutilisation d'outils IT déjà implémentés vont bien au-delà d'une simple réduction des coûts. Les analystes s'accordent à dire que la simplification des outils améliore souvent les opérations et rend les collaborateurs plus efficaces.

Le partage des plateformes d'outils peut aussi :

- Améliorer la collaboration entre départements
- Alléger la charge administrative de chaque équipe
- Renforcer la cybersécurité globale

Ainsi, les équipes de sécurité peuvent appliquer des remédiations tactiquement proactives sans avoir recours à des outils de niche adaptés à un seul cas d'usage. Mais cela n'est possible que si la Sécurité et l'IT élargissent leur approche dans une compréhension commune de l'importance du « Shift Left » et vont plus loin en ne cherchant pas uniquement à réduire le nombre de tickets ou à diminuer le nombre d'applications utilisées.

02

Définir le « Shift Left » au-delà des DevSecOps :

À la recherche d'un terrain d'entente entre les approches de l'IT et de l'équipe Sécurité

Dans cette section :

1. Définitions différentes du « Shift Left » pour l'IT et la Sécurité
2. Une approche partagée pour réussir le « Shift Left »

ivanti

Définitions différentes du « Shift Left » pour l'IT et la Sécurité

Bien que les équipes Sécurité et IT emploient l'expression « Shift Left », chacune a une conception différente de l'approche. Ces différences augmentent les tensions entre les équipes, malgré leurs similarités et objectifs communs.

	Le « Shift Left » de la sécurité pour les DevSecOps	Le « Shift Left » de l'IT pour la gestion des tickets de support
Définition	Les risques sont identifiés par les outils et les spécialistes lors du développement, plutôt qu'à la dernière minute avant le déploiement final.	Les problèmes IT potentiels sont identifiés par la technologie, avant que les utilisateurs finaux ne les remarquent et ne créent des tickets de support.
Focus	L'accent est mis sur le développement du produit et/ou du processus dans le cadre d'un modèle de release DevSecOps.	L'accent est mis sur la gestion des services liés aux obligations du centre de support IT envers les utilisateurs finaux internes.
Résultats immédiats	Déploiement accéléré des produits et processus via une remédiation proactive en continu.	Le nombre global de soumissions de ticket de support est réduit, ainsi que le taux d'escalades au niveau supérieur.
Autres avantages	Culture d'entreprise de type « la sécurité d'abord », car la sécurité n'est plus une préoccupation de dernière minute. Élimination des silos car le département Sécurité n'est plus un régulateur externe mais est un membre à part entière de l'équipe.	La résolution des problèmes est effectuée par des experts IT moins spécialisés. Le coût global de main-d'œuvre est réduit car le nombre de tickets de support diminue.
Impact sur le calendrier	En adoptant une approche proactive de la sécurité (le sujet n'est pas abordé à la dernière minute avant la livraison), le calendrier de développement des produits et processus devient plus prévisible (voire étendu), avec moins de risques connus pour la sécurité.	Les collaborateurs IT disposent de davantage de temps et de ressources pour leur développement professionnel, et pour des tâches plus stratégiques et proactives à bande passante plus élevée.

Finalement, aussi différentes que soient les conceptions du « Shift Left » pour les équipes de sécurité et IT, les cas d'utilisation de ces deux départements partagent plusieurs aspects fondamentaux.

En fait, ces deux modèles montrent la nécessité (pour les deux équipes) d'une remédiation proactive et plus rapide des problèmes, très en amont du processus, pour éviter de coûteuses urgences de dernière minute.

Une approche partagée du « Shift Left » pour les équipes Sécurité et IT

Chez Ivanti, nous utilisons l'expression « Shift Left » pour désigner tout processus stratégique capable d'éviter l'escalade et de corriger les incidents avant qu'ils ne deviennent vraiment des problèmes ou des urgences… souvent, même, avant que toute partie prenante externe ne soit consciente de l'existence de l'incident en question !

Ainsi, le « Shift Left » devient une approche culturelle d'une remédiation proactive automatique couvrant plusieurs départements, qui unit des processus auparavant en silos pour créer une seule approche fondamentale unificatrice.

Bien que cette définition reflète tout à fait le cas d'usage principal de l'équipe IT (corriger les problèmes avant qu'ils ne surviennent et que quiconque n'ait connaissance du problème), cette approche du « Shift Left » s'aligne étroitement sur l'objectif de l'équipe Sécurité, à savoir créer un écosystème proactif et réactif, au-delà des implémentations ou considérations propres aux DevSecOps.

Par sa nature même (résoudre les problèmes avant que les humains ne s'en aperçoivent), l'automatisation joue un rôle important pour aider tous les départements dans leur « Shift Left ». Et c'est particulièrement vrai pour les cas d'usage communs à la Sécurité et à l'IT, comme les deux équipes vont le découvrir dans le chapitre suivant.

Qu'est-ce que le « Shift Left » ?

Dans ce guide, nous appelons « Shift Left » les processus stratégiques et automatisations tactiques servant à **identifier les petits problèmes, éviter leur escalade et les corriger avant qu'ils ne deviennent des urgences plus importantes…** souvent, avant que toute partie prenante externe ne s'aperçoive qu'un problème a surgi.

03

Outils IT + Sécurité :

Cas d’usage pratiques permettant aux équipes de sécurité de partager des outils IT

Dans cette section :

1. ITAM et ITSM + Sécurité
2. UEM + Sécurité

ivanti

Outils IT courants utilisés pour la sécurité : ITAM, ITSM et UEM

Parmi tous les outils IT que l'équipe Sécurité pourrait utiliser, nous allons nous concentrer sur deux plateformes de solution courantes : la gestion des services, et la gestion des périphériques et des terminaux.

Ces solutions représentent en fait trois solutions distinctes :

1. Gestion des actifs IT (ITAM).
2. Gestion des services IT (ITSM).
3. Gestion unifiée des terminaux (UEM), qui inclut aussi des clients et des fonctions MDM (gestion moderne des périphériques).

Même si le département IT est traditionnellement chargé de surveiller ces technologies et dispose du budget nécessaire, l'équipe Sécurité peut quand même collaborer avec ses partenaires IT.

Avec ce partenariat, les solutions ponctuelles et la pile de produits de niche deviennent une plateforme transverse polyvalente et robuste, capable de survivre aux purges de consolidation.

Solutions et outils IT courants

Gestion des services

ITAM (Gestion des actifs IT)

- Mise à jour automatique de la liste/base de données des actifs de l'entreprise
- Suivi des variables standard et par défaut des actifs, utilisateurs et activités

ITSM (Gestion des services IT)

- Vitrine principale des tâches de l'équipe IT jouant un rôle de gestion de projets
- Peut contenir des wiki, des FAQ et des fonctions de création de formulaires internes
- Peut héberger des automatisations back-end liées à l'IT

Gestion des périphériques et des terminaux

UEM (Gestion unifiée des terminaux)

- Gestion fondamentale des terminaux et contrôle des politiques
- Peut contenir des clients MDM, figurant sur chaque périphérique et poste client de l'entreprise

ITAM et ITSM + Sécurité

Dans cette section :

- Définir l'ITAM et l'ITSM
- Cas d'usage ITAM et ITSM appliqués à la sécurité
- « Shift Left » de la sécurité avec l'ITAM et l'ITSM

Définitions rapides : ITAM et ITSM

Outils de gestion des actifs IT (ITAM)	Outil de gestion des services IT (ITSM)
L'ITAM assure la gestion des éléments de configuration (CI), comme les actifs matériels et logiciels.	L'ITSM améliore la capacité du département IT à répondre aux demandes de suivi, de réponse et de technologie de service émanant de l'utilisateur final et de clients internes.
Cet outil permet aux entreprises de configurer, optimiser et suivre les CI tout au long de leur cycle de vie, de l'achat à la fin de vie.	L'ITSM peut aussi inclure une fonction permettant aux utilisateurs de corriger en « self-service » les problèmes techniques les plus simples pour éviter de faire appel au centre de support.

L'ITAM existe rarement sans une plateforme ITSM partenaire, même s'il est possible d'implémenter des produits ITSM sans y recourir.

Une bonne plateforme réunissant ITAM et ITSM fait généralement le suivi de ces informations :

- Date et informations de l'achat d'origine.
- Propriétaires et utilisateurs des périphériques.
- Politiques d'application d'accès utilisateur actuellement appliquées.
- OS, applications et logiciels actuellement installés, et leur utilisation.
- Emplacement du périphérique.
- Type de périphérique.
- Performances, usage et état de conformité.

Cas d’usage ITAM et ITSM appliqués à la sécurité

Lorsque les équipes collaborent efficacement, et que les politiques et les configurations appropriées sont en place, les plateformes ITAM et ITSM peuvent fournir des informations précieuses aux équipes de sécurité :

1

Découverte dynamique des actifs

2

Opportunités de CMDB (Base de gestion des configurations)

3

Amélioration de la GRC (Gouvernance, risques et conformité)

4

Options d’automatisation IT uniques pouvant être reconfigurées pour faciliter les tâches de sécurité essentiellement manuelles

1 Sécurité et découverte des actifs

La découverte et la gestion des actifs constituent les bases d'un programme de sécurité. En fait, les principaux frameworks CSF (Cybersecurity Framework) et les réglementations sur la protection des données considèrent tous la découverte des actifs comme une phase fondamentale de la construction d'un système sécurisé.

Pourquoi ? La première étape d'une cyberattaque réussie est généralement la reconnaissance. L'acteur malveillant cherche premièrement à obtenir une bonne visibilité des CI, actifs et systèmes de l'entreprise, afin de savoir quoi viser et comment lancer l'attaque.

Exigences liées à la découverte des actifs dans les CSF sélectionnés

CSF	Section concernée	Citation sur la découverte des actifs
NIST Cybersecurity Framework	First Core Function: Identify	« Identifier : Développer une compréhension organisationnelle pour gérer les risques de cybersécurité des systèmes, personnes, **actifs**, données et capacités. »
Center for Internet Security (CIS) Critical Security Controls, V8	1st Control: Inventory	**« Gérer activement (inventorier, suivre et corriger) tous les actifs de l'entreprise** (périphériques des utilisateurs finaux, notamment portables et mobiles ; périphériques réseau ; périphériques non IT/Internet des objets (IoT) ; et serveurs) connectés à l'infrastructure physiquement, virtuellement, à distance et dans le Cloud, pour **connaître avec précision la totalité des actifs** qu'il faut surveiller et protéger dans l'entreprise. » « Prend aussi en charge **l'identification des actifs non autorisés ou non gérés** devant être supprimés ou corrigés. »
Australia Cyber Security Centre: Essential Eight	Maturity Levels Overview	« Ce système inclut la **découverte des actifs**, étape importante pour prévenir les attaques à tous les niveaux de maturité. »
Directive 2022/2555 (NIS2) de l'Union européenne	Paragraph 44	« Les CSIRT [Équipes de réponse aux incidents de sécurité des ordinateurs] doivent être capables, sur demande d'une entité essentielle ou importante, de **surveiller les actifs connectés à Internet,** à la fois sur site et hors site, afin d'identifier, de comprendre et de gérer le risque organisationnel global de cette entité en matière de menaces nouvellement identifiées ou de vulnérabilités critiques de la supply chain. »

Ainsi, tous ces frameworks stipulent que, pour se défendre contre les cyberattaques, votre équipe de sécurité doit avoir une connaissance précise de ce qu'elle protège.

Bien entendu, en pratique, la plupart des entreprises tendent à constater un angle mort de 20-30 % dans la visibilité de leurs actifs réseau.

En fait, seuls 47 % des professionnels IT affirment que leur entreprise a une visibilité totale sur tous les périphériques qui tentent d'accéder à son réseau.

Pourtant, les fonctions de découverte automatique des actifs déjà présentes dans différentes plateformes de technologie IT (y compris les produits ITSM et ITAM) permettraient aux équipes Sécurité d'analyser proactivement les risques associés aux actifs technologiques et à leurs utilisateurs.

« Si vous ne connaissez pas ce qui constitue votre environnement, vous ne pouvez pas le sécuriser.

En matière de gestion des vulnérabilités, votre première préoccupation doit être **de comprendre votre surface d'attaque et ce qui est visible. »**

- Chris Goettl
VP of Endpoint Security Product Management, Ivanti

Pour le département IT, la découverte automatisée des actifs permet de rapprocher les achats de périphérique et de logiciels budgétés des périphériques présents sur le réseau et des statistiques d'utilisation.

Si vous les synchronisez avec un outil ITSM, ces statistiques peuvent être associées aux demandes de support des utilisateurs, afin de contextualiser les tickets IT et les interruptions éventuelles..

Pour les équipes de sécurité, ces mêmes fonctions de découverte des actifs des solutions IT peuvent servir à respecter les exigences de découverte des actifs des différents frameworks de sécurité.

En outre, le cas d'usage de la découverte automatisée des actifs peut être poussé encore plus loin que ses paramètres par défaut ne le suggèrent. Il aidera ainsi les équipes Sécurité de différentes manières :

Détecter

le périphérique d'un fournisseur et contrôler son accès pour se conformer à des politques d'accès tierces

Analyser

les périphériques à distance pour vérifier leur conformité aux politiques de sécurité et mises à jour de correctifs de l'entreprise

Isoler ou remédier

les périphériques en transit

2 Sécurité et CMDB

Connaître vos actifs est une étape indispensable pour une implémentation proactive de la sécurité. Cependant, pour que votre équipe comprenne vraiment le paysage de risques global de votre entreprise, vous devez savoir comment les différents périphériques, applis et utilisateurs interagissent.

La base de données CMDB qui gère les configurations du département IT fournit des détails essentiels sur ces relations.

Alors qu'un outil ITAM suit le cycle de vie des actifs, une base CMDB (souvent hébergée sur une plateforme ITSM) gère les relations entre les divers CI (éléments de configuration) et leur environnement.

Comme l'outil ITAM, la CMDB inclut des informations de base sur les actifs et les utilisateurs, notamment le nom de l'utilisateur d'un poste de travail donné et sa localisation. Mais elle inclut également des informations contextuelles, comme la liste des périphériques et des logiciels qui interagissent avec le poste de travail en question.

Pour un technicien de sécurité expérimenté, ces relations révèlent le degré d'exposition du CI aux risques et lui indique comment atténuer cette exposition.

3 Sécurité et GRC

La cartographie de ces relations et activités sur le réseau permet aussi de comprendre et d'appliquer la GRC (Gouvernance, risques et conformité) en temps réel et de manière contextualisée.

Comment l'ITAM et l'ITSM facilitent la GRC de la sécurité

Gouvernance

Plus de contexte grâce au partage des données
Personne ne souhaite donner un ordre que personne ne suivra… ou qui n'a pas d'intérêt pour son équipe ou son entreprise.

Les équipes IT et de sécurité peuvent aider les dirigeants à comprendre le paysage actuel des risques, des utilisateurs et des actifs de leur entreprise en rédigeant des politiques pertinentes et sensées à partir des données collectées par les outils ITAM et ITSM.

Politiques par défaut via le back-end
En s'appuyant sur les systèmes back-end déjà administrés par l'équipe IT, l'équipe de sécurité s'assure que les politiques, contrôles et documents relatifs à la sécurité sont bien organisés et facilement accessibles.

Cela garantit également que les politiques de sécurité sont par défaut incluses dans la documentation plus large de l'entreprise, qui informe sur les processus technologiques des différents départements.

Risques

Cartographie de la surface d'attaque via la découverte
Avec leurs produits ITSM et ITAM, les équipes de sécurité peuvent cartographier la surface d'attaque potentielle de leur entreprise, et analyser la composition du réseau, des périphériques et des utilisateurs.

Une meilleure compréhension de la surface d'attaque exposée aux pirates aide à définir les politiques et tactiques de sécurité qui fonctionneront le mieux pour l'environnement de menaces et les activités réseau propres à l'entreprise.

Déclencheurs d'automatisation via la CMDB
Les équipes de sécurité peuvent utiliser les CI actuels pour créer des variables personnalisées spécifiques à la sécurité, qui font ensuite l'objet d'un suivi dans la CMDB de l'ITAM à la fois en tant que déclencheurs de formules automatisées et de composantes de ces formules.

Conformité

Gestion des fournisseurs via la collecte de données
En s'appuyant sur les données collectées via les listes ITAM et en mettant constamment à jour les plateformes ITSM, les équipes de sécurité peuvent rédiger des contrats fournisseurs qui soutiennent et garantissent que les pratiques sont en conformité avec les politiques de leur entreprise, avec à la clé une réduction des risques de sécurité de la supply chain.

Gestion des postes client via la découverte
Les fonctionnalités de découverte des actifs permettent aux équipes IT et Sécurité d'identifier les périphériques non autorisés sur les réseaux d'entreprise sensibles.

Ces fonctionnalités peuvent aussi prendre en charge l'envoi d'alertes de non-conformité aux périphériques, la segmentation réseau, voire la mise en quarantaine directe du poste client si nécessaire… le tout déployé et appliqué par d'autres outils IT, comme les clients UEM et MDM.

Gestion de la sécurité via les politiques IT
Les fonctionnalités IT qui appliquent les politiques informatiques d'ordre général dans toute l'entreprise peuvent aussi signaler et appliquer si nécessaire des protocoles de sécurité, notamment en plaçant des garde-fous pour les Admins IT qui aident des utilisateurs avec leurs tickets de support, et en envoyant des alertes en cas de violation d'une politique ou sur la base d'indicateurs de menace interne.

Répercussions dans le monde réel

Expérimentation imaginaire - Une tablette à l'hôpital

Imaginez un moment que vous travaillez dans un hôpital.

Vos équipes IT et de sécurité font le suivi des postes client dotés de fonctions Internet, y compris les tablettes, que seul le personnel médical peut utiliser.

Cependant, un spécialiste de la sécurité remarque des activités bizarres sur une tablette qui ne devrait accéder qu'aux bases de données et intranets de l'hôpital.

En fait, cette tablette a consigné un accès à un navigateur Internet externe… et des tentatives de téléchargement d'applis de jeu « sujettes à des fuites ».

Comme ce comportement suspect a été signalé via l'automatisation ITSM/ITAM (en partie grâce à des journaux CMDB et des variables de CI), votre équipe Sécurité fait une enquête et interroge les utilisateurs les plus récemment connectés.

Finalement, la personne en charge des chambres situées à cet étage admet avoir autorisé (de manière informelle) le personnel à laisser les patients utiliser cette tablette pour surfer occasionnellement sur Internet pendant qu'ils recevaient un traitement.

(C'est en fait un service de pédiatrie qui est installé à cet étage !)

Il apparaît clairement que cette personne n'a pas respecté les politiques et protocoles internes conçus pour protéger tout le monde (même les enfants !) des pirates.

Cependant, l'équipe de sécurité peut choisir de ne pas sanctionner cet utilisateur final non conforme, partant du principe qu'il avait de bonnes intentions, et qu'il ne s'agissait ni de paresse ni d'une mauvaise attitude.

À la place, elle peut travailler avec l'équipe IT et redéployer de vieilles tablettes bientôt en fin de vie pour que les patients les utilisent.

Ces tablettes permettent aux patients de jouer à des jeux (approuvés par l'équipe Sécurité) pendant leur traitement, tout en restant isolées des intranets sensibles de l'hôpital, avec un suivi automatique des activités malveillantes.

Bien que sa mise en place risque, au début, de donner quelques sueurs à toutes les personnes impliquées, cette solution est triplement gagnante :

Les **patients** se sentent entourés et bien traités, comme auparavant.

Les **deux équipes Sécurité et IT** ne deviennent pas les « départements du non » en appliquant une politique que les utilisateurs tentent activement de contourner.

Les **utilisateurs finaux** (dans ce cas le personnel médical) n'ont pas à partager leurs tablettes avec les patients. Ils se sentent en sécurité, ce qui les rend plus enclins à respecter sans rechigner les futures demandes des équipes Sécurité et IT.

4 « Shift Left » de la charge de travail de la sécurité grâce aux automatisations ITAM et ITSM

Si vous envisagez de partager les outils IT (notamment l'ITAM et l'ITSM) pour les cas d'usage de sécurité, réfléchissez à la façon dont vous pouvez utiliser les automatisations et implémentations actuelles, centrées sur l'IT, pour encourager le « Shift Left » de votre équipe.

Vous découvrirez que vous pouvez vous engager dans davantage d'actions de sécurité avec moins d'efforts (bien au-delà des alertes de base et des jauges des tableaux de bord) et envisager une remédiation des risques réellement proactive.

1 **Améliorez les options en self-service pour les utilisateurs finaux**

avec des questions et des demandes de sécurité, afin de libérer vos analystes les plus expérimentés de l'identification des hameçonnages.

2 **Unifiez la résolution des incidents de sécurité**

avec des logiciels de tickets IT et des files d'attente de priorisation (alimentées par les formulaires de demande) pour améliorer la priorisation, le suivi et la contextualisation.

3 **Réorientez les automatisations IT à l'arrière-plan**

pour vos objectifs de sécurité, car ces automatisations peuvent réparer les périphériques avant la création de tickets, peuvent renforcer la sécurité des environnements de postes client et repérer les activités malveillantes.

ivanti

Automatisation n°1 :

Améliorer le self-service de sécurité pour un support « de niveau zéro »

Le système que vous utilisez actuellement pour alléger la charge des centres de support IT peut s'avérer utile pour la sécurité !

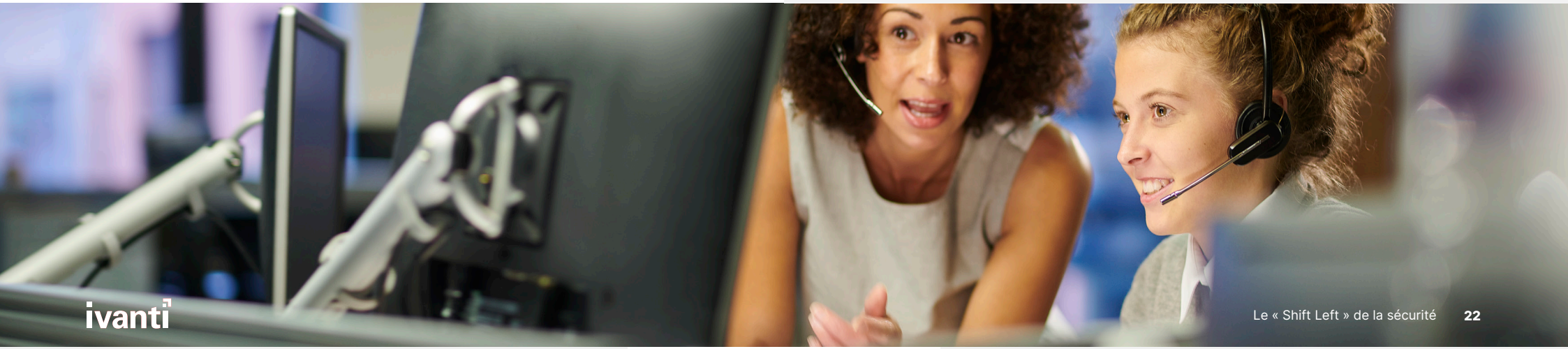
En centralisant les questions et demandes courantes liées à la sécurité (notamment, comment activer l'authentification à deux facteurs, signaler une attaque par hameçonnage ou demander la réinitialisation d'un mot de passe), vous permettez aux utilisateurs finaux de résoudre eux-mêmes leurs problèmes au lieu de demander directement l'aide de l'équipe Sécurité.

Si vous regroupez les réponses, les informations et les demandes relatives à la sécurité en un seul endroit, avec la même infrastructure que celle du département IT, les utilisateurs finaux sauront exactement où aller (après tout, ce sera au même endroit que pour les informations IT !) et ils ne chercheront pas à contourner le système.

****

Dans votre wiki dédié à la sécurité, pensez à inclure :

- **Toutes les politiques de sécurité en vigueur :** chacune est précédée d'une liste à scanner mentionnant les utilisateurs et périphériques concernés par chaque politique (limitations ou permissions accordées, le processus relatif aux demandes d'exception et son emplacement, et (le plus important) la façon dont cette politique protège l'entreprise.
- **Des informations sur comment demander de nouveaux mots de passe ou noms d'utilisateur.**
- **Des informations sur comment demander l'approbation d'un nouveau fournisseur ou logiciel par l'équipe Sécurité,** ainsi que la raison pour laquelle la Sécurité doit approuver toute appli ponctuelle et comment cela protège l'entreprise.
- **Des informations sur comment implémenter la 2FA** (authentification à 2 facteurs) sur chacun des périphériques et applications pris en charge par l'entreprise.
- **Des feuilles de route de politique de sécurité** applicables aux implémentations futures planifiées, telles qu'approuvées pour les communications avec les parties prenantes internes.



Automatisation n°2 :

Unifier les files d'attente de tickets de sécurité avec des données de périphérique et d'utilisateur contextualisées

La plateforme ITSM que vous utilisez actuellement pour les tickets de centre de support peut servir à créer des files d'attente spécifiques pour les questions de sécurité et la priorisation de la remédiation.

Vous pouvez même implémenter des formulaires de demande d'accès aux fichiers ou d'exemption de politique dans votre wiki dédié à la sécurité, pour un support utilisateur de niveau zéro en « self-service ».

Ces formulaires peuvent ensuite être utilisés pour alimenter une file d'attente publique centralisée, au lieu de finir dans les boîtes mail de spécialistes qui risquent de les ignorer pour se consacrer à des « priorités plus urgentes ».

Enfin, ces demandes peuvent facilement être réaffectées et résolues par le personnel de sécurité moins expérimenté, libérant ainsi votre main-d'œuvre stratégique pour les sujets les plus pressants.

Si votre équipe Sécurité a mis en place un wiki, elle peut se référer aux politiques qui y figurent pour justifier sa décision d'accorder ou de refuser les permissions d'accès demandées… même pour les dirigeants !

Automatisation n°3 :

Réorienter l'automatisation IT pour l'appliquer à des cas d'usage de sécurité proactive étendus

Les options d'automatisation IT proactives et de réparation qui se déclenchent sur la base de paramètres spécifiques dans les outils ITAM et ITSM peuvent être clonées et adaptées à des objectifs de sécurité.

Automatisation IT pour des cas d'usage de sécurité

Déprovisionnement

Assurez-vous que les informations d'authentification des collaborateurs ou des fournisseurs qui quittent l'entreprise sont décommissionnées au moment où leur contrat est résilié ou au changement d'état de l'utilisateur.

Évaluation des valeurs de référence

L'automatisation peut collecter et agréger les « valeurs de référence » concernant les activités de votre entreprise, ce qui vous aide à connaître l'impact futur de la sécurité sur la productivité et à détecter d'éventuelles intrusions.

Signalement des activités malveillantes

Émission d'une alerte en cas de potentielle menace interne ou de compromission d'un compte, déclenchée par les CI hors norme, et demandant la révision manuelle du périphérique ou de l'utilisateur par un analyste de sécurité humain.

Surveillance du déploiement

Lors du déploiement de correctifs ou de politiques, vous pouvez paramétrer l'automatisation de façon à surveiller les perturbations sur la base de cadences waterfall prédéterminées, et les classer par priorités selon le profil des utilisateurs ou des périphériques, tel que cela est régi par les workflows actuels

UEM + Sécurité

Dans cette section :

- Définir l'UEM et le MDM
- Cas d'usage UEM appliqués à la sécurité
- « Shift Left » de la sécurité avec les automatisations UEM

Définitions rapides : UEM et MDM

Gestion unifiée des terminaux (UEM)	Gestion des périphériques mobiles (MDM)
L'UEM est une plateforme technologique IT que les administrateurs système utilisent pour gérer plusieurs postes de travail ou terminaux (périphériques, matériel et autres technologies) depuis un écran ou un tableau de bord unique. L'UEM couvre une large gamme de systèmes d'exploitation (OS) et de nombreux types de périphériques provenant de divers fournisseurs et développeurs.	Souvent appelé gestion « moderne » des périphériques, le MDM était auparavant une technologie de niche autonome qui permettait aux équipes IT de contrôler et d'appliquer des politiques, des configurations et des logiciels aux smartphones, tablettes et autres postes client prenant en charge les API MDM. Cependant, le MDM se limitait souvent aux périphériques exécutant des systèmes d'exploitation spécifiques, et les équipes IT devaient exécuter plusieurs outils MDM simultanément pour gérer tous les périphériques. Aujourd'hui, bien que les éditeurs d'OS et les fabricants de périphériques de niche publient toujours des produits MDM ponctuels pour gérer leurs terminaux, les solutions UEM complètes incluent des fonctions MDM dans leur plateforme.

Les plateformes UEM permettent aux équipes IT (et maintenant, aux équipes Sécurité) de gérer leurs actifs matériels et logiciels avec une seule plateforme et un seul tableau de bord, quels que soient :

- l'OS,
- le type de périphérique,
- l'emplacement du périphérique ou le lieu d'accès, ou
- les permissions spécifiques de l'utilisateur.

Cas d’usage UEM appliqués à la sécurité

Les clients UEM et MDM de votre équipe IT peuvent être reconfigurés pour répondre aux besoins de l’équipe Sécurité :

Déploiement proactif des périphériques des nouveaux collaborateurs avec des contrôles d’accès axés sur la sécurité pour des profils de périphérique et d’utilisateur spécifiques

Contrôles robustes des périphériques IoT (Internet of Things) et segmentations réseau afin de verrouiller les périphériques difficiles à mettre à jour et à suivre (ils constituent un point d’accès au réseau pour les pirates)

Un socle commun, applicable à tous les OS et périphériques, pour toutes les extensions et les cas d’usage (applicables aussi bien à l’IT qu’à la Sécurité) qui sera utile en cas de pression budgétaire et d’augmentation des besoins

Sécurité et onboarding des périphériques

L'intégration de la sécurité dans les processus IT existants peut se faire au nouveau de l'onboarding des nouveaux collaborateurs, c'est particulièrement simple si votre entreprise effectue actuellement des déploiements hybrides ou entièrement à distance.

Après tout, l'IT est responsable du provisionnement des nouveaux périphériques configurés avec les logiciels et permissions d'accès appropriés pour des utilisateurs qui risquent de ne jamais mettre un pied dans les bureaux.

Ce processus offre à l'équipe de sécurité une opportunité unique de s'assurer que même les utilisateurs et périphériques distants sont configurés de manière sécurisée dès le départ, avant même qu'ils ne se connectent à un réseau d'entreprise.

Les solutions UEM permettent aux administrateurs IT de définir des profils d'utilisateur et de périphérique préconfigurés sur les nouveaux ordinateurs portables ou de bureau, à partir des machines virtuelles (VM) créées au préalable.

Si vous combinez cela à un outil ITSM, les personnes en charge du recrutement peuvent utiliser un portail en self-service pour les réquisitions et les permissions, sans impliquer activement aucun membre du département IT avant la réquisition proprement dite et la configuration du périphérique/profil.

Votre département IT a certainement déjà mis en place un processus pour l'onboarding des nouveaux utilisateurs. Demandez-leur :

- quelles sont les étapes déjà en place,
- comment ils utilisent leurs outils UEM pour le déploiement, et
- à quelle étape votre équipe de sécurité et vos politiques de sécurité pourraient s'immiscer dans leurs procédures opérationnelles standard.

Répercussions dans le monde réel

Intégration de politiques de sécurité dès le premier jour

Interrogé dans le cadre d'une étude TEI menée pour Ivanti par Forrester Consulting, un ingénieur intégration travaillant chez un détaillant de chaussures a déclaré que son équipe passait deux à trois jours à installer et configurer des logiciels par périphérique.

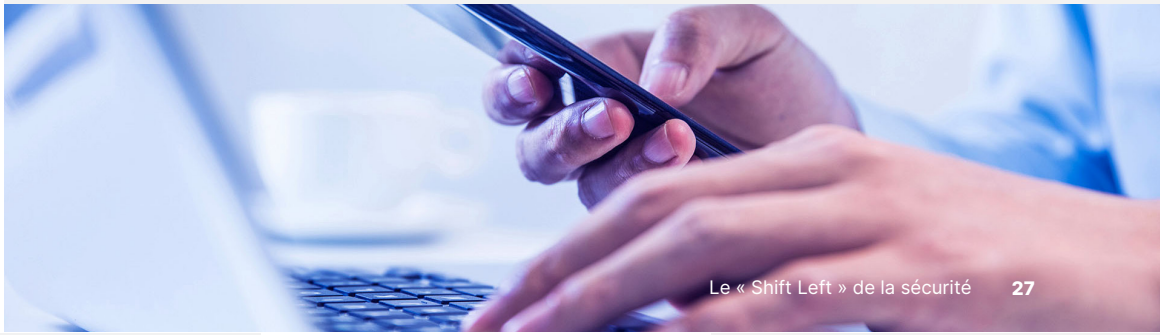
Après l'implémentation d'Ivanti Neurons for UEM, cette personne déclarait :

« Maintenant, une fois l'image créée, il suffit d'installer Ivanti et de faire un glisser-déplacer du périphérique dans les tâches logicielles. Cela prend cinq à dix minutes. En fin de journée, nous vérifions que toutes les applications sont présentes. Cela nous a permis d'accélérer significativement le processus d'onboarding des utilisateurs. »

Les activités de configuration de votre équipe doivent être intégrées dès l'onboarding au lieu d'être traitées ultérieurement, lorsque vos collaborateurs en auront le temps.

Vous devez cependant négocier avec vos partenaires IT les permissions, applications et droits d'accès par défaut les moins intrusifs pour chaque profil d'utilisateur, équipe ou type de périphérique dans votre entreprise.

FORRESTER®



Sécurité et IoT

Les politiques de sécurité des postes client IoT (distribuées et appliquées via des clients UEM et MDM) représentent une fantastique opportunité de création de valeur lorsque votre équipe de sécurité cherche à réutiliser la pile technologique IT existante.

Après tout, les attaques visant l'IoT ont représenté plus de 12 % de toutes les attaques par malware dans le monde en 2021, contre moins de 1 % en 2019.

Pourtant, 47 % des professionnels IT interrogés déclarent que leur entreprise n'applique aucune politique de conformité IoT.

Comment l'expliquer ? Ces entreprises ont peut-être une politique IoT, mais les spécialistes interrogés n'en connaissent pas l'existence, ne savent pas qu'ils devraient en avoir une, ou ne savent pas comment l'implémenter.

Pourtant, les données de sécurité fournies par vos équipes et spécialistes devraient vous permettre de remédier à la vulnérabilité des périphériques vulnérables connectés à Internet, à la fois dans l'entreprise et sur les lieux de travail distants, grâce aux fonctions relativement simples de segmentation réseau et d'analyse UEM.

Répercussions dans le monde réel

Les dangers liés aux thermomètres

Consécutivement à l'exploitation d'une vulnérabilité du thermomètre de l'aquarium situé dans son hall, un casino nord-américain a découvert les conséquences catastrophiques qu'une mauvaise gestion IoT pouvait avoir sur ses opérations.

Comme cet aquarium connecté à Internet n'était pas correctement isolé du réseau du casino, les pirates ont pu se déplacer latéralement dans l'infrastructure Cloud du casino pour mener leur attaque.

Sécurité et intégration multi-OS

Même si notre eBook traite principalement de la façon dont vous pouvez « recycler » vos outils et plateformes IT existants, nous savons qu'à terme les risques et besoins de votre entreprise vont dépasser les politiques de sécurité et options de mise en œuvre offertes par vos outils actuels.

Pourtant, les solutions UEM représentent une rampe de lancement particulièrement bien positionnée pour intégrer les futurs déploiements d'outils de sécurité dans le profil d'accès de chaque périphérique et utilisateur, quel que soit l'endroit où il se trouve ou l'OS qu'il exécute.

Après tout, même la solution UEM comprend un client installé directement sur chaque périphérique que l'entreprise possède et gère.

Il vous suffit vraiment de quelques clics pour que d'autres outils de sécurité soient installés sur le même périphérique via le client UEM, ce qui renforce immédiatement la sécurité des postes client sans nuire à la productivité des utilisateurs finaux de votre entreprise… un gain immense pour vos alliés de l'IT.

Déploiement des futures options de sécurité via les outils UEM et MDM

PM (Gestion des correctifs) et RBVM (Gestion des vulnérabilités basée sur les risques)

Au-delà des fonctions d'automatisation et de surveillance offertes par les plateformes ITSM, ITAM et UEM, vous pouvez combiner la solution UEM aux solutions de gestion des correctifs et des vulnérabilités basée sur les risques, pour apporter une réponse proactive et transparente aux risques et remédier aux vulnérabilités activement exploitées.

En associant des solutions PM et RBVM à une plateforme IT configurée pour la sécurité, vos équipes Sécurité et IT peuvent contextualiser les correctifs les plus urgents sur la base des vulnérabilités activement exploitées. Leur liste peut être recoupée avec les informations fournies par la plateforme ITAM/ITSM sur vos actifs et distribuées par votre outil UEM dans le respect des SLA de sécurité IT.

MTD (Protection contre les menaces mobiles)

Même si les configurations et paramètres de l'outil UEM peuvent contribuer à limiter les dommages initiaux causés par un clic sur un lien d'hameçonnage (en particulier s'il a été associé à une solution de gestion des correctifs, ce qui entrave sérieusement la capacité des pirates à élever leurs privilèges ou à se déplacer sur le réseau !), cet outil reste moins efficace que si vous associez une politique à une solution de défense contre les menaces mobiles (MTD) multi-OS.

Les meilleures solutions MTD peuvent fonctionner via le client UEM d'un périphérique enrôlé (détenu par l'entreprise ou utilisé dans un programme BYOD), tout en détectant les activités potentiellement malveillantes et les attaques par hameçonnage, en les isolant, en mettant les périphériques en quarantaine et en émettant des alertes de manière dynamique.

« Shift Left » de la charge de travail de la sécurité grâce à l'UEM

Tout comme l'ITAM et l'ITSM offrent des possibilités d'automatisation axées sur l'IT réutilisables pour le « Shift Left » de la sécurité, les outils UEM comprennent aussi un certain nombre d'options d'automatisation qui s'avèrent utiles pour atteindre vos objectifs de sécurité.

Les outils UEM offrent des fonctionnalités d'automatisation et d'implémentation spécifiques qui permettent aux équipes de sécurité de :

Garantir une conformité à 100 % à la politique de décommissionnement des collaborateurs quittant l'entreprise et d'élimination des « informations d'authentification zombies » des fournisseurs tiers.

Appliquer des politiques de sécurité aux périphériques BYOD ou activement gérés autorisés à accéder aux réseaux de l'entreprise, que ce soit au bureau ou en télétravail.

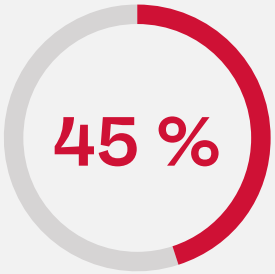
Passer au crible les enregistrements compilés axés sur la sécurité des périphériques, lors de la réponse à un incident ou pour la contextualisation des alertes.

1 Garantie de conformité à la politique de décomissionnement relative aux « informations d'authentification zombies »

Dans une enquête internationale menée par Ivanti auprès de plus de 900 professionnels de la sécurité, 68 % seulement des personnes interrogées déclarent que leur entreprise a suivi les conseils de déprovisionnement des informations d'authentification en cas de fin de contrat ou de démission d'un collaborateur, sous-traitant tiers ou autre fournisseur.

En fait, 45 % de ces professionnels de la sécurité disent soupçonner que d'anciens collaborateurs et sous-traitants ont toujours un accès actif aux systèmes et fichiers de l'entreprise grâce à d'anciennes informations de connexion jamais détruites : les « informations d'authentification zombies ».

Les fonctions d'automatisation des plateformes UEM et des clients MDM hébergés sur les périphériques permettent un décomissionnement immédiat des informations d'authentification zombies lorsque le profil interne d'un utilisateur signale que ce dernier n'est plus un collaborateur actif de l'entreprise, ce qui élimine de futures menaces externes liées aux actifs des anciens collaborateurs.



des professionnels de la sécurité disent soupçonner (voire être sûrs) que d'anciens collaborateurs et sous-traitants ont toujours un accès actif aux systèmes ou fichiers, que ce soit par des noms d'utilisateur, des informations de connexion ou des mots de passe toujours actifs.

2 Application de politiques de sécurité sur tous les périphériques de poste client gérés, au bureau ou à distance

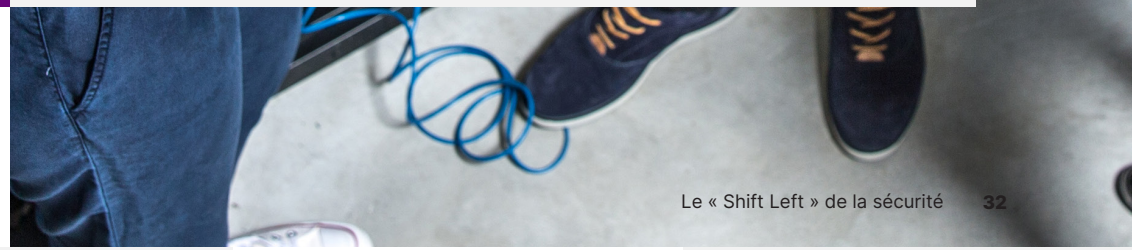
Bien sûr, l'erreur humaine restera toujours le point faible de toute politique de sécurité. Cependant, l'application de solutions et de politiques de sécurité via la plateforme UEM de l'équipe IT permet d'atténuer certains des risques créés par vos utilisateurs finaux les moins impliqués, surtout s'ils travaillent à distance ou en mode hybride.

Par exemple, de nombreuses techniques de reconnaissance initiale et d'intrusion utilisées par les acteurs de la menace peuvent être bloquées en adoptant des mesures appropriées de découverte des actifs, de segmentation réseau et de surveillance des périphériques.

Toutes ces mesures de remédiation peuvent être exécutées via des solutions UEM pourvues de fonctionnalités axées sur la sécurité et configurées à cet effet.

De plus, en déployant une solution UEM dotée de politiques et de configurations axées sur la sécurité, les entreprises ne sont plus dépendantes des utilisateurs qui devaient auparavant s'abonner aux mises à jour ou aux applications de sécurité nécessaires.

Au lieu de cela, les périphériques gérés par UEM sont automatiquement enrôlés dans le calendrier de mise à jour ou d'installation approprié… sans aucune intervention de l'utilisateur !



3 Examen des enregistrements relatifs aux périphériques hébergés par l'outil UEM lors de la réponse aux incidents

Les journaux de suivi des périphériques et des utilisateurs créés par la plateforme UEM peuvent être exploités par la sécurité (le personnel IT les utilise et les consulte généralement pour réparer les périphériques des utilisateurs finaux).

Si l'entreprise a des raisons de croire qu'un collaborateur représente une menace interne, l'équipe Sécurité peut rechercher dans les enregistrements de ses périphériques des signes d'installation et d'utilisation illégales d'outils de niveau Admin système, comme PowerShell.

Le système de l'entreprise peut aussi avertir que l'activité d'un « utilisateur » ordinaire montre qu'il exécute soudain des techniques de mise en réseau avancées sur son périphérique géré.

Ce type d'activité peut signifier qu'il ne s'agit pas du tout de l'utilisateur autorisé, mais d'un pirate qui se cache derrière les informations d'authentification authentiques (mais infectées) de cet utilisateur et tente d'élever ses privilèges dans le réseau de l'entreprise.

Avec les configurations, les alertes et les outils de sécurité adaptés, il est possible de détecter ces activités sur un poste client ou un périphérique mobile bien avant que le pirate ne se déplace latéralement dans le réseau de l'entreprise ou n'obtienne des permissions élevées de niveau Admin.

Enfin, comme la hausse des tarifs des cyberassurances exerce une pression supplémentaire sur les finances déjà tendues des entreprises, les équipes IT et Sécurité prennent conscience qu'elles doivent appliquer des politiques plus strictes et mettre en place des alertes sur les activités des utilisateurs afin de remédier proactivement aux risques et de réduire les primes d'assurance.

ivanti

04

Tous les chemins mènent à la DEX :

Dans cette section :

1. Pourquoi l'IT et la Sécurité doivent-elles se préoccuper de la DEX
2. Comment la DEX back-end des piles technologiques partagées profite aussi aux administrateurs techniques

La DEX, l'atout secret de l'équipe Sécurité lors du « Shift Left » avec l'IT

Tout au long de ce guide, nous avons montré que les équipes Sécurité peuvent se réinventer, tout en réduisant leur empreinte technologique, en « recyclant » les fonctionnalités ITSM, ITAM et UEM utilisées par l'IT.

Cependant, les entreprises peuvent tirer un avantage supplémentaire de l'utilisation conjointe et de la consolidation de leurs outils IT et de sécurité : l'amélioration de l'expérience numérique des collaborateurs, la DEX.

Les avantages liés à la DEX concernent toute l'entreprise bien au-delà des seuls utilisateurs finaux. Voici quelques-uns des cas d'usage axés sur :

Les besoins de la Sécurité

Les besoins de l'IT

Les besoins généraux des administrateurs

71 %

des organisations à la pointe en matière de sécurité affirment que la DEX des utilisateurs finaux est l'une de leurs principales priorités, voire un élément clé de leurs politiques de sécurité.

(Soit 20 points de plus que dans les entreprises moins matures !)

La DEX des utilisateurs finaux est bénéfique pour les équipes Sécurité et IT

Bien que les départements Sécurité et IT se préoccupent tous deux de l'expérience numérique des collaborateurs pour des raisons différentes, l'amélioration de la DEX des utilisateurs finaux est bénéfique pour tous !

Avantages de la DEX pour l'équipe Sécurité

Avantage	Pourquoi c'est important pour l'équipe Sécurité
L'amélioration de l'expérience utilisateur freine le Shadow IT.	Lorsque les périphériques ou applis fournis par l'entreprise leur paraissent trop lourds ou frustrants, les collaborateurs se tournent vers des périphériques ou applis non approuvés (Shadow IT). Ce Shadow IT crée des vulnérabilités sur le réseau et peut exposer l'entreprise au cybercrime : en 2022, 12,8 % des cyberattaques dans le Cloud impliquaient le Shadow IT. En donnant la priorité à la DEX des utilisateurs finaux, les entreprises facilitent l'utilisation des applications et périphériques autorisés par l'équipe Sécurité pour les utilisateurs finaux, et diminuent le Shadow IT. Pourquoi se donner la peine d'installer une appli tierce si ce qu'on a déjà fonctionne ?
L'implémentation back-end invisible des politiques de sécurité encourage la mise en conformité tacite des utilisateurs.	Les entreprises peuvent (et elles le font !) diffuser leurs politiques sur papier pour imposer aux utilisateurs finaux de se protéger en exécutant ou en évitant certaines opérations. Sinon, l'équipe Sécurité peut tout simplement implémenter une automatisation back-end qui applique ces politiques en mode silencieux aux profils des périphériques gérés et des utilisateurs réseau. Les utilisateurs ont connaissance de ces politiques uniquement s'ils réalisent une opération non autorisée. Sinon, ils ne savent même pas que ces restrictions existent. Ce type d'implémentation favorisant la DEX permet aux entreprises de ne plus compter seulement sur la bonne volonté et la mémoire de l'utilisateur final, mais sur de solides implémentations back-end qui ne sollicitent pas l'utilisateur !
Les contrôles de sécurité compatibles avec le travail hybride offrent un confort utilisateur indépendant de l'emplacement.	Avec le développement du télétravail et du travail hybride, les équipes de sécurité savent que la sécurité du réseau et des périphériques doit être renforcée ou que des utilisateurs sont susceptibles d'apporter au bureau des machines potentiellement infectées. D'où la nécessité de recourir à des plateformes IT back-end comme l'UEM et l'ITAM, capables de suivre, gérer et sécuriser tous les types de périphériques, indépendamment de l'OS, qu'ils soient sur site ou à distance ! L'équipe Sécurité est alors en mesure de protéger l'entreprise sans obliger les collaborateurs à venir travailler au bureau.

Le saviez-vous ?

Le département IT de votre entreprise a sans doute déjà mis en place des mesures DEX en continu pour booster la productivité des utilisateurs finaux.

En s'associant à l'équipe Sécurité, vos responsables IT auront des arguments supplémentaires pour justifier leur pile technologique désormais partagée… et cela leur permettra de poursuivre leur programme DEX, alors qu'il aurait pu être considéré comme trop abstrait pour que les dirigeants concernés acceptent cet investissement supplémentaire.

Avantages de la DEX pour l'équipe IT

Avantage de la DEX	Pourquoi c'est important pour l'équipe IT
La réduction des problèmes d'expérience utilisateur diminue le nombre des tickets de centre de support et accélère le service.	Si les périphériques fonctionnent comme les utilisateurs le souhaitent (sans interruption pour redémarrage ni lenteur de traitement pour cause de RAM insuffisante), ils n'ont aucune raison d'émettre des tickets de support. Après avoir implémenté un outil ITSM axé sur la DEX, l'équipe IT d'une organisation religieuse a constaté les bénéfices suivants : diminution du nombre de tickets et expérience de service 90 % plus satisfaisante pour le personnel du centre de support.
L'autoréparation par l'utilisateur réduit le coût de la main-d'œuvre IT.	Si les formulaires des demandes de support et de dépannage sont stockés à un emplacement facilement accessible aux utilisateurs finaux, ces derniers pourront résoudre eux-mêmes leurs problèmes (sans solliciter vos spécialistes IT fortement rémunérés). Après avoir implémenté un portail en self-service basé sur l'ITSM, avec une technologie back-end supplémentaire, une université a constaté que ses étudiants comme son personnel adoptaient totalement cette nouvelle technologie IT… notamment par l'utilisation généralisée des nouvelles fonctions d'auto-assistance sur les périphériques connectés au réseau.
Les technologies axées sur la DEX résolvent les problèmes à la racine et pas seulement en surface.	Les piles technologiques axées sur la DEX permettent à l'équipe IT de rapidement évaluer et consulter les périphériques et l'activité des utilisateurs, quel que soit l'endroit où le périphérique défaillant se trouve dans le monde. Ces insights (associés à des fonctions d'automatisation sophistiquées capables de « réparer » des problèmes plus banals et plus courants) permettent aux professionnels IT de diagnostiquer et résoudre plus rapidement les problèmes. Le périphérique est réparé au premier essai, lors du premier ticket, sans que l'utilisateur final n'ait à se plaindre encore et encore du même problème.

Avantages des piles technologiques partagées pour la DEX des administrateurs

Une expérience numérique des collaborateurs (DEX) d'excellence ne se limite pas aux utilisateurs finaux. Les administrateurs qui emploient ces technologies doivent eux aussi bénéficier d'une DEX de qualité !

Avantages supplémentaires de la DEX pour les admins IT et Sécurité

Avantage de la DEX	Pourquoi c'est important pour les administrateurs
Des outils et périphériques qui fonctionnent permettent aux utilisateurs d'accomplir les tâches pour lesquelles on les paie.	31 % des professionnels IT et de sécurité interrogés ont envisagé de démissionner de leur poste actuel, en partie en raison de problèmes technologiques. Pourquoi démotiver vos actifs les plus coûteux, les êtres humains, alors qu'il suffirait d'améliorer leur expérience de vos technologies pour les retenir ?
Les plateformes et tableaux de bord partagés axés sur la DEX améliorent les compétences et la compréhension de la collaboration entre les départements.	Le partage d'outils intuitifs entre les départements permet d'avoir une compréhension partagée des informations et une présentation transparente des problèmes. Ce partage des connaissances et du contexte augmente l'empathie, évite les malentendus et améliore la coopération entre tous les départements. De plus, les compétences se transmettent rapidement d'un département à l'autre, car tous partagent une compréhension fondamentale des plateformes sous-jacentes.
Le partage de la pile technologique pourrait permettre de récupérer jusqu'à 9 % de la perte de productivité des administrateurs chaque année.	Selon un article récent de la revue Harvard Business Review, les utilisateurs de technologies qui passent leur temps à jongler entre les programmes voient leur taux de productivité se réduire. La main-d'œuvre intellectuelle qui travaille sur ordinateur change de plateforme, d'interface, d'écran ou de microtâche en moyenne 1 200 fois par jour. Ces personnes perdent ainsi, selon les estimations, quatre heures par semaine de travail et 9 % de leur travail rémunéré annuel. Avec une plateforme globale partagée (ou, au moins, une pile technologique offrant des interfaces et des tableaux de bord similaires !) les administrateurs IT et Sécurité ne sont plus exposés à ces pertes de temps, ils peuvent se concentrer sur les tâches qui leur sont affectées, sans distraction.

Références

- Australian Cyber Security Centre. (30 June 2017). “Essential 8 Maturity Model”: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Bowermaster, P. (February 2023). “Shift Left to Risk-Based Proactive Security Management.” CIO’s The Future of Work Summit.
- Center for Internet Security. (2021). “Critical Security Controls Version 8”: https://www.cisecurity.org/controls/v8
- Forrester. (2022). “The Total Economic Impact of Ivanti Unified Endpoint Management (UEM) Solutions”: https://rs.ivanti.com/reports/forrester-tei-of-ivanti-uem-solutions-2022.pdf
- Forrester. (2022). “The Total Economic Impact of the Ivanti Enterprise Service Management. A Forrester Total Economic Impact Study Commissioned by Ivanti”: https://rs.ivanti.com/reports/forrester-tei-ivanti-enterprise-service-management-platform-2021.pdf
- GDPR.EU. (n.d.) “GDPR Checklist for Data Controllers”: https://gdpr.eu/checklist
- Goettl, C. (25 March 2021). “Automated Patch Management and Team Swarming are Key Security Practices.” Ivanti: https://www.ivanti.com/blog/automated-patch-management-and-team-swarming-are-key-security-practices
- Goettl, C., & Masserini, J. (1 September 2022). “Vulnerability Management in Real Life: 5 Best Practices from Real-World RBVM Programs.” Ivanti: https://www.ivanti.com/webinars/2022/vulnerability-management-irl-5-best-practices-from-real-world-rbvm-programs
- Goettle, C. & Stryker, A. (11 May 2023). “Vulnerability Patch Prioritization Problems: Cybersecurity Research Results Part 2.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12876518-vulnerability-patch-prioritization-problems-cybersecurity-research-results-part-two
- Harvard Business Review. (29 August 2022). “How Much Time and Energy Do We Waste Toggling Between Applications?”: https://hbr.org/2022/08/how-much-time-and-energy-do-we-waste-toggling-between-applications
- Ivanti. (18 August 2018). “7 Experts on What Shift Left Means for IT Departments”: https://www.ivanti.com/blog/7-experts-on-what-shift-left-means-for-it-departments
- Ivanti. (2022). “The NIST Cybersecurity Framework (CSF): Mapping Ivanti’s Solutions to CSF Controls”: https://www.ivanti.com/resources/v/doc/ivi/2694/fa2e133f20a8
- Ivanti. (2022). “The Ultimate Guide to Risk-Based Patch Management”: https://www.ivanti.com/resources/v/doc/ivi/2705/11190ce11e80
- Ivanti. (2023). “Press Reset: A 2023 Cybersecurity Status Report”: https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
- Ivanti. (2023). “ITSM+ Toolkit”: https://www.ivanti.com/resources/v/doc/ivi/2760/e094c24df239

- Ivanti. (2023). “The Ultimate Guide to Unified Endpoint Management (UEM)”: https://www.ivanti.com/resources/v/doc/ivi/2508/b7d55619d0ee
- Ivanti. (28 June 2022). “2022 Digital Employee Experience Report”: https://www.ivanti.com/resources/v/doc/ivi/2700/4e528f833de3
- Ivanti. (n.d.) “IT Jargon Explained: CMDB:” https://www.ivanti.com/glossary/cmdb
- Ivanti. (n.d.) “IESO Shifts Left for Streamlined IT Operations”: https://www.ivanti.com/customers/ieso
- Ivanti. (n.d.) “Southstar Bank “Shifts Left” with Ivanti Neurons”: https://www.ivanti.com/customers/southstar-bank
- Miller, T., & Spicer, D., Stryker, A. (19 January 2023). “IT vs Security: When Hackers Patch for Profit.” Security Insights: https://ivantiinsights.buzzsprout.com/1554237/12071546-it-vs-security-when-hackers-patch-for-profit
- Morning Consult and IBM. (3 October 2022). “IBM Security Incident Responder Study”: https://www.ibm.com/downloads/cas/XKOY5OLO
- National Institute of Standards and Technology. (2018). “Framework for Improving Critical Infrastructure Cybersecurity” (p14): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Official Journal of the European Union. (14 December 2022). “Directive (EU) 2022/2555 of the European Parliament and of the Council”: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
- Oltsik, J. (2022). “ESG Research Report: Technology Perspectives from Cybersecurity Professionals.” Enterprise Strategy Group - Information Systems Security Association International: https://www.esg-global.com/hubfs/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf
- Perri, L. (2023, April 19). “Top Strategic Cybersecurity Trends for 2023.” Gartner: https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023
- Pickering, D. (2022, May 5). “What is DevSecOps? How Great Developers Shift Left for Security.” Ivanti: https://www.ivanti.com/blog/what-is-devsecops-how-great-developers-shift-left-for-security
- Rundle, J. and Nash, K. (2023, May 22). “Security Chiefs Trim the Fat.” The Wall Street Journal: https://www.wsj.com/articles/security-chiefs-trim-the-fat-as-budgets-bite-83c82f99
- SAM. (July 2022). “IoT Security Landscape Report”: https://securingsam.com/wp-content/uploads/2022/04/SAM_IOT-Security-Report.pdf
- Shackleford, Dave. (March 2022). “SANS 2022 Cloud Security Survey”: https://www.sans.org/white-papers/sans-2022-cloud-security-survey
- Verma, A., Goettl, C., & Hindman, M. (2022). “How to Win Budget and Influence Non-InfoSec Stakeholders for Your 2023 Cybersecurity Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program

Le « Shift Left » de la sécurité

Comment favoriser des environnements de sécurité réactifs avec les outils IT d'aujourd'hui

ivanti

For more information, or to contact Ivanti, please visit ivanti.com