ivanti

Faites de votre adversaire votre meilleur allié

5 façons d'aligner l'équipe Sécurité sur l'IT

Des objectifs communs, mais des approches différentes

Même si les équipes Sécurité et IT visent toutes deux le bon fonctionnement de leur entreprise, leurs angles d'approche sont différents : l'équipe Sécurité cherche à éviter tout impact négatif, et l'équipe IT à améliorer les résultats globaux de l'entreprise.

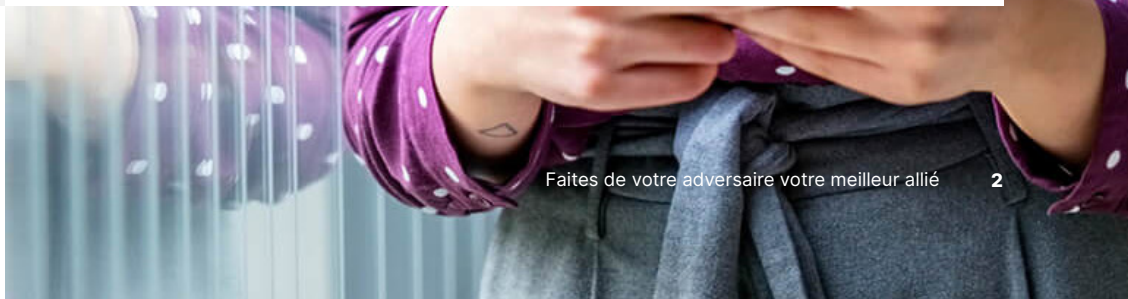
Obligations organisationnelles réciproques de la Sécurité et de l'IT

Équipe Sécurité : limiter les perturbations des opérations

La Sécurité limite en permanence les risques de perturbations liées aux cyberattaques (menaces internes ou externes), via diverses implémentations tactiques, et des analyses et des résolutions stratégiques et proactives des menaces.

Équipe IT : faciliter l'obtention de résultats opérationnels

L'IT booste la productivité des utilisateurs finaux par l'implémentation et la maintenance de technologies transparentes et la résolution des problèmes matériels et logiciels susceptibles d'affecter les résultats et la production des autres équipes.



Pourtant, lorsqu'elles coopèrent, ces deux divisions atteignent plus efficacement leurs objectifs.

Les processus fonctionnent bien lorsque l'équipe IT s'associe aux équipes de sécurité, et que des stratégies et processus proactifs sont mis en place en amont, avant que l'équipe Sécurité ne sollicite ses partenaires IT.

Mais comment faire pour que les objectifs et initiatives de l'équipe Sécurité reçoivent l'adhésion de l'équipe IT ? Comment faire en sorte que l'IT soutienne vos stratégies de sécurité et vous aide à les mettre en place ? Ne transformez pas vos collègues de l'IT en ennemis passifs, prêts à sacrifier les objectifs de sécurité pour leurs propres priorités internes !

Trois avantages de l'alliance Sécurité-IT

De meilleurs résultats, plus rapidement

L'équipe IT sera davantage encline à mettre en place des mises à jour et des correctifs qui nécessitent du temps et des ressources si une relation de confiance est établie avec l'équipe Sécurité.

Des ressources partagées pour réduire les dépenses technologiques globales

Quand les équipes se font confiance, elles peuvent partager les mêmes outils pour atteindre des objectifs différents. Le partage des ressources réduit les frais généraux organisationnels des centres de coûts.

Des pratiques de sécurité réalistes et durables

L'équipe Sécurité dépend de l'équipe IT pour l'implémentation des protocoles de sécurité. Si les demandes sont trop difficiles à satisfaire ou sont trop chronophages pour l'équipe IT, il sera difficile d'assurer la maintenance des protocoles et des règles de sécurité.

Cet eBook traite des sujets suivants :

01 **Expliquer l'enjeu des plans de sécurité, des changements et des demandes** avant leur implémentation… à la fois pour les administrateurs IT et les utilisateurs finaux concernés.

02 **Réduire l'impact des politiques de sécurité** sur les budgets, le calendrier et l'allocation des ressources IT.

03 **Faire des compromis** partout où l'équipe Sécurité peut se permettre d'être flexible. (Ne pas laisser la Sécurité devenir le « département du Non ».)

04 **Développer et atteindre des objectifs communs,** en utilisant le même langage, les mêmes tableaux de bord et les mêmes métriques chaque fois que c'est possible.

05 **Offrir proactivement de l'aide** (soutien administratif, expertise technique, ressources partagées, etc.).

Ne l'oublions pas, vos équipes Sécurité et IT partagent le même objectif final : améliorer la productivité et la sécurité du lieu de travail.

Ce document est fourni uniquement à titre d'information. Aucune garantie ne pourra être fournie ni attendue. Ce document contient des informations confidentielles et/ou qui sont la propriété d'Ivanti, Inc. et de ses sociétés affiliées (désignés collectivement ici sous le nom « Ivanti »). Il est interdit de les divulguer ou de les copier sans l'autorisation écrite préalable d'Ivanti.

Ivanti se réserve le droit de modifier le présent document, ou les caractéristiques produit et descriptions associées, à tout moment et sans avis préalable. Ivanti n'offre aucune garantie pour l'utilisation du présent document, et refuse toute responsabilité pour les éventuelles erreurs qu'il contient. Ivanti n'est pas non plus tenu de mettre à jour les informations de ce document. Pour consulter les informations produit les plus récentes, visitez le site www.ivanti.fr.

ivanti

01

Expliquer l’enjeu :

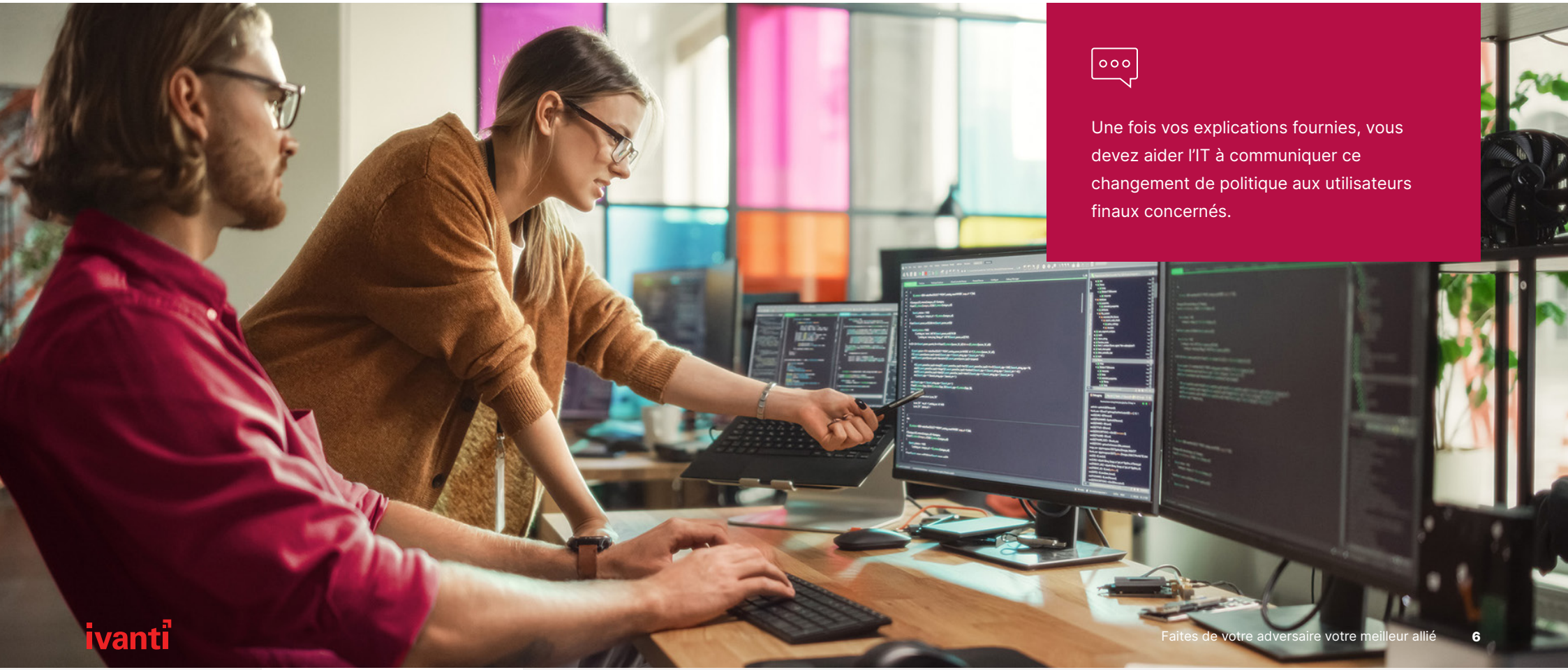
Évitez de décréter des changements, expliquez toujours vos plans de sécurité, les raisons du changement et l’enjeu de vos demandes.

ivanti

Ne pas oublier pas le « pourquoi »

Les décisions de sécurité non expliquées peuvent gêner le département IT. Par manque de temps, certaines demandes sont parfois émises sans expliquer les raisons du changement ni laisser de temps à la réflexion.

Par exemple, si votre équipe Sécurité décide de désactiver des périphériques mémoire amovibles, il est préférable de commencer par organiser une réunion avec l'équipe IT afin de lui exposer vos arguments. Vous pouvez expliquer à l'IT que la désactivation de certains types de périphériques permet à votre entreprise de réduire ses frais de cyberassurance, d'éviter les pertes de données dues aux menaces internes et externes, et de réduire son exposition aux risques.



Une fois vos explications fournies, vous devez aider l'IT à communiquer ce changement de politique aux utilisateurs finaux concernés.

Votre communication conjointe doit comprendre :

Une explication claire des éléments impactés, sans jargon. Par exemple, la rédaction interne d'une politique de sécurité visant à interdire certains périphériques peut mentionner les termes « lecteurs externes », « clés USB » ou « tout support pouvant stocker des fichiers et se connecter à un ordinateur par câble », au lieu de l'expression « périphériques mémoire amovibles ».

- Le document détaillant votre politique de sécurité doit aussi préciser ce qui n'est pas impacté, à savoir, ici, les souris, claviers, haut-parleurs et autres périphériques connectés par câble à l'ordinateur.

Un délai précis, donné au plus tard un ou deux jours avant le changement, afin que les utilisateurs aient le temps de trouver d'autres arrangements, et ne soient pas accidentellement empêchés d'utiliser leur clé USB sur leur ordinateur portable avant une présentation commerciale.

Les exceptions à cette stratégie (ainsi que le processus d'application de ces exceptions) pour décourager les utilisateurs d'implémenter des solutions de contournement répondant à leur « situation unique ».

Les personnes à contacter ou les emplacements sur lesquels se connecter pour anticiper les questions fréquentes, répondre aux demandes de dépannage courantes et gérer les cas extrêmes inattendus.

En l'absence de communication, l'équipe IT est submergée de plaintes et de tickets lors du déploiement du protocole de sécurité… et elle risque de retourner cette frustration et cette colère contre l'équipe Sécurité.

02

Limiter l’impact :

Réfléchissez en amont à l’impact des politiques de sécurité sur les budgets, le calendrier et les ressources IT.

ivanti

Anticiper (et limiter) l'impact sur l'équipe IT

Soyez conscient que l'équipe IT doit répondre à beaucoup de demandes. Elle gère peut-être un autre projet plus important, ou bien ne dispose pas du personnel nécessaire pour accomplir les tâches relatives à votre demande.

Recherchez des outils et systèmes qui facilitent la mise en œuvre de vos politiques de sécurité, demandes et correctifs… à l'inverse de ce que l'équipe Sécurité de l'exemple qui suit a infligé à son département IT.

Répercussions dans le monde réel

L'équipe Sécurité d'une université a obligé l'équipe IT à interroger les étudiants pour obtenir des mots de passe temporaires de 24 heures.

L'équipe de sécurité de l'université a décidé, un jour, de mettre en place un système de vérification en deux étapes pour tous les utilisateurs du campus… y compris l'ensemble de la population étudiante, qui égarait ou perdait fréquemment ses périphériques.

Si un étudiant avait besoin de demander un nouveau mot de passe temporaire pour accéder au réseau et aux ressources de l'université, l'équipe Sécurité imposait :

1. Une vérification en face à face de l'identité du demandeur, en personne ou sur Zoom.
2. Au cours de la réunion, le demandeur devait présenter des pièces d'identité officielles et répondre à plusieurs questions de sécurité.
3. L'équipe pouvait alors émettre des informations d'authentification temporaires… valides seulement 24 heures.
4. Si un étudiant ne retrouvait pas son ancien périphérique (ou n'en obtenait pas de nouveau) au cours de ces 24 heures, il fallait recommencer tout le processus !

Si l'équipe Sécurité avait fait l'effort de consulter le département IT avant la mise en œuvre de cette politique si lourde, elle aurait su que la solution la plus élégante était de diviser le réseau :

- En mettant en place un réseau étudiant plus limité avec des mesures d'authentification moins sévères.
- En réservant la procédure des entretiens à un réseau plus restreint, mais plus sensible : le personnel de l'université.

(Après tout, les collaborateurs adultes ont généralement une plus grande motivation et une plus grande capacité mentale à suivre leurs périphériques que de jeunes étudiants.)

Cette division du réseau permet de tenir compte des besoins de l'équipe IT, tout en sécurisant les périphériques personnels des étudiants malgré les pertes fréquentes lors des soirées universitaires.

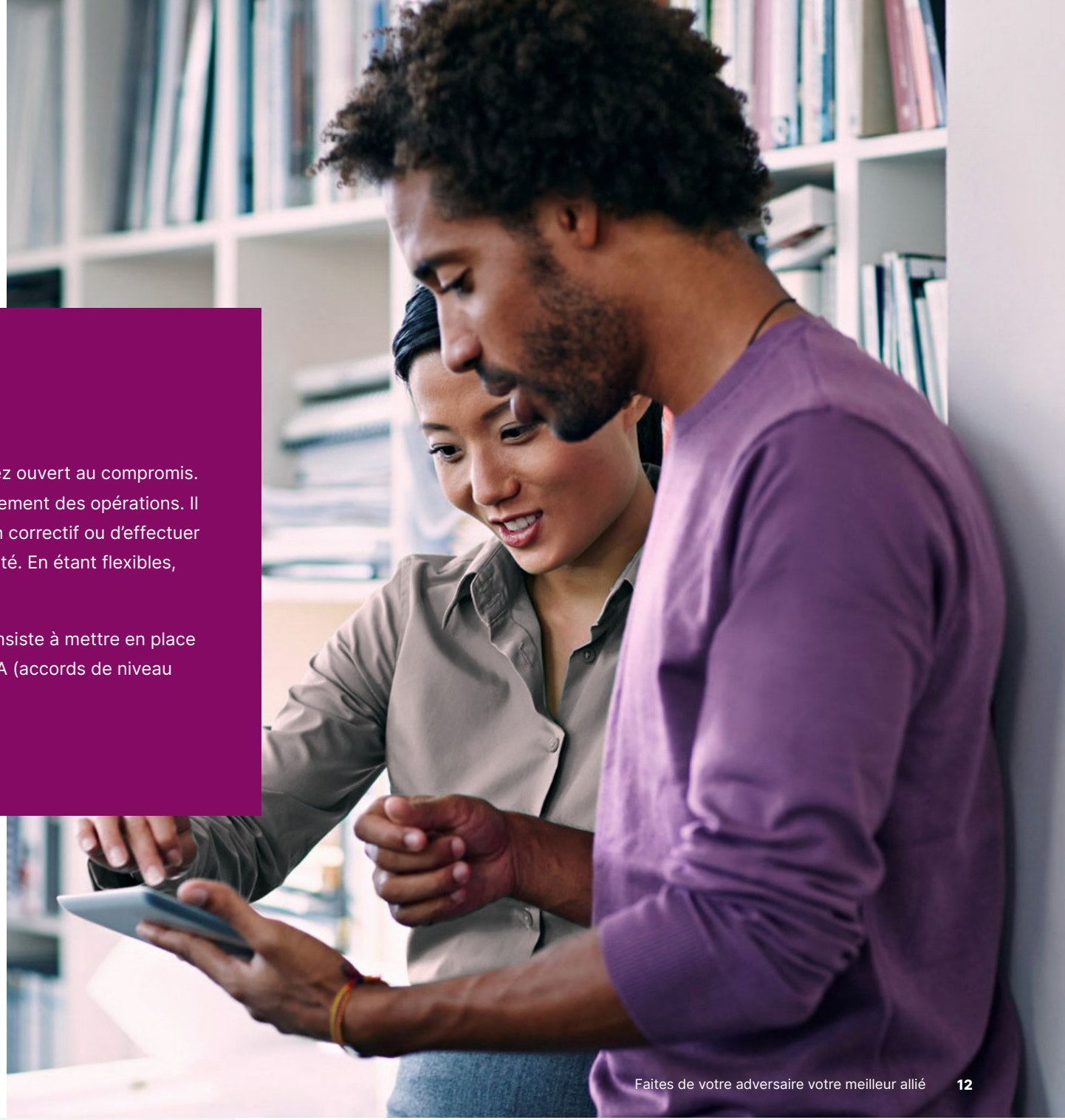
03

Faire des compromis

Soyez flexible dans la mesure du possible pour ne pas devenir le « département du Non ».

ivanti

L’art du compromis



Lors de vos interactions avec les autres départements, soyez ouvert au compromis. Après tout, la priorité de l’IT est de garantir le bon fonctionnement des opérations. Il est possible que son planning ne permette pas de publier un correctif ou d’effectuer un changement dans les délais souhaités par l’équipe Sécurité. En étant flexibles, Sécurité et IT trouvent généralement un terrain d’entente.

L’une des façons d’obtenir proactivement cette flexibilité consiste à mettre en place des fenêtres de service et des accords sous la forme de SLA (accords de niveau de service).

Un SLA doit définir pour chaque étape les attentes en matière de collaboration et de délais, afin que chacun sache ce qui va être réalisé, quand et par qui. Il doit inclure :

Toutes les définitions. Vous devez vraiment expliquer les bases, même pour des éléments aussi évidents que ce que votre entreprise appelle une « vulnérabilité exploitée » !

Les spécifications nécessaires et les piles technologiques déployées à chaque étape d'un processus conjoint.

- Ces processus peuvent inclure toutes sortes d'éléments, des déploiements de correctifs à l'implémentation de nouvelles politiques.

Les critères de priorisation. Réfléchissez à qui relève de « l'urgence » dans l'équipe Sécurité, par rapport à ce que ce terme désigne pour l'équipe IT.

- Des échelles internes personnalisées, des rubriques et d'autres méthodes d'évaluation internes peuvent aider à normaliser cette partie du processus. Développez ces éléments avec votre équipe IT dans le cadre du processus d'élaboration des SLA.

La fréquence des communications au cours des projets communs. Par exemple, il peut s'agir des questions suivantes liées aux processus :

- Quand l'équipe IT peut-elle s'attendre à avoir un retour de l'équipe Sécurité concernant le déploiement de correctifs spécifiques pour un Patch Tuesday donné ?
- Quand l'équipe Sécurité peut-elle s'attendre à recevoir un retour de l'équipe IT concernant des problèmes ou pour confirmer la réussite d'un déploiement de correctifs ?
- À quel point une demande ouverte (par l'une ou l'autre équipe) peut-elle être fermée en raison de l'absence de réponse ? À quel moment faut-il inclure des responsables dans la chaîne ?

Les attentes en matière de délais « standard » et de livraison pour chaque type de projet et pour chaque équipe… ainsi qu'une liste explicite et bien décrite des exceptions à la procédure standard.

Le nom des personnes à contacter ou ayant un rôle spécifique dans chaque département.

- Ces personnes seront notamment chargées d'éviter toute confusion concernant les politiques et procédures du SLA, ainsi que d'examiner et de mettre à jour ce SLA chaque année avec leurs homologues.

04

Développer et viser des objectifs conjoints avec l'IT

ivanti

Établir des objectifs partagés

Comme nous l'avons déjà dit, même si les équipes Sécurité et IT ont une approche différente, elles partagent le même objectif : assurer un fonctionnement aussi fluide que possible pour l'entreprise, les utilisateurs et les processus.

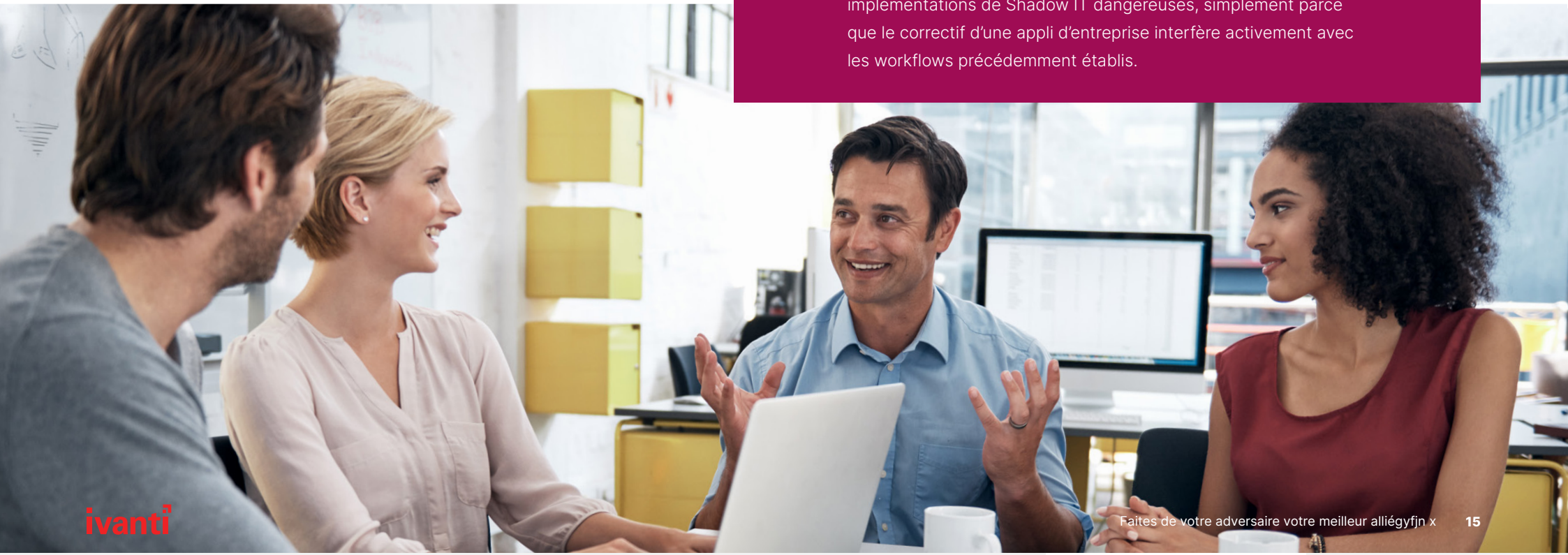
Par conséquent, cela vaut la peine de prendre le temps de définir ces objectifs communs avec les dirigeants IT. Il faut aussi créer des indicateurs de performances clés (KPI), des tableaux de bord et autres mesures partagées, afin de renforcer ces objectifs tous les jours.

Prenons par exemple le déploiement de correctifs. (C'est un exemple récurrent dans cet eBook, pour une bonne raison !)

Les deux équipes IT et Sécurité veulent que les technologies de l'entreprise fonctionnent correctement. Par conséquent, aucun des deux départements ne veut qu'un correctif interrompe le workflow, même si leurs raisons sont différentes :

L'équipe IT ne souhaite pas devoir gérer une multitude de tickets de support suite au déploiement d'un correctif qui provoque le plantage d'un utilitaire ou des connexions au réseau.

L'équipe Sécurité ne veut pas frustrer les utilisateurs finaux et les pousser à adopter des solutions de contournement ou des implémentations de Shadow IT dangereuses, simplement parce que le correctif d'une appli d'entreprise interfère activement avec les workflows précédemment établis.



Fixer des objectifs communs pour ne pas recourir à des stratégies d'évitement

Parfois, la solution choisie par l'équipe IT consiste tout simplement à ne pas déployer des correctifs… surtout si l'équipe Sécurité ne peut pas garantir qu'ils ne vont pas perturber des workflows indispensables aux activités. Face aux réticences de l'IT, l'équipe Sécurité doit alors retirer son projet de déploiement.

Pourtant, ni la Sécurité ni l'IT ne souhaitent gérer une fuite de données. C'est pourtant ce qui se produit lorsque les périphériques et applications ne reçoivent pas régulièrement de mises à jour contre les exploitations actives.

Bien que le blocage des cyberattaques est une responsabilité qui incombe à l'équipe Sécurité, l'équipe IT est aussi concernée en cas de violation de sécurité.

En effet, c'est elle qui doit restaurer les systèmes technologiques le plus rapidement possible, même si l'équipe Sécurité garantit que la sauvegarde est sûre et que tous les intrus ont été évincés du réseau.

Quelle priorité l'équipe IT devra-t-elle supprimer de sa liste si une attaque se produit sur un système non patché ?

Il est donc dans l'intérêt des deux équipes d'élaborer une stratégie robuste de gestion des correctifs, qui fonctionne pour chacune, en gardant à l'esprit cet objectif fondamental commun : éviter à tout prix l'interruption des processus de l'entreprise.

Offrir de l’aide :

Partagez proactivement vos ressources administratives, votre expertise technique et autres outils.

La réciprocité améliore la collaboration

Si vous demandez une faveur à l'équipe IT (comme emprunter et adapter sa pile technologique, ses politiques et des processus IT actuels pour vos propres cas d'usage de sécurité), vous devez lui donner quelque chose en échange.

Cela implique souvent le partage de la responsabilité financière des outils et des projets communs (chaque équipe consacrant ainsi à l'outil partagé un budget inférieur à ce qu'il lui coûterait s'il était payé séparément), mais cette aide peut prendre diverses formes.

Au bout du compte, en partageant leurs outils et leurs ressources, les équipes Sécurité et IT réduisent leurs coûts globaux et améliorent leur collaboration.

Les outils, tableaux de bord et rapports partagés créent un contexte qui permet aux deux équipes de mieux se comprendre. Cet aperçu de l'univers de l'autre favorise l'empathie et la confiance.

Connaître les valeurs et les priorités de l'IT aide l'équipe Sécurité à adhérer aux différents projets de manière à la fois pratique et respectueuse de ses partenaires IT.

Et cette adhésion est encore plus rapide si l'équipe Sécurité apporte son aide en cours de route… dans les limites du raisonnable, évidemment.

3 façons créatives pour l'équipe Sécurité d'aider l'équipe IT (hormis l'aspect budgétaire)

Soutien administratif	De nombreuses personnes (y compris le personnel IT) trouvent difficile la partie administrative de leur travail. Si cela peut améliorer l'opinion que l'autre département a de vous, offrez-lui d'assumer cette charge, dans la mesure du possible. Par exemple, si l'équipe IT prévoit qu'une nouvelle politique de sécurité va impacter les files d'attente de tickets, nommez un spécialiste en sécurité pour répondre à tous les tickets et requêtes des utilisateurs liés à cette nouvelle politique. Vous pouvez aussi faire une adaptation de la politique de sécurité à l'attention des utilisateurs ayant un profil moins technique, puis demander à votre équipe Communications de la partager avec les parties prenantes internes.
Expertise technique	Il peut arriver que vous suggériez un nouveau processus (ou une nouvelle politique de sécurité) qui vous semble simple, mais n'est pas clair pour vos contacts IT. Proposez dans ce cas d'organiser une session de formation à l'attention du personnel IT chargé de l'implémentation technique. Vous pouvez aussi, si vous avez le temps, prendre à votre charge la configuration des paramètres. (Assurez-vous que toutes les instructions de dépannage seront faciles à trouver pour le personnel IT chargé de la maintenance !) En retour, demandez aux administrateurs IT de former le personnel de sécurité pour que votre équipe ait une compréhension élémentaire du mode de fonctionnement de l'IT dans votre entreprise… même si ce sont des anciens de l'équipe IT !
Ressources partagées	L'équipe Sécurité peut aussi demander à utiliser les capacités techniques de l'équipe IT (nous abordons ce point dans notre ebook : « Réussir le "Shift Left" de la sécurité ».) Cependant, il n'existe aucune raison de ne pas mettre certains outils axés sur la sécurité à la disposition de l'équipe IT, notamment pour ce qui concerne l'accès aux supports de formation ou de développement professionnel dont vous disposez pour votre propre équipe. Cela permettra à l'équipe IT de mieux comprendre les obligations et la position de l'équipe Sécurité, ce qui ne peut que vous aider à traiter les futures demandes de l'équipe IT.

Répercussions dans le monde réel

Collaboration en essaim pour une meilleure gestion des risques de sécurité hors bande

Les équipes Sécurité et IT planifient toutes deux leur mois en fonction des publications mensuelles du « Patch Tuesday », avec un calendrier précis de test, installation pilote et déploiement global, en traitant méthodiquement tous les problèmes d'implémentation.

Cependant, certains correctifs se retrouvent « hors bande », forçant tout le monde à se démener pour deux raisons.

1. **Les publications de correctifs ou solutions de remédiation « hors bande » correspondent généralement à des exploitations actives,** qui exigent une implémentation immédiate.

2. **Les équipes doivent mettre de côté d'autres tâches critiques** pour donner la priorité au correctif nouvellement publié… tâches qui restent problématiques une fois l'urgence traitée.

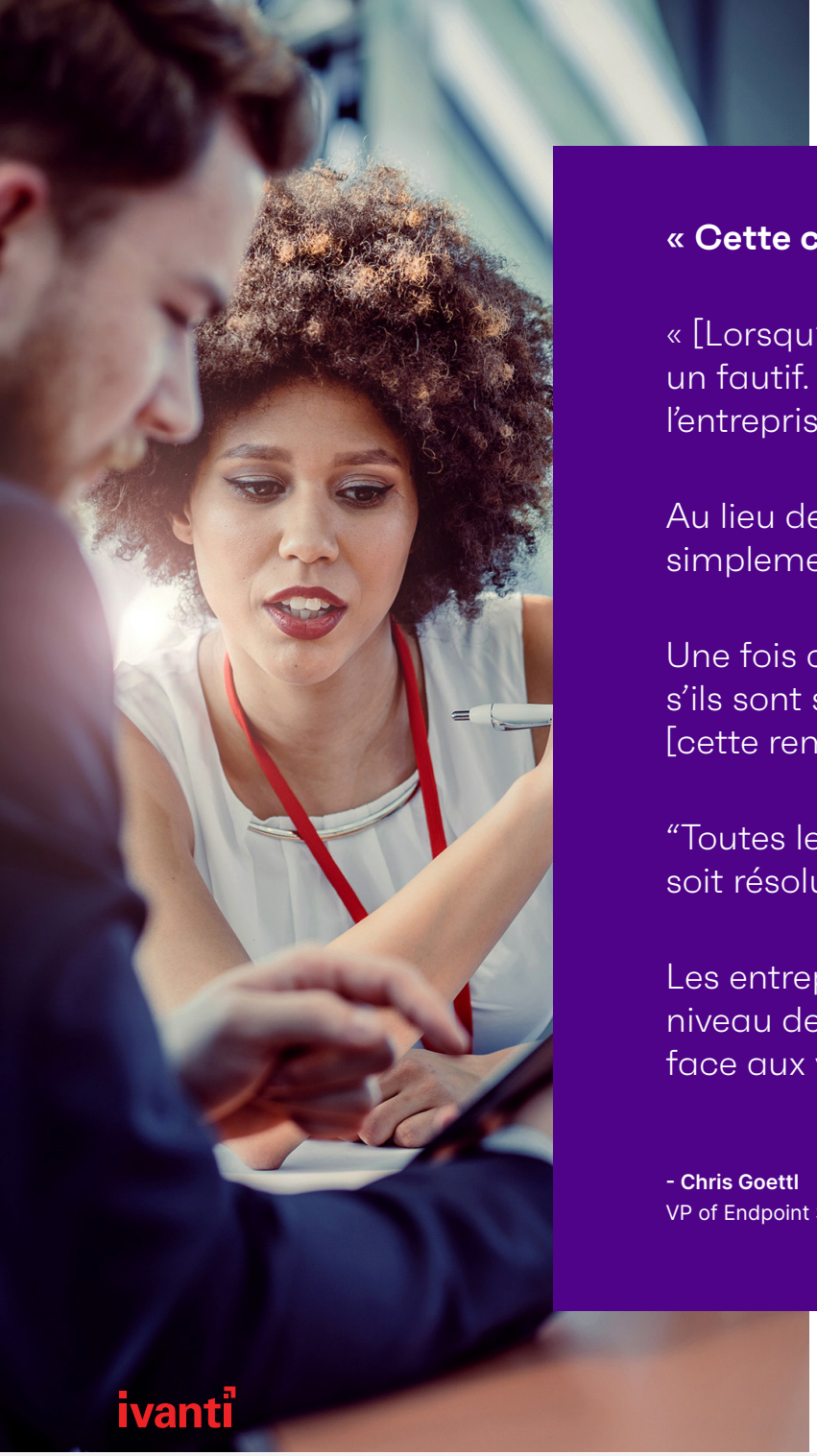
Au lieu de crier « tout le monde sur le pont » pour faire face à ces urgences, les entreprises matures ont développé la collaboration en « essaim ».

- Elles mettent en place une **équipe transverse (équipes Sécurité et IT incluses) composée d'experts chargés des correctifs hors bande.**

- En cas de publication d'un correctif hors bande, **ces équipes « collaborent en essaim »** autour du correctif ou de la remédiation d'urgence, se concentrant entièrement sur son traitement.

- Pendant ce temps, leurs départements respectifs **poursuivent les tâches et projets régulièrement planifiés.**

En créant ces équipes pluridisciplinaires en amont de la publication des correctifs hors bande, les entreprises maintiennent leur cap en traitant rapidement les urgences inévitables.



« Cette collaboration en essaim révolutionne notre culture d'entreprise. »

« [Lorsqu'on traite des risques hors bande], on ne cherche pas à trouver un fautif. Le plus souvent, la vulnérabilité n'est la faute de personne dans l'entreprise.

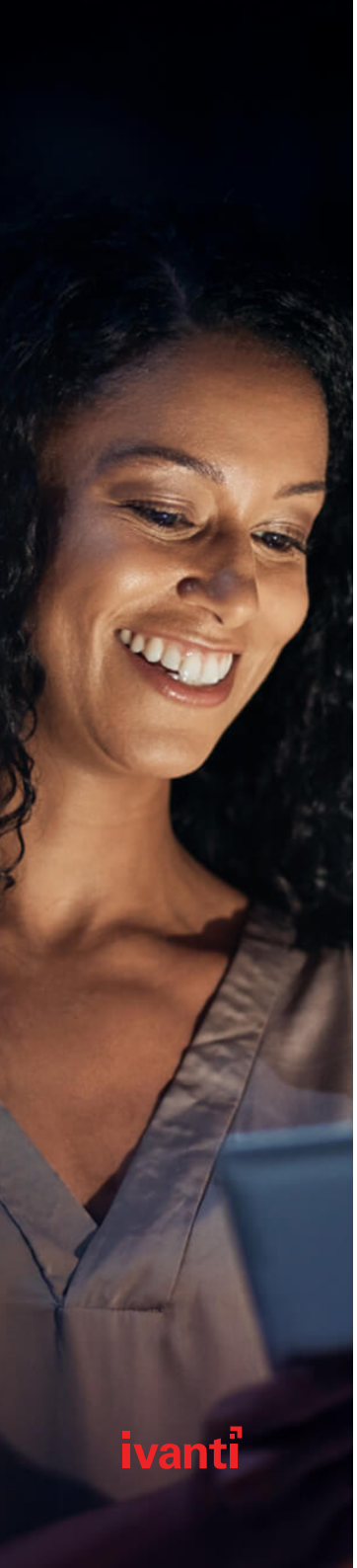
Au lieu de cela, lorsqu'on travaille en essaim, on considère qu'il faut simplement identifier la personne la plus à même de résoudre le problème.

Une fois cette personne identifiée, tous les acteurs de l'entreprise savent que, s'ils sont sollicités pour l'aider pendant cette session de travail en essaim, alors [cette remédiation] est leur nouvelle priorité.

"Toutes les autres priorités passent au second plan jusqu'à ce que le problème soit résolu.

Les entreprises qui ont recours à la collaboration en essaim offrent un niveau de réponse plus sain et une réponse généralement plus rapide face aux vulnérabilités. »

- Chris Goettl
VP of Endpoint Security Product Management, Ivanti



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/2694/63935da433e2
- 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

Références

- 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://rs.ivanti.com/ivi/2700/4e528f833de3.pdf
- 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 Program.” Ivanti: https://www.ivanti.com/webinars/2022/win-budget-and-influence-non-infosec-stakeholders-for-your-2023-cybersecurity-program
- Shackleford, Dave. (March 2022). “SANS 2022 Cloud Security Survey”: https://8645105.fs1.hubspotusercontent-na1.net/hubfs/8645105/white-paper/sans-2022-cloud-security
- 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

Faites de votre adversaire votre meilleur allié

5 façons d'aligner l'équipe Sécurité sur l'IT

ivanti

Pour de plus amples informations ou pour contacter Ivanti, visitez www.ivanti.fr

Copyright © 2023, Ivanti. Tous droits réservés. IVI-2783 AS/DH/NH