Sécurité OT : cap sur une approche holistique

Zoom sur les nouveaux enjeux de cybersécurité pour les technologies opérationnelles (OT)

verizon business

Remodelée par les avancées de la quatrième révolution industrielle, l'industrie exige aujourd'hui des services et systèmes rapides, sécurisés et résilients. La sécurisation des technologies opérationnelles (OT) constitue une priorité pour les entreprises, au même titre que la mise en place de mécanismes solides de surveillance et de réponse en cas de problèmes.

Car si la connectivité entre applications et équipements OT offre réellement un nouveau champ des possibles aux entreprises, elle peut aussi ouvrir des brèches dans lesquelles utilisateurs malintentionnés et cybercriminels s'engouffreront très vite.

Historiquement, les réseaux OT étaient isolés des réseaux IT et de l'Internet pour garantir leur sécurité et leur fiabilité. Cette époque est désormais révolue.

Découvrez dans ce livre blanc comment sécuriser les réseaux OT intégrés pour qu'ils deviennent un levier de croissance, et non un danger de tous les instants.

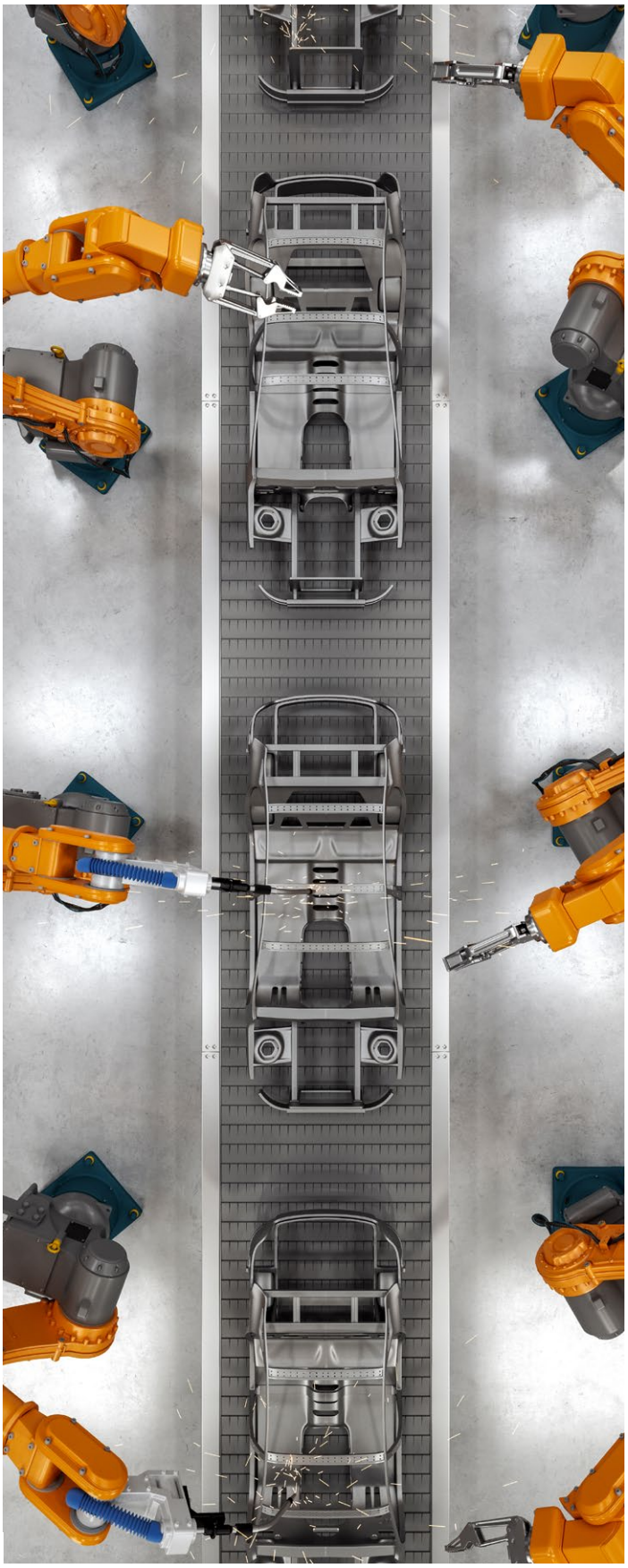
Si le marché de la sécurité OT tend à placer la focale sur l'inventaire des actifs et la détection des menaces et des vulnérabilités, la protection doit rester une priorité.

Repenser la cybersécurité à l'ère de l'Industrie 4.0

La quatrième révolution industrielle, ou Industrie 4.0, se distingue par une fusion des technologies qui brouille les lignes entre les sphères du physique, du digital et du biologique.

Des robots autonomes à l'Edge Computing, en passant par la connectivité avancée et le pilotage à distance en temps quasi réel, les entreprises adoptent toutes les technologies possibles et imaginables. Seulement voilà, l'évolution de ces opérations, désormais étroitement liées au cloud, exige une totale remise à plat des architectures de sécurité. D'où la nécessité, entre autres, de déployer le Zero Trust pour garantir des contrôles de sécurité rigoureux.

Source – [1]The Forrester Wave™: Operational Technology Security Solutions, Q2 2024, Forrester.



Loin d'être un fardeau de plus, cette refonte doit au contraire être perçue comme un creuset d'opportunités pour simplifier et optimiser l'architecture des entreprises. Un des avantages réside notamment dans la collecte de gigantesques jeux de données destinés à l'analytique, dans tout un éventail de domaines allant du traitement des incidents à l'amélioration des produits.

Les nouveaux moteurs de croissance apportent leur lot de risques

Évolution OT

Après avoir migré l'IT dans le cloud, les entreprises font de même avec l'OT pour gagner en efficacité. En parallèle, elles commencent à déployer l'IA pour la maintenance prédictive et l'automatisation, tout en repensant leurs modes de collaboration externes pour des raisons de contrôles de sécurité et de rentabilité.

> Ainsi, 80 % des DSI se disent prêts à adopter l'IA et l'automatisation d'ici 2028 pour placer l'agilité et la data au service de l'entreprise. »
>
> **Prédictions des DSI** en région Asie/Pacifique* pour 2024 et à plus long terme selon IDC

Risques de la convergence IT/OT

La connectivité grandissante entre les réseaux IT et OT contribue à l'expansion de la surface d'attaque, un phénomène d'autant plus alarmant que les systèmes OT d'ancienne génération n'ont généralement pas été conçus dans une optique de cybersécurité.

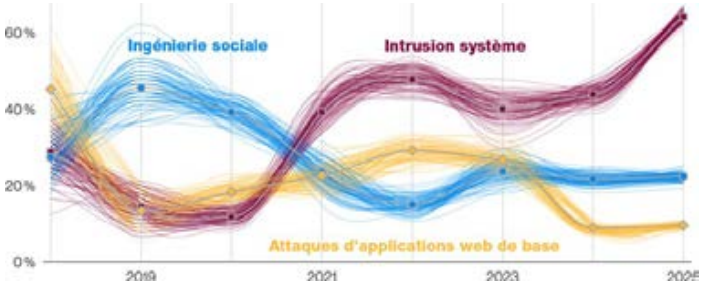
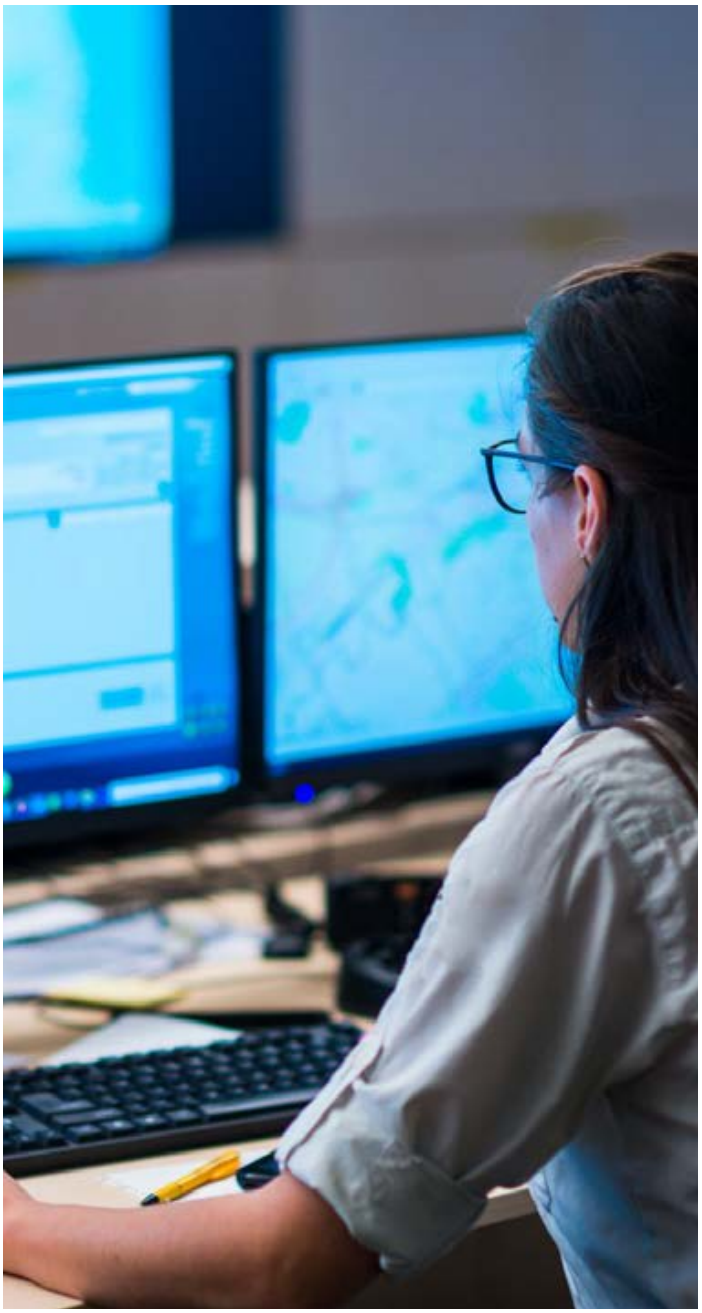


Figure 1. Évolution chronologique des principaux schémas d'attaque à l'origine de compromissions dans l'industrie

Source – Figure 1 : rapport DBIR 2025 de Verizon

Sur le terrain, l'impact est déjà palpable. D'après le Verizon Data Breach Investigations Report (DBIR) 2025, le nombre d'intrusions système dans le monde a bondi depuis 2020, avec une augmentation particulièrement notable l'an passé dans l'industrie. Ce secteur a également enregistré une forte hausse des compromissions de données, avec près de 1 607 incidents confirmés au sein de PME et d'ETI.

Si l'appât du gain continue de dominer chez les attaquants, il est intéressant de noter que 20 % des compromissions industrielles relevaient de cas d'espionnage, contre seulement 3 % l'année précédente.



Systèmes obsolètes et non corrigés

Nombre d'environnements OT dépendent encore de systèmes d'exploitation dépassés et de logiciels dont le support fournisseur est au mieux lacunaire, au pire inexistant. De même, qui dit patching et mise à jour de ces systèmes, dit immobilisation de la production et manque à gagner. D'où le casse-tête.

Absence de visibilité et de gestion des actifs

Très souvent les entreprises ne disposent pas d'un inventaire clair des actifs OT connectés, ce qui complique l'évaluation des risques. Le Shadow OT et les terminaux non documentés peuvent introduire d'autres vulnérabilités inconnues.

Ransomwares et cybermenaces

Selon le rapport DBIR 2025, les attaques par ransomware constituent la principale cause de compromission pour le secteur industriel. Les acteurs cyber tendent à exploiter le manque de segmentation entre l'IT et l'OT, pour ensuite se déplacer latéralement et perturber d'autres opérations.

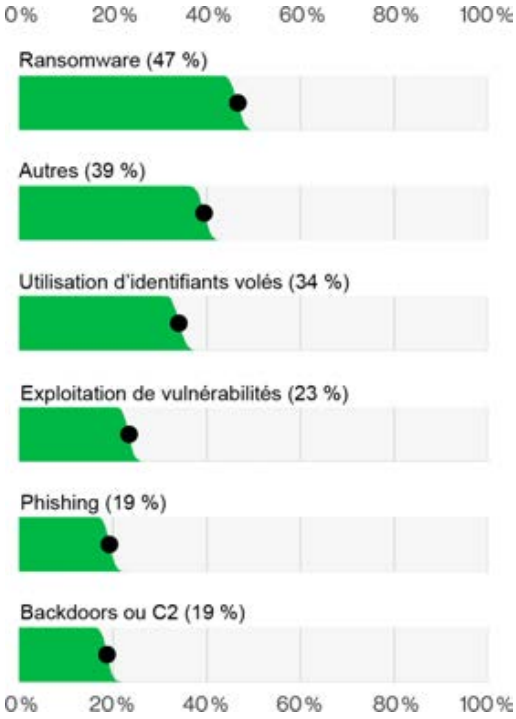


Figure 2. Principaux vecteurs de compromission dans l'industrie

Les incidents par ransomware étaient présents dans 44 % de toutes les compromissions recensées dans le DBIR 2025, soit une hausse de 32 % par rapport à l'édition 2024. Malgré cette envolée, le montant moyen de la rançon versée a baissé de 150 000 $ à 115 000 $. Ce recul s'explique en partie par le nombre croissant d'entreprises victimes qui refusent de céder au chantage.

Autre constat, les ransomwares visent de manière disproportionnée les PME et ETI. Pour preuve, ils comptent pour 88 % des compromissions dans ces dernières, contre 39 % dans les entreprises de plus grande taille.

Source – Figure 1 : rapport DBIR 2025 de Verizon | Figure 3 : Verizon

Le casse-tête de la conformité et de la réglementation

Les entreprises doivent se conformer à une multitude de frameworks de cybersécurité et de réglementations sectorielles, à l'instar du National Institute of Standards and Technology (NIST) du ministère américain du Commerce, des standards IEC 62443 et des recommandations de l'Agence américaine pour la cybersécurité et la sécurité des infrastructures (CISA). Ajoutez à cela des supply chains mondialisées, et l'équation de la conformité se corse davantage pour les entreprises en général, et les petites structures en particulier.

Risques liés aux tiers et à la supply chain

L'accroissement du nombre de fournisseurs, sous-traitants et prestataires multiplie les points d'exposition à travers vos réseaux OT connectés. De fait, des vérifications robustes des identités et un contrôle des accès Zero Trust s'imposent comme deux impératifs pour ces accès à distance.

Pénuries de compétences et de talents

Force est de constater que les professionnels de la cybersécurité dotés de compétences en sécurité OT sont une denrée rare. Quant aux nouvelles recrues, elles ne sont pas forcément sensibilisées aux problématiques de cybersécurité, ce qui peut augmenter le risque de menaces internes ou d'erreurs humaines.

Définir une stratégie de sécurité OT

Des frameworks comme le CFS du NIST, NIST 800-53, ISO 27K, IEC 62443, NIST 800-82 et la formation CIP (Critical Infrastructure Protection) du NERC (North American Electric Reliability Corporation) proposent une approche cohérente pour gérer tout programme de cybersécurité et établir une stratégie de sécurité OT sur mesure.

Figure 3. Éléments d'une stratégie de sécurité OT complète

Une stratégie de sécurité simplifiée doit combiner a minima les composantes suivantes au sein d'une structure de gouvernance :

- Un cadre complet de gestion des actifs pour tenir un inventaire à jour de votre parc OT (âge, date de fin de support, version des logiciels/du firmware, etc.).
- Des bilans de sécurité périodiques du réseau OT pour identifier les failles ou lacunes de sécurité.
- Une architecture réseau multi-couche, dotée d'une zone IT démilitarisée (DMZ) qui fournit un accès simplifié et fiable aux applications hébergées dans le cloud.
- Une surveillance continue des menaces pour optimiser les capacités de détection au sein des réseaux OT. Son champ d'action doit couvrir les couches réseau et applicative et utiliser les règles YARA (Yet Another Recursive Acronym) pour détecter les malwares propres à l'OT.
- Une Threat Intelligence spéciale OT au service d'une détection et d'une prévention en amont. Pour ce faire, elle doit puiser dans une combinaison de données CTI du domaine public et des autorités étatiques, des flux CTI sectoriels, des feeds open-source et communautaires, ainsi que des flux privés de fournisseurs et prestataires.
- Un plan de réponse à incident bien pensé et éprouvé, capable de détecter les menaces en amont.

Framework de sécurité OT : les phases de transformation

Ces différentes étapes illustrent le parcours idéal de transformation de la sécurité de votre réseau OT. Si vous choisissez Verizon pour vous accompagner dans cette démarche, il est fort probable que nous suivrons ce processus.

Libre à votre entreprise de commencer à la phase la mieux adaptée à ses besoins et à son niveau de maturité opérationnelle. En parallèle, il est important de garder ces points de gouvernance et d'organisation OT à l'esprit :

- Aspects de l'entreprise concernés par l'innovation et une évolution future.
- Planification et application de la stratégie par les dirigeants au niveau corporate et des business units.
- Identification d'un « champion » de la sécurité OT dans chaque usine ou division, chargé d'assurer la planification et l'application du programme à son niveau.

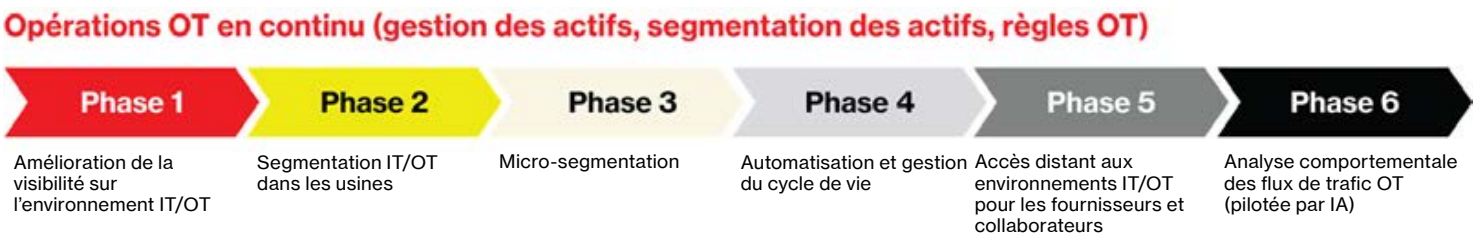


Figure 4. Framework de sécurité OT : les phases de transformation

PHASE 1 : amélioration de la visibilité OT

Nos services de conseil en sécurité (Verizon Security Consulting Services) ont pour mission d'approfondir votre compréhension des équipements IT et OT interconnectés dans vos usines, entrepôts et autres environnements de ce type. Pour ce faire, nous menons, sur site ou à distance, un inventaire et un bilan complets des actifs en usine pour vous offrir une vue à 360° sur votre parc OT et ses facteurs de risque.

PHASE 2 : segmentation IT/OT

Verizon vous aide à segmenter vos réseaux OT et IT à l'aide de contrôles et protections de base, comme l'implémentation ou la réutilisation de pare-feu matériels ou virtuels. Par ailleurs, il est recommandé d'activer ces contrôles de sécurité, a minima :

- Prévention des menaces
- Antimalware
- Protection DNS (Domain Name System)

Nos experts certifiés facilitent l'implémentation et la configuration de contrôles de sécurité, tandis que les équipes de Verizon Managed Security Services (MSS) peuvent superviser ces opérations depuis nos centres des opérations de sécurité (SOC).

PHASE 3 : micro-segmentation

Il s'agit de segmenter l'environnement OT. Pour ce faire nous développons des plans d'action personnalisés, reproductibles sur tous les sites de l'entreprise. L'objectif : favoriser la simplification et la standardisation. Cette phase permet ainsi de clarifier les différentes zones et politiques de sécurité. Précision, les Verizon Security Consulting Services peuvent développer et implémenter ces plans d'action sur des contrôles de sécurité existants (Phase 2).

PHASE 4 : mise en place de l'automatisation et de la gestion du cycle de vie

C'est dans cette phase que commence le développement de playbooks spécifiques destinés à créer et à actualiser des règles de segmentation de l'OT. Pour ce faire nous utilisons les outils disponibles, les systèmes de tickets et le développement de scripts.

La gestion du cycle de vie sert à maintenir les équipements conformes aux contrôles de sécurité exigés. Si aucune maintenance adaptée n'est possible, les appareils seront placés dans une zone de sécurité renforcée.

Source – Figure 4 : Verizon

PHASE 5 : accès distant à l'environnement OT pour les fournisseurs et collaborateurs

Dans cette phase, nous activons des services d'accès à distance selon le principe du Zero Trust et du « besoin d'en savoir ». Ensuite, nous implémentons les contrôles d'accès pour les collaborateurs et différents fournisseurs, et prenons en charge les solutions basées sur des agents et le navigateur.

PHASE 6 : activation de l'automatisation et de contrôles de sécurité avancés (principalement pilotés par IA)

Prévention des pertes de données (DLP), système de prévention des intrusions (IPS), analyse comportementale des entités et des utilisateurs (UEBA)... tous ces contrôles de sécurité augmentés par l'IA améliorent la visibilité sur les flux de trafic OT et IT. Ces précieuses informations servent à créer de nouveaux playbooks ou à actualiser ceux déjà en place. Autre atout, elles permettent d'améliorer la réponse aux incidents OT et de mettre au point des services OT basés sur la tromperie des attaquants.

Modèle opérationnel recommandé pour les environnements OT

Chez Verizon, notre longue expérience des programmes de transformation pour les environnements industriels nous permet de recommander une structure organisationnelle taillée pour l'Industrie 4.0.

Ce schéma représente une structure qui a largement fait ses preuves dans les nombreux programmes IT/OT que nous avons menés.

Il va sans dire que ce n'est pas une solution universelle. Vos objectifs à court terme exigeront peut-être une structure plus en phase avec votre stratégie métier, tandis que votre vision à long terme nécessitera sans doute de réorganiser l'entreprise et tous ses processus.

Notre structure organisationnelle propose de placer toutes les technologies horizontales transverses et leurs ressources associées sous la responsabilité de la direction des systèmes d'information (DSI) du groupe, cette DSI ayant la charge des services courants fournis à la business unit. Chaque business unit est dirigée par un directeur des technologies (CTO) ou une fonction DSI responsable des différentes technologies opérationnelles.

Selon un reporting matriciel, les DSI de ces divisions rendent compte non seulement à la division en question, mais aussi à la DSI du groupe tout en siégeant au conseil des DSI. Ce dernier a pour mission de définir des lignes et une gouvernance communes sur les questions technologiques. Un responsable de la sécurité des systèmes d'information (RSSI) aura la responsabilité des fonctions de sécurité et siégera aussi au conseil des DSI.

En tant que prestataire de services de sécurité, Verizon propose aux entreprises des services managés de transformation et de prise en charge de la gestion, ainsi que d'autres services de sécurité managés. L'objectif est de vous permettre de ne négliger aucune de ces spécialisations et ainsi de faire la différence.

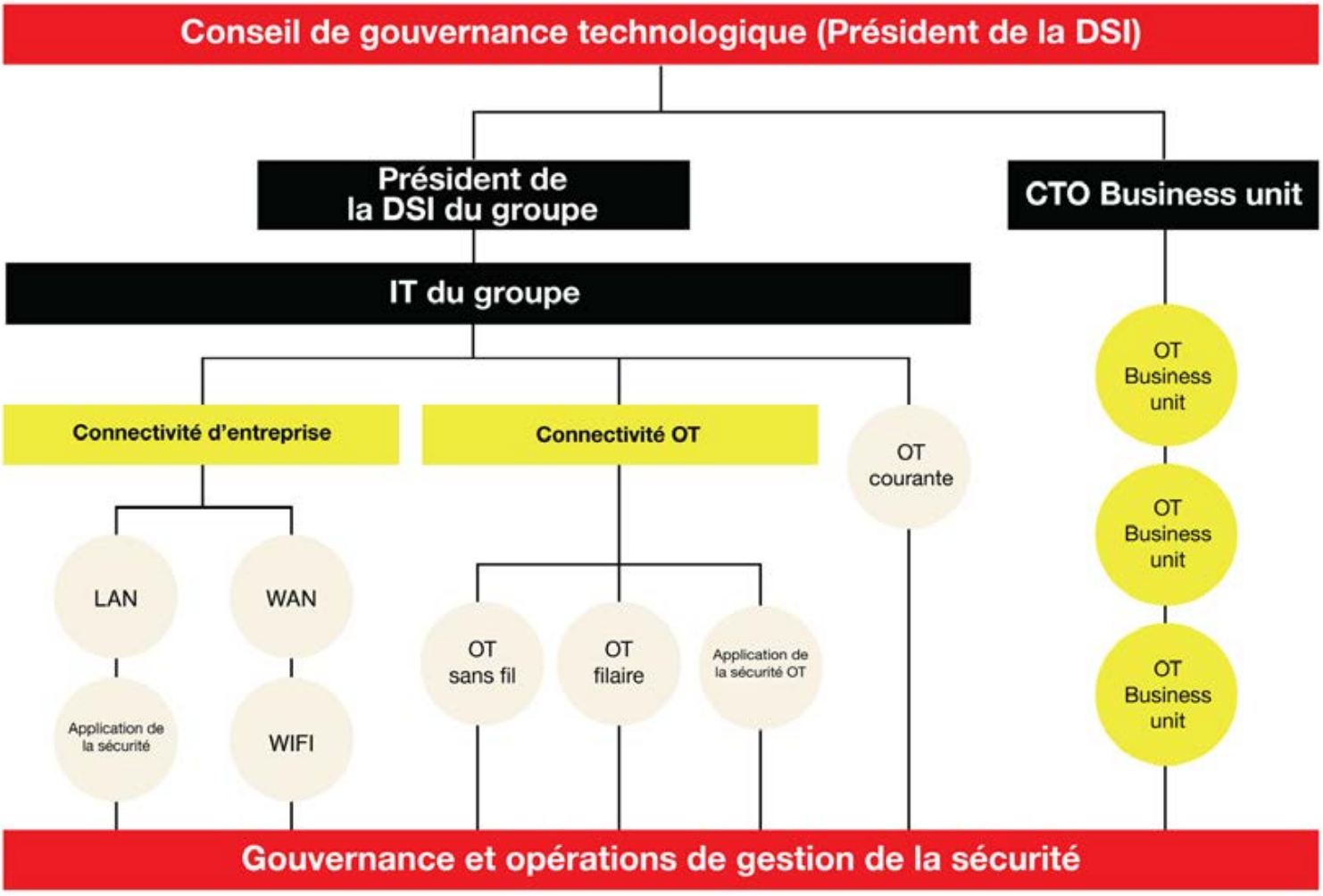


Figure 5. Modèle opérationnel OT courant pour les entreprises

Source – Figure 5 : Verizon

Conclusion

Grâce à l'approche de sécurité holistique pour l'OT de Verizon, les entreprises peuvent trouver la solution parfaitement en phase avec leurs besoins et leurs budgets. Elles sont ainsi mieux armées pour affronter et neutraliser les cybermenaces.

En savoir plus

Pour découvrir comment Verizon peut vous aider à protéger votre entreprise contre les menaces, contactez votre conseiller Verizon et rendez-vous sur notre site verizon.com/business/fr-fr/solutions/secure-your-business

Auteur et contributeurs

Auteur

Marc Borking, OT SME and Principal Security Consultant, Consulting Services, Verizon Business

Contributeurs

Ashish Khanna, Directeur senior et Responsable, Security Consulting Services EMEA

Stephen Young, Directeur, Security Consulting Services, Verizon Business

Beat Kueng, Directeur associé, Architecture des solutions de sécurité EMEA

Chris Zijderveld, Directeur associé, Security Consulting Services

Ali Akl, Responsable risques et résilience, Security Consulting Services EMEA

David Samreth, Consultant principal, Consulting Services

Étude de cas : grand groupe industriel mondial

Avec la généralisation de l'automatisation dans toutes ses opérations, ce grand groupe industriel mondial a commencé à constater une hausse du trafic entre ses systèmes IT et OT. Le problème, c'est que cela s'accompagnait aussi d'une augmentation des risques de sécurité et d'un élargissement de la surface d'attaque. Pour poursuivre sa croissance sans compromettre la protection des personnes, données et infrastructures, l'entreprise a pris les devants. Un bilan complet de la sécurité de ses environnements OT existants lui a permis d'identifier plusieurs impératifs.

Impératifs métiers :

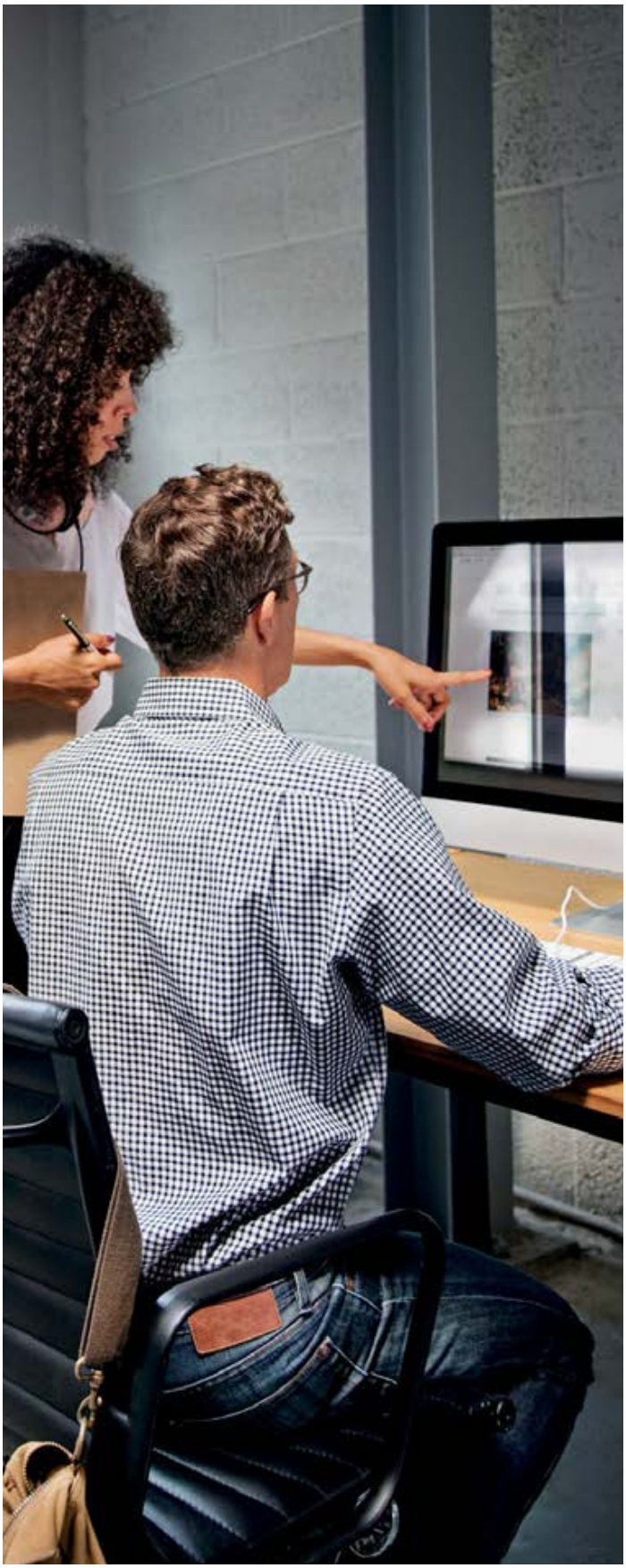
- Moderniser l'infrastructure de sécurité existante qui avait fait son temps
- Dresser un état des lieux clair de la situation : architecture en place, besoins de sécurité, politiques de segmentation, workflows métiers, équipements et processus
- Cerner les risques de sécurité engendrés par l'absence de segmentation
- Implémenter des contrôles de sécurité pour protéger les actifs de l'entreprise
- Aligner les configurations sur les politiques de sécurité
- Réduire les risques face à des menaces en pleine évolution
- Transformer l'environnement pour le préparer aux enjeux de croissance et de conformité

Solution :

- Inventaire et évaluation sur site des environnements OT dans les usines
- Mise en place d'une base de données de gestion des configurations et conception d'une architecture adaptée
- Création d'un modèle de politique de sécurité, et d'un modèle de segmentation OT/IT Installation de pare-feu on-prem, nouveaux ou réaffectés, et configuration de nouveaux segments, politiques et zones de sécurité avant de passer le relais aux experts des Verizon Managed Security Services
- Implémentation d'une segmentation LAN dans les plus de 25 usines à travers le monde, facilitant ainsi la conduite d'un inventaire IoT
- Mise au point progressive des politiques de sécurité
- Automatisation des playbooks pour simplifier la segmentation OT

Avantages et résultats :

- Neutralisation des cyber-risques grâce à l'isolation des réseaux IT et OT et à la micro-segmentation des différents segments OT
- Optimisation de la surveillance des équipements de sécurité grâce aux Verizon MSS
- Amélioration de la visibilité sur les équipements et les workflows métiers
- Renforcement de la conformité selon les nouvelles exigences et les menaces mondiales
- Création d'un nouvel environnement de sécurité porteur de croissance



Enseignements tirés :

Passer de la théorie à la pratique demande du temps, comme nous avons pu le constater sur nombre de projets précédents. Mais dans ce cas précis, le client a dû redéfinir le périmètre avant même que le projet ne commence. Une fois le feu vert obtenu, il nous a fallu collecter les données nécessaires, recruter les bonnes personnes, identifier les bons commutateurs et implémenter les configurations adaptées... ce qui a pris plus de temps que prévu. Pour compliquer un peu plus la donne, l'entreprise a connu des délais d'exécution plus longs en raison de priorités métiers contradictoires.

Mettre en place une équipe dédiée pour le client

La désignation d'une équipe dédiée à ce projet a permis d'accélérer les choses. Dès qu'un premier site a été mis en place, l'équipe en a tiré des enseignements au niveau des processus, de la conception et les éventuels pièges à éviter. Elle a ainsi pu travailler de plus en plus vite sur les sites suivants. Par ailleurs, la captation du trafic réseau et des données (via les ports SPAN) nous a donné du fil à retordre. La micro-segmentation a pris plus de temps que prévu en raison des conséquences potentielles sur l'activité. Les flux de trafic des différents actifs n'étaient pas toujours connus, ce qui a obligé l'équipe à multiplier les analyses de journaux de pare-feu avant d'activer une règle d'interdiction. En outre, l'incapacité des commutateurs d'ancienne génération à gérer la configuration ou la charge supplémentaire a compliqué un peu plus la détection des actifs.Mais la redirection du trafic via le pare-feu a permis de résoudre le problème.

Aligner, informer, inclure et motiver

La coordination s'est avérée essentielle. En effet, l'automatisation exige un alignement parfait entre les différentes équipes pour que les playbooks fonctionnent comme prévu.

Par ailleurs, il est apparu que les fournisseurs bénéficiaient d'un accès trop permissif aux équipements. Le seul moyen de limiter cet accès était par SSH (Secure Shell), RDP (Remote Desk Protocol) ou par des méthodes basées sur le navigateur.

Autre enseignement, il est important d'envoyer directement aux fournisseurs des demandes claires de changement d'architecture pour que ce soit fait dans les temps. Notons par ailleurs que la collecte et l'analyse du trafic sont des processus gourmands en ressources qui nécessitent une planification et une budgétisation rigoureuses.

Zoom sur la transformation

Phase 1

- La mise en place d'un point de contact dédié a nettement simplifié la communication et garanti l'alignement de toutes les activités du projet.
- L'inventaire et la configuration de départ ont été complets et méticuleux.
- Au problème de captation du trafic réseau, nous avons trouvé une solution innovante qui consiste à router les données via le pare-feu.
- Même s'il a fallu décaler la date de lancement du projet, ce temps de préparation supplémentaire nous a permis d'établir un plan final plus complet et mieux aligné, condition essentielle à une implémentation réussie.

Phase 2

- Les restrictions régionales et les réglementations représentaient un vrai défi pour le déploiement initial des pare-feu.
- Nous sommes parvenus à respecter toutes les obligations légales et à garantir un déploiement conforme dans chaque région.
- Lancée sur un rythme prudent, la première phase de segmentation a joué un rôle essentiel dans l'instauration d'un processus fluide, reproductible et accéléré sur les autres sites.

Phase 3

- La deuxième phase de micro-segmentation exigeait une approche graduelle pour éviter toute perturbation.
- C'est là que les insights récoltés auprès de notre équipe locale ont fait toute la différence.
- Nous avons passé au crible les journaux de pare-feu pour bien cerner tous les flux d'actifs et faire preuve d'une très grande précision.

Phase 4

- Le développement de playbooks d'automatisation efficaces passait par un alignement des différentes équipes.
- Une fois que l'action de ces dernières a pu être coordonnée, nous avons pu créer des solutions qui fonctionnent en parfaite synergie.

Phase 5

- Verizon a aidé l'entreprise à adopter un modèle d'accès plus sécurisé pour les fournisseurs.
- Elle a ainsi établi un nouveau standard qui autorise l'accès uniquement par SSH, RDP et des méthodes basées sur le navigateur.
- Pour implémenter ce changement, l'entreprise mise sur des échanges directs et une collaboration étroite avec ses partenaires. L'objectif : répondre à leurs besoins d'accès tout en veillant à ce qu'ils se conforment à la nouvelle architecture.

Phase 6

- Les analyses comportementales aident à mieux comprendre et décrypter l'activité réseau.

verizon business