Garantir la sécurité des logiciels en périphérie de réseau

LA SÉCURITÉ DOIT COUVRIR L'ENSEMBLE DES DISPOSITIFS ET L'INTÉGRALITÉ DE LEURS CYCLES DE VIE

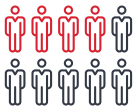
WIND

Les trois dynamiques affectant la sécurité

En 2025, on dénombrera 2 milliards de PC et 42 milliards d'objets connectés dans le monde.

En 2025, on dénombrera 2 milliards de PC et 42 milliards d'objets connectés dans le monde. La quasi-totalité de ces appareils reposera sur le cloud d'une façon ou d'une autre, et 80% de l'ensemble des données que nous créons, utilisons et qui constituent notre identité passeront par le cloud 5G. Cependant, actuellement, seuls 11,5% de l'ensemble des entreprises mènent leurs transformations numériques avec succès.[1] En d'autres termes, la majorité des organisations éprouvent encore de grandes difficultés à se préparer au monde axé sur le numérique qui les attend.

La sécurité fait partie de ces problématiques. Imaginez à quel point il peut être difficile de concevoir des protocoles de sécurité dans un monde en pleine évolution. Plus de la moitié des responsables des systèmes d'information sont confrontés à une multitude de problématiques directement liées à leurs initiatives de transformation numérique : des risques de cybersécurité accrus (53%), la sophistication des méthodes des cybercriminels (56%), ainsi que l'augmentation de la surface d'attaque (53%). À ces menaces s'ajoutent une autre préoccupation partagée par 40% des RSSI, directeurs techniques et DSI, à savoir les potentiels problèmes liés à la rigidité de leurs infrastructures — ces dernières étant généralement étroitement associées aux systèmes embarqués.[2]



40% des RSSI, directeurs techniques et DSI sont préoccupés par les potentiels problèmes liés à la rigidité de leurs infrastructures — ces dernières étant généralement étroitement associées aux systèmes embarqués.

Intéressons-nous en détail à trois dynamiques évoluant constamment dans le secteur.

1 *Forbes/Inc.Digital*
2 *media.nominet.uk/wp-content/uploads/2019/07/Cyber-Security-in-the-Age-of-Digital-Transformation.pdf*

EMERSON
Network Power

COMMENT EMERSON A RENDU SON SYSTÈME OVATION DCS ENCORE PLUS CONNECTÉ ET SÉCURISÉ ?

Grâce au machine learning, à la simulation de systèmes entiers, et à Wind River.

Ovation™ est un système de contrôle distribué (DCS) conçu pour accroître la fiabilité des centrales, et évoluant au gré des progrès technologiques. La plateforme a reçu le label Qualified terrorism Technology (technologie anti-terrorisme qualifiée) du ministère de la Sécurité intérieure des États-Unis dans le cadre de la loi U.S. SAFETY Act.

Emerson utilise les solutions Wind River pour gérer l'intégralité du cycle de vie d'Ovation. L'entreprise a ainsi accéléré ses processus de développement grâce à des équipements virtuels ; fait tourner son DCS sur le système d'exploitation VxWorks ; simulé l'intégralité de l'environnement physique de la centrale ; et modélisé le bon fonctionnement du système de contrôle — un élément essentiel sur le plan de la sécurité opérationnelle. Cette solution offre des points de référence quant aux paramètres et aux performances du système, et permet d'identifier les anomalies avant que les systèmes de production ne soient affectés.

WIND

Dynamique #1

LA VALEUR DES DONNÉES EST DÉSORMAIS UN FACTEUR PLUS DYNAMIQUE QUE LE 0,1% DE LEUR CYCLE DE VIE INITIAL

La tendance d'avenir n'est clairement pas de se focaliser sur les dispositifs. Dans un monde désormais axé sur le numérique, la valeur des informations est en effet un paramètre bien plus dynamique. Le fait que 75% des dirigeants de grandes entreprises affirment avoir vu le temps dont ils disposaient pour prendre des décisions diminuer de 200%[3] illustre bien le besoin de données rapidement disponibles pour les soutenir dans cette tâche.

Provenant de milliers ou de millions d'emplacements différents, et souvent simultanément, les données sont plus que jamais intrinsèquement dynamiques. Leur utilité dépend de leur capacité à fournir des informations sur des moments clés.[4] Ces derniers peuvent ne représenter que 0,1% du cycle de vie d'un appareil traditionnel. Mais dans le monde dynamique d'aujourd'hui, les informations collectées les 99,9% du temps restant peuvent être précieuses pour d'autres composantes de l'infrastructure. En d'autres termes, à l'heure de l'hyperconnexion, les données ont une valeur multidimensionnelle qui s'étend souvent bien au-delà de ce pour quoi les appareils sont initialement conçus.

L'importance de la révolution en cours au niveau des dispositifs est accentuée par la difficulté à sécuriser ces informations : plus de la moitié de l'ensemble des équipements IoT sont vulnérables à des attaques de sévérité moyenne ou élevée. En outre, 98% du trafic issus de ces équipements — dispositifs médicaux inclus — ne sont pas chiffrés.[5] Pourtant, certains types de données nécessitent une approche subtile en matière de confidentialité. En effet, en raison de leur nature dynamique, elles sont susceptibles d'entrer soudainement dans la catégorie des données personnelles (P2I), ces dernières étant soumises à diverses réglementations dans le monde.[6]

> Les données produisent en réalité une sorte d'effet de réseau : plus il y a d'appareils connectés en temps réel, plus la valeur des informations et données augmente pour l'organisation.

98%

du trafic issus de ces équipements — dispositifs médicaux inclus — ne sont pas chiffrés

3 *Forbes/Inc.Digital*
4 *The Digital Helix*
5 *threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609*
6 *www.varonis.com/blog/data-privacy*

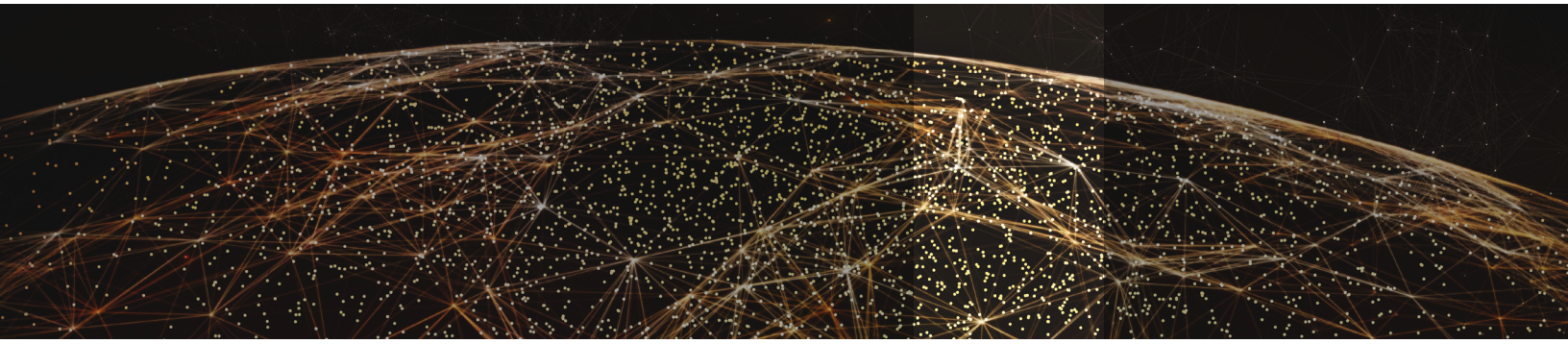
Dynamique #2

LA SÉCURITÉ : UNE AFFAIRE DE PARTENARIATS (EN INTERNE COMME EN EXTERNE)

Imaginez qu'un composant d'une machine industrielle ait la tâche complexe de gérer les transferts d'énergie d'un réseau électrique. Ce composant peut également se retrouver au sein de 10 autres produits de partenaires fonctionnant tous en liaison. Vous voulez en savoir plus sur ses performances, et découvrir comment l'écosystème de données global génère des informations à valeur ajoutée et utilisables en temps réel. Ou imaginons que vous souhaitiez voir comment ces données pourraient être orchestrées à l'avenir. Dans les secteurs de la production ou de la distribution d'énergie, de la fabrication de dispositifs médicaux, de l'aviation ou encore de la défense, il est possible d'obtenir les réponses à ces questions, les systèmes d'alimentation des appareils allant au-delà de leur fonction principale.

Les données produisent en réalité une sorte d'effet de réseau : plus il y a d'appareils connectés en temps réel, plus la valeur des informations et données augmente pour l'organisation. Selon les résultats d'une étude menée par Forbes/Inc.Digital sur les stratégies de transformation numérique, 8 dirigeants sur 11 sont convaincus que la puissance des données constitue un ingrédient important de leurs futurs succès dans une industrie en pleine transition numérique. Et plus l'écosystème sera riche en partenaires, plus la puissance potentielle des données sera élevée. Cet argument peut paraître abstrait, mais de récents travaux menés par le groupe Cognitive Systems d'IBM montrent que les intelligences artificielles (IA) les plus efficaces et rentables sont celles qui allient l'ensemble des quatre formats que sont le machine learning (apprentissage statistique), le deep learning (apprentissage profond), l'analyse visuelle et le traitement automatique du langage naturel, tout cela simultanément. En d'autres termes, celles qui exploitent plusieurs jeux de données en temps réel. L'IA étant désormais quasiment omniprésente, la puissance des partenariats autour de la donnée est énorme, et représente une valeur bien plus grande que ce qu'un seul écosystème serait capable de produire.

8 dirigeants sur 11 sont convaincus que la puissance des données constitue un ingrédient important de leurs futurs succès dans une industrie en pleine transition numérique.



Dynamique #3

À L'HEURE DU TOUT NUMÉRIQUE, L'AVENIR EST, PAR DÉFINITION, INCERTAIN. VOTRE INFRASTRUCTURE DE SÉCURITÉ PEUT-ELLE FAIRE FACE À UN TEL NIVEAU D'AMBIGUÏTÉ ?

L'avenir digital sera placé sous le signe de l'ambiguïté. Les transformations sont des processus complexes, et nos modèles et la fourniture de sécurité sont tout aussi difficiles à maîtriser. Cependant, les grandes entreprises (celles du classement Fortune Global 2000) réussissant leurs transitions sont bien plus confiantes quant à leur avenir, les environnements ainsi créés leur permettant de gérer cette ambiguïté.

À la fois instable, incertain, complexe et ambigu (ou VUCA, pour volatile, uncertain, complex and ambiguous) le monde actuel nécessite que nous cherchions de nouvelles façons d'assurer notre sécurité. Les entreprises doivent impérativement s'adapter à cette réalité, les pourcentages de transitions numériques réussies étant pour l'instant faibles (seulement 11,5% du taux de croissance annuel cumulé — TCAC — depuis 2013).[7] Nous devons donc bâtir un avenir où nous serons capables de sécuriser nos données, d'en extraire des connaissances pour les utiliser en temps réel et, enfin, de les partager sur une multitude d'écosystèmes.

Avant l'avènement du numérique, le concept de sécurité était bien maîtrisé. Mais aujourd'hui, les organisations doivent adapter leurs approches au quotidien, c'est le cas pour l'IA, le cloud et la 5G. La priorité des développeurs et en matière de gestion des applications doit être de créer un avenir basé sur des équipements de périphérie intelligents (Intelligent Edge), conçus pour un monde dynamique.

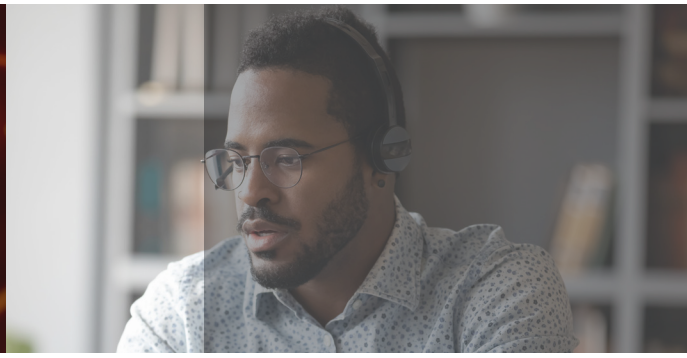
Pour savoir où vous en êtes dans votre préparation pour le monde de demain, posez-vous les 3 questions élémentaires suivantes

1. Tenez-vous compte d'un nombre croissant de nouvelles exigences en matière de sécurité pour vos appareils ?
2. L'instabilité, l'incertitude, la complexité et l'ambiguïté du monde dans lequel nous vivons sont-elles considérées comme un atout par votre organisation, et les exigences de sécurité représentent-elles des freins ou des accélérateurs ?
3. Votre stratégie de sécurité sera-t-elle très différente dans cinq ans au gré de votre transformation numérique ?

> "En utilisant un modèle de simulation (VxWorks Simulator) en parallèle avec le système embarqué physique équivalent, nous bénéficions ainsi d'une référence absolue, et sommes potentiellement en mesure de détecter les comportements anormaux avant qu'ils ne se manifestent sous la forme d'une défaillance du système."
>
> **—Rick Kephart,**
> *Vice-président du développement de logiciels chez Emerson*

7 *Inc.Digital*

L'Edge, ou la périphérie de réseau



Notre mission est de construire et sécuriser un monde tourné vers le numérique malgré deux changements majeurs : 1 une transition massive vers l'edge computing, (le traitement en périphérie de réseau) en particulier en ce qui concerne la collecte, le traitement et le stockage des données d'entreprise ; et 2 un changement générationnel au sein des professionnels qui seront chargés de développer et d'exploiter les systèmes connectés et intelligents essentiels de demain.

Si en 2018, seuls 10% des données d'entreprises ont été collectées et traitées à l'extérieur d'un centre de données traditionnel, en 2025, ce pourcentage dépassera les 75%.[8] Pendant ce temps, en 2020, les milléniaux sont devenus la population la plus représentée au sein de la population active.[9]

L'EXPÉRIENCE COMPTE

La génération des développeurs et responsables de production les plus expérimentés en matière de systèmes embarqués traditionnels approche de l'âge de la retraite, et le réservoir d'ingénieurs talentueux qui attendent en coulisses est bien plus limité. Quatre-vingt-deux pour cent des dirigeants font état d'une pénurie de candidats qualifiés, et 60% des entreprises identifient les postes d'ingénieurs en électrotechnique comme les plus difficiles à pourvoir.[10] L'expérience en matière de systèmes IoT est essentielle pour en assurer la sécurité, les erreurs de programmation étant la cause première de vulnérabilités, si l'on en croit la base de données CVE : " Les systèmes d'exploitation et firmware sont les plus ciblés : les erreurs de programmation, les lacunes au niveau des contrôles des accès et les systèmes d'authentification déficients permettent de procéder à des attaques au niveau le plus bas de cette couche logicielle, mais les vulnérabilités non divulguées représentent également un problème courant"[11]

8 *www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders*
9 *Forbes/Inc.Digital*
10 *www.semi.org/en/node/581*
11 *www.cse.psu.edu/~pdm12/cse597g-f15/readings/cse597g-embedded_systems.pdf*

TOSHIBA

COMMENT TOSHIBA SÉCURISE SES DONNÉES PERSONNELLES DANS UN MARCHÉ OU LE CYBERCRIME DEVRAIT COÛTER 5 200 MILLIARDS DE DOLLARS AUX ENTREPRISES AU COURS DES 5 PROCHAINES ANNÉES ?

60% des fuites survenues en 2019 étaient liées à des vulnérabilités pour lesquelles un correctif était disponible, mais n'avait pas été appliqué. Wind River Linux aide Toshiba à changer la donne.

En 2019, plus de 45 fiches par jour ont été créées dans le dictionnaire CVE. Conscient des risques pour les données personnelles en sa possession, le conglomérat et fabricant de matériel électronique et informatique Toshiba s'est associé à Wind River pour les sécuriser et réduire ses coûts. L'équipe de sécurité de Wind River surveille constamment la base de données CVE à la recherche de problèmes potentiels affectant VxWorks, ainsi que l'ensemble des fonctionnalités du noyau de Wind River Linux, des packages destinés aux utilisateurs et des outils. En outre, l'éditeur suit également les notifications des agences et organisations du gouvernement des États-Unis, à l'image de l'Institut national des normes et de la technologie (NIST) et de l'US-CERT. Enfin, Wind River est également inscrit à des listes de diffusion publiques et privées spécialisées dans la sécurité.

L'ACCÈS AVANT TOUT

Les appareils IoT et autres équipements installés en périphérie de réseau sont souvent physiquement accessibles, et donc exposés à une variété d'attaques peu fréquentes dans des environnements plus contrôlés À ces risques s'ajoute le fait que ces systèmes sont librement disponibles sur le marché : les cybercriminels ont donc tout le loisir de développer leurs attaques. En outre, les dispositifs personnels de taille réduite et n'étant pas conçus dans un souci de sécurité ne sont pas toujours régulièrement mis à jour. Ils sont donc susceptibles d'offrir un accès facile au réseau étendu auquel ils sont connectés. Selon les résultats d'une enquête publiée en 2018 par Ponemon Institute, 97% des professionnels chargés de la gestion des risques estiment que les objets connectés et intelligents non sécurisés pourraient être à l'origine d'une faille de sécurité catastrophique.[12]

Les trois questions que vous devez vous poser lors du déploiement d'équipements en périphérie de réseau :

1. Avez-vous à portée de main des ingénieurs possédant les qualifications nécessaires pour le développement, le déploiement et la maintenance des appareils et systèmes IoT contemporains ?
2. Avez-vous mis en œuvre une stratégie basée sur une expérience digitale garantissant que vos équipements puissent être utilisés aisément par une majorité de milléniaux natifs du numérique ?
3. Avez-vous une connaissance parfaite de la chaîne d'approvisionnement dont dépendent vos équipements (y compris votre chaîne d'approvisionnement en logiciels) et couvrant vos fournisseurs de produits de rechange ?

"Chaque jour apporte son lot de mises à jour liées à des failles potentielles. Nous avons une équipe spécialisée dans ce domaine, et qui travaille avec Wind River pour faire en sorte d'identifier les risques connus et d'y répondre rapidement pour nos détaillants."

—Gregg Margosian,
COO, Toshiba

97% des professionnels chargés de la gestion des risques estiment que les objets connectés et intelligents non sécurisés pourraient être à l'origine d'une faille de sécurité catastrophique.

12 *sharedassessments.org/wp-content/uploads/2018/04/2018-IoTThirdPartyRiskReport-Final-04APR18.pdf*

Définir une politique de sécurité

49% des équipes de conception considèrent la définition d'une politique de sécurité comme un de leurs projets les plus importants.

CIA Triad est un modèle de référence permettant de guider le développement de politiques de sécurité des dispositifs en définissant les principes nécessaires à la protection des accès, utilisations, divulgations, perturbations, modifications ou destructions non autorisés.

Ce modèle repose sur les trois principes suivants :

- **La confidentialité,** pour protéger les données des systèmes IoT. Cela inclut les données en mouvement, au repos ou hébergées par un appareil, les données en cours de traitement par l'appareil, et les données entrantes ou sortantes.
- **L'intégrité,** dans le but de garantir que les données des appareils n'ont pas été modifiées ou supprimées par un pirate. Ceci inclut les données générées ou utilisées par le dispositif embarqué, ainsi que les données de ses programmes internes (son système d'exploitation, ses applications, ses données de configuration, etc.).
- **La disponibilité,** pour faire en sorte que l'appareil IoT fonctionne comme prévu. Le but est de s'assurer que les cybercriminels ne puissent pas en altérer le fonctionnement normal. Ce paramètre est d'une importance cruciale pour les équipements chargés de tâches vitales ou critiques.

Les équipes de projet déterminent quelles composantes du CIA Triad sont nécessaires en fonction des risques, des exigences réglementaires, et des besoins de protection de la propriété intellectuelle, puis comparent ces facteurs aux coûts, aux performances, et à l'environnement opérationnel utilisé pour le déploiement de l'appareil. Il n'existe aucune solution universelle pour protéger un équipement ou un système de l'ensemble des attaques potentielles. À la place, l'adoption d'une approche multidimensionnelle basée sur différents systèmes de contrôle permettra d'ériger un véritable bouclier de protection et de renforcer la cybersécurité.

Il n'existe aucune solution universelle pour protéger un équipement ou un système de l'ensemble des attaques potentielles. À la place, l'adoption d'une approche multidimensionnelle basée sur différents systèmes de contrôle permettra d'ériger un véritable bouclier de protection et de renforcer la cybersécurité.

Les questions que vous devez vous poser lors du déploiement d'équipements en périphérie de réseau

ÊTES-VOUS EN PHASE DE RÉUSSIR VOTRE TRANSFORMATION, OU EN TRAIN D'ÉTENDRE VOTRE SURFACE D'ATTAQUE PAR INADVERTANCE ?

Voici cinq questions à vous poser dans le cadre de votre transformation numérique

Les univers des systèmes embarqués et des technologies opérationnelles (OT) convergent de plus en plus vers le numérique, et le cycle de vie des appareils s'étend pour leur permettre d'élargir le champ de leurs fonctionnalités et aller au-delà du modèle de service réactif traditionnel. Dans ce contexte, des stratégies radicalement différentes devront être mises en œuvre pour concevoir, déployer, orchestrer et adapter de façon sécurisée les systèmes critiques de nouvelle génération.

1. Votre stratégie de sécurité se focalise-t-elle sur les points de terminaison, ou repose-t-elle sur une approche couvrant l'intégralité de vos systèmes, incluant le cloud, et mettant en place une chaîne de responsabilité des données au cœur de votre transformation numérique ?
2. Avez-vous établi une méthodologie pour le développement simultané des fonctionnalités et composantes de sécurité de vos systèmes IoT ? Si oui, cette méthodologie peut-elle faire face à la prolifération des menaces inhérentes à toute transformation numérique ?
3. L'architecture de vos systèmes permet-elle d'assurer une gestion efficace et la mise à jour de vos équipements en périphérie de réseau depuis la phase de déploiement ? Êtes-vous en mesure d'anticiper les nouvelles menaces et de profiter de la flexibilité nécessaire pour garantir la sécurité de vos appareils installés sur le terrain pour les décennies à venir ?
4. Vos outils de sécurité reconnaissent-ils les divers protocoles spécifiques de vos systèmes IoT, et dans le cas contraire, comment ferez-vous pour détecter les intrusions exploitant ces protocoles alors que la transformation numérique accélère la convergence entre les systèmes d'information de l'entreprise et la périphérie de réseau ?
5. Le périmètre de sécurité de votre entreprise englobe-t-il les équipements déployés sur le terrain, et sinon, comment comptez-vous garantir une connectivité sécurisée entre ces équipements et votre organisation ?

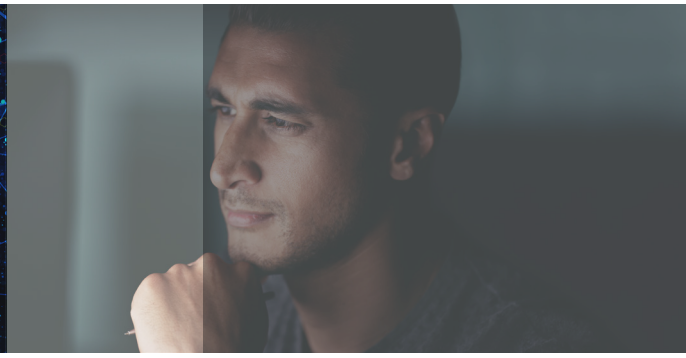
VOS DONNÉES SONT-ELLES EXPOSÉES ?

Voici trois questions à vous poser lors de la création et du déploiement d'équipements orientés données

Les fabricants d'équipements doivent adopter le nouveau modèle numérique basé sur l'interconnectivité et le dynamisme des données. Il leur faut aujourd'hui concevoir leurs systèmes de sécurité pour tenir compte à la fois des données en mémoire ou stockées, de celles transitant sur un réseau, et des clés utilisées pour chiffrer ces données. Dans le même temps, ils doivent également s'assurer que leurs logiciels et équipements soient durcis, afin d'éviter toute action susceptible de compromettre l'intégrité des données. Votre organisation a-t-elle mis en place une approche complète en matière de sécurité et de confidentialité des données, ou vos efforts de développement se focalisent-ils sur la sécurité des points de terminaison ?

1. Les systèmes que vous développez feront-ils partie des 98% d'appareils IoT transmettant des informations sans protection, ou assurerez-vous le chiffrement de vos données ?
2. Avez-vous une parfaite connaissance de l'environnement où vos systèmes seront déployés, des attaques dont cet environnement pourrait faire l'objet, et de la façon dont cet environnement pourrait ou pas être à l'origine de problématiques de confidentialité ?
3. Avez-vous mis en place une stratégie de tests afin de faire face à l'éventail complet de menaces pour la sécurité de vos données ?

Pourquoi choisir Wind River



Depuis plus de 40 ans, Wind River aide les leaders technologiques du monde entier à proposer les équipements les plus sécurisés, génération après génération.

Et dans cette nouvelle ère d'autonomie et de connectivité, l'entreprise continue de montrer la voie. De l'aérospatiale au ferroviaire, en passant par l'automobile, les dispositifs médicaux, les usines de fabrication et autres réseaux de communication, nos logiciels sous-tendent les systèmes critiques des infrastructures les plus essentielles.

Nos technologies sont au cœur de plus de 2 milliards d'équipements dans le monde, et s'accompagnent de services aux entreprises de premier plan, d'une assistance client primée, et d'un puissant écosystème de partenaires.

Nos clients bénéficient de plateformes dernier cri, robustes et fiables protégeant la confidentialité et l'intégrité de leurs données, et garantissant une disponibilité maximale grâce à des intégrations en douceur avec leurs systèmes et à une collaboration parfaite entre développeurs. Nos plateformes font également office de socles pour vous aider à innover de façon sécurisée, et à protéger vos équipements des menaces actuelles et à venir.

Nos solutions éprouvées et sécurisées par défaut, et notre grande expérience vous permettent de concevoir vos appareils avec l'assurance de vous appuyer sur des technologies leaders, en sachant que vos données privées sont protégées, que vos systèmes critiques sont isolés, et que l'ensemble de votre écosystème bénéficie de capacités intégrées et sécurisées de gestion des systèmes. Vous pouvez ainsi limiter les risques, accélérer vos processus itératifs, et effectuer des déploiements en toute confiance tout au long du cycle de vie de vos produits.

Nos plateformes font également office de socles pour vous aider à innover de façon sécurisée, et à protéger vos équipements des menaces actuelles et à venir.

Wind River est l'un des leaders mondiaux dans le domaine des logiciels pour la périphérie de réseau intelligente. Wind River propose un portefeuille complet, soutenu par des services professionnels et un support de niveau international et par un large écosystème de partenaires. Les logiciels et l'expertise de Wind River accélèrent la transformation numérique des systèmes d'infrastructures critiques qui exigent les plus hauts niveaux de sûreté, de sécurité, de performance et de fiabilité.

Annexe

Fiche : La sécurité à l'heure du tout numérique

PRÊTS POUR LE NOUVEAU MONDE INSTABLE, INCERTAIN, COMPLEXE ET AMBIGU DU TOUT NUMÉRIQUE ?

1. Tenez-vous compte d'un nombre croissant de nouvelles exigences en matière de sécurité pour vos appareils ?
2. L'instabilité, l'incertitude, la complexité et l'ambiguïté du monde dans lequel nous vivons sont-elles considérées comme un atout par votre organisation, et les exigences de sécurité représentent-elles des freins ou des accélérateurs ?
3. Votre stratégie de sécurité sera-t-elle très différente dans cinq ans au gré de votre transformation numérique ?

ÊTES-VOUS EN PHASE DE RÉUSSIR VOTRE TRANSFORMATION, OU EN TRAIN D'ÉTENDRE VOTRE SURFACE D'ATTAQUE PAR INADVERTANCE ?

1. Votre stratégie de sécurité se focalise-t-elle sur les points de terminaison, ou repose-t-elle sur une approche couvrant l'intégralité de vos systèmes, incluant le cloud, et mettant en place une chaîne de responsabilité des données au cœur de votre transformation numérique ?
2. Avez-vous établi une méthodologie pour le développement simultané des fonctionnalités et composantes de sécurité de vos systèmes IoT ? Si oui, cette méthodologie peut-elle faire face à la prolifération des menaces inhérentes à toute transformation numérique ?
3. L'architecture de vos systèmes permet-elle d'assurer une gestion efficace et la mise à jour de vos équipements en périphérie de réseau depuis la phase de déploiement ? Êtes-vous en mesure d'anticiper les nouvelles menaces et de profiter de la flexibilité nécessaire pour garantir la sécurité de vos appareils installés sur le terrain pour les décennies à venir ?
4. Vos outils de sécurité reconnaissent-ils les divers protocoles spécifiques de vos systèmes IoT, et dans le cas contraire, comment ferez-vous pour détecter les intrusions exploitant ces protocoles alors que votre transformation numérique accélère la convergence du système d'information de l'entreprise et de la périphérie du réseau ?
5. Le périmètre de sécurité de votre entreprise englobe-t-il les équipements déployés sur le terrain, et sinon, comment comptez-vous garantir une connectivité sécurisée entre ces équipements et votre organisation

VOS DONNÉES SONT-ELLES EXPOSÉES ?

1. Les systèmes que vous développez feront-ils partie des 98% d'appareils IoT transmettant des informations sans protection, ou assurerez-vous le chiffrement de vos données ?
2. Avez-vous une parfaite connaissance de l'environnement où vos systèmes seront déployés, des attaques dont cet environnement pourrait faire l'objet, et de la façon dont cet environnement pourrait ou pas être à l'origine de problématiques de confidentialité ?
3. Avez-vous mis en place une stratégie de tests afin de faire face à l'éventail complet de menaces pour la sécurité de vos données ?

AVEZ-VOUS LES CONNAISSANCES NÉCESSAIRES POUR RÉUSSIR VOTRE DÉPLOIEMENT VERS LA PÉRIPHÉRIE DE RÉSEAU ?

1. Avez-vous à portée de main des ingénieurs possédant les qualifications nécessaires pour le développement, le déploiement et la maintenance des équipements et systèmes IoT contemporains ?
2. Avez-vous mis en œuvre une stratégie basée sur une expérience digitale garantissant que vos équipements puissent être utilisés aisément par une majorité de milléniaux natifs du numérique ?
3. Avez-vous une connaissance parfaite de la chaîne d'approvisionnement dont dépendent vos équipements (y compris votre chaîne d'approvisionnement en logiciels) et couvrant vos fournisseurs de produits de rechange ?