Techniques pour optimiser la sécurité

Renforcer la protection et accélérer la résolution d'incidents tout en maîtrisant les coûts.

KEYSIGHT TECHNOLOGIES

Roxana Magdo
Director, Business Development
Keysight EMEA

Stratégie de Sécurité : Enseignements tirés des incidents récents

CONSTRUCTION D'UNE ARCHITECTURE RÉSEAU RÉSILIENTE

Quand on fait des erreurs de stratégie dans la gestion de sa sécurité les conséquences sont doubles: au niveau de l'entreprise mais aussi au niveau de la responsabilité personnelle des dirigeants

SECURITYWEEK
CYBERSECURITY NEWS. INSIGHTS & ANALYSIS

Cybersecurity Leaders Spooked by SEC Lawsuit Against SolarWinds CISO

The SEC's lawsuit against the CISO of SolarWinds is leaving CISOs across the industry spooked and reevaluating their roles.

By Mike Lennon
October 31, 2023

Récemment, the US Securities and Exchange Commission (SEC) a déposé une plainte civile contre SolarWinds et son ancien vice-président de la sécurité et de l'architecture, pour la manière dont ils ont géré l'attaque de la "supply chain" qui a été révélée à la fin de 2020. Les allégations affirment que SolarWinds n'avait aucune politique ou pratique en place, pour la plupart, du cadre NIST Security Framework, bien qu'ils l'aient officiellement déclarée mis en œuvre.

Stratégie de Sécurité : Enseignements tirés des incidents récents

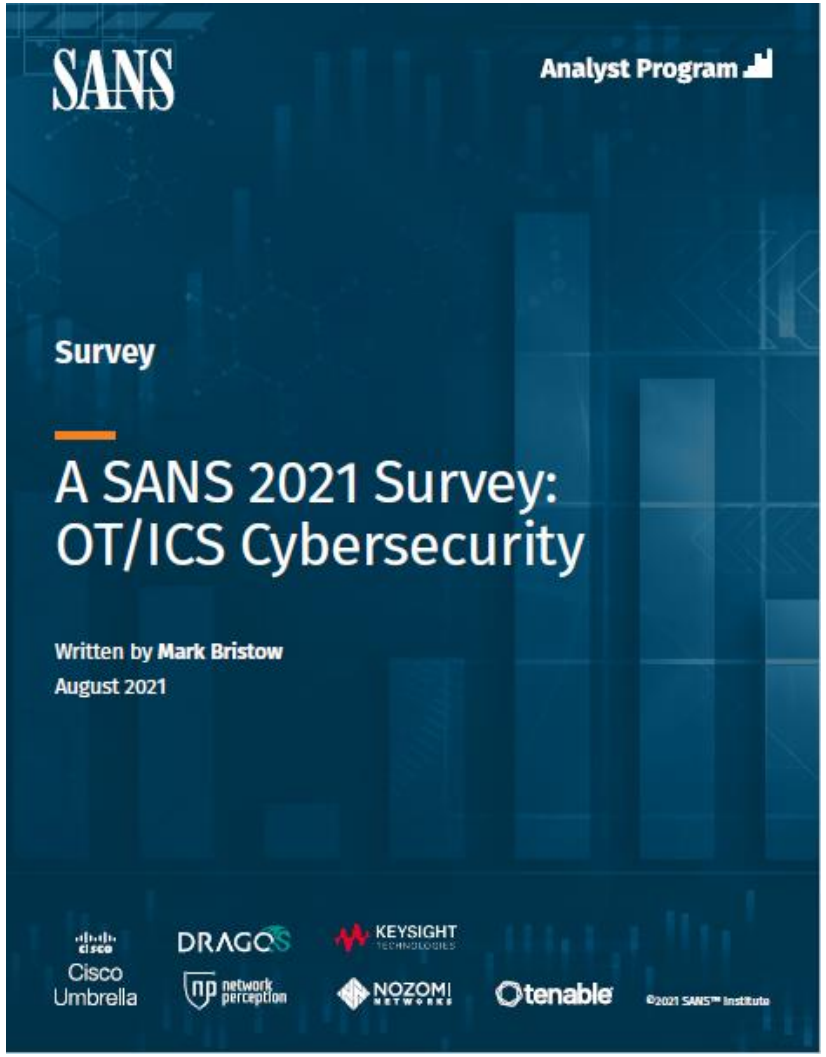
COMBIEN PEUT-ON INVESTIR DANS LA SÉCURITÉ ET OÙ S'ARRÊTE-T-ON?

Un des secrets pour bien protéger le réseau, c'est d'avoir une architecture de réseaux versatile qui permettra de:

- **facilement remplacer ou upgrader les outils de sécurité et monitoring**
- **rester toujours à jour avec les derniers développements (menaces et outils de protection)**
- **être conforme à la législation et aux règles de sécurité, comme NIS2 ou d'autres réglementations spécifiques à chaque industrie**

Qu'est-ce que l'on sait sur les réseaux industriels?

SANS SURVEY FROM 2021 ON OT/ICS CYBERSECURITY



<u>L'enquête a reçu plus de 480 réponses.</u>

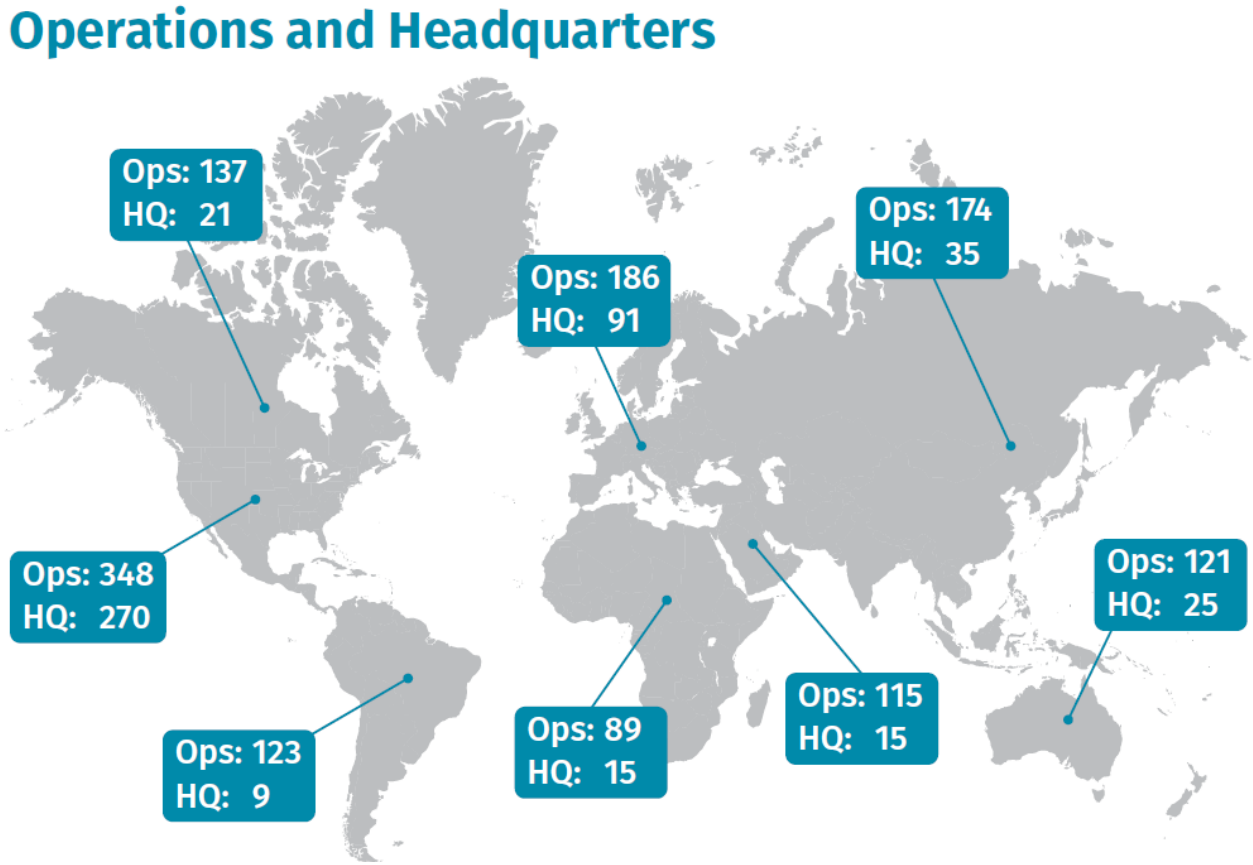
*** 12,5 % des personnes interrogées étaient confiantes de n'avoir pas subi de compromission au cours de la dernière année.**

*** 48 % des participants à l'enquête ne savent pas s'ils ont été victimes d'un incident.**

Les entreprises industrielles dans le monde sont-elles bien sécurisées ?

SANS SURVEY FROM 2021 ON OT/ICS CYBERSECURITY

- **Presque toutes les personnes interrogées ont indiqué avoir rencontré au moins un incident au cours de la dernière année.**
- **90 % des incidents ont eu un certain niveau d'impact sur les process.**
- **Pourtant, seuls les incidents de grande envergure comme l'attaque de Colonial font la une des journaux.**



Les entreprises industrielles dans le monde sont-elles bien sécurisées ?

SANS SURVEY FROM 2021 ON OT/ICS CYBERSECURITY

- **Les inventaires d'actifs continuent de représenter un défi pour la plupart des organisations.**
- **Le défi majeur : Il y a 59,4 % d'intégration technique des technologies OT héritées et vieillissantes dans des systèmes informatiques modernes.**

Conclusion: l'un des plus grands défis auxquels nous sommes confrontés est de trouver des moyens de protéger et de surveiller les anciens actifs ainsi que les réseaux OT-IT connectés. L'enjeu est de maîtriser les coûts tout en restant à jour avec les dernières technologies.

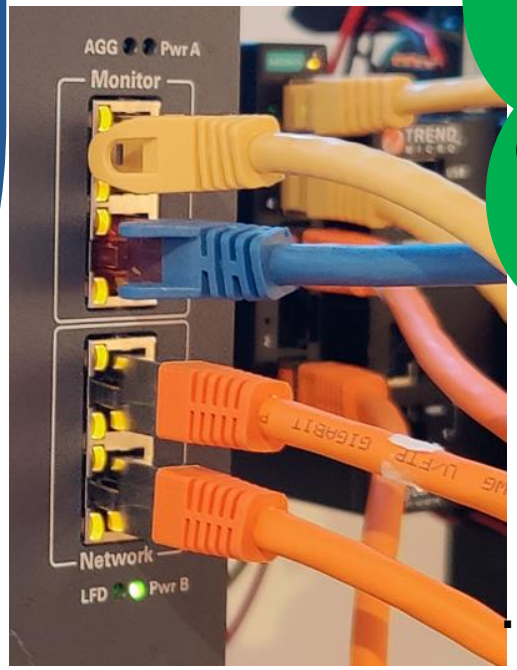
Technique numéro 1 : situation

MANQUE DE PORTS DISPONIBLES POUVANT ÊTRE UTILISÉS EN MODE MIRRORING

ÉTUDE DE CAS:

BESOIN D'ANALYSER LES PAQUETS D'UN SWITCH QUI N'A AUCUN PORT MIROIR DISPONIBLE (SPAN)

Une façon importante de maintenir la sécurité du réseau OT est d'utiliser différents outils de sécurité. Ces outils doivent analyser les données qui circulent à travers le réseau pour détecter les violations ou les risques potentiels.



SOLUTION:

UTILISER DES TAPS POUR OBTENIR UNE COPIE DU TRAFIC DU SWITCH

Connecter un TAP au port du switch est une solution rapide et sûre qui ne nécessite pas de planifier une longue fenêtre de maintenance

KEYSIGHT TECHNOLOGIES

Technique numéro 2 : situation

LES ÉQUIPEMENTS ANCIENS POSENT TOUJOURS UN DÉFI EN TERMES DE GESTION ET DE SÉCURITÉ

ÉTUDE DE CAS:

ANALYSER LES PAQUETS D'UN SWITCH QUE "NOUS NE VOULONS PAS TOUCHER ☺"

Nous avons tous entendu parler de cette situation: il y a d'anciens switchs dans le réseau, installés dans le passé par des tiers. Ensuite, nous n'avons pas la possibilité de les mettre à jour ou de les remplacer et ils fonctionnent très bien. Nous ne voulons pas modifier la config.

SOLUTION:

CONNECTER DES TAPS AUX PORTS EXISTANTS ET RÉCUPÉRER UNE COPIE DU TRAFIC.

Une copie du trafic peut être récupérée depuis le switch sans configurer de port SPAN. Ajouter un TAP ne nécessite aucune modification de la configuration du switch.

KEYSIGHT TECHNOLOGIES

Technique numéro 3 : situation

AJOUTER UNE SONDE AUGMENTE LE NIVEAU DES RISQUES DE SECURITÉ

ÉTUDE DE CAS:

AJOUTER UNE SONDE AUGMENTE LA SURFACE D'ATTAQUE

De nombreuses solutions de sécurité fonctionnent à travers des appareils déployés dans le réseau OT pour collecter une copie du trafic depuis les switches, puis le transmettre à un serveur d'analyse centralisé. Ces appareils représentent un risque, tout comme tout autre élément matériel

SOLUTION:

TAPS:

* **PAS ADRESSABLES PAR ADRESSE IP**
* **PAS DE MÉMOIRE**
* **FAIL OPEN (EN CAS DE PANNE LE TAP SE COMPORTE COMME UN FIL)**

L'une des principales préoccupations lors de l'ajout d'éléments au niveau SCADA inférieur est l'introduction de risques additionnels L'utilisation de TAPs offre une visibilité sans compromettre la sécurité.

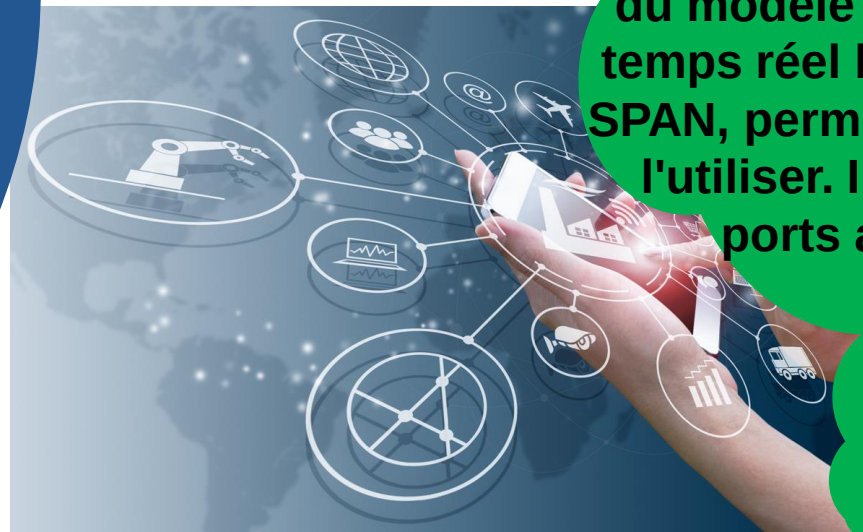
Technique numéro 4 : situation

PLUSIEURS OUTILS DOIVENT ACCÉDER SIMULTANÉMENT AU MÊME TRAFIC

ÉTUDE DE CAS:

LE MÊME TRAFIC DOIT ÊTRE ANALYSÉ PAR DIFFÉRENTS OUTILS SIMULTANÉMENT. SOUVENT, LES SOURCES SONT À DES VITESSES DIFFÉRENTES.

Le défi est de distribuer simultanément le trafic à différents outils pour réaliser des analyses croisées.



SOLUTION:

AGRÉGER LE TRAFIC COLLECTÉ DU RÉSEAU OT À TRAVERS DES TAPS ET LES PORTS SPAN DANS UN PACKET BROKER

Un packet broker au niveau 4 de l'architecture du modèle SCADA collecte et réplique en temps réel le trafic des TAPs et des ports SPAN, permettant à plusieurs outils de l'utiliser. Il dispose de plusieurs ports avec des vitesses variées

KEYSIGHT TECHNOLOGIES

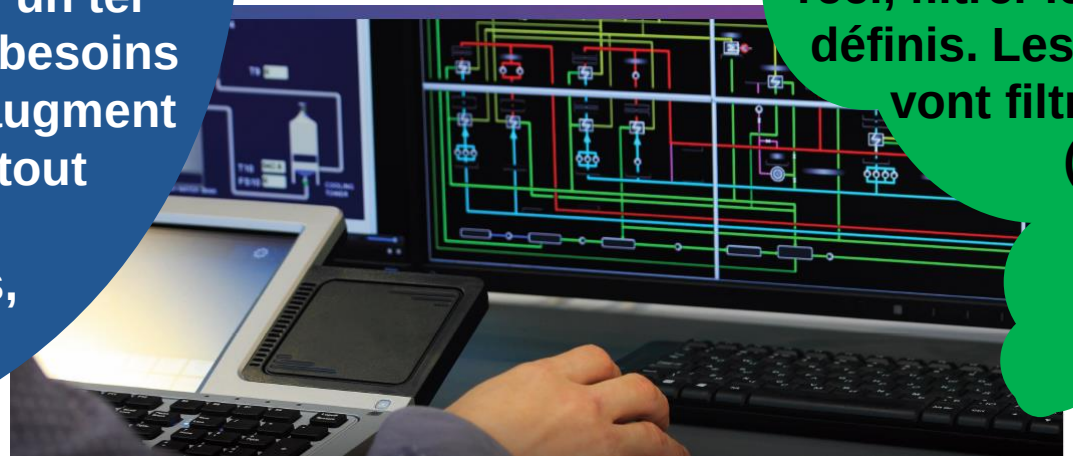
Technique numéro 5 : situation

BESOIN DE FILTRER LE TRAFIC QUI EST DIRIGÉ VERS CHAQUE OUTIL

ÉTUDE DE CAS:

LES OUTILS N'ONT PAS BESOIN D'ANALYSER TOUS LES TYPES DE TRAFIC

Dans de nombreux cas, il y a du trafic qui circule dans le réseau OT et qui n'a pas besoin d'être soumis à l'inspection des outils de sécurité. Envoyer un tel trafic aux outils augmente les besoins en bande passante(ports) et augment les coûts d'investissement, tout en ajoutant des tâches supplémentaires inutiles, telles que le filtrage.



SOLUTION:

AGRÉGER LE TRAFIC COLLECTÉ DU RÉSEAU OT À TRAVERS LES TAPS ET LES PORTS SPAN DANS UN PACKET BROKER

Les packet brokers peuvent, en plus de recevoir et de répliquer le trafic en temps réel, filtrer le trafic par des critères définis. Les plus performants, vont filtrer le trafic applicatif (ISO Niveau 7).

KEYSIGHT TECHNOLOGIES

Technique numéro 6 : situation

IL EST DIFFICILE DE PLANIFIER DES FENÊTRES DE MAINTENANCE

ÉTUDE DE CAS:

PLANIFIER DES FENÊTRES DE MAINTENANCE POUR TOUS LES OUTILS QUI ANALYSENT LE TRAFIC EST UN DÉFI.

L'utilisation de plusieurs outils améliore la posture de sécurité, mais cela augmente le défi de les maintenir, ainsi que de changer les configurations ou de les mettre à jour sans perturber le réseau.

SOLUTION:

QUAND LES OUTILS SONT CONNECTÉS À UN PACKET BROKER, ILS PEUVENT ÊTRE DÉCONNECTÉS INDIVIDUELLEMENT EN TOUTE SÉCURITÉ SANS IMPACTER LE RÉSEAU.

Le packet broker continuera d'envoyer le trafic aux outils pertinents même si l'un des outils est déconnecté pour maintenance ou des changements de configuration.

Technique numéro 7 : situation

LES RÉSEAUX INDUSTRIELS SONT SOUVENT SOUMIS À DES TEMPÉRATURES ET À UNE HUMIDITÉ EXTRÊMES. ENVIRONNEMENTS HOSTILES

ÉTUDE DE CAS:

LE RÉSEAU OT EST SOUMIS À DES CONDITIONS ENVIRONNEMENTALES HOSTILES COMME UNE TEMPERATURE OU HUMIDITÉ EXTRÊMES.

Un bon nombre des éléments du réseau industriel fonctionnent soit dans de petits espaces / rack, soit dans des racks montables en DIN. Cependant, malgré ces limitations, le trafic doit être récupéré pour être envoyé aux outils de sécurité.

SOLUTION:

IL EXISTE DES TAPS SPÉCIFIQUES INDUSTRIELS MONTABLES EN DIN ET DES PACKET BROKERS QUI RÉSISTENT À LA CHALEUR ET À L'HUMIDITÉ

Pour l'environnement exigeant, les TAPs et Packet Brokers renforcés peuvent supporter des températures jusqu'à 85 °C et une humidité jusqu'à 95 %.

KEYSIGHT TECHNOLOGIES

Technique numéro 8 : situation

SURVEILLER LES ÉLÉMENTS VIRTUALISÉS DU RÉSEAU OT.

ÉTUDE DE CAS:

L'IHM OU L'HISTORIAN SONT VIRTUALISÉS. ILS DOIVENT ÊTRE SURVEILLÉS AU MEME TITRE QUE LE RESTE DE L'INFRASTRUCTURE.

Dans de nombreux réseaux industriels tout comme dans le monde de l'IT, certains éléments commencent à être virtualisés. Cependant, le trafic qui passe à travers ceux-ci doit toujours être capturé et analysé.

SOLUTION:

LES TAPS VIRTUELS PEUVENT REPRODUIRE UNE COPIE DU TRAFIC DE L'IHM OU DE L'HISTORIAN, QUE CE SOIT À PARTIR DU CLOUD OU DES RÉSEAUX VIRTUELS PRIVÉS

De la même manière que les TAPs spécifiques à l'industrie copient le trafic du réseau OT traditionnel, il existe des TAPs virtuels qui offrent la même fonctionnalité

KEYSIGHT TECHNOLOGIES

Technique numéro 9 : situation

ANALYSE FORENSIQUE : LE TRAFIC DOIT ÊTRE INSPECTÉ À DIFFÉRENTS POINTS, NOTAMMENT HMI-PLC.

ÉTUDE DE CAS:

BESOIN DE COMPRENDRE SI L'IHM A ÉTÉ COMPROMISE ET SOUHAITE ANALYSER LE TYPE DE COMMANDES QU'ELLE ENVOIE AU PLC.

Lorsqu'une violation est suspectée et que le trafic doit être compris à chaque niveau du réseau SCADA, comme la segmentation a été réalisée, nous devons analyser le trafic qui circule entre l'IHM et le PLC, par exemple, sans perturber le fonctionnement du réseau.

SOLUTION:

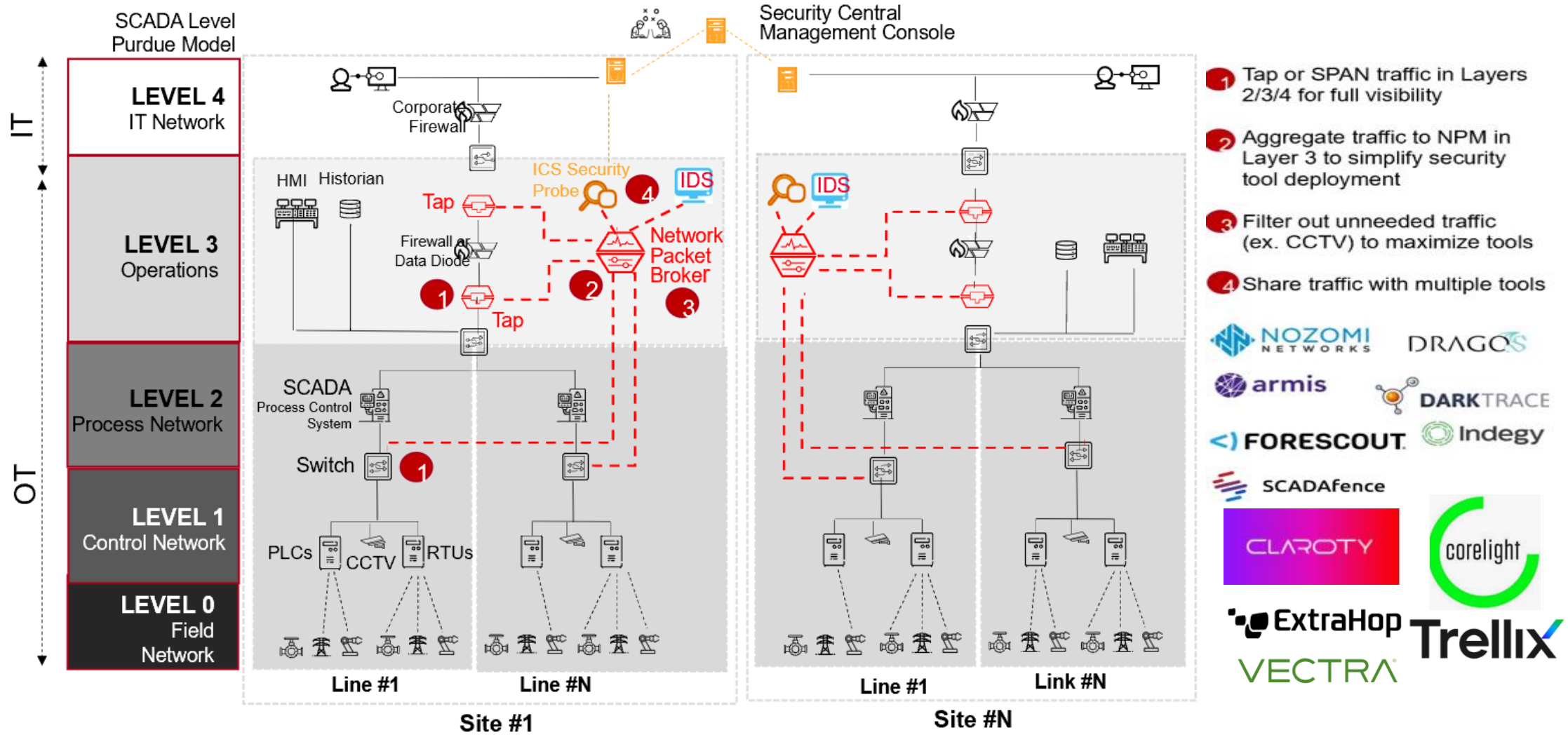
AVOIR DES TAPS CONNECTÉS AUX SWITCHES QUI ROUTENT LE TRAFIC ENTRE L'IHM ET LE PLC OFFRE UN MOYEN RAPIDE ET SIMPLE D'INTERCEPTER CE TRAFIC

En récupérant simplement le trafic depuis le TAP, sans perturber le réseau, ce trafic peut être inspecté à l'aide de Wireshark ou d'outils similaires.

KEYSIGHT TECHNOLOGIES

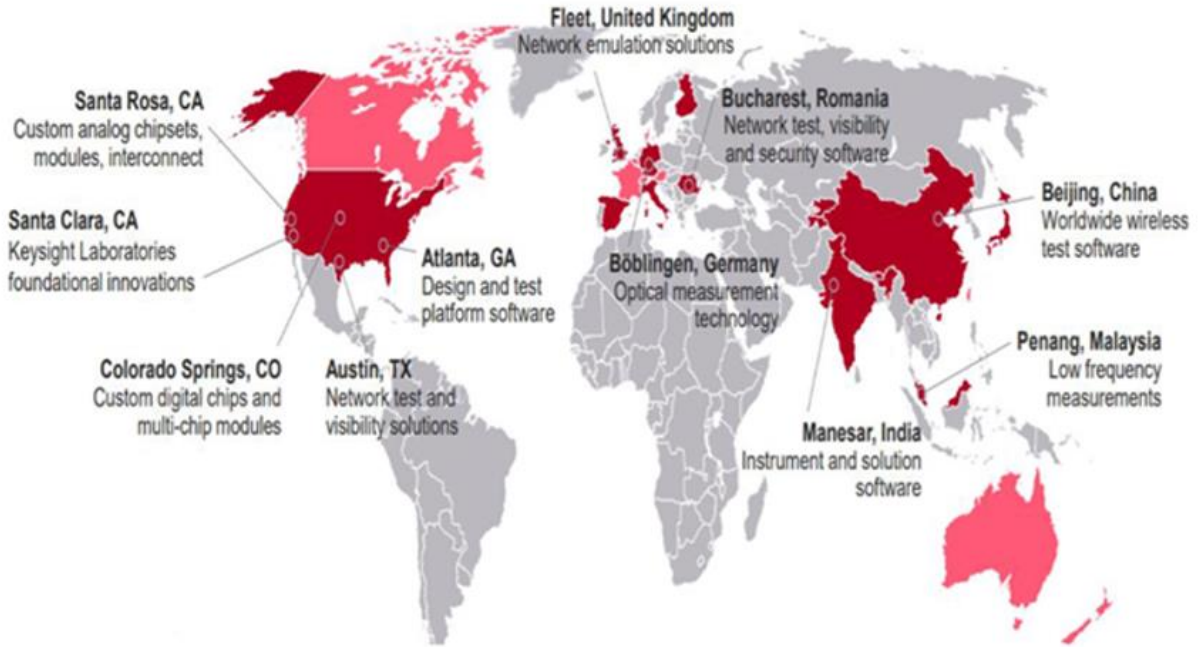
Visibilité pour surmonter les défis en maîtrisant les coûts.

ICS/OT SECURITY VISIBILITY REFERENCE ARCHITECTURE



POURQUOI KEYSIGHT

LA SEULE ENTREPRISE OFFRANT UNE VISIBILITÉ COMPLÈTE SUR LES RÉSEAUX IT, OT, CLOUD ET PRIVÉS, Y COMPRIS DANS DES ENVIRONNEMENTS INDUSTRIELS HOSTILES .



5.4Bn USD revenue
33Bn market capitalisation
14,300 employees
32,000 customers in 100+ countries

- 25 of 25 Top Auto electronics suppliers
- 25 of 25 Top Semiconductor suppliers
- 25 of 25 Top Engineering & Tech Uni's
- 29 of 30 Top Technology companies
- 24 of 25 Top Telecom equipment co's
- 23 of 25 Top Aerospace and Defence contractors.

- $700m annual R&D investment
- 13 R&D centres around the world
- 3,000 patents
- Strategic University Research

- Network and Mobile 5G, WIFI 6, 6G
- Driverless Vehicles and IoT
- Aerospace and Defence
- Quantum and next gen security


Merci pour votre temps !
KEYSIGHT
TECHNOLOGIES