

TECHNOLOGIES OPÉRATIONNELLES

Un système radar ne reçoit pas de mise à jour logicielle à 2 heures du matin. C'est bien là le problème.

Quelque part, sur une chaîne de production, en ce moment même, un automate fonctionne avec un micrologiciel vieux de dix ans, connecté à un réseau que tout le monde pensait isolé. Il fonctionne sans problème depuis des années. C'est précisément pour cette raison que personne ne l'a examiné de près.



La véritable exposition

En 2017, un logiciel malveillant baptisé Triton a été découvert sur les systèmes instrumentés de sécurité d'une usine pétrochimique en Arabie saoudite, les systèmes dont le seul rôle est d'arrêter un processus en toute sécurité lorsque quelque chose tourne mal. C'était la première attaque connue conçue spécifiquement pour désactiver le filet de sécurité lui-même, et non uniquement le processus qu'il protège. La fabrication pour la défense et la maintenance aérospatiale reposent sur la même catégorie de systèmes de contrôle critiques pour la sécurité.

01

Les technologies opérationnelles ont été conçues pour la disponibilité et la sécurité physique. —

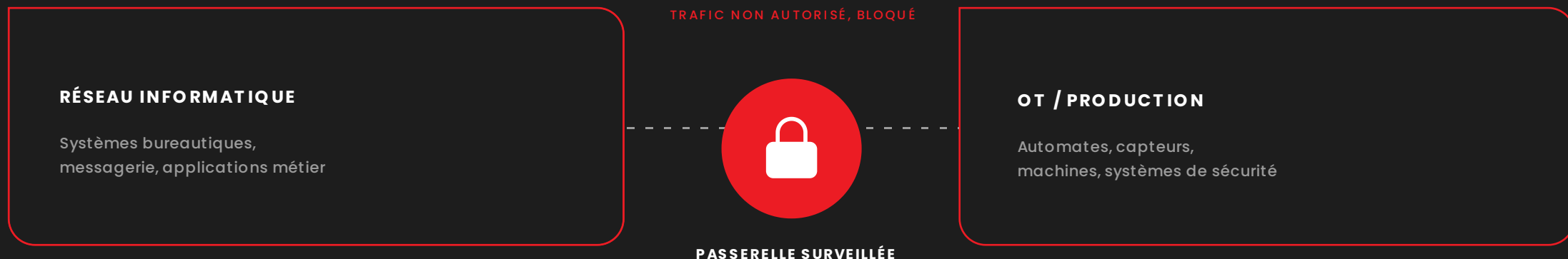
Les systèmes qui font tourner les radars, les chaînes de maintenance avionique, la fabrication d'armement et les chantiers navals n'ont pas été conçus pour un réseau hostile. À mesure que l'informatique et les technologies opérationnelles se connectent davantage l'une à l'autre, cet écart devient le point d'entrée.

2010

En 2010, Stuxnet a démontré qu'une attaque contre des équipements physiques n'a pas besoin de ressembler à une cyberattaque classique. Elle peut prendre la forme d'une vanne qui se comporte étrangement, ou d'une machine qui fonctionne légèrement hors tolérance.

02

L'écart entre l'informatique et les technologies opérationnelles que la plupart des environnements n'ont pas encore comblé. —



Pourquoi c'est important au salon AAD

La fabrication aéronautique et de défense repose sur des équipements qui n'ont jamais été conçus en pensant à un réseau hostile, et une grande partie ne peut pas être remplacée selon un cycle de renouvellement classique. Traiter la sécurité OT comme un simple prolongement de la sécurité IT passe à côté du problème. Nous travaillons sur le terrain, pas seulement dans la salle des serveurs, car c'est là que se situe la véritable exposition.

03

Ce que nous faisons

Nous évaluons et sécurisons les systèmes qui font tourner la production, la maintenance et la logistique, sans arrêter la chaîne pour autant.



Évaluations de sécurité OT et ICS/SCADA alignées sur la norme IEC 62443, menées par des personnes qui comprennent que sur une chaîne de production, la sécurité physique passe avant tout.



Conception de la segmentation réseau IT/OT, de sorte qu'une compromission du réseau bureautique ne puisse pas atteindre les systèmes qui comptent réellement.



Revue de risques sur les systèmes existants, pour les équipements qu'on ne peut pas simplement corriger, remplacer ou mettre hors ligne pour un scan.



Planification de la réponse aux incidents conçue spécifiquement pour les environnements de production, où l'arrêt se mesure en bien plus qu'en argent.

Un cycle de correctifs conçu pour des ordinateurs portables ne convient pas à une machine qui tourne depuis avant même l'existence d'internet.

Nous travaillons avec les équipements que vous avez réellement, pas avec ceux qu'un référentiel générique suppose que vous avez.

DISystems – Conseil en cybersécurité et GRC en Afrique du Sud, dans la région de la SADC et à l'international, en partenariat avec **Cyberantix™**

CONTACTEZ-NOUS À L'ADRESSE :
tsepang@disystems.co.za
 pour convenir d'un rendez-vous et en savoir plus.

