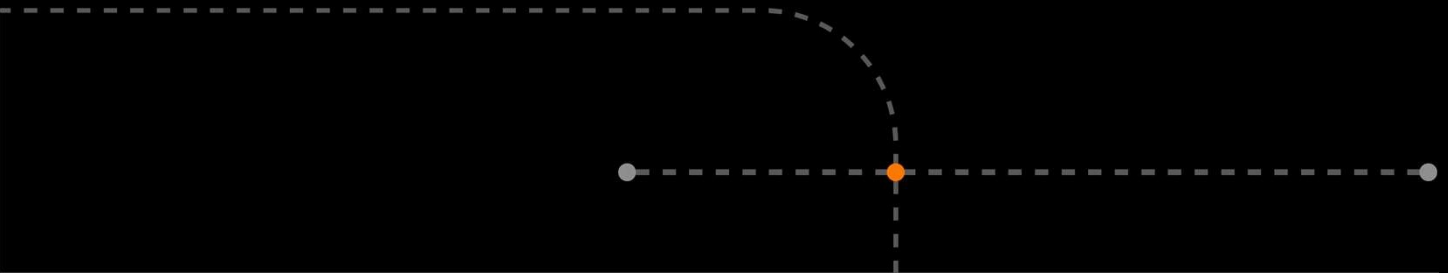
Orange
Cyberdefense

Cybersécurité et Industrie



orange™

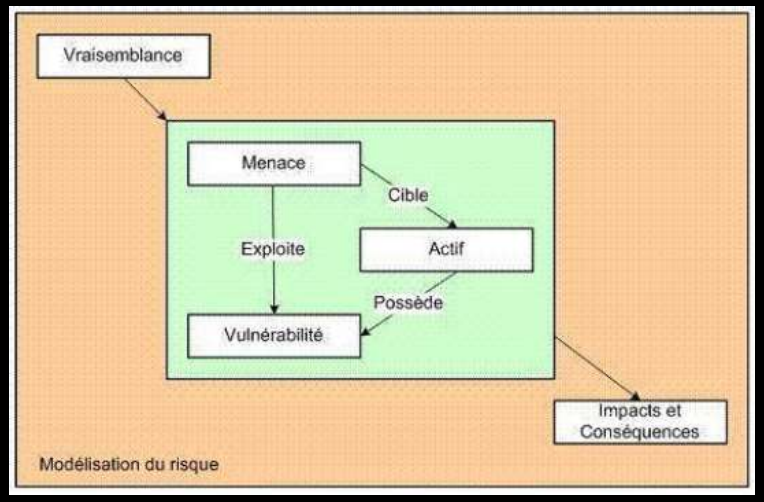
Les besoins

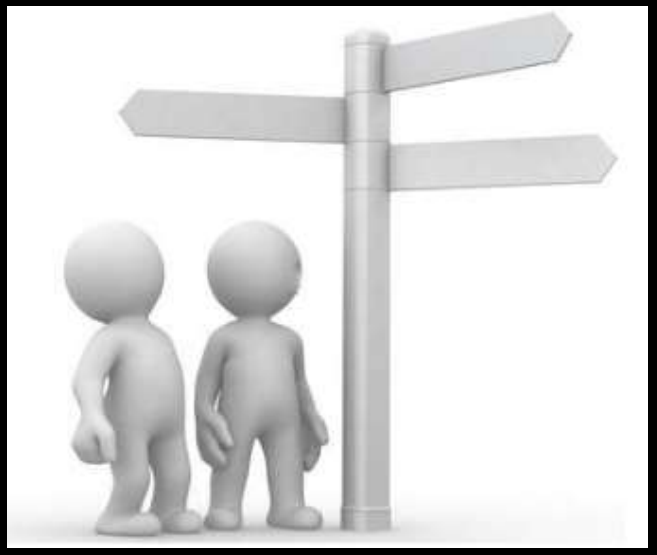
- La qualification des besoins de sécurité peut dépendre de nombreux facteurs, qu'ils soient économiques, juridiques, etc.

- **Intégrité**
- **Confidentialité**
- **Disponibilité**
- **Traçabilité**

Les besoins

- La sécurité est un centre de coûts qu'il faut maîtriser
- Il doit être pris en compte dès le début du projet
- Le design doit répondre aux besoins



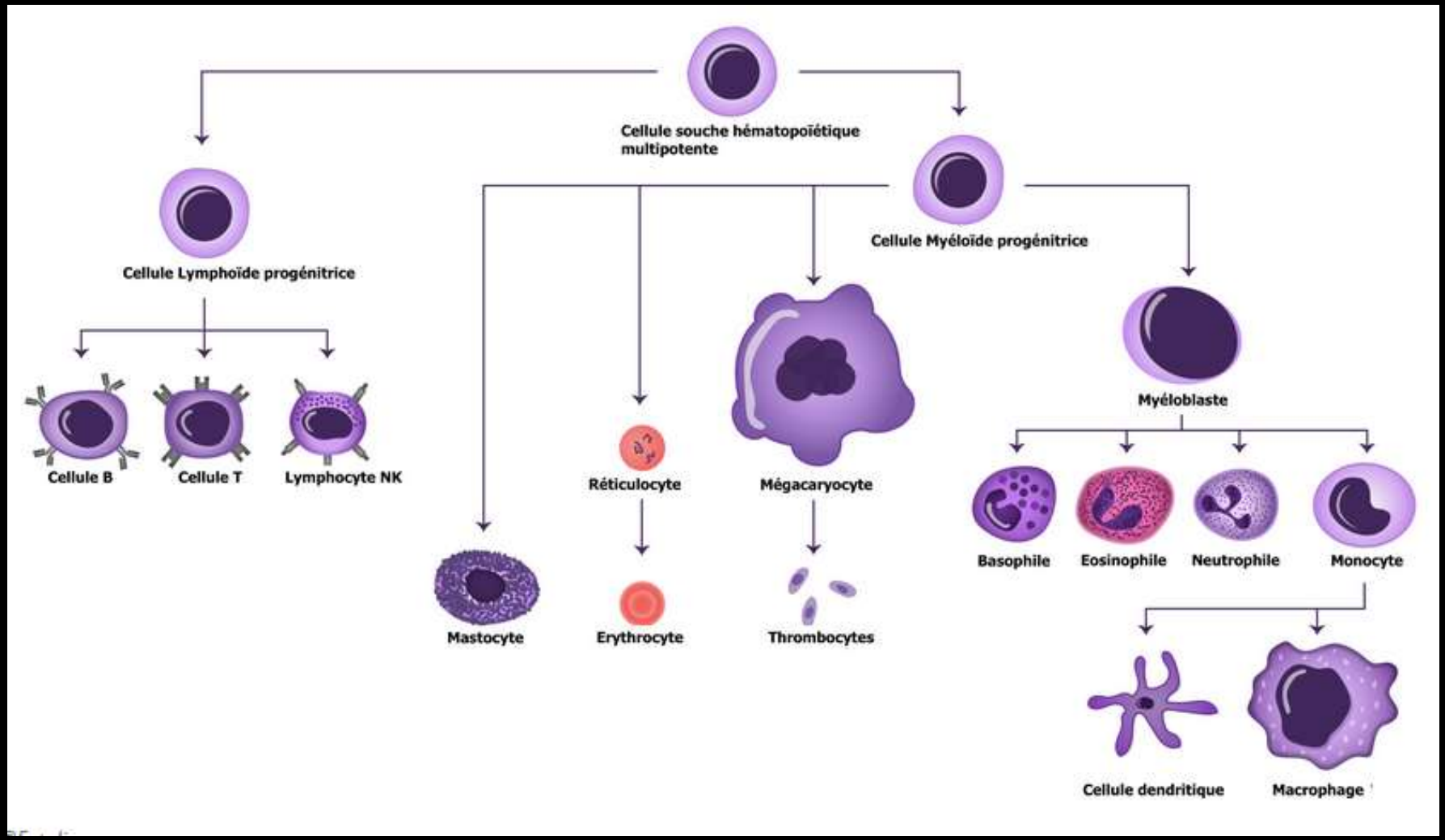


Commençons par le début…

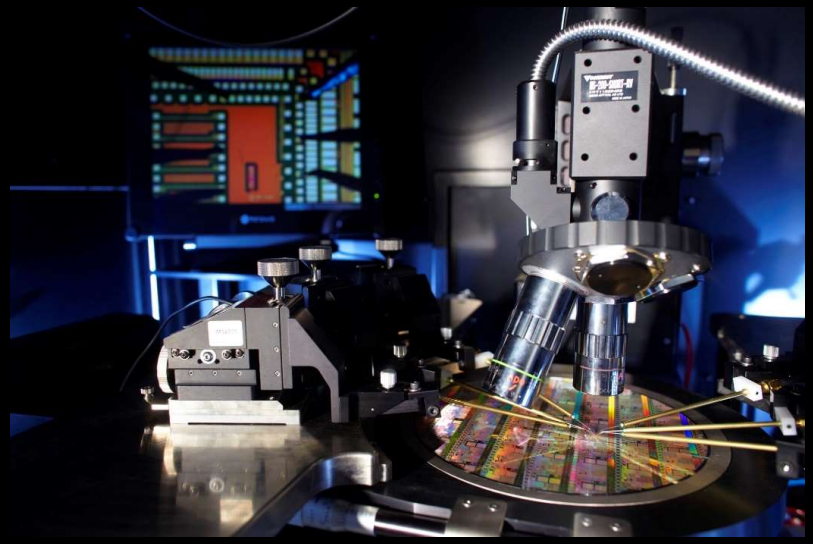
- Il y a 13,8 Milliards d'années

- Il y a 70 ans

Petite comparaison


Cellule souche hématopoïétique multipotente
Cellule Lymphoïde progénitrice
Cellule Myéloïde progénitrice
Cellule B
Cellule T
Lymphocyte NK
Réticulocyte
Mégacaryocyte
Myéloblaste
Mastocyte
Erythrocyte
Thrombocytes
Basophile
Eosinophile
Neutrophile
Monocyte
Cellule dendritique
Macrophage

Mesure de protection



- Détection des changements matériels
- Calculs désynchronisés
- Ajout de senseur qui détecte les attaques par perturbations
- Sécuriser le microcode (HCODE)
- Durcir la couche logicielle
- Effectuer une veille technologique (I'M TECH, HackerNews,…)

Les applications

Les applications

Les applications

L'intelligence artificielle (IA) est « **l'ensemble des théories et des techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence** »

Merci Wikipédia ☺

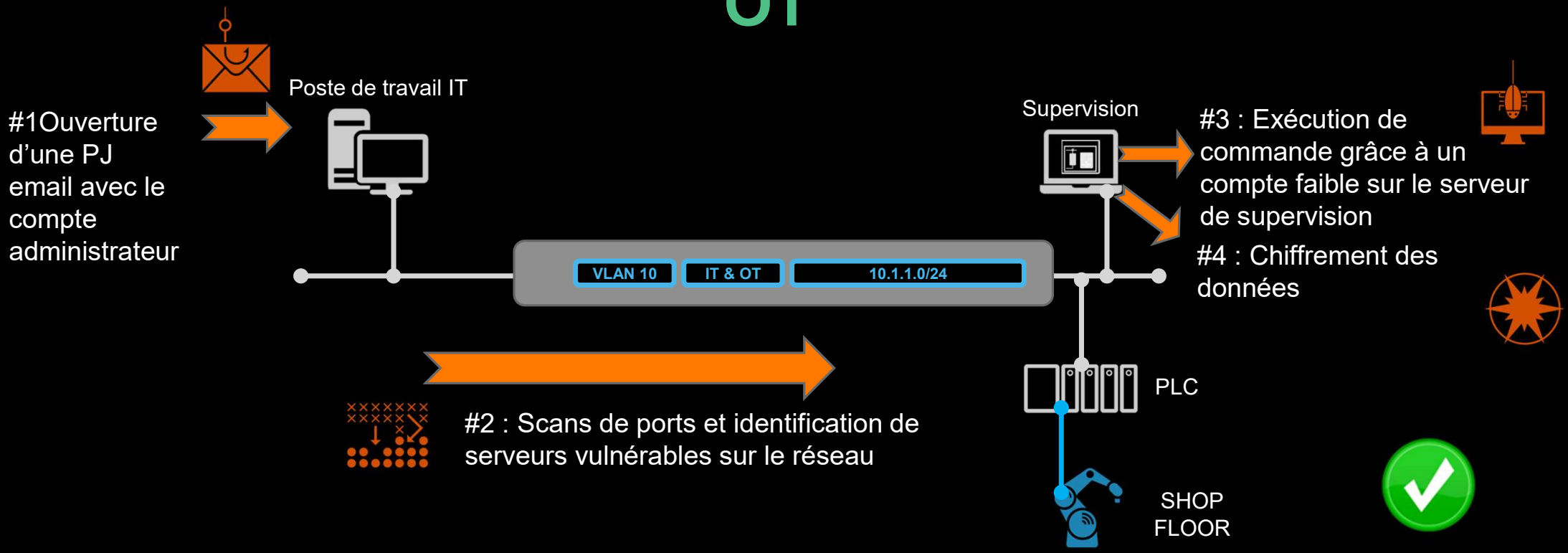
Les applications

Machine Learning

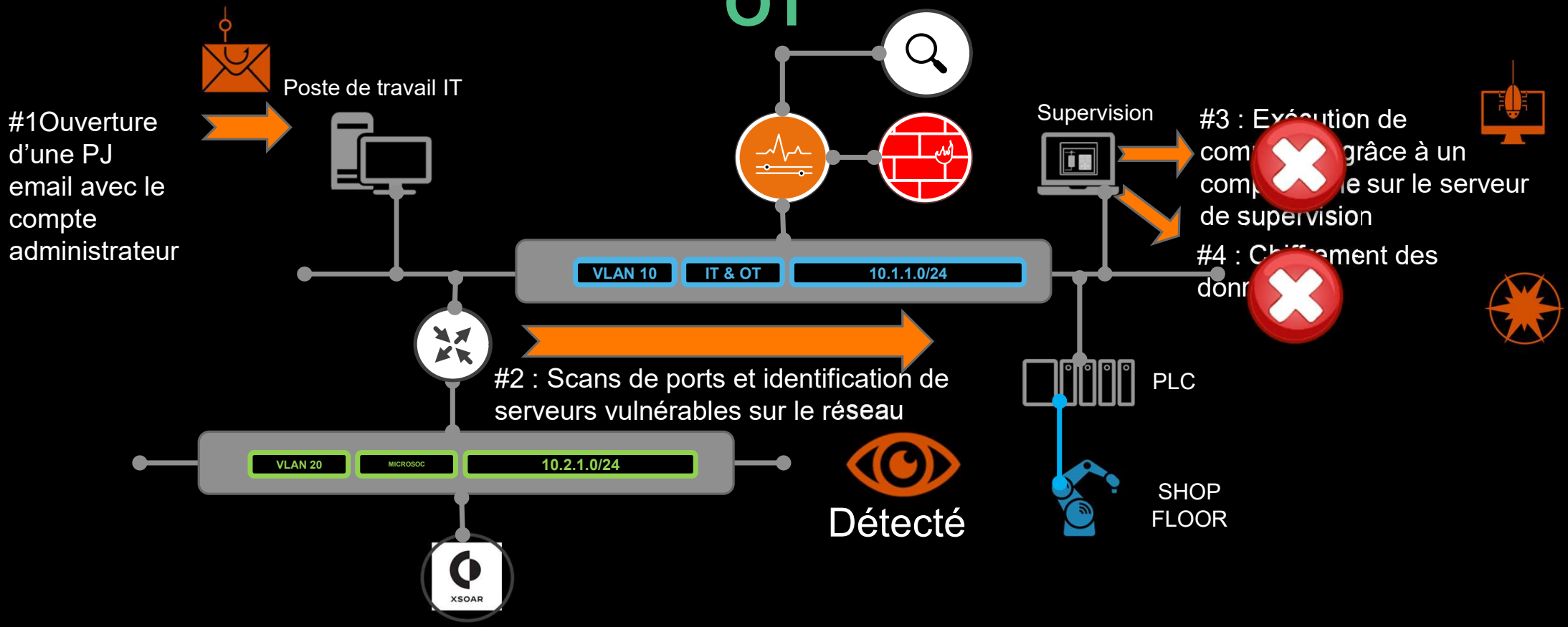
Deep Learning

Décision : communication et/ou application

Scénario #1 : Type ransomware avec impact OT



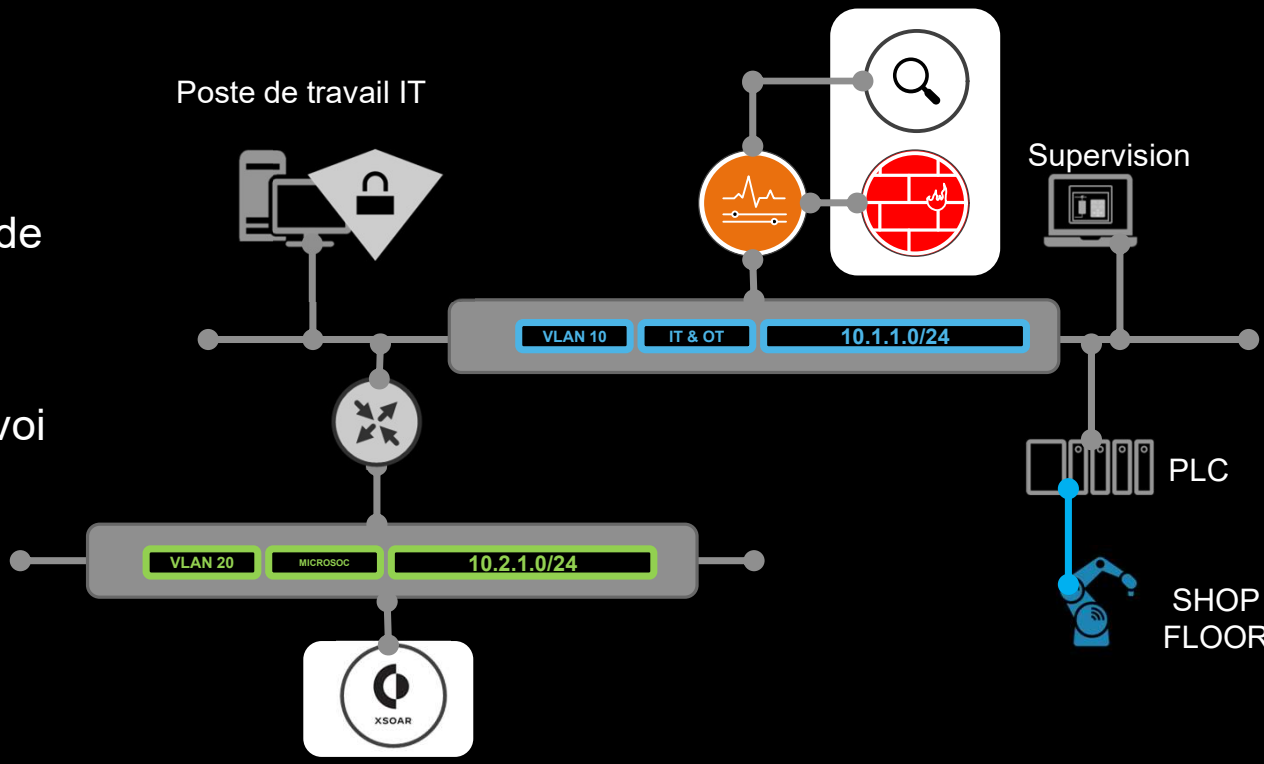
Scénario #1 : Type ransomware avec impact OT



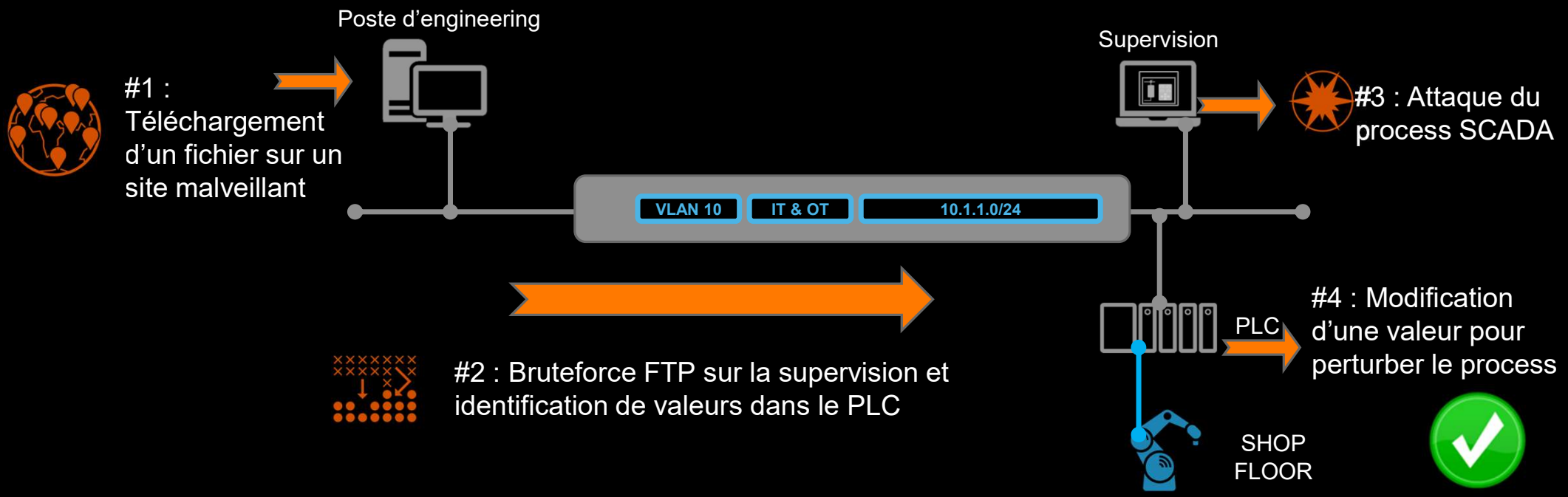
Que s’est-il passé ?

1- La sonde Nozomi remonte une alerte lors de l’identification de scan de port.

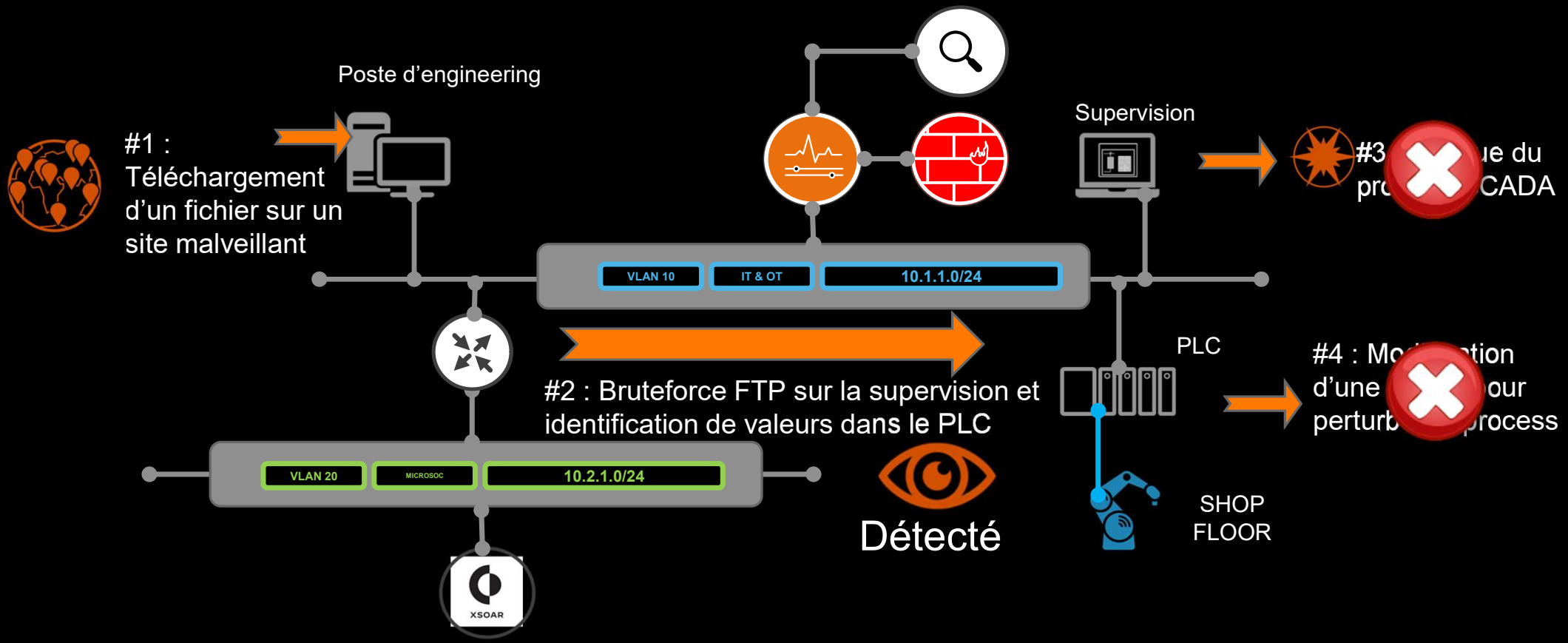
2- Le XSOAR récupère l’alerte et envoi l’ordre au firewall d’isoler la machine effectuant ces scans



Scénario #2 : Type attaque ciblée OT



Scénario #2 : Type attaque ciblée OT



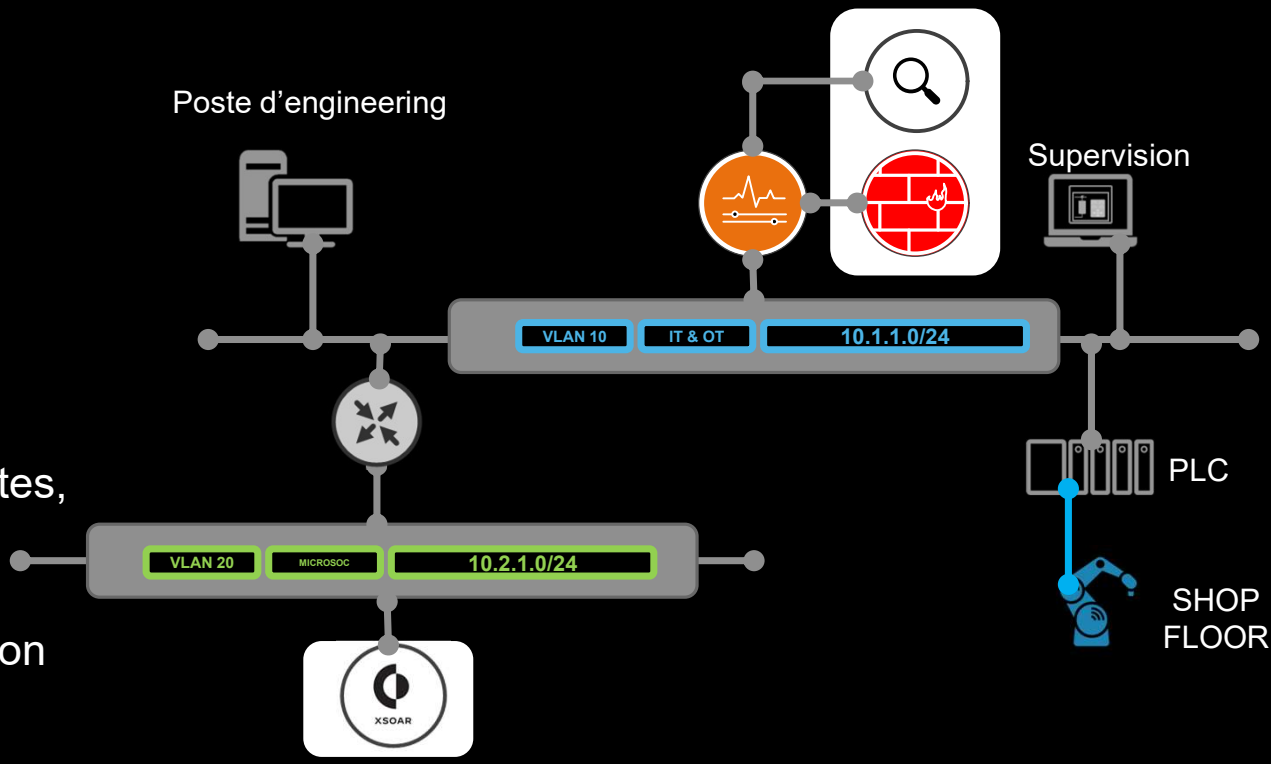
Que s’est-il passé ?

Nozomi remonte une alerte lors des deux actions suivantes :

- Bruteforce FTP
- Identification de valeur dans l’automate

Lorsque le XSOAR récupère les alertes, il effectue les actions suivantes :

- Changement de politique firewall permettant le blocage des connexion modbus et SMB



Type d’attaque

Phishing

Intrusion physique

Mail

Attaque Radio

Phoning

Réseaux Sociaux

Réseaux Industriels

Web

Exemples d’attaque

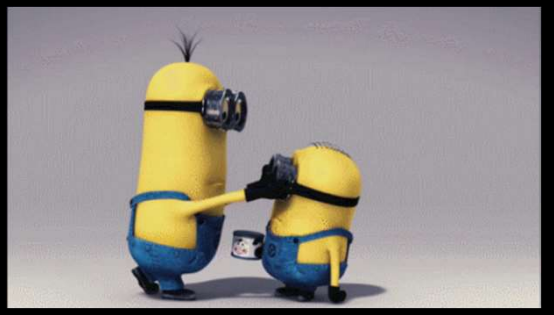
L'eau d'une station d'épuration manipulée par des hackers

Par Arnaud Devillard le 28.03.2016 à 16h48, mis à jour le 28.03.2016 à 16h48

L'opérateur de télécommunications américain Verizon révèle dans un rapport une cyberattaque ayant touché à la composition et à la distribution d'eau potable d'une station. Le système informatique était perclus de failles.

Une plainte déposée après une cyberattaque au CHU de Rouen

Ce qu'il faut retenir



- La sécurité parfaite n'existe pas
- La sécurité doit être pensé en amont
- La sécurité peut vous rapporter de l'argent (ou du moins, permet de ne pas en perdre ☺)
- Les attaques utilisant l'ingénierie sociale fonctionne presque à tous les coups

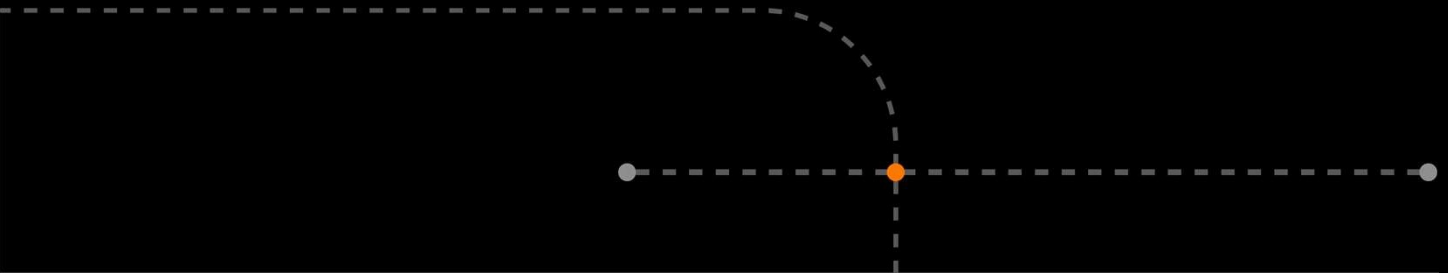
« Un ordinateur sécurisé est un ordinateur débranché et stocké dans un entrepôt vide » Ramy Badir

« Il est toujours possible de trouver une personne assez aimable pour brancher l'ordinateur.» Kevin Mitnic

Orange
Cyberdefense

Merci

orangecyberdefense.com



orange™