Fiche produit

Xplore.

See-First Intelligence

Xplore.

Solution de visibilité, de cartographie et de détection pour les réseaux industriels et les systèmes critiques.

ON NE PEUT PROTÉGER QUE CE QUE L'ON CONNAÎT

Une vue complète et à jour de l'infrastructure opérationnelle est nécessaire pour lancer toute démarche de cybersécurité industrielle. Xplore établit l'inventaire exhaustif des actifs OT, cartographie les flux réellement observés et identifie les vulnérabilités des systèmes.

DÉCOUVERTE NON INTRUSIVE PAR CONCEPTION

Xplore analyse une copie du trafic réseau, sans injection de paquets, ou installation d'agent lourd. L'inventaire est complété grâce à des scripts et exécutables légers, maîtrisés (SAE). Les opérations sont ainsi préservées, y compris sur les équipements anciens ou fragiles.

UNE MONTÉE EN MATURITÉ PROGRESSIVE

Audit nomade en quelques heures, puis cartographie continue et monitoring avant supervision avancée des attaques. Le même logiciel couvre les trois phases, sans investissement monolithique. Les données du premier jour alimentent les baselines de détection.

DÉCOUVERTE OT NON INTRUSIVE
- Analyse passive du trafic
- Collecte maîtrisée

CARTOGRAPHIE OT LA PLUS COMPLÈTE DU MARCHÉ
- Vues logique, Purdue, réseau, métier, géographique
- Matrice des flux exhaustive

MODE AUDIT OU SUPERVISION
- Déploiement nomade
- Sondes fixes, suivi continu

DÉTECTION BOOSTÉE PAR IA
- 4 moteurs complémentaires
- Analyse comportementale
- Alertes contextualisées

CONFORMITÉ
- NIS2
- IEC 62443

Conception et développement en France.

Le Brain

- Centralisation et analyse temps réel du trafic des sondes
- Interface d'administration et de visualisation intégrée
- Injection locale de fichiers de capture de trafic (PCAP) pour les sites totalement isolés
- Bac d'alertes et bac de vulnérabilités embarqués
- Déploiement sur appliance physique ou virtuelle

Sondes de collecte passive

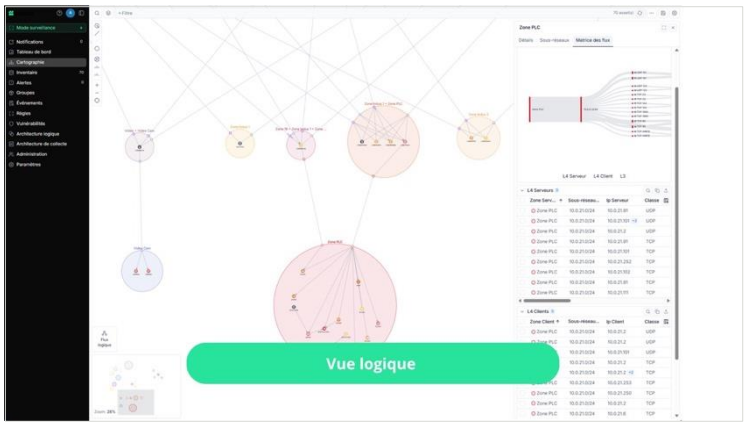
- Sondes matérielles ou virtuelles
- Collecte via port mirroring (SPAN, RSPAN, ERSPAN) ou TAP réseau
- Copie du trafic, sans interaction avec les équipements
- Support de tunneling VLAN et GRE pour déporter la sonde
- Support des flux IPFIX et NetFlow
- Écoute dans le domaine de broadcast

Enrichissement et sites isolés

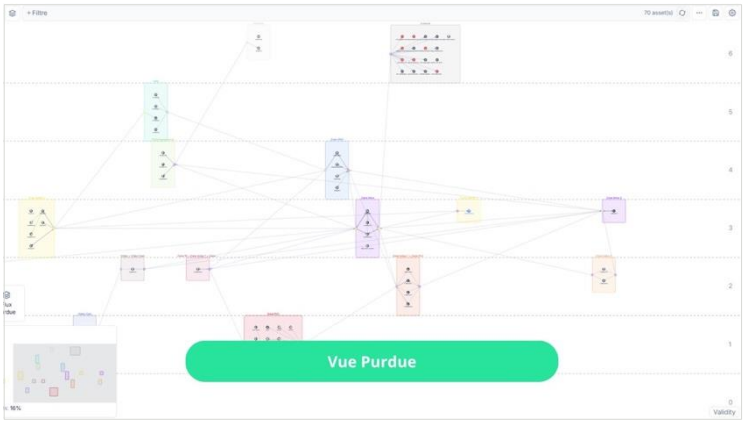
- SAE-N : récupération de la localisation des actifs sur les ports physiques des switches
- SAE-S : recensement des applications installées, des logiciels vulnérables et inventaire des périphériques USB
- SAE-dv : enrichissement sur DeltaV
- Collector (boîtier de collecte à faible coût), pour les petits sites isolés ou déportés

Cartographie multi-vues.

Cinq représentations natives du réseau, générées à partir des mêmes données. Chaque vue s'adresse à des profils métier différents et s'exporte au format Draw.io ou Visio.



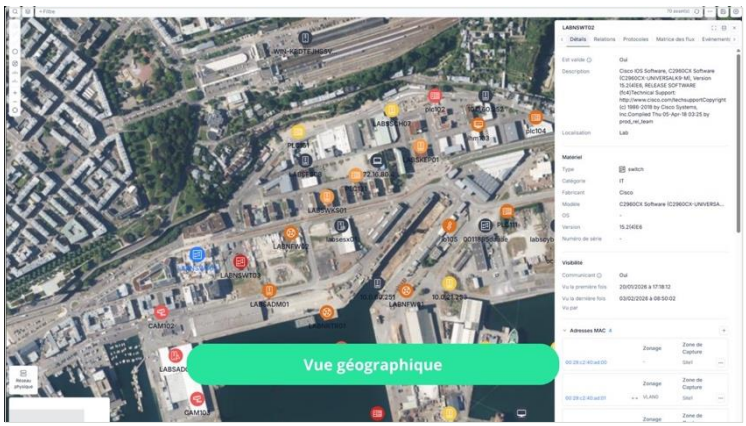
Affiche les différentes zones réseau avec leurs équipements et les flux entre ces zones (ou entre équipements).



Organise la cartographie selon le modèle IEC 62443, pour automaticiens et responsables OT.

Permet de créer et visualiser des zones fonctionnelles liées au métier, pour les équipes opérationnelles.

Affiche un mix entre la vue Purdue et une vue réseau classique, intégrant la détection des routeurs et firewalls.



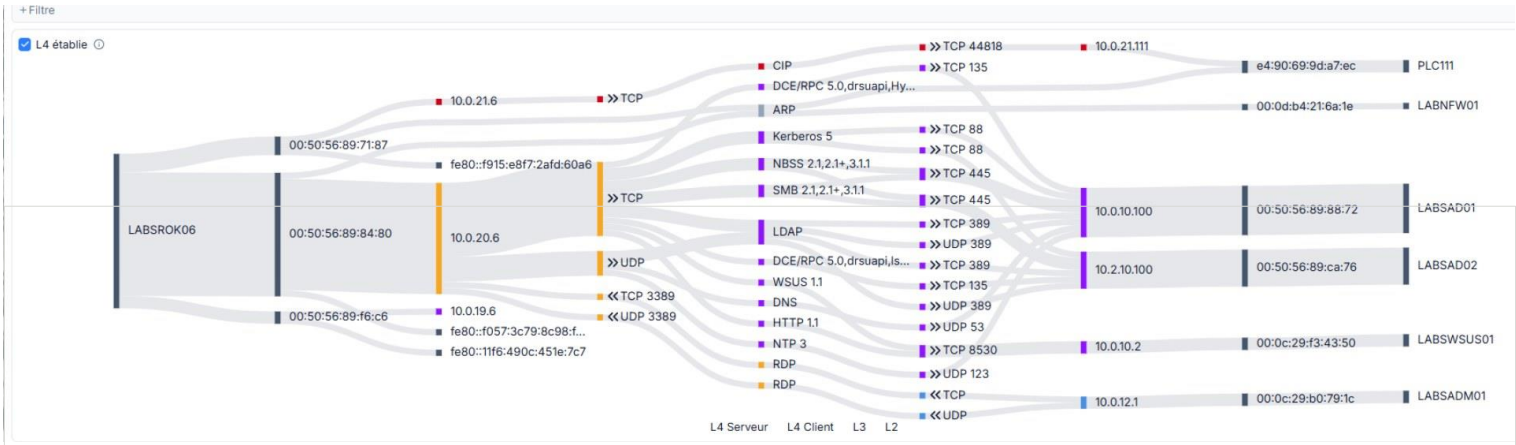
Localise physiquement les équipements critiques ou vulnérables pour les responsables de site et responsables OT.

Une seule donnée, cinq lectures

- Les cinq vues sont générées automatiquement ou manuellement à partir du même jeu de données
- Xplore fonctionne en cœur de réseau, sur les réseaux non routés et sur les périmètres isolés
- Les configurations de firewalls et de switches peuvent être injectées comme référence
- Xplore distingue alors le supposé connu du réellement observé
- Export Draw.io et Visio pour les projets de migration ou de remédiation

Matrice des flux.

Xplore restitue les communications réellement observées sur le réseau. Pour chaque actif, zone ou lien, Xplore affiche les équipements en communication. Les protocoles apparaissent avec le sens de chaque échange et les zones impliquées. La décomposition OSI va de la couche de liaison de données jusqu'à la couche applicative. Les matrices de flux des différents conduits peuvent servir de base aux revues régulières de règles de pare-feu.



Décomposition des communications d'un actif, de la couche 2 à la couche applicative, avec le sens de chaque échange.

Gestion des risques.

Inventaire orienté risques

- Vue d'inventaire tabulaire, triable et filtrable par type de matériel, mainteneur, criticité, vulnérabilités, année d'achat…
- Risque évalué selon plusieurs critères : impacts métier ou opérationnels, disponibilité, traçabilité, priorité de récupération…
- Vulnérabilités identifiées grâce aux métadonnées de la collecte passive ou par enrichissement
- Liste des vulnérabilités partageable avec un SOC, un VOC ou un gestionnaire de vulnérabilités

Chemins d'attaque, priorisation

- Identification des actifs vulnérables, par code couleur dans la cartographie
- Chemins d'attaque réalistes visibles directement dans les vues
- Détection des accès distants non autorisés ou des machines avec un double attachement réseau
- Patch management contextuel, basé sur la cartographie
- Identification des actifs vitaux à isoler en priorité et génération automatique des configurations d'isolation pour Seclab Xchange

Protocoles analysés

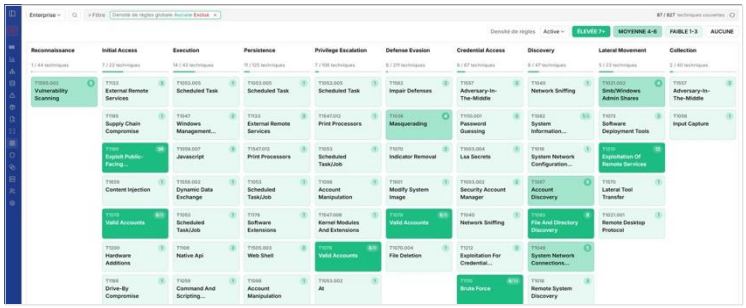
- Protocoles IT standards
- Protocoles industriels comme Modbus TCP/RTU, S7comm, EtherNet/IP, OPC-DA et OPC-UA, BACnet, DNP3, IEC 60870-5-104, PROFINET, et bien d'autres.
- Protocoles de niveau 2 non routés également pris en charge, par écoute dans les domaines de broadcast
- Flux IPFIX et NetFlow

Détection intelligente.

Xplore repose sur quatre moteurs de détection complémentaires, rattachés à des tags MITRE ATT&CK pour offrir une vue synthétique de la couverture de détection. La philosophie de Xplore est de partir des événements redoutés et des données cartographiques pour cibler un jeu de règles pertinent et maîtrisable dans le temps.

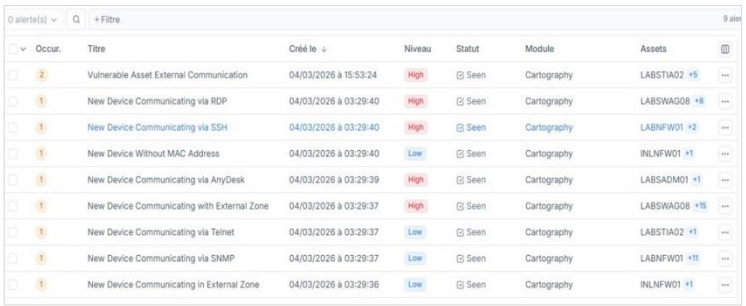
Les quatre moteurs de détection

Détection cartographique	Surveille la stabilité de l'environnement : nouveaux équipements, changements de configuration, adresses IPv6 inattendues, écarts à la baseline, connexions vers des zones Internet. Les règles peuvent être construites directement depuis la cartographie.
Signatures Sigma	Moteur de détection basé sur un format reconnu du monde système, étendu par Seclab au réseau. Lisible, documentable et annotable, il reste compréhensible par les équipes OT.
Signatures Suricata	Moteur Suricata exécuté en parallèle. Xplore contextualise l'alerte avant transmission au SOC. Une adresse IP seule n'a aucun sens pour un analyste extérieur qui ne connaît pas l'usine ou le processus industriel concerné.
Comportemental IA	Apprentissage automatique des patterns habituels du réseau et identification des déviations. S'appuie sur la stabilité caractéristique des environnements industriels.



Couverture MITRE ATT&CK

Densité de règles par tactique et par technique, pour piloter la couverture réelle.



Bac d'alertes contextualisées

Chaque alerte porte ses assets, sa zone et son moteur de détection d'origine.

Alertes, routage et forensic

- Bac d'alertes autonome, ou transmis vers un SIEM externe
- Routage par nature et criticité des alertes vers le bon interlocuteur
- Enregistrement continu des flux, PCAP récupérable depuis une alerte pour analyse forensic.

Livrables de conformité

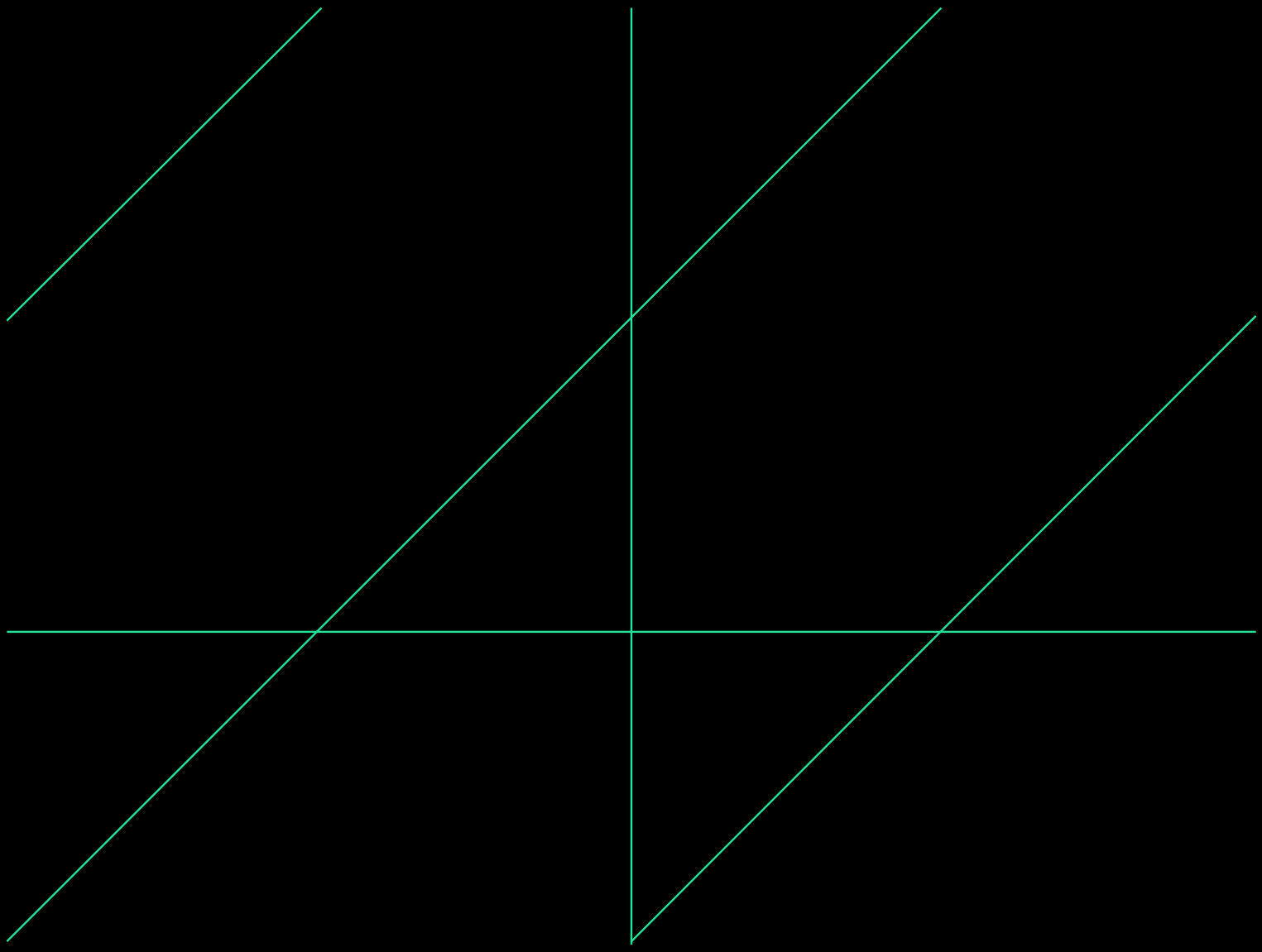
- NIS2 : inventaire auditable, cartographie documentée, analyse de segmentation, traçabilité
- IEC 62443 : vue Purdue, zones et conduits
- LPM : rapports d'audit consolidés et couverture MITRE ATT&CK

Écosystème

- Intégrations : firewalls, SIEM, SOC, bastions, PAM, IAM, CMDB
- Composant de la plateforme Xcore de Seclab comprenant Xchange pour l'isolation physique des réseaux et Xport pour le contrôle des accès USB.

seclab®

Next-Gen OT
Cybersecurity Platform



205 impasse John Locke
34470 Pérols, France.

seclab-security.com