



SecureProd

SecureProd Morocco

AI-Powered Protection for Moroccan Industry

Industrial Cybersecurity 4.0



Sécurité Industrielle Marocaine

SecureProd

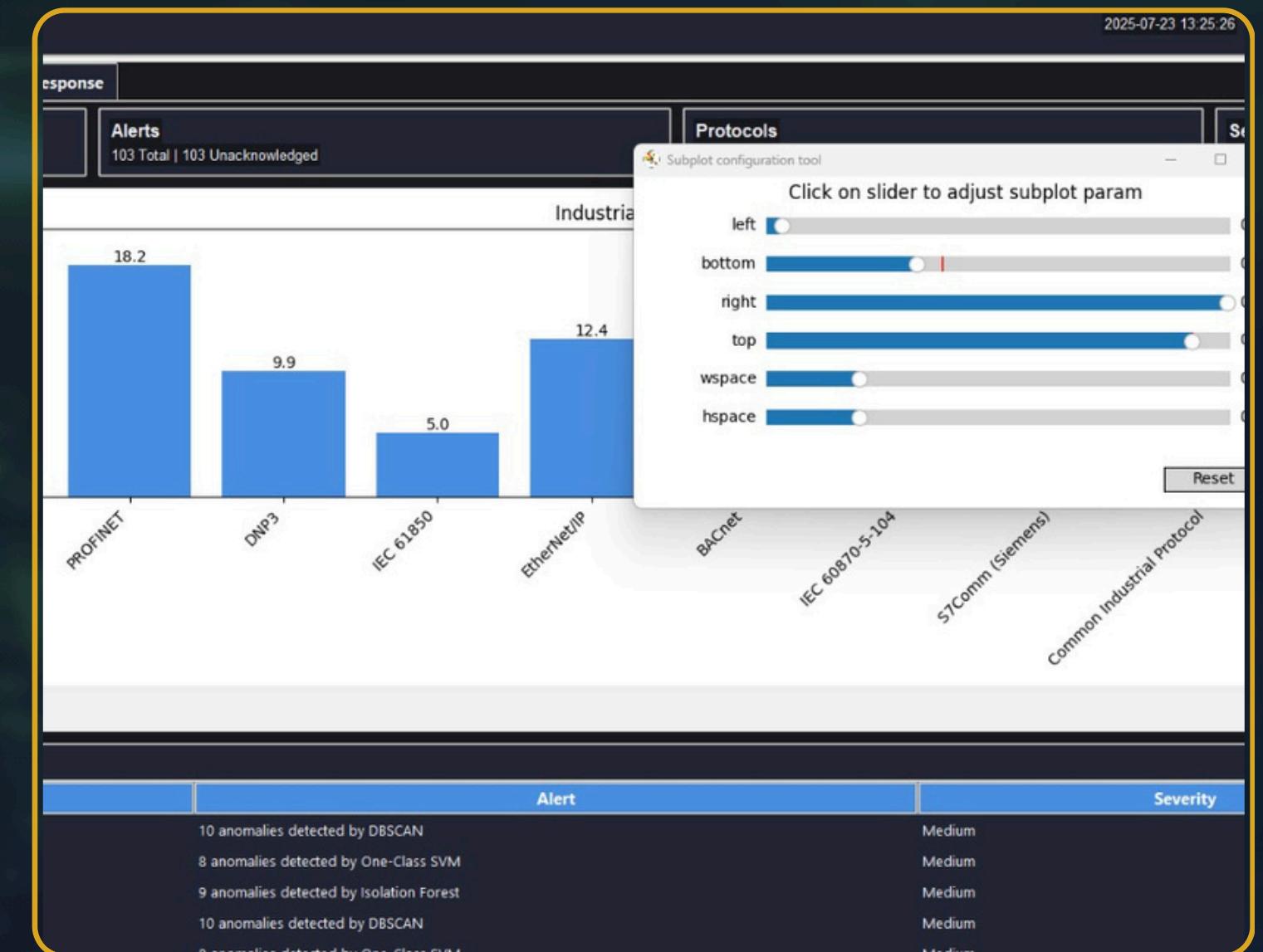
Plateforme de défense cyber avancée pour les environnements industriels, propulsée par l'intelligence artificielle et l'apprentissage supervisé

Cybersecurity Challenges

- Augmentation de 54 % des attaques SCADA/ICS
- Protocoles vulnérables : Modbus TCP et DNP3
- Manque d'expertise locale en cybersécurité des systèmes industriels (OT)

SOLUTION

- Détection d'anomalies par IA
- Protection multi-protocoles
- Visualisation 3D des menaces
- Rapports de sécurité automatisés



Paysage des Menaces Industrielles



Injection de Commandes Modbus

Manipulation des registres et fonctions

Critique



Usurpation de Serveur OPC UA

Certificats falsifiés et connexions non autorisées

Élevé



Arrêt CPU S7Comm

Code fonction 0x29 non autorisé

Critique



Usurpation GOOSE IEC 61850

Paquets multicast anormaux

Élevé



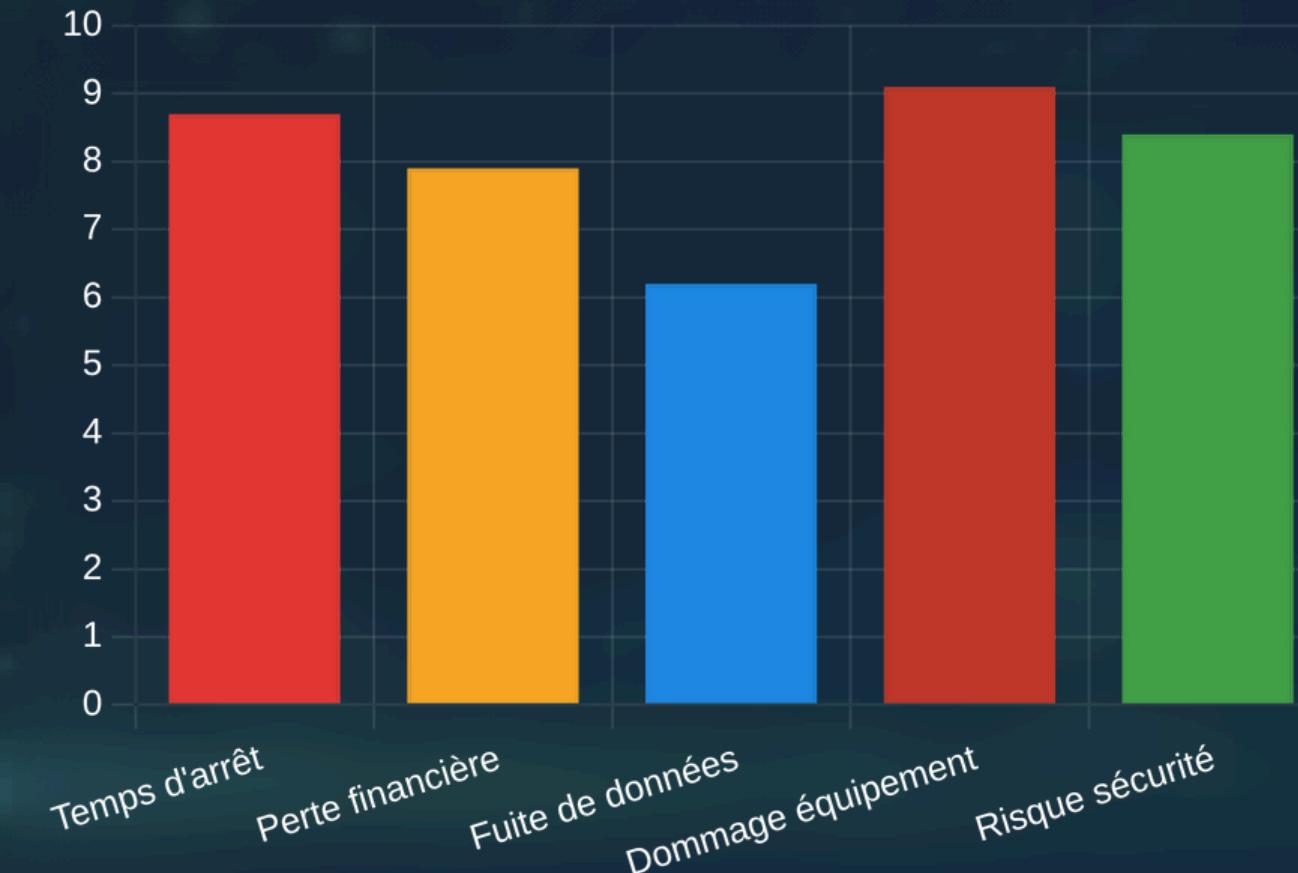
Attaque DoS DNP3

Fragments de couche application malformés

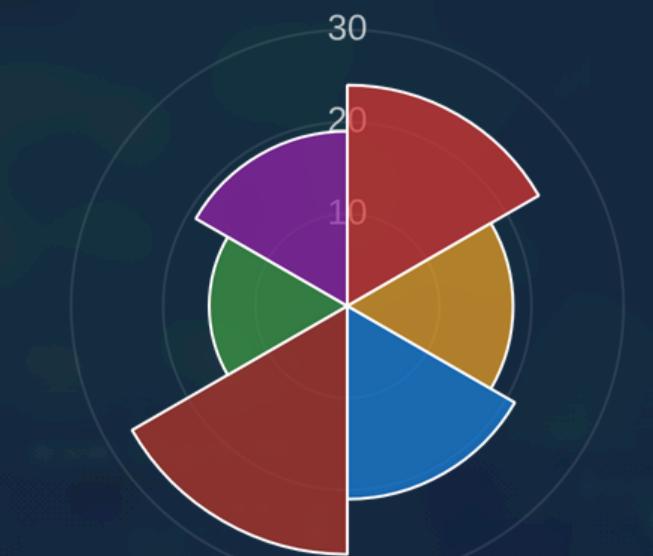
Critique

Source: Analyse des attaques industrielles détectées par ScureProd, 2025

Impact des Cyberattaques



Vulnérabilités par Protocole



- Modbus/TCP
- OPC UA
- DNP3
- S7Comm
- IEC 61850
- EtherNet/IP

Source: Base de données CVE et rapports ScureProd, 2025

Défis de Détection Industrielle



Signatures d'attaques inconnues

Les attaques zero-day contournent les défenses basées sur signatures



Trafic industriel hétérogène

Multiples protocoles propriétaires et formats de données



Faux positifs coûteux

Les alertes erronées provoquent des arrêts de production inutiles



Temps de détection critique

Chaque minute compte dans les environnements OT

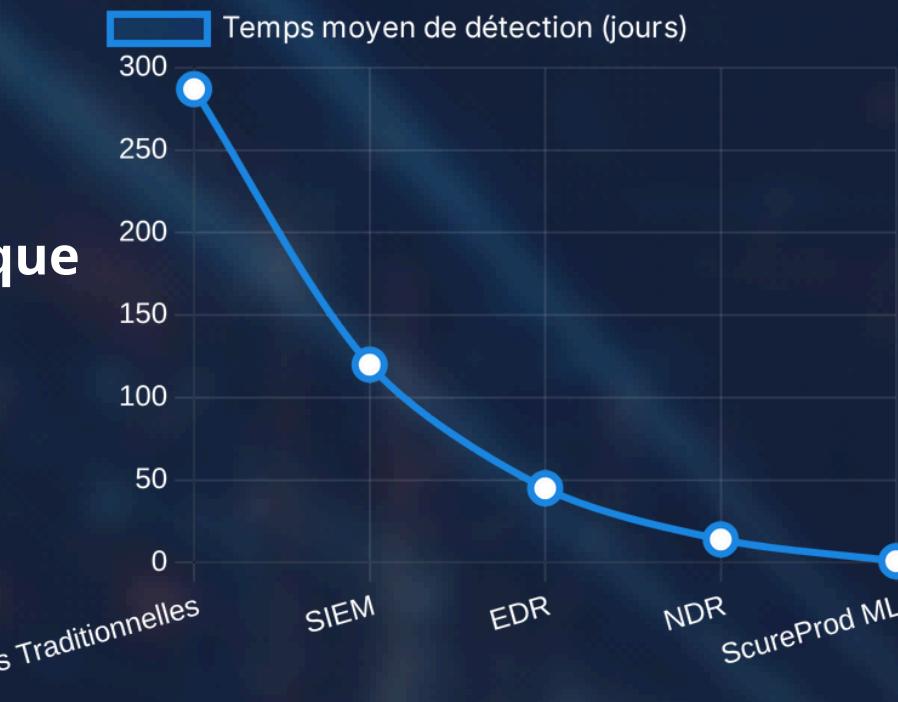


Systèmes legacy vulnérables

Équipements anciens sans capacités de sécurité modernes

Cycle de Vie d'une Attaque

Chronologie de Détection



Reconnaissance

Scan des ports et énumération des protocoles industriels

Jour 0

Accès Initial

Exploitation des vulnérabilités des protocoles

Jour 1-7

Persistante

Installation de backdoors et modification des configurations

Jour 8-30

Impact

Manipulation des commandes et sabotage des processus

Jour 30+

Solution Alimentée par l'IA



Système de Défense à 3 Couches

Intelligence Artificielle

Machine Learning

Python



Déetecter

Détection d'anomalies par IA/ML qui identifie les comportements suspects dans les systèmes industriels en temps réel.

94.7% précision

Apprentissage supervisé



Prévenir

Automatisation Zero-Trust qui applique des politiques de sécurité strictes et isole les systèmes compromis.

Segmentation automatique

Prévention proactive



Répondre

Playbooks d'incidents qui orchestrent la réponse aux menaces avec des procédures automatisées et guidées.

40% réponse plus rapide

Orchestration Python

Intelligence des Menaces Marocaines

94.7%

Précision

Modèles entraînés sur des données locales

Apprentissage Automatique Supervisé

1 Collecte de Données

Trafic réseau industriel, journaux d'événements



2 Prétraitement

Normalisation, NLP arabe/français



3 Entraînement du Modèle

Classification, détection d'anomalies

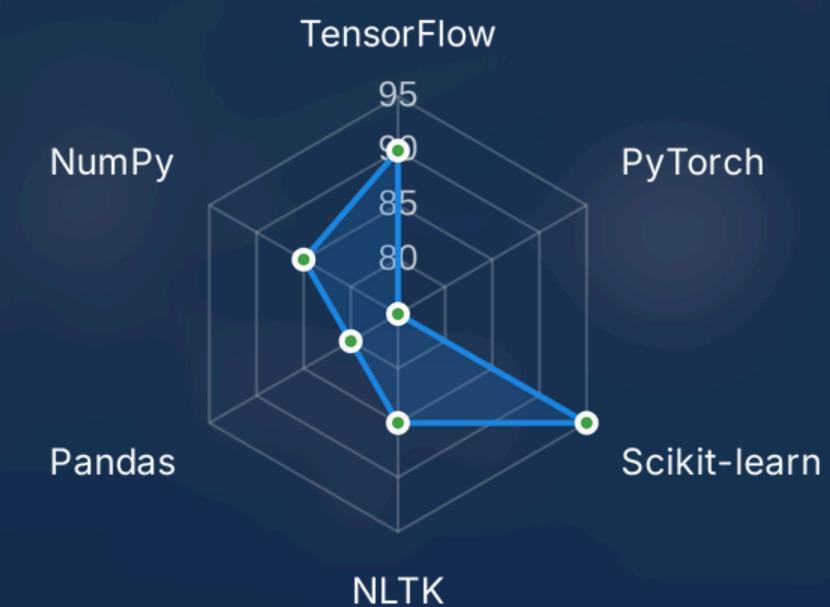


4 Validation & Déploiement

Tests sur données marocaines, API



Technologies Python



Architecture Technique



Python 3.11

Langage principal pour le backend et l'IA



scikit-learn & TensorFlow

Bibliothèques d'apprentissage automatique



Matplotlib & D3.js

Visualisation de données avancée



Scapy & pymodbus

Analyse et manipulation des protocoles industriels



Tkinter & OpenGL

Interface utilisateur et rendu 3D

Source: Documentation technique ScureProd, 2025

Pipeline de Données



Architecture en Couches



Interface Utilisateur

Dashboard

Alertes

Rapports



Logique Métier

Détection

Analyse

Réponse



Données & IA

Modèles ML

Stockage

Historique



Connecteurs Industriels

Modbus

OPC UA

DNP3

Surveillance en Temps Réel



Capacités de Détection

- Visualisation du trafic des protocoles**
Mesure en paquets par minute (pkts/min)
- Détection d'anomalies en temps réel**
Identification des pics de trafic anormaux
- Isolation automatique des menaces**
Réponse immédiate aux incidents détectés
- Analyse historique des tendances**
Identification des modèles de comportement

Statut des Protocoles

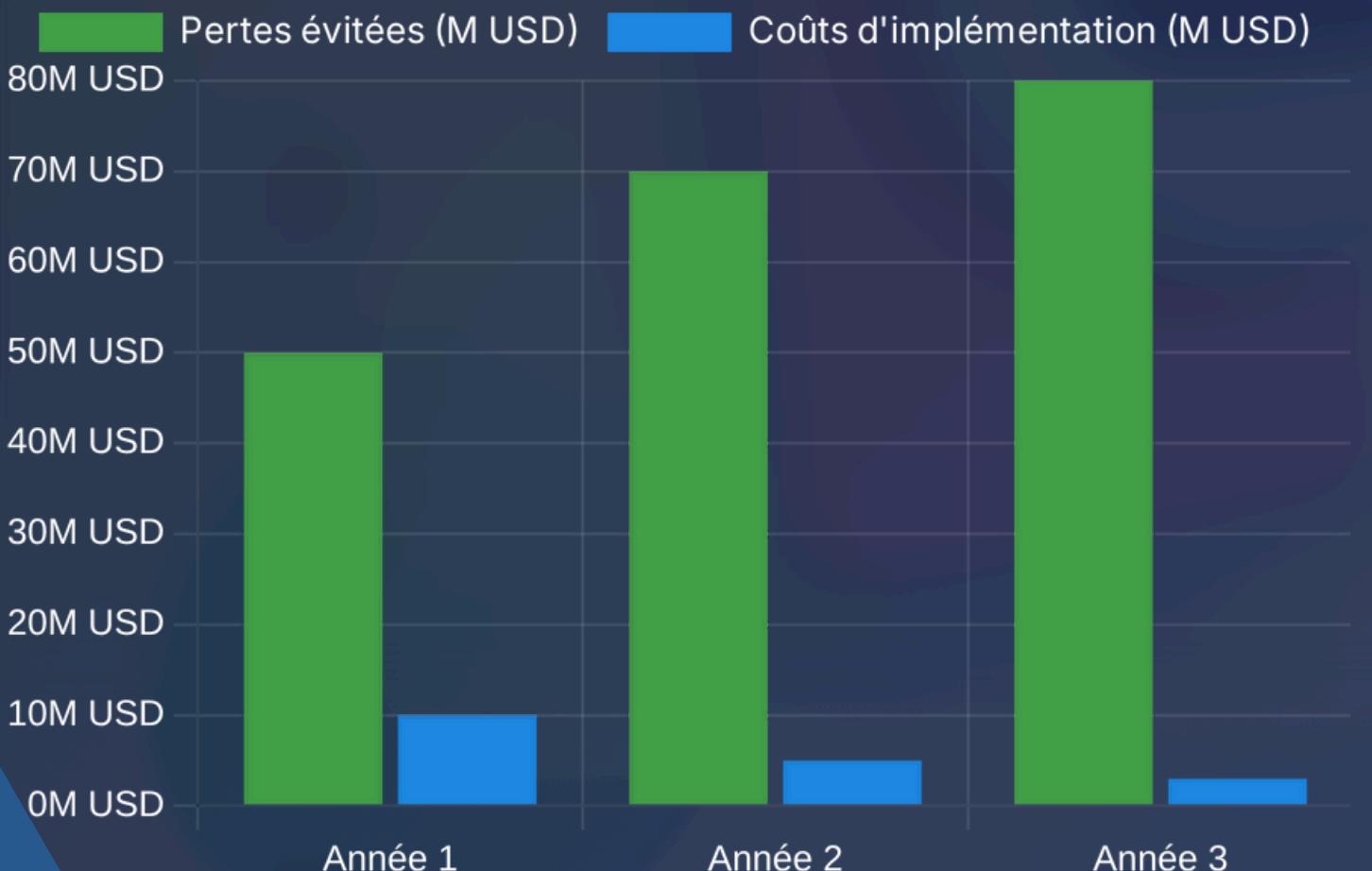
Normal	OPC UA	Normal	Modbus/TCP
Alerte	DNP3	Normal	PROFINET

Impact Potentiel

~200M USD

Pertes économiques annuelles évitables

(Secteur manufacturier marocain, basé sur le rapport 2015-2025)



Améliorations Clés Projetées



Temps de détection

Réduction de 287 jours à <1 jour

~99.7%



Incidents de sécurité

Réduction des incidents critiques

~70%



Précision de détection

Augmentation de la précision des alertes

+90%



Temps de réponse

Accélération de la remédiation

-50%

Projections basées sur l'analyse du Rapport Cybersécurité Industrielle Maroc 2015-2025

Retour sur Investissement Projeté

42.5%

Taux de compromission ICS au Maroc

(Top 3 mondial - Kaspersky ICS CERT 2025)



Opportunité de Marché



Secteur Manufacturier

40.39% des systèmes ICS ciblés par malware

45 entreprises



Pertes Économiques

Pertes cumulées documentées (2015-2025)

244M USD

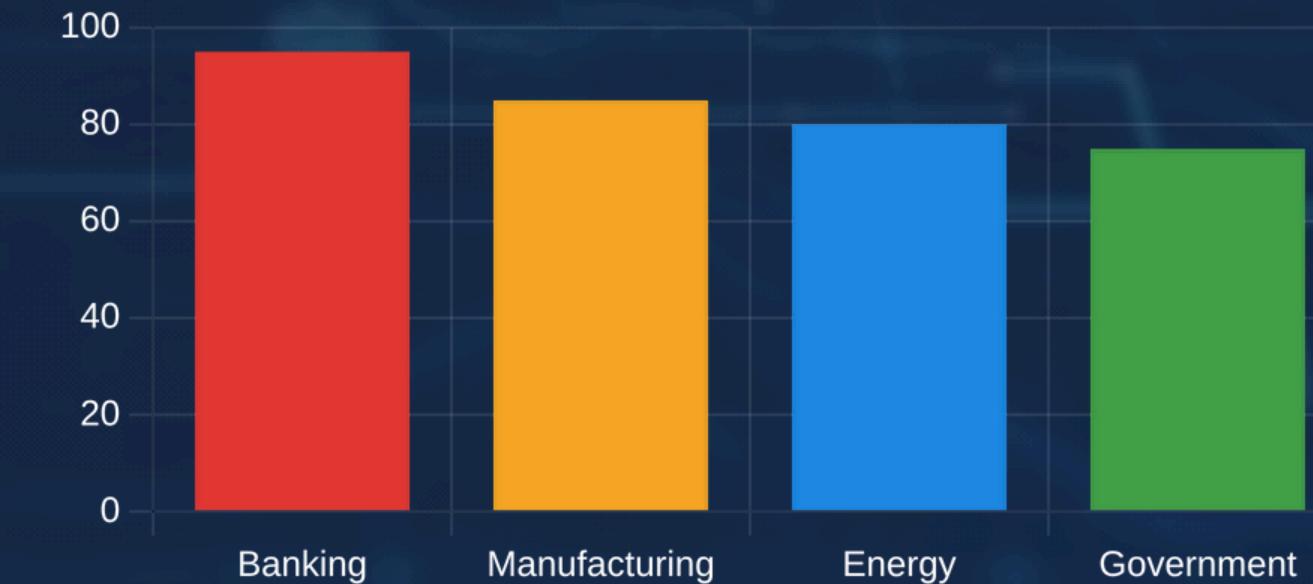


Croissance des Incidents

Augmentation des cyberattaques industrielles

+650%

Comparaison Sectorielle



Contactez-nous

**Today, we monitor threats.
Tomorrow, we prevent them
before they start. Welcome to
SECURE PROD**



Notre Équipe



Belkebir kaouthar
offensive web security



REDA OUZIDANE
ingenieur industrielle



ILYASS ALAMI
Expert Cybersécurité



Demander une Démonstration

Découvrez comment ScureProd peut protéger votre infrastructure
industrielle