AYI NEDJIMI Consultants

Détection intrusion environnement SCADA et systèmes ICS

Catégorie : Sécurité Industrielle OT/ICS Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide détection d'intrusion en environnement SCADA et ICS : déploiement de sondes passives, règles Snort/Suricata OT, analyse comportementale réseau.

Résumé exécutif

La détection d'intrusion en environnement SCADA et ICS présente des défis uniques liés aux contraintes de disponibilité absolue, aux protocoles propriétaires non supportés par les outils IT classiques, et à l'impossibilité de déployer des agents de sécurité sur les automates programmables dont les ressources sont dimensionnées au plus juste. Ce guide détaille les architectures de détection passive utilisant des TAP réseau et des ports miroir, les règles de signatures spécifiques OT pour les moteurs Snort et Suricata, l'analyse comportementale réseau exploitant le déterminisme des communications industrielles cycliques, et l'intégration de ces capacités dans un SOC convergent IT/OT capable de détecter et de qualifier les menaces avancées ciblant les systèmes de contrôle industriels des infrastructures critiques nationales et européennes soumises aux exigences réglementaires NIS 2.

Les environnements SCADA et ICS constituent des cibles de choix pour les attaquants étatiques et les groupes cybercriminels sophistiqués, car leur compromission peut entraîner des impacts physiques majeurs sur les infrastructures critiques. Détecter une intrusion dans ces environnements exige une approche radicalement différente de la détection IT classique. Les systèmes de détection d'intrusion traditionnels, conçus pour analyser le trafic HTTP, DNS et TLS, sont aveugles face aux protocoles industriels comme Modbus, DNP3, EtherNet/IP ou IEC 61850. Les contraintes opérationnelles interdisent le déploiement d'agents de sécurité sur les automates et les HMI, dont les ressources processeur et mémoire sont dimensionnées au plus juste pour leur fonction de contrôle. La détection passive, basée sur l'analyse du trafic réseau capturé sur des ports miroir, s'impose comme le paradigme dominant pour la surveillance de sécurité en environnement OT, permettant une visibilité complète sans aucun risque d'impact sur les processus industriels critiques.

Architecture de détection passive en environnement OT

Le déploiement de capacités de détection en environnement OT repose sur une **architecture de capture passive** exploitant les ports miroir (SPAN) des commutateurs industriels ou des TAP réseau (Test Access Point) physiques. Les TAP passifs, qui copient le trafic sans possibilité de l'altérer, sont préférés dans les environnements critiques car ils garantissent qu'aucune défaillance de l'outil de détection ne peut impacter les communications industrielles. Chaque segment réseau OT significatif doit disposer d'un point de capture.

Les sondes de détection se positionnent à plusieurs niveaux de l'architecture Purdue. Au niveau de la **DMZ industrielle**, une sonde surveille les flux entre IT et OT pour détecter les tentatives de traversée non autorisées. Au niveau 2 (supervision), les sondes analysent les communications entre les serveurs SCADA/HMI et les automates. Au niveau 1, dans les installations critiques, des sondes dédiées surveillent les échanges entre automates et les communications avec les systèmes instrumentés de sécurité. Cette architecture multi-niveaux, intégrée à un SOC convergent IT/OT, offre une couverture de détection complète.

Les solutions commerciales de détection OT comme Nozomi Networks Guardian, Dragos Platform et Claroty CTD combinent analyse protocolaire profonde, découverte automatique des actifs et détection d'anomalies basée sur l'apprentissage automatique. Ces plateformes décodent nativement des dizaines de protocoles industriels et construisent une baseline comportementale du réseau OT pour identifier les déviations suspectes.

Mon avis : L'investissement dans une plateforme de détection OT commerciale est justifié pour les infrastructures critiques, mais les organisations avec des budgets contraints peuvent construire une première capacité de détection significative avec des outils open source (Suricata, Zeek) complétés par des règles communautaires spécifiques OT. L'essentiel est de commencer la surveillance du réseau OT plutôt que d'attendre le budget idéal.

Comment configurer Suricata pour les protocoles industriels ?

Suricata, le moteur IDS/IPS open source, supporte nativement la détection sur plusieurs protocoles industriels depuis la version 6.0. Le parseur Modbus intégré permet d'écrire des règles inspectant le contenu des trames Modbus : numéro de fonction, adresse de registre, valeur écrite. Le parseur DNP3 analyse les couches application du protocole, et des parseurs communautaires existent pour EtherNet/IP et S7comm (protocole Siemens).

Les règles Suricata spécifiques OT suivent la syntaxe standard enrichie de mots-clés protocolaires. Une règle détectant une tentative d'écriture Modbus sur un registre critique utilise le mot-clé *modbus.function* pour filtrer sur la fonction 16 (Write Multiple Registers) combiné avec l'adresse de registre. Le jeu de règles **ET OPEN ICS** de Proofpoint/Emerging Threats fournit une base de signatures couvrant les attaques connues contre les protocoles industriels. Ces règles doivent être complétées par des signatures personnalisées reflétant les spécificités de chaque installation, suivant les principes de détection engineering.

La configuration de Suricata pour l'OT diffère de la configuration IT standard. Le mode IDS passif est impératif : jamais de mode IPS inline sur un réseau OT de production. Le fichier suricata.yaml doit activer les parseurs de protocoles industriels, définir les réseaux OT dans les variables HOME_NET, et ajuster les seuils de détection pour limiter les faux positifs dans un environnement où chaque alerte doit être investiguée. L'intégration avec une plateforme de log management centralise les alertes OT et IT.

Source de règles	Protocoles couverts	Licence	Mise à jour
ET OPEN ICS	Modbus, DNP3, EtherNet/IP	Open Source	Quotidienne
Dragos Threat Intel	Multi-protocoles OT	Commerciale	Continue
CISA ICS Advisories	Vulnérabilités spécifiques	Publique	Par advisory
Suricata ICS ruleset	Modbus, DNP3, S7comm	Open Source	Communautaire
Custom site rules	Spécifique installation	Interne	Manuelle

Analyse comportementale réseau pour la détection OT

L'analyse comportementale exploite une caractéristique fondamentale des réseaux OT : leur **déterminisme**. Contrairement aux réseaux IT où les flux varient constamment, les communications OT suivent des patterns prévisibles et stables. Un automate communique cycliquement avec les mêmes dispositifs, utilise les mêmes fonctions protocolaires et transmet des valeurs dans des plages déterminées par le processus physique supervisé. Toute déviation de cette baseline constitue un signal d'alerte potentiel.

La phase d'apprentissage (*baselining*) dure typiquement 2 à 4 semaines et doit couvrir l'ensemble des modes de fonctionnement du processus industriel : production normale, démarrage, arrêt, changement de lot, maintenance. Les algorithmes d'apprentissage automatique construisent un modèle des communications normales capturant les relations entre dispositifs, les intervalles de communication, les séquences de fonctions protocolaires et les distributions de valeurs dans les registres. **Zeek** (anciennement Bro), avec ses scripts de parsing OT, constitue un excellent outil open source pour cette analyse comportementale, générant des logs structurés exploitables par des outils de corrélation.

Les indicateurs comportementaux les plus pertinents en OT incluent l'apparition de nouvelles connexions entre dispositifs, les changements de fréquence de communication, l'utilisation de fonctions protocolaires inhabituelles (commandes de programmation d'automate en dehors des fenêtres de maintenance), les valeurs de processus sortant des plages normales et les scans réseau caractéristiques de la phase de reconnaissance d'un attaquant. L'approche de threat hunting complète cette détection automatisée par une recherche proactive de menaces.

L'attaque Colonial Pipeline en mai 2021, bien que ciblant initialement les systèmes IT, a conduit à l'arrêt préventif du plus grand pipeline de produits raffinés des États-Unis pendant six jours. L'absence de capacité de détection et de visibilité suffisante sur les flux entre IT et OT a empêché l'opérateur de déterminer rapidement si le réseau OT était compromis, forçant un arrêt par précaution avec des conséquences économiques majeures. Une surveillance comportementale de la DMZ industrielle aurait fourni cette assurance en quelques heures.

Pourquoi les signatures IT classiques sont insuffisantes en OT ?

Les jeux de signatures IDS traditionnels (Snort community rules, ET PRO) détectent efficacement les menaces IT courantes : exploitation de vulnérabilités web, communications C2 connues, exfiltration de données. Cependant, les attaques spécifiques OT utilisent des vecteurs que ces signatures ne couvrent pas. Une commande Modbus d'écriture de registre est syntaxiquement identique qu'elle soit légitime ou malveillante ; seul le contexte (source, destination, moment, registre ciblé, valeur écrite) permet de différencier les deux.

Les **attaques living-off-the-land** en OT exploitent les fonctionnalités natives des protocoles industriels pour atteindre leurs objectifs. Reprogrammer un automate via les fonctions de transfert de programme intégrées au protocole S7comm ou télécharger une nouvelle configuration via DNP3 sont des opérations légitimes détournées à des fins malveillantes. La détection repose alors sur des règles contextuelles : ces opérations sont-elles effectuées depuis un poste d'ingénierie autorisé, pendant une fenêtre de maintenance planifiée, par un utilisateur authentifié ? Ce sont les méthodes documentées dans le cadre MITRE ATT&CK for ICS qui guident la rédaction de ces règles contextuelles.

Votre SOC est-il capable de distinguer une commande de reprogrammation d'automate légitime d'une tentative d'attaque Triton/TRISIS ?

Quelles métriques pour évaluer la détection OT ?

L'efficacité d'un système de détection OT se mesure par des **métriques spécifiques** adaptées aux contraintes industrielles. Le taux de faux positifs est critique : en environnement OT, chaque alerte peut mobiliser une équipe d'intervention et potentiellement déclencher un arrêt de précaution. Un taux de faux positifs élevé conduit inévitablement à l'alert fatigue et à l'ignorance des alertes légitimes. L'objectif est un taux inférieur à 5% après la phase d'optimisation initiale.

Le *MTTD* (Mean Time To Detect) mesure le délai moyen entre le début d'une activité malveillante et sa détection. Pour les attaques OT sophistiquées comme Triton, qui comportent des phases de reconnaissance prolongées, le MTTD peut être réduit en détectant les activités préparatoires (scans réseau, énumération de protocoles, accès aux postes d'ingénierie) plutôt que l'action terminale. Le taux de couverture des techniques MITRE ATT&CK for ICS mesure le pourcentage de techniques d'attaque documentées pour lesquelles au moins une règle de détection existe. La mise en place d'un processus de réponse aux incidents OT garantit que les détections mènent à des actions correctives efficaces.

Faut-il un SOC dédié OT ou un SOC convergent ?

Le débat entre **SOC dédié OT** et **SOC convergent IT/OT** divise les praticiens. Le SOC dédié offre une expertise approfondie en protocoles industriels et en processus de production, mais représente un coût prohibitif pour la majorité des organisations et crée des silos de détection. Le SOC convergent mutualise les ressources et permet la corrélation entre événements IT et OT, essentielle pour détecter les attaques qui traversent la frontière IT/OT comme Colonial Pipeline ou l'attaque ukrainienne.

L'approche recommandée est le **SOC convergent avec spécialisation OT**. Le SIEM central agrège les alertes IT et OT, mais des analystes formés aux spécificités industrielles traitent les alertes OT avec des playbooks adaptés. Les données OT (alertes IDS, logs de pare-feu industriels, événements de surveillance comportementale) alimentent des dashboards dédiés. Les cas d'usage de détection OT (changement de firmware non planifié, nouvelle connexion vers un automate critique, modification de configuration SCADA) sont documentés et testés régulièrement via des exercices de simulation Purple Team adaptés aux scénarios ICS.

À retenir : La détection d'intrusion en environnement OT repose sur trois piliers complémentaires : la détection par signatures spécifiques aux protocoles industriels (Suricata, Snort), l'analyse comportementale exploitant le déterminisme des réseaux OT (Zeek, plateformes NDR OT), et la corrélation contextuelle intégrant la connaissance du processus industriel. Le déploiement en mode passif via des TAP réseau garantit l'absence d'impact sur la production.

Sources et références : CISA ICS · ANSSI

Comment intégrer la threat intelligence OT dans la détection ?

L'intégration de la **threat intelligence spécifique OT** enrichit considérablement les capacités de détection en environnement SCADA. Les sources de renseignement cyber industriel incluent les advisories CISA ICS-CERT, les rapports techniques de Dragos sur les groupes de menaces OT (CHERNOVITE, KAMACITE, ELECTRUM), les bulletins de sécurité des fabricants d'automates et les indicateurs de compromission partagés par les ISAC sectoriels comme E-ISAC pour l'énergie ou WaterISAC pour le traitement de l'eau.

Les indicateurs de compromission OT diffèrent significativement des IOC IT classiques. Au-delà des adresses IP et des hachages de fichiers malveillants, les IOC OT incluent des séquences de commandes protocolaires caractéristiques, des modifications spécifiques de registres d'automates, des patterns de communication C2 utilisant des protocoles industriels comme canal de communication, et des signatures de firmware modifié. L'opérationnalisation de cette intelligence passe par la traduction en règles de détection Suricata, en requêtes Zeek, et en cas d'usage SIEM qui corrèlent les indicateurs réseau avec le contexte opérationnel du site industriel. Les équipes de détection doivent maintenir une veille active sur les groupes de menaces ciblant leur secteur industriel spécifique, alimentant continuellement le cycle de détection engineering avec les nouvelles tactiques, techniques et procédures identifiées dans les rapports de threat intelligence OT publiés par la communauté de cybersécurité industrielle internationale.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr