AYI NEDJIMI Consultants

Threat intelligence pour environnements OT et sources ICS

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

Guide threat intelligence OT : sources de renseignement cyber industriel, groupes APT ciblant les ICS, IOC spécifiques et intégration SOC OT en 2026.

Résumé exécutif

La threat intelligence appliquée aux environnements OT diffère fondamentalement de son équivalent IT par la nature des menaces ciblant les systèmes de contrôle, les sources d'information spécialisées dans le renseignement cyber industriel, et les indicateurs de compromission spécifiques aux protocoles et aux automates des systèmes de contrôle industriels. Ce guide cartographie l'écosystème complet de renseignement cyber OT incluant les ISAC sectoriels et les éditeurs spécialisés, analyse les groupes de menaces actifs ciblant les infrastructures industrielles comme CHERNOVITE, ELECTRUM et XENOTIME, détaille les IOC spécifiques ICS allant au-delà des simples adresses IP, et fournit une méthodologie structurée d'intégration de la CTI dans les opérations de sécurité OT pour anticiper et détecter les attaques sophistiquées contre les systèmes de contrôle industriels critiques des organisations.

Le renseignement sur les cybermenaces (Cyber Threat Intelligence, CTI) appliqué aux environnements de technologie opérationnelle constitue une discipline émergente portée par la multiplication des attaques ciblant les systèmes industriels. Les groupes de menaces capables de compromettre des automates programmables, de développer des malwares ciblant des protocoles SCADA ou de saboter des processus physiques via des cyberattaques représentent une catégorie d'adversaires distincte des cybercriminels IT traditionnels. Leur compréhension exige des sources de renseignement spécialisées, des analystes formés aux technologies industrielles et des processus d'opérationnalisation adaptés aux contraintes OT. La maturité en threat intelligence OT d'une organisation se mesure à sa capacité à transformer le renseignement brut en actions défensives concrètes : règles de détection sur les sondes réseau OT, indicateurs de compromission intégrés aux pare-feu industriels, et scénarios d'attaque alimentant les exercices de simulation et les plans de réponse aux incidents industriels. Cette chaîne de valeur du renseignement cyber industriel nécessite une collaboration étroite entre les équipes de sécurité IT, les spécialistes OT et les analystes CTI pour produire un renseignement actionnable dans le contexte opérationnel spécifique de chaque site industriel.

Cartographie des groupes de menaces ciblant les ICS

Dragos maintient la taxonomie la plus détaillée des groupes de menaces OT, identifiant plus de vingt groupes d'activité distincts ciblant les systèmes industriels. **CHERNOVITE**, le groupe derrière le malware PIPEDREAM/INCONTROLLER découvert en 2022, a développé le premier framework d'attaque modulaire capable de cibler simultanément des automates de différents

constructeurs (Schneider Electric, Omron) et des serveurs OPC UA. **ELECTRUM**, lié aux attaques contre le réseau électrique ukrainien de 2016 avec le malware Industroyer/CrashOverride, cible spécifiquement les protocoles IEC 61850 et IEC 104 des sous-stations électriques.

XENOTIME, responsable de l'attaque Triton/TRISIS contre les contrôleurs de sécurité Triconex, représente la menace la plus alarmante car il a franchi la frontière entre la compromission OT et l'attaque des systèmes instrumentés de sécurité (SIS) conçus pour protéger les vies humaines. *KAMACITE*, associé au groupe Sandworm du GRU russe, a démontré des capacités d'attaque contre les réseaux électriques, les systèmes de distribution d'eau et les infrastructures de transport. Ces groupes disposent de ressources étatiques et d'une patience opérationnelle permettant des campagnes d'infiltration s'étalant sur plusieurs mois avant l'action finale, comme documenté dans le framework MITRE ATT&CK for ICS.

L'attaque contre le réseau électrique ukrainien du 23 décembre 2015, attribuée au groupe SANDWORM/KAMACITE, illustre l'utilisation sophistiquée du renseignement opérationnel par les attaquants. Après des mois de reconnaissance et d'infiltration des réseaux IT des trois opérateurs de distribution électrique, les attaquants ont utilisé leur connaissance détaillée des systèmes SCADA pour ouvrir simultanément les disjoncteurs de 30 sous-stations, privant 230 000 foyers d'électricité pendant plusieurs heures. L'attaque incluait un composant de sabotage des firmwares des convertisseurs série-Ethernet pour empêcher la reprise de contrôle à distance.

Comment structurer les sources de CTI OT ?

Les sources de renseignement cyber OT se répartissent en quatre catégories selon le modèle Traffic Light Protocol (TLP). Les **sources ouvertes** (OSINT) incluent les advisories ICS-CERT/CISA (plus de 400 par an), les bulletins de sécurité des constructeurs d'automates (Siemens ProductCERT, Schneider PSIRT, Rockwell Advisories), les rapports publics de Dragos, Mandiant et Claroty Team82, et les conférences spécialisées (S4, ICS Cyber Security Conference).

Les **sources communautaires** partagées via les ISAC (Information Sharing and Analysis Centers) sectoriels fournissent un renseignement contextuel précieux. L'E-ISAC pour l'énergie, le WaterISAC pour l'eau, l'A-ISAC pour l'automobile et le NH-ISAC pour la santé facilitent le partage d'indicateurs et de rapports entre pairs du même secteur, souvent sous TLP:AMBER. Ces échanges permettent de bénéficier du retour d'expérience d'organisations ayant subi des attaques similaires sans attendre la publication de rapports publics. L'intégration avec les pratiques de threat hunting maximise la valeur de ces sources partagées.

Les **sources commerciales** (Dragos WorldView, Mandiant Advantage Threat Intelligence, Recorded Future ICS module) offrent un renseignement enrichi avec des IOC actionnables, des rapports détaillés sur les groupes de menaces et des alertes précoces sur les vulnérabilités et les campagnes d'attaque en cours. Enfin, les **sources internes** (logs des sondes OT, alertes IDS, résultats de threat hunting) constituent un renseignement de première main reflétant les menaces réellement observées dans l'environnement spécifique de l'organisation.

Source CTI OT	Type	Fréquence	Actionnabilité
CISA ICS Advisories	OSINT	Quotidienne	Vulnérabilités + mitigations
Dragos WorldView	Commerciale	Continue	IOC + TTPs + contexte
ISAC sectoriels	Communautaire	Variable	Alertes + IOC sectoriels
ProductCERT constructeurs	OSINT	Mensuelle	Patches + workarounds
MITRE ATT&CK for ICS	OSINT	Trimestrielle	TTPs + détection
Sondes OT internes	Interne	Temps réel	Alertes opérationnelles

Mon avis : La plupart des organisations industrielles consomment du renseignement cyber OT de manière passive, lisant les rapports sans les opérationnaliser. La valeur réelle de la CTI réside dans sa transformation en règles de détection déployées sur les sondes, en indicateurs recherchés proactivement dans les logs et en scénarios d'exercice testant la préparation des équipes. Un rapport Dragos lu et classé est du renseignement gaspillé ; un rapport transformé en dix règles Suricata OT est du renseignement actionné.

Quels IOC spécifiques aux menaces OT surveiller ?

Les indicateurs de compromission OT se distinguent des IOC IT classiques par leur nature technique. Au-delà des indicateurs réseau traditionnels (adresses IP, domaines C2, hachages de fichiers), les **IOC spécifiques ICS** incluent des séquences de commandes protocolaires caractéristiques d'une attaque (séquence Modbus de lecture de configuration suivie d'une écriture de programme), des modifications spécifiques de registres automates (changement de mode de fonctionnement, modification de consignes de sécurité), des patterns de communication anormaux entre dispositifs OT et des signatures de firmware ou de programme modifié.

Le malware *PIPEDREAM/INCONTROLLER* illustre la sophistication des IOC OT modernes. Ses composants TAGRUN (ciblant OPC UA), CODECALL (ciblant Schneider Electric Modicon) et OMSHELL (ciblant Omron NJ/NX) utilisent les protocoles industriels légitimes pour interagir avec les automates, rendant la détection par signatures réseau seule insuffisante. La détection repose sur l'identification de séquences comportementales : l'énumération des serveurs OPC UA suivie du téléchargement de la configuration d'un automate Modicon via le protocole UMAS, combinée à un transfert de fichier vers un automate Omron via FINS. L'approche de détection engineering permet de traduire ces séquences en règles de corrélation efficaces au sein du SIEM.

Pourquoi le renseignement sur les vulnérabilités OT diffère du IT ?

La gestion des vulnérabilités OT se heurte à des **contraintes d'applicabilité** sans équivalent en IT. Une vulnérabilité critique (CVSS 9.8) sur un automate en production ne peut pas être corrigée par un patch déployé dans la nuit : le correctif nécessite un arrêt de production planifié, un test

préalable sur un système de spare et une procédure de rollback. Le score CVSS, conçu pour les systèmes IT, ne reflète pas la criticité réelle en contexte OT où la disponibilité prime sur la confidentialité.

Le système de scoring **SSVC** (Stakeholder-Specific Vulnerability Categorization) de CISA, adapté aux décisions de priorisation OT, intègre l'exploitabilité active, l'impact sur la sûreté et la présence de mesures compensatoires. Les organisations matures maintiennent une base de données de vulnérabilités OT corrélant chaque advisory ICS-CERT avec leur inventaire d'actifs pour identifier immédiatement les systèmes impactés et évaluer le risque résiduel en tenant compte des mesures compensatoires déjà déployées (segmentation, pare-feu protocolaire, surveillance). L'architecture de SOC convergent intègre cette gestion des vulnérabilités OT dans le flux opérationnel de sécurité quotidien.

Votre processus de gestion des vulnérabilités distingue-t-il les CVE affectant vos systèmes OT de celles concernant uniquement votre parc IT ?

Faut-il partager ses IOC OT avec la communauté ?

Le partage de renseignement cyber entre organisations du même secteur industriel renforce la posture de sécurité collective. Les mécanismes de partage structurés via **STIX/TAXII** permettent l'échange automatisé d'indicateurs entre plateformes de threat intelligence. Les ISAC sectoriels fournissent un cadre de confiance et des règles de partage (TLP) protégeant les informations sensibles des organisations contributrices.

Les réticences au partage, souvent liées à la crainte de révéler des faiblesses de sécurité ou de violer des obligations de confidentialité, sont compréhensibles mais contre-productives. Les réglementations comme NIS 2 encouragent explicitement le partage d'informations sur les cybermenaces entre entités essentielles. Un attaquant ciblant un opérateur électrique cible probablement d'autres opérateurs du même secteur ; le partage rapide des IOC découverts lors d'un incident permet à tous de déployer des défenses proactives avant d'être ciblés à leur tour. L'intégration des flux de partage dans le processus d'incident response structure cette collaboration en cas de crise.

Comment opérationnaliser la CTI OT dans le SOC ?

L'opérationnalisation de la threat intelligence OT suit un processus structuré en quatre étapes. La première étape est le **triage des rapports** : chaque advisory ICS-CERT, rapport de Dragos ou alerte ISAC est évalué pour sa pertinence par rapport à l'inventaire d'actifs de l'organisation. Un rapport sur une vulnérabilité Siemens S7-1500 n'a aucune valeur opérationnelle pour un site utilisant exclusivement des automates Allen-Bradley. Ce filtrage initial, idéalement automatisé par corrélation avec la CMDB OT, réduit le volume de renseignement à traiter et concentre l'attention sur les menaces réellement pertinentes pour l'environnement spécifique de l'organisation.

La deuxième étape est la **traduction en règles de détection**. Les indicateurs de compromission réseau (adresses IP, domaines, patterns protocolaires) sont convertis en signatures Suricata ou en requêtes Zeek déployées sur les sondes OT. Les TTPs (Tactics, Techniques and Procedures)

documentées dans les rapports sont traduites en cas d'usage de corrélation SIEM. Par exemple, le rapport Dragos sur CHERNOVITE décrivant l'utilisation du protocole UMAS pour interagir avec les automates Schneider se traduit en une règle détectant les commandes UMAS depuis des sources non autorisées, selon les principes de détection engineering avancée.

La troisième étape est la *recherche proactive* (threat hunting) utilisant les indicateurs comportementaux du rapport pour rechercher rétroactivement dans les logs et les captures réseau OT des traces d'activité similaire. Cette recherche peut révéler qu'un groupe de menaces a déjà effectué une reconnaissance du réseau OT sans avoir été détecté. La quatrième étape est l'intégration dans les exercices de simulation : les scénarios d'attaque documentés dans les rapports CTI alimentent les exercices tabletop et les tests Purple Team adaptés au contexte ICS, permettant de valider la capacité de l'organisation à détecter et répondre aux menaces identifiées par le renseignement.

Sources et références : CISA ICS · ANSSI

Comment évaluer la maturité CTI OT de son organisation ?

Le modèle de maturité CTI OT s'évalue sur cinq niveaux. Le niveau 1 (réactif) se limite à la lecture occasionnelle des advisories ICS-CERT sans processus structuré. Le niveau 2 (informé) intègre une veille régulière avec un abonnement aux sources pertinentes et une diffusion aux équipes concernées. Le niveau 3 (opérationnel) traduit systématiquement le renseignement en actions défensives : règles de détection, mesures compensatoires et plans de réponse. Le niveau 4 (proactif) pratique le threat hunting OT basé sur les rapports CTI et contribue au partage communautaire via les ISAC. Le niveau 5 (stratégique) influence les décisions d'architecture et d'investissement par l'analyse des tendances de menaces à long terme ciblant le secteur industriel spécifique. La majorité des organisations industrielles se situent entre les niveaux 1 et 2, alors que les menaces qu'elles affrontent exigent un niveau 3 minimal pour les systèmes critiques.

À retenir : La threat intelligence OT repose sur un écosystème de sources spécialisées (CISA ICS-CERT, Dragos, ISAC sectoriels, constructeurs) produisant des IOC spécifiques aux protocoles et systèmes industriels. L'opérationnalisation du renseignement en règles de détection, en indicateurs de recherche proactive et en scénarios d'exercice transforme l'information brute en capacité défensive concrète contre les groupes de menaces ciblant les systèmes de contrôle industriels.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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