AYI NEDJIMI Consultants

Incident response en OT particularités et contraintes ICS

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

Guide incident response OT : particularités de la réponse aux incidents en environnement industriel, playbooks ICS, forensique automates et.

Résumé exécutif

La réponse aux incidents cybersécurité en environnement OT obéit à des règles fondamentalement différentes de l'incident response IT en raison des impacts physiques potentiels sur les personnes et l'environnement. La priorité absolue à la sûreté des personnes et à la continuité des processus critiques, l'impossibilité d'isoler brutalement un automate pilotant un réacteur chimique ou une turbine de centrale électrique, et la nécessité d'une coordination étroite entre équipes cyber et équipes d'exploitation OT imposent des playbooks spécifiques, des procédures de confinement graduelles et des compétences hybrides combinant forensique numérique et connaissance des processus industriels. Ce guide détaille les particularités de l'IR en environnement industriel avec des recommandations opérationnelles pour chaque phase de la réponse aux incidents affectant les systèmes de contrôle.

Lorsqu'un incident de cybersécurité frappe un environnement industriel, la réponse ne peut pas suivre les mêmes réflexes que dans un contexte IT. Isoler un serveur compromis en datacenter est une action standard qui interrompt temporairement un service ; isoler un automate compromis pilotant un réacteur chimique ou une turbine de centrale électrique peut provoquer un emballement thermique, une surpression ou une panne de distribution affectant des milliers de foyers. Cette réalité physique transforme chaque décision de réponse en un arbitrage complexe entre la nécessité de contenir la menace cyber et l'impératif de maintenir le processus industriel dans un état sûr. Les équipes de réponse aux incidents OT doivent maîtriser à la fois les techniques forensiques numériques et la compréhension des processus industriels qu'elles protègent, une double compétence rare qui justifie la création de capacités dédiées intégrant des automaticiens, des ingénieurs procédé et des spécialistes cybersécurité travaillant en synergie pour protéger simultanément les systèmes informatiques et les processus physiques critiques des installations industrielles ciblées par les attaquants.

La sûreté avant la sécurité : principe fondamental de l'IR OT

Le principe cardinal de l'incident response OT est la **priorité absolue à la sûreté** des personnes et de l'environnement. Toute action de réponse doit être évaluée à travers ce prisme avant exécution. Déconnecter un réseau OT pour contenir un malware peut sembler logique d'un point de vue cybersécurité, mais si cette déconnexion prive les opérateurs de la supervision d'un processus dangereux, elle crée un risque de sûreté supérieur au risque cyber initial.

La hiérarchie des priorités en IR OT suit un ordre strict : sûreté des personnes, protection de l'environnement, intégrité des équipements, continuité de la production, puis investigation et remédiation cyber. Cette hiérarchie peut conduire à des décisions apparemment contre-intuitives pour un analyste IR IT : laisser un malware actif sur un HMI tout en maintenant la supervision du processus, ou basculer en commande manuelle locale plutôt que d'isoler le réseau OT compromis. La formation croisée entre équipes cyber et OT, structurée selon les principes d'incident response adaptés au contexte industriel, développe la compréhension mutuelle nécessaire à ces décisions critiques.

Lors de l'incident Colonial Pipeline en mai 2021, l'opérateur a choisi d'arrêter préventivement le pipeline entier pendant six jours, non pas parce que le réseau OT était confirmé compromis, mais par incapacité à vérifier rapidement l'intégrité des systèmes de contrôle. Cette décision, coûtant des millions de dollars et provoquant des pénuries de carburant sur la côte Est américaine, illustre le coût de l'absence de visibilité OT et de playbooks IR spécifiques. Une capacité de forensique OT rapide aurait permis de confirmer ou d'infirmer la compromission du réseau de contrôle en quelques heures plutôt qu'en jours.

Comment adapter les phases de l'IR au contexte OT ?

La phase de **détection et analyse** en OT s'appuie sur les sondes de surveillance réseau industriel, les logs des pare-feu OT et les alertes des systèmes de détection d'anomalies. L'analyste IR OT doit distinguer une anomalie cyber d'un dysfonctionnement de processus : une valeur aberrante sur un capteur peut signaler une manipulation malveillante ou simplement une panne instrumentale. La corrélation avec les événements du système de supervision SCADA et les journaux du processus industriel aide à trancher, en complément des techniques de détection engineering spécifiques aux protocoles OT.

La phase de **containment** (confinement) en OT privilégie l'isolation granulaire plutôt que la coupure brutale. Le blocage ciblé de flux suspects via les pare-feu industriels, la révocation d'accès spécifiques sur les comptes compromis et l'activation de règles de surveillance renforcée constituent des mesures de confinement proportionnées. Le passage en mode dégradé (commande manuelle locale, réduction de charge, arrêt contrôlé d'un sous-système) se décide conjointement entre l'équipe IR et le responsable d'exploitation selon des critères prédéfinis dans les playbooks.

La phase d'**eradication** et de recovery en OT requiert une validation rigoureuse avant le retour en production. La vérification de l'intégrité des programmes automates par comparaison avec les sauvegardes de référence, la requalification des systèmes de supervision et le test fonctionnel du processus industriel en mode progressif (démarrage à charge réduite) garantissent un redémarrage sûr. Cette phase mobilise les équipes d'automatisme et de procédé en plus des équipes cyber, suivant les procédures de disaster recovery adaptées au contexte industriel.

Phase IR	Adaptation OT	Acteur principal	Risque spécifique
Détection	Sondes OT passives + corrélation SCADA	SOC OT	Confusion anomalie cyber/ procédé
Confinement	Isolation granulaire, pas de coupure réseau	IR + Exploitation	Impact sûreté si isolation brutale
Éradication	Vérification intégrité PLC + restauration	IR + Automatisme	Programme PLC corrompu non détecté
Recovery	Démarrage progressif + requalification	Exploitation + Procédé	Redémarrage avec système compromis
Lessons learned	REX incluant impact production + sûreté	Toutes équipes	Cloisonnement des retours d'expérience

Mon avis : La majorité des plans de réponse aux incidents que j'ai audités en environnement industriel sont des copier-coller de plans IT avec le mot « OT » ajouté. Ces plans sont dangereux car ils prescrivent des actions (isolation réseau immédiate, scan antivirus complet, reimaging des systèmes) potentiellement catastrophiques en contexte OT. Chaque playbook IR OT doit être co-écrit avec les équipes d'exploitation et validé lors d'exercices de simulation réalistes avant toute utilisation en situation réelle.

Pourquoi la forensique OT diffère radicalement de la forensique IT ?

La *forensique OT* se heurte à des limitations techniques considérables. Les automates programmables ne génèrent pas de logs de sécurité exploitables. L'extraction du contenu mémoire d'un PLC nécessite des outils spécialisés et une connaissance du format propriétaire de chaque constructeur. Les protocoles industriels ne journalisent pas nativement les commandes reçues, rendant impossible la reconstruction de la chronologie des actions malveillantes sans capture réseau préalable.

Les captures réseau (**PCAP**) constituent la source forensique la plus précieuse en environnement OT. L'analyse des trames protocolaires permet de reconstituer les commandes envoyées aux automates, les modifications de registres et les transferts de programmes. Les outils comme Dragos Platform et Nozomi Networks conservent un historique des communications OT analysable rétroactivement lors d'une investigation. La rétention de ces captures, dimensionnée selon les principes de gestion des logs, doit couvrir une période suffisante pour détecter les attaques à progression lente caractéristiques des groupes APT ciblant les systèmes industriels.

Votre infrastructure de capture réseau OT conserve-t-elle suffisamment d'historique pour investiguer une attaque ayant débuté il y a six mois ?

Quels exercices de simulation pour tester l'IR OT ?

Les exercices de simulation constituent le moyen le plus efficace de valider les playbooks IR OT et de développer les réflexes des équipes. Les **exercices tabletop** réunissent les équipes cyber, OT, sûreté et direction autour d'un scénario d'attaque déroulé étape par étape. Le scénario décrit l'évolution de l'attaque (compromission initiale via phishing, mouvement latéral vers le réseau OT, modification d'un programme automate) et les participants discutent les décisions de réponse à chaque étape, révélant les lacunes dans les procédures et la coordination.

Les exercices *Purple Team OT*, plus avancés, simulent des attaques réelles sur un environnement de test reproduisant l'architecture de production. L'équipe Red simule les actions d'un groupe de menaces OT (reconnaissance, exploitation de vulnérabilités, manipulation de protocoles industriels) tandis que l'équipe Blue détecte et répond en temps réel. Ces exercices, planifiés avec les mêmes précautions qu'un pentest OT, valident l'ensemble de la chaîne de détection et de réponse dans des conditions réalistes. Les résultats alimentent l'amélioration continue des capacités de SOC convergent IT/OT.

Faut-il externaliser la capacité IR OT ?

Le maintien d'une capacité IR OT interne 24/7 représente un investissement considérable que seules les grandes organisations industrielles peuvent justifier. L'**externalisation partielle** vers des prestataires spécialisés en IR OT (Dragos, Nozomi Networks, Mandiant ICS) constitue une alternative pragmatique. Le modèle retainer, avec un contrat de prestation prénégocié garantissant un temps de réponse défini, permet de mobiliser rapidement des experts en forensique industrielle et en réponse aux incidents OT sans supporter le coût permanent d'une équipe dédiée.

Le modèle hybride optimal combine une équipe interne de premier niveau (SOC OT pour la détection et le confinement initial) avec un prestataire externe pour l'investigation approfondie et la remédiation complexe. La préparation est clé : le prestataire doit disposer en amont de la documentation de l'architecture OT, d'accès VPN pré-configurés et sécurisés, et d'une connaissance des processus industriels spécifiques du site. Un exercice annuel avec le prestataire valide les procédures de mobilisation et la capacité effective d'intervention dans les délais contractuels.

Comment constituer une équipe IR OT compétente ?

La constitution d'une équipe de réponse aux incidents OT requiert un **profil de compétences hybride** alliant cybersécurité et connaissance des systèmes industriels. Les membres clés incluent un analyste forensique formé aux protocoles OT (capable d'analyser des captures Modbus, DNP3 ou S7comm), un ingénieur automatisme connaissant la programmation et le fonctionnement des automates du site, un spécialiste réseau maîtrisant l'architecture de segmentation OT/IT, et un coordinateur ayant l'autorité pour prendre des décisions impactant la production. Cette équipe doit pouvoir être mobilisée en dehors des heures ouvrées via un processus d'astreinte documenté et testé régulièrement.

La formation croisée entre les membres de l'équipe renforce sa résilience opérationnelle. Les analystes cyber suivent des formations en automatisme industriel pour comprendre les implications de leurs actions de réponse sur les processus physiques. Les automaticiens sont sensibilisés aux techniques d'attaque ciblant les automates et aux indicateurs de compromission spécifiques aux protocoles qu'ils utilisent quotidiennement. Les certifications spécialisées comme le *GRID* (GIAC Response and Industrial Defense) du SANS Institute valident cette double compétence essentielle pour les intervenants en réponse aux incidents sur les systèmes de contrôle industriels. Les exercices réguliers de simulation, incluant des scénarios inspirés des attaques réelles documentées par Nozomi Networks et Dragos, maintiennent les compétences opérationnelles de l'équipe et identifient les besoins de formation continue.

Sources et références : CISA ICS · ANSSI

Quelles leçons tirer des incidents OT majeurs pour améliorer l'IR ?

L'analyse des incidents OT majeurs révèle des **patterns récurrents** exploitables pour améliorer les processus de réponse. Le temps de séjour moyen des attaquants dans les réseaux OT avant détection dépasse souvent six mois, comme observé lors des attaques ukrainiennes où les groupes SANDWORM et ELECTRUM ont opéré pendant des mois dans les réseaux IT et OT des opérateurs électriques avant l'action finale. Cette durée prolongée de compromission non détectée souligne l'importance de la détection proactive via le threat hunting en environnement OT.

Les retours d'expérience montrent également que la phase de recovery après un incident OT est considérablement plus longue et complexe qu'en IT. La requalification des automates, la vérification de l'intégrité de chaque programme, la validation du fonctionnement correct de chaque boucle de régulation et le redémarrage progressif du processus industriel nécessitent des jours voire des semaines de travail méthodique. Les organisations qui investissent dans la préparation de la phase de recovery, incluant des sauvegardes vérifiées des programmes automates, des procédures de requalification documentées et des automates de spare pré-configurés, réduisent significativement le temps de retour à la normale après un incident majeur affectant leurs systèmes de contrôle industriels.

À retenir : L'incident response OT place la sûreté des personnes et la continuité des processus critiques au-dessus de l'investigation cyber. Les playbooks doivent être co-construits avec les équipes d'exploitation, la forensique OT repose sur les captures réseau plutôt que sur les logs système, et chaque action de confinement doit être évaluée pour son impact sur le processus industriel avant exécution. Les exercices de simulation réguliers valident la préparation des équipes.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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