# Cybersécurité de l'industrie manufacturière

## Guide stratégique : Focus sur la détection et la réponse managées (MDR)

Cybersecurity
**Progress. Protected.**

# Table des matières

# Introduction : Une approche multicouche préventive

Le secteur manufacturier est confronté à des cybermenaces sans précédent qui tirent parti de techniques avancées pour exploiter les activités de transformation numérique. Selon le Rapport d'enquête de Verizon sur les atteintes à la sécurité des données en 2025, les ransomwares ont été impliqués dans 35 % de toutes les atteintes à la sécurité dans l'industrie manufacturière en 2024. Ces incidents ciblent de plus en plus les infrastructures critiques, les systèmes de contrôle industriel et les chaînes d'approvisionnement, ce qui augmente considérablement le risque et l'impact potentiel d'une attaque réussie.

Le coût de ces incidents est vertigineux. SOC Radar indique que le coût moyen d'une atteinte à la sécurité des données dans le secteur manufacturier augmente régulièrement en raison de la complexité accrue du numérique et de la sophistication des attaquants (Rapport de SOCRadar sur le paysage des menaces).

Afin de gérer ces risques croissants, les fabricants devraient envisager d'adopter une approche proactive et préventive conçue pour minimiser la surface d'attaque, réduire les coûts et la complexité, et améliorer la cyber-hygiène.

Les ransomwares ont été impliqués dans

**35 %**

de toutes les atteintes à la sécurité dans l'industrie manufacturière en 2024.

Source : Rapport d'enquête de Verizon sur les atteintes à la sécurité des données en 2025

Les effectifs de sécurité restent un défi majeur. Selon Verizon, les lacunes et les pénuries de compétences dans le secteur manufacturier limitent considérablement la capacité des organisations à mener des opérations de sécurité 24/7, ce qui les rend vulnérables aux menaces persistantes (Rapport de Verizon).

Les acteurs de menaces n'ont besoin d'aboutir qu'une seule fois pour causer des dommages importants. C'est pourquoi l'approche la plus mature en matière de cybersécurité d'entreprise associe une prévention multicouche à la détection et la réponse. Cependant, de nombreux fabricants sont confrontés à des difficultés :

- **LACUNES EN MATIÈRE DE COMPÉTENCES ET DE CONNAISSANCES :**
Difficulté à doter les centres d'opérations de sécurité (SOC) fonctionnant 24/7 de suffisamment de personnel.

- **COMPLEXITÉ :**
Expertise limitée dans la maîtrise des plateformes de détection et de réponse avancées.

- **CYBERMENACES SOPHISTIQUÉES :**
Utilisation croissante par les attaquants de l'IA et de l'automatisation pour accélérer et multiplier les atteintes à la sécurité.

- **CONTRAINTES BUDGÉTAIRES :**
Coûts initiaux élevés pour l'infrastructure de sécurité et le personnel qualifié.

- **PRESSIONS LIÉES À LA CONFORMITÉ :**
Les exigences réglementaires renforcent l'urgence de la préparation de la cybersécurité. C'est pourquoi de nombreux fabricants se tournent vers la détection et la réponse managées (MDR). Ce faisant, ils ont accès à l'expertise et l'efficacité d'une équipe de SecOps tierce utilisant des outils d'IA sophistiqués pour intervenir et endiguer rapidement les menaces.

Les meilleurs services de MDR automatisent le suivi et le reporting afin d'améliorer la conformité et renforcer en permanence la cyber-résilience, pour permettre aux équipes internes de se concentrer sur les opérations de fabrication essentielles.

**5,56**
**millions USD**

étaient le coût moyen d'une atteinte à la sécurité des données dans l'industrie manufacturière en 2024.

ce qui représente

**+18 %**

par rapport à 2023, et fait de l'industrie le troisième secteur le plus touché parmi les 17 étudiés.

Source : *OnWire : Coût d'une atteinte à la sécurité des données dans l'industrie, 2024*.

# Pourquoi le MDR est devenu indispensable dans l'industrie manufacturière

Les opérations de fabrication modernes reposent sur un ensemble d'outils dans le cloud, de machines reliées à des objets connectés et des chaînes d'approvisionnement complexes, qui sont autant d'éléments qui élargissent la surface d'attaque. Le Rapport de Verizon confirme que 73 % des atteintes à la sécurité dans l'industrie manufacturière impliquent des acteurs externes, l'intrusion dans les systèmes étant le vecteur le plus courant.

En particulier, 15 % des atteintes à la sécurité touchent des fournisseurs tiers, ce qui représente une augmentation de 68 % du risque lié à la chaîne d'approvisionnement, d'une année sur l'autre. Les acteurs de menaces sont également de plus en plus organisés et professionnalisés. Comme indiqué dans le Rapport de SOCRadar sur le paysage des menaces, les attaquants s'appuient sur des ransomwares en tant que services (RaaS), des outils d'IA et des identifiants volés pour s'introduire plus rapidement et plus efficacement dans les réseaux de fabrication.

Pour contrer ces risques, les fabricants ont besoin du MDR, qui est une approche de cybersécurité agile et évolutive. Il a été démontré que l'intégration de la télémétrie, de l'analyse et de l'expertise humaine par le MDR améliore l'efficacité de la gestion des vulnérabilités et des menaces jusqu'à 60 % par rapport aux méthodes de sécurité traditionnelles (Rapport de SOCRadar).

## DE LA PRÉVENTION AU MDR

Les équipes de sécurité internes ont souvent des difficultés à faire face aux volume, à la variété et à la sophistication des cybermenaces. Les ransomwares restent une préoccupation majeure, avec 33 % des atteintes à la sécurité impliquant des ransomwares ou des techniques d'extorsion. Une tendance notable est l'exploitation des vulnérabilités zero-day, qui a connu une augmentation de 180 % par rapport à l'année précédente. L'utilisation d'identifiants volés reste également une méthode courante pour les attaquants, apparaissant dans près d'un tiers de toutes les atteintes à la sécurité.

La fréquence des attaques de ransomwares contre les gouvernements, les entreprises, les consommateurs et les appareils devrait augmenter pour passer à une attaque

**toutes les 2 secondes d'ici à 2031**

Source : *Cybercrime Magazine : Les 10 principales prévisions et statistiques de cybersécurité pour 2024*.

« Les services d'IA facilitent l'accès, augmentent le nombre de cybercriminels, et renforcent leurs moyens en améliorant l'échelle, la vitesse et l'efficacité des méthodes d'attaque existantes. »

James Babbage, Directeur général chargé des menaces à l'Agence nationale du Royaume-Uni contre la criminalité.

Les acteurs de menaces utilisent ces outils pour réduire le délai entre l'accès initial et le vol de données ou le déploiement d'un ransomware. Il s'agit d'un défi non seulement dans le contexte des ransomwares, mais également de l'ensemble des menaces ciblant les organisations : malwares d'extraction de cryptomonnaie, botnets, chevaux de Troie bancaires et logiciels espions.

L'impact cumulé de ces tendances devrait attirer l'attention des responsables de la cybersécurité dans le secteur manufacturier sur une vérité inéluctable : la motivation des cybercriminels à atteindre leurs objectifs dépasse souvent de loin la préparation des entreprises via des mesures préventives. Ils se donnent beaucoup de mal pour s'introduire dans l'environnement des entreprises sans être vus.

C'est pourquoi elles doivent équilibrer la prévention avec la détection et le traitement. C'est sur cela que se concentre l'approche de prévention d'ESET, en combinant plusieurs couches de technologies de sécurité. Elle a pour objectif de protéger en empêchant les malwares et les acteurs malveillants de pénétrer dans le système d'un utilisateur et de l'endommager.

Toutefois, si ces mesures sont contournées par des acteurs sophistiqués, il existe des moyens de détection et de réponse rapides et fiables pour atténuer les menaces avancées qui parviennent à compromettre un système. Il s'agit non seulement de verrouiller toutes les portes et les fenêtres, mais également d'installer des alarmes pour détecter tous les mouvements suspects si quelqu'un pénètre à l'intérieur de la maison.

Le Managed Detection & Response est un atout essentiel à cet égard. Il permet aux équipes chargées des opérations de sécurité (SecOps) de bénéficier d'une visibilité inégalée sur leur environnement informatique via une seule et même interface, et de repérer les anomalies grâce à des alertes hyper fiables. Le Managed Detection & Response est une évolution de l'EDR, qui optimise la détection, l'investigation, la réponse et la recherche de menaces en temps réel.

## L'XDR VOUS PERMET DE RÉPONDRE À PLUSIEURS QUESTIONS CLÉS SUR UNE CYBERATTAQUE :

Comment a-t-elle commencé ?

Où a-t-elle commencé ?

Quand a-t-elle commencé ?

Quels sont les endpoints infectés ?

Est-elle maîtrisée ?

Comment pouvons-nous l'éviter à l'avenir ?

Il unifie les détections pertinentes pour la sécurité sur les endpoints avec la télémétrie des outils de sécurité et d'entreprise, tels que la visibilité et l'analyse du réseau (NAV), la sécurité de la messagerie, la gestion des identités et des accès, la sécurité du Cloud, etc. Il s'agit d'une plateforme conçue pour le Cloud qui repose sur une infrastructure de big data pour fournir aux équipes de sécurité de la flexibilité, de l'évolutivité et des possibilités d'automatisation.

Plus important encore, il peut vous aider à prendre des mesures correctives rapides pour résoudre les incidents avant qu'ils n'aient un impact grave sur l'entreprise.

Cependant, même avec l'aide de l'XDR, les équipes de SecOps sont confrontées à des défis majeurs d'un point de vue organisationnel, en particulier les lacunes en matière de compétences, la complexité des outils, les contraintes de budgets et de ressources, l'intégration des outils, ainsi que l'évolution rapide du paysage des menaces. C'est pourquoi beaucoup d'entreprises manufacturières se tournent vers le MDR, qui est le moyen le plus efficace de détecter et de contenir des menaces sophistiquées en constante évolution.

## COMMENT LE MDR RÉPOND AUX MENACES ACTUELLES

Bien qu'il puisse varier d'un prestataire à l'autre, un service de MDR devrait inclure au moins les éléments suivants :

- **Surveillance et détection des menaces 24/7 :**
  Surveillance en continu du réseau, des endpoints et des environnements Cloud d'une organisation.

- **Recherche proactive des menaces :**
  Contrairement aux mesures de sécurité traditionnelles qui réagissent aux alertes, le MDR implique une recherche proactive qui permet d'identifier les menaces persistantes avancées (APT) et les vulnérabilités zero-day.

**51 %**

**est le nombre**

d'organisations qui ont formellement mis en place des méthodologies de recherche de menaces en 2024, contre 35 % en 2023.

Source : *SANS : L'évolution de la chasse aux menaces en entreprise : details de l'enquête SANS de 2024*.

- **Analyse et réponse d'experts :**
  L'expertise des professionnels de la sécurité permet une analyse nuancée et une prise de décision rapide, ce qui est essentiel pour faire face à des incidents de sécurité complexes.

- **Threat intelligence globale :**
  Des données télémétriques précises, actuelles, pertinentes, et collectées dans le monde entier, fournissant des informations utiles pour une réponse rapide aux incidents et une recherche optimisée des menaces.

Les organisations qui utilisent la télémétrie peuvent obtenir jusqu'à

# 60 %

# d'amélioration

de leur capacité à traiter les vulnérabilités et les menaces par rapport à celles qui s'appuient uniquement sur des mesures de sécurité traditionnelles.

Source : *Forrester : Les quatre étapes d'une sécurité plus proactive, 2024*.

- **Améliorations constantes :**
  En analysant les incidents passés, en utilisant des renseignements avancés sur les menaces, en se concentrant sur les menaces réelles et en fournissant des bilans et des rapports réguliers sur la sécurité, les services de MDR aident à prévenir la récurrence d'attaques similaires en permettant aux équipes d'améliorer la cyber-résilience.

## FONCTIONS CLÉS DU MDR

Le MDR peut apporter des avantages considérables aux organisations qui souhaitent atténuer les cyber-risques, mais qui ne disposent pas des ressources internes nécessaires, en les aidant efficacement à combler les lacunes en matière de compétences, réduire les coûts, et améliorer la détection et la réponse. Une solution performante doit permettre aux organisations de :

### Superviser

Des chasseurs de menaces expérimentés surveillent activement l'ensemble de l'environnement informatique du client ainsi que les malwares et les groupes de pirates afin de fournir des connaissances de haut niveau sur la situation.

### Détecter

Les acteurs de menaces utilisent d'innombrables méthodes pour se faufiler à travers les défenses du périmètre, mais avec l'analyse comportementale, ils peuvent être repérés et rapidement bloqués.

### Trier

Une première évaluation et une catégorisation des alertes permettent de filtrer les faux positifs et recueillir les informations nécessaires.

### Hiérarchiser

Des analyses intelligentes classent ces alertes en fonction de leur gravité afin de veiller à ce que les menaces les plus critiques soient traitées en premier. Il s'agit d'une phase critique du workflow de MDR, étant donné que de nombreuses équipes informatiques sont confrontées à un volume d'alertes trop important.

### Enquêter

Les outils automatisés et l'expertise humaine se combinent pour approfondir l'analyse des alertes à partir des données et des journaux afin de comprendre leur nature et leur portée. Ils doivent déterminer si une alerte est réellement positive ou non, et quelles mesures doivent être prises pour la résoudre.

### Répondre

Un service de MDR efficace fournit soit des actions de réponse de base pour bloquer et contenir une menace, soit un confinement et une remédiation complète de tous les systèmes compromis. Il peut s'agir de réinitialiser un mot de passe, appliquer des correctifs à des endpoints spécifiques, ou même réinstaller des ordinateurs.

## Les avantages de l'externalisation de la détection et de la réponse sont simples mais impressionnants :

- Le prestataire du service de MDR se charge de gérer la technologie du back-end, ce qui permet au personnel de se concentrer sur des tâches stratégiques de grande valeur plutôt que de crouler sous les alertes de sécurité.
- Le prestataire du service de MDR peut également optimiser la technologie du back-end pour s'aligner sur le profil de risque et l'infrastructure de chaque client.
- La détection et la réponse étant gérées par un tiers, il n'est pas nécessaire de verser des salaires élevés pour attirer et fidéliser les meilleurs talents.
- Les clients peuvent bénéficier des économies d'échelle de leur prestataire, de sa capacité à attirer les meilleurs talents, ainsi que de sa connaissance des autres entreprises clientes et des environnements de menaces.

## FONCTIONNALITÉS ESSENTIELLES À RECHERCHER DANS UNE SOLUTION DE MDR

Avec le grand nombre de solutions de MDR qui inondent le marché, il peut être difficile de savoir par où commencer. Recherchez un prestataire capable de proposer au moins les éléments suivants :

### Prise en main et réglage rapides

Les règles de détection, les exclusions et les paramètres devront être adaptés à chaque environnement informatique et aux menaces auxquelles l'entreprise est confrontée. Il est souhaitable d'accélérer l'intégration, mais pas au détriment des performances de détection, qui doivent être optimisées dès le premier jour. N'oubliez pas que la protection offerte par le MDR s'améliore généralement avec le temps.

### Vitesse

Réduisez le délai de détection et de réponse aux incidents de plusieurs mois à quelques minutes avec votre fournisseur de MDR. Vous devez stopper l'attaque dans ses phases initiales (découverte, mouvement latéral, persistance) avant que la charge utile ne soit déclenchée.

### Service 24/7

Les acteurs de menaces opèrent à partir de tous les fuseaux horaires et frappent souvent aux premières heures du jour ou pendant les week-ends et les jours fériés. Cela signifie que le MDR doit être opérationnel jour et nuit. Les indicateurs de compromission et d'attaque doivent faire l'objet d'une enquête immédiate, en temps réel.

### Solution facile à utiliser avec une interface simple et une courbe d'apprentissage réduite

La solution doit donc être accessible même aux novices de la sécurité informatique. Le tableau de bord, facile à utiliser, apporte une vision claire de l'état de la sécurité et des alertes importantes.

### Notifications personnalisables et options de reporting avancées

Afin de recevoir automatiquement ou à la demande des rapports sur les incidents, l'état de l'environnement et d'autres informations.

Il est ainsi facile de présenter l'état de la cybersécurité aux dirigeants, recevoir des alertes en temps utile et générer des rapports utiles pour les audits et la conformité.

### Compatibilité sans faille avec différentes infrastructures

Intégration efficace avec des outils de SIEM, de SOAR, des outils de ticketing, et bien d'autres. Vous devez pouvoir intégrer sans problème vos environnements mêmes s'ils comprennent plusieurs systèmes d'exploitation, des logiciels de sécurité existants ou des infrastructures sur site et dans le Cloud.

### Infrastructure technologique complète

La technologie sous-jacente est un élément clé d'une solution de MDR. Elle devrait inclure la détection et la réponse au niveau des endpoints ou étendues (XDR), la gestion des informations et des événements de sécurité (SIEM), ainsi que l'orchestration de la sécurité et la réponse (SOAR). Ces moyens devraient être fournis par le fournisseur de la solution de MDR ou par des outils tiers reliés par des API.

### Automatisation et IA

L'IA peut jouer un grand rôle dans l'identification des comportements anormaux et l'analyse de grands volumes de données pour trouver des signes de compromission ou d'attaque.

L'automatisation permet également d'exécuter rapidement une série d'actions visant à isoler les systèmes et contenir les menaces. Elles doivent cependant toujours être considérées comme une aide et non comme un substitut à l'expertise des analystes humains.

### Intelligence humaine

Aussi importantes que soient l'IA et l'automatisation, elles ont des limitations que seuls des experts humains peuvent adresser efficacement. Les professionnels expérimentés de la cybersécurité peuvent ajouter une compréhension contextuelle aux anomalies comportementales signalées par l'IA afin de déterminer si une alerte est réellement malveillante. Cela permet de réduire les faux positifs. Les humains sont également plus à même de s'adapter aux nouvelles menaces émergentes en temps réel.

### Threat Intelligence

Des flux de renseignements sur les menaces régulièrement mis à jour, générés par le fournisseur de services de MDR ou par des tiers, sont un élément clé de tout service de MDR efficace. Les informations devraient être collectées à partir de la télémétrie et analysées par des équipes d'experts en Threat Intelligence afin de révéler les méthodes d'attaque et les contre-mesures efficaces.

### Recherche de menaces

La recherche systématique et continue des menaces devrait faire partie de l'offre standard de tout service de MDR, afin d'éliminer les attaques les plus évasives.

### Remédiation

Aucune règle établie ne spécifie qui du fournisseur de services ou du client doit s'occuper de la remédiation/atténuation une fois qu'une menace a été découverte. Les acheteurs de services informatiques doivent rechercher l'offre qui correspond le mieux à leurs besoins et leurs capacités internes.

### Harmonisation

Veillez à ce que le service de MDR s'aligne sur le reste de l'environnement informatique, notamment en ce qui concerne l'intégration des informations produites dans les systèmes de gestion des tickets et les flux de travail internes.

Le fournisseur doit être en mesure de générer des rapports d'incidents et des informations sur l'état d'avancement pour une transparence totale.

### Conformité

Le service de MDR doit être en mesure de respecter toutes les exigences du client en matière de confidentialité, de résidence ou de conservation des données, ainsi que toutes les stipulations exigées par les polices d'assurance.

Le marché du MDR devrait croître à un taux de croissance annuel composé (TCAC) d'environ

# 24 %

de 2024 à 2029.

Source : *MarketsAndMarkets : Marché de la détection et de la réponse managées (MDR), 2024*.

# 5 raisons pour lesquelles les fabricants choisissent ESET MDR

ESET propose l'un des services de MDR les plus rapides et les plus efficaces du marché. Sa puissance réside dans l'association gagnante de l'homme et de l'IA pour identifier les comportements anormaux.

1. **Protection complète pour les environnements les plus réglementés et les plus isolés :** les services peuvent être fournis via le cloud, mais également par des équipements sur site dans des environnements isolés, ce qui permet de répondre aux besoins de l'industrie manufacturière qui a des normes réglementaires strictes.

2. **Détection et résolution en temps réel dans les 6 minutes, 24/7/365 :** avec ESET MDR, la recherche proactive de menaces s'appuie sur des renseignements à l'échelle mondiale provenant de plus de 100 millions d'endpoints. Les enquêtes menées par des experts permettent de détecter et de contenir les menaces en 5 à 10 minutes, 20 minutes en moyenne, en fonction de leur gravité. Le MDR offre une résolution rapide au niveau choisi : confinement immédiat des menaces suivi d'une notification au client avec les étapes suivantes recommandées (au besoin), ou avec MDR Ultimate, confinement des menaces et remédiation complète par les experts d'ESET.

3. **Minimum de bruit, maximum de protection :** l'IA et l'expertise humaine sont combinées pour atteindre des taux de protection de 99,6 % et un minimum de fausses alarmes (AV Comparatives, Business Security Test 2024, Août – Novembre). ESET utilise l'IA pour réduire le bruit et automatiser les processus, tandis que les experts en cybersécurité (tous en interne, aucun externalisé) s'occupent des communications et du contrôle de la qualité.

4. **Tableaux de bord consolidés et rapports conviviaux :** les clients obtiennent la visibilité dont ils ont besoin : le personnel informatique sur le terrain accède à un tableau de bord personnalisable qui offre une visibilité unique avec de puissantes fonctionnalités d'analyse ; les cadres dirigeants reçoivent des rapports d'incidents hebdomadaires et mensuels faciles à comprendre.

5. **Offre groupée attrayante avec tarification flexible :** le MDR aide les fabricants à économiser de l'argent tout en se conformant aux réglementations sectorielle set aux normes d'assurance en matière de cybersécurité, grâce à une protection complète qui comprend : la sécurité de nouvelle génération des endpoints, l'authentification multifacteur (MFA), le chiffrement, la gestion des vulnérabilités et des correctifs, et la défense contre les menaces mobiles pour chaque poste que vous achetez sans frais supplémentaires.

**COMME ÉLÉMENT D'UNE SÉCURITÉ GLOBALE :**
Les services ESET MDR et ESET MDR Ultimate peuvent être achetés dans le cadre de niveaux d'abonnement ESET PROTECT spécifiques pour prendre en charge une sécurité multicouche holistique.Ce sont des options plus complètes combinant des produits et des services de prévention,de détection et de réponse. Managés via une interface unique, ils comprennent :

### ESET PROTECT MDR
*Idéal pour les petites et moyennes entreprises*

- Console d'administration
- Protection pour endpoints
- Sécurité des serveurs
- Défense contre les menaces avancées
- Chiffrement intégral des disques
- Gestion des vulnérabilités et des correctifs
- Détection et réponse étendues
- Authentification multifacteur
- **Service MDR**
- **Service Premium Support**

### ESET PROTECT MDR Ultimate
*Idéal pour les grandes entreprises*

- Console d'administration
- Protection pour endpoints
- Sécurité des serveurs
- Défense contre les menaces avancées
- Chiffrement intégral des disques
- Gestion des vulnérabilités et des correctifs
- Détection et réponse étendues
- Authentification multifacteur
- **Service MDR Ultimate**
- **Service Premium Support Ultimate**

# Conclusion

La cybersécurité est un élément essentiel des opérations informatiques des fabricants. Pourtant, dans la plupart des cas, ce n'est pas leur centre d'intérêt principal, et cela ne devrait pas l'être. Elles doivent pouvoir se concentrer sur leur coeur de métier et laisser aux experts le soin de lutter contre une cohorte diversifiée, déterminée et croissante d'acteurs de menaces. C'est là qu'interviennent les partenaires de confiance, qui apportent des ressources étendues et des décennies d'expertise dans le secteur de la sécurité.

ESET MDR est conçu pour être compatible avec différentes infrastructures de fabrication. Il protège vos chaînes d'approvisionnement et votre technologie opérationnelle, assurant une intégration transparente avec vos systèmes de sécurité ICS et industriels existants, offrant une posture de sécurité unifiée pour les environnements de fabrication, réduisant le risque d'accès non autorisé ,sécurisant votre infrastructure cloud, et facilitant la conformité avec les politiques de gouvernance et de réglementation en matière de sécurité.

Des services sur mesure sont disponibles pour répondre aux différents besoins des entreprises manufacturières de toutes tailles. Il est temps d'éliminer les cyber-risques avec l'aide d'un expert.

**EN SAVOIR PLUS**

# À QUOI RESSEMBLE UN DÉPLOIEMENT EFFICACE DU MDR ?

## Electrical Consultants, Inc.

ECI est une société de conseil en conception et en ingénierie, spécialisée dans les projets d'infrastructure et de services publics d'électricité. Avec plus de 37 bureaux régionaux aux États-Unis et au Canada, ECI prend en charge l'ingénierie et la construction d'installations à haute tension et à grande échelle, en veillant à ce que chaque projet soit abordé avec innovation, précision et un dévouement envers l'excellence.

L'entreprise était confrontée à un défi important en matière de personnel, avec seulement une petite équipe dédiée à la gestion de la cybersécurité, ce qui rendait particulièrement difficile la surveillance en dehors des heures de bureau et la réponse rapide aux menaces. ECI avait besoin d'un moyen fiable et économique de surveiller les menaces et d'y répondre 24 heures sur 24 afin de protéger ses biens et ses opérations.

La mise en œuvre d'ESET MDR s'est faite simplement et n'a nécessité que des ajustements minimes. L'équipe de sécurité d'ESET a procédé à une évaluation initiale approfondie et a affiné les paramètres d'alertes pour optimiser la détection des menaces. Tout au long du processus de mise en œuvre, un ingénieur d'ESET a fourni une assistance pratique, garantissant une transition fluide et efficace.

« ESET MDR a détecté de nombreuses menaces et incidents que nous aurions manqués ou auxquels nous n'aurions pas réagi aussi rapidement. Dans au moins un cas, ESET MDR a permis d'éviter qu'un petit incident ne devienne un problème majeur pour notre entreprise. »

# À propos d'ESET

## **Défense proactive.** Notre activité consiste à minimiser la surface d'attaque.

Prenez une longueur d'avance sur les cybermenaces connues et émergentes grâce à notre approche préventive reposant sur l'IA et l'expertise humaine.

Bénéficiez d'une protection de haut niveau grâce à notre cyber threat intelligence interne, compilée et examinée depuis plus de 30 ans, qui alimente notre vaste réseau de R&D dirigée par des chercheurs reconnus. ESET protège votre organisation afin qu'elle puisse maximiser le potentiel de la technologie.

**Prévention multicouche**

**IA de pointe associée à une expertise humaine**

**Threat intelligence de renommée mondiale**

**Support local et personnalisé**

eset®
Cybersecurity
**Progress. Protected.**