VARS

Whitepaper

PROTECTION CONTRE LES INTRUSIONS POUR LES ENTREPRISES DU SECTEUR DE L'ÉNERGIE

Propulsée par Cynet

Défis d'entreprise

Généralement considérées comme des infrastructures critiques, les entreprises du secteur de l'énergie misaient traditionnellement sur l'inaccessibilité de leur environnement technologique interne pour se protéger des menaces. Aujourd'hui, les entreprises du secteur de l'énergie se concentrent sur la modernisation de leur réseau, en augmentant la connectivité entre les technologies de l'information (TI) et les technologies opérationnelles (TO) afin de fournir une myriade d'avantages et d'efficiences opérationnels. L'environnement s'est étendu à des points d'accès à distance et à des appareils en réseau utilisés tout au long de la chaîne d'approvisionnement pour améliorer la collaboration, l'accès et le contrôle. Cette interconnexion expose toutefois les entreprises du secteur de l'énergie à des risques considérables.

Les réseaux interconnectés et automatisés augmentent la surface d'attaque des menaces internes et externes. Les anciens systèmes de contrôle industriel (SCI) pour lesquels il est parfois impossible d'effectuer des mises à jour ou d'appliquer des correctifs sont particulièrement vulnérables aux menaces. Les environnements du secteur de l'énergie sont conçus pour optimiser la productivité et sont souvent dépourvus des contrôles de sécurité nécessaires à leur protection.

Les défis de la protection des environnements du secteur de l'énergie sont amplifiés par l'obligation d'assurer des services « en permanence ». Les contrôles de sécurité doivent être très précis et de plus en plus automatisés afin d'identifier et de réagir instantanément aux risques réels. Cela nécessite une visibilité totale sur l'ensemble de l'infrastructure afin de garantir une détection et une intervention rapides et efficaces aux menaces. Les menaces qui peuvent rapidement entraver ou interrompre complètement les opérations, comme les rançongiciels, doivent être découvertes et traitées le plus rapidement possible.

Les entreprises du secteur de l'énergie subissent également une pression accrue de la part des autorités de réglementation gouvernementales pour mettre en place des solutions de protection contre les menaces avancées. Les normes de protection NERC (National Electric Reliability Corporation) CIP (Critical Infrastructure Protection) et le cadre NIST (National Institute of Standards and Technology) CSF (Cybersecurity Framework) exigent des opérateurs qu'ils améliorent considérablement leur capacité à se protéger contre les cybermenaces, notamment par une visibilité en temps réel de l'ensemble de l'environnement afin de rapidement détecter et intervenir lors d'attaques avancées.

Principaux défis en matière de sécurité

Il est souvent impossible d'effectuer des mises à jour, d'appliquer des correctifs et de protéger adéquatement les applications et les systèmes existants

Le recours aux logiciels antivirus et de protection contre les logiciels malveillants traditionnels offre une protection limitée contre les menaces plus récentes telles que les rançongiciels et les attaques par crypto-verrouillage

« Sans Cynet, nous aurions eu besoin d'au moins cinq solutions différentes pour atteindre le même objectif, sans parler du temps et des coûts nécessaires pour que ces différentes solutions puissent fonctionner ensemble, à supposer que cela soit possible. »

CISO, Entreprise du secteur de l'énergie

« Nous étions submergés par les alertes de notre précédent fournisseur de EDR. La plateforme Cynet XDR est beaucoup plus précise et automatise la plupart des tâches à effectuer. »

Directeur de la sécurité, Entreprise du secteur de l'énergie

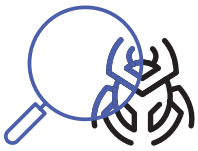
Principaux défis en matière de cybersécurité

La protection d'un environnement dans le secteur de l'énergie peut représenter un défi de taille, surtout lorsque l'environnement contient une combinaison de technologies anciennes et modernes, accessibles à une variété d'intervenants internes et de fournisseurs externes tout au long de la chaîne d'approvisionnement. Les fournisseurs d'énergie, en particulier ceux considérés comme de petite et de moyenne taille, sont confrontés à des défis similaires en matière de protection contre les menaces.

Augmentation des cyberattaques

Les agences gouvernementales de renseignement ont émis de nombreuses alertes aux opérateurs d'infrastructures critiques concernant les cybermenaces. Toutes les entreprises de ce secteur sont de plus en plus ciblées par des groupes criminels organisés et par des acteurs étatiques très habiles. Les attaques contre les fournisseurs d'énergie ont augmenté en volume et en sophistication. Les cyberattaques peuvent non seulement entraîner des vols de propriété intellectuelle et des interruptions de service, mais également avoir des conséquences plus graves si les contrôleurs de sécurité critiques sont perturbés.

La numérisation et l'interconnexion signifient que les criminels peuvent attaquer le périmètre et, en bout de ligne, se frayer un chemin jusqu'à des actifs d'infrastructure précieux. De simples attaques par hameçonnage ou de type cheval de Troie sur les points d'accès des employés ou des sous-traitants peuvent permettre d'accéder au réseau de l'entreprise. L'utilisation de techniques furtives de mouvement latéral et d'escalade de droits d'accès peut éventuellement permettre un accès illimité à l'ensemble de l'environnement.



Visibilité limitée sur l'ensemble de l'environnement

De nombreuses entreprises du secteur de l'énergie continuent d'avoir recours à des logiciels antivirus et de protection contre les logiciels malveillants qui ne peuvent détecter qu'une fraction des attaques avancées. Ces solutions ne fonctionnent généralement pas ou offrent une protection limitée sur les anciennes versions des systèmes d'exploitation sur lesquelles il est impossible d'effectuer des mises à jour ou d'appliquer des correctifs. En définitive, même les meilleures techniques heuristiques ou de détection des logiciels malveillants basées sur le comportement ne peuvent pas détecter et prévenir 100% des menaces.

De nombreuses entreprises du secteur de l'énergie exercent leurs activités sur plusieurs sites éloignés et utilisent des applications et des systèmes différents selon les sites. Ce manque d'uniformité pose des défis supplémentaires car les mesures de protection et les risques de sécurité peuvent différer d'un site à l'autre.

Pour étendre la protection au-delà des solutions d'antivirus, les entreprises ont recours à des outils supplémentaires tels que les outils de détection et d'intervention sur les points d'accès (EDR) et sur les réseaux (NDR). Les solutions EDR sont nées de la constatation que les menaces sont détectées après avoir réussi à contourner un point d'accès, puisqu'un logiciel antivirus n'arrive pas à les anticiper. Les solutions EDR surveillent donc en permanence les points d'accès afin de détecter les activités malveillantes et les comportements du système qui indiqueraient une intrusion.

Les solutions NDR étendent la protection au réseau afin de fournir une visibilité supplémentaire sur l'ensemble de l'environnement. Si une attaque contourne d'une manière ou d'une autre un logiciel antivirus et une solution EDR, la possibilité de détecter les mouvements latéraux et d'autres indicateurs de trafic réseau pourrait permettre de découvrir un acteur menaçant qui a réussi à s'infiltrer dans l'environnement.

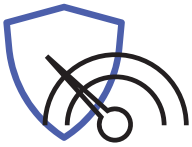
Principaux défis en matière de cybersécurité

(suite)

Dispositifs de contrôle de sécurité cloisonnés

Bien que chacun des contrôles de sécurité décrits précédemment améliore la visibilité nécessaire dans l'ensemble de l'environnement, ils ne sont pas sans inconvénient. Tout d'abord, les solutions EDR et NDR sont reconnues pour générer des fausses alertes. Les analystes de sécurité traquent celles-ci ou ont tendance à ignorer toutes les alertes, sauf celles qui semblent présenter les plus grands risques. Dans le premier cas, les analystes perdent un temps considérable. Dans le second cas, ignorer des alertes est contraire aux bonnes pratiques de sécurité et expose l'entreprise à des risques d'intrusion.

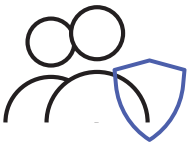
Les dispositifs de contrôle cloisonnés signifient également que l'équipe de sécurité doit surveiller et accéder à un plus grand nombre de « tableaux de bord » lorsqu'elle examine des menaces potentielles. Comme chaque outil de sécurité dispose d'une console de gestion distincte et présente les informations différemment, il est difficile pour les analystes de sécurité de donner un sens à toutes les informations présentées, puis de lier les activités entre les différents contrôles de sécurité pour avoir une vue d'ensemble. C'est pourquoi les attaques furtives sont capables de contourner les environnements dotés de plusieurs niveaux de contrôle



Des équipes de sécurité réduites avec des ressources limitées

Si l'on met de côté les dispositifs de contrôle cloisonnés, lesquels impliquent plusieurs manipulations, la plupart des outils de sécurité nécessitent un investissement humain significatif pour fonctionner. Lorsque des menaces sont découvertes, les analystes en sécurité doivent investiguer pour en déterminer la cause, puis découvrir l'étendue complète de l'attaque dans l'ensemble de l'environnement.

Une fois la cause et l'étendue de la menace déterminées, il faut remédier à toutes les composantes de celle-ci. Cela implique souvent d'accéder à plusieurs systèmes, ce qui peut s'avérer un processus long et fastidieux.



Des équipes de sécurité réduites avec une expertise limitée en matière de cybersécurité

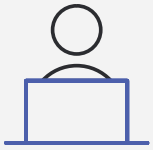
Avec l'évolution rapide du spectre des menaces, même les équipes de sécurité les plus importantes et les mieux financées sont vulnérables envers celles-ci. Il suffit d'étudier les intrusions commises dans les grandes entreprises pour se rendre compte que même les meilleurs experts en cybersécurité, dotés d'outils de pointe, ont du mal à protéger leurs organisations. Pour les équipes de sécurité réduites qui disposent de budgets technologiques et d'une expertise en cybersécurité limités, le risque d'intrusion augmente de façon exponentielle.

L’approche Cynet-VARS

Cynet a été conçu pour les équipes de cybersécurité réduites dont les ressources, l’expertise en cybersécurité et les budgets technologiques sont limités. Cynet XDR fournit une plateforme unique et unifiée pour prévenir et détecter automatiquement les vecteurs d’attaque auxquels sont confrontées les entreprises dans le secteur de l’énergie, investiguer sur ceux-ci et y remédier. La visibilité sur les points d’accès, les réseaux et les activités des utilisateurs, ainsi que la puissance de la simulation de ressources offrent la protection la plus élargie et la plus approfondie contre toutes les menaces.

Cynet XDR est la seule solution qui déclenche une investigation automatisée à la suite de chaque alerte quant aux points d’accès, aux utilisateurs ou aux réseaux, en dévoilant entièrement la cause et la portée de l’alerte et en appliquant toutes les mesures correctives nécessaires pour éliminer complètement la menace. Cynet offre également un large éventail d’actions correctives automatisées et pouvant être personnalisées pour traiter les incidents en fonction de vos préférences. De plus, Cynet offre les services d’une équipe d’experts en cybersécurité pour renforcer et guider votre équipe 24 heures sur 24, 7 jours sur 7. Cette offre est incluse dans la plateforme Cynet 360.

Les avantages de Cynet pour le secteur de l’énergie



Facile à déployer et à exploiter

L’agent Cynet peut être déployé sur plus de 5 000 points d’accès en moins d’une heure. Alors que de nombreuses solutions nécessitent des mois pour être déployées et devenir pleinement fonctionnelles, Cynet est prêt dans les 24 heures suivant le déploiement et fournit toutes les informations et protections disponibles dans la plateforme. La console Cynet a été conçue pour être intuitive et sans effort, de sorte que les petites équipes de sécurité n’ont pas besoin de plusieurs années d’expertise pour l’utiliser.

Visibilité totale dès la première utilisation

Cynet XDR offre une visibilité complète et de multiples points de télémétrie, ce qui permet de réduire les faux positifs et de détecter rapidement les menaces furtives. Une plateforme unique et unifiée de détection et d’intervention étendues (XDR) fournit un antivirus de nouvelle génération (NGAV), la détection et l’intervention sur les points d’accès (EDR), la détection et l’intervention sur le réseau (NDR), une analyse du comportement des utilisateurs et des entités (UEBA) et une technologie de simulation, le tout entièrement intégré et facilement configurable avec le tableau de bord unique qui est inclus.

Les avantages de Cynet pour le secteur de l'énergie

(suite)

Protection automatisée

L'*Incident Engine* de Cynet effectue automatiquement toutes les investigations sur les menaces et les mesures d'intervention requises, en identifiant la cause fondamentale et la portée complète des menaces à haut risque et en prenant les mesures appropriées pour éradiquer complètement la menace dans l'ensemble de l'environnement. Cynet offre en outre une liste de stratégies qui peuvent être exécutées automatiquement en réponse à une menace détectée pour une intervention immédiate ou qui peuvent être déclenchées manuellement pour fournir plus de supervision et de contrôle. Les actions d'intervention autonomes de Cynet offrent la protection complète que les petites équipes de sécurité surchargées recherchent.

Supervision de la détection et des interventions gérées incluse

Tous les clients de Cynet sont automatiquement protégés par un service complet de détection et d'interventions gérées (MDR), lequel est inclus dans la plateforme Cynet sans frais supplémentaires. Les petites équipes de sécurité des entreprises du secteur de l'énergie peuvent compter sur l'équipe MDR de Cynet (CyOps) pour surveiller de façon proactive leur environnement 24 heures sur 24, 7 jours sur 7, afin de s'assurer que rien n'est négligé. Elles peuvent contacter VARS à tout moment pour obtenir des conseils sur la configuration de la plateforme Cynet. CyOps leur offre une expertise en matière d'investigation des attaques et les guide dans toutes les interventions nécessaires. CyOps devient un prolongement de l'équipe de sécurité de l'entreprise du secteur de l'énergie, ajoutant des ressources et une expertise de classe mondiale en matière de cybersécurité.

Résumé

Protéger les environnements du secteur de l'énergie des cyberattaques représente un véritable défi, surtout avec une équipe de sécurité réduite et moins expérimentée. Avec des budgets limités, la plupart de ces entreprises de petite et de moyenne taille ne peuvent pas obtenir, intégrer et exploiter les contrôles de sécurité nécessaires pour protéger leur organisation contre les menaces avancées. Les entreprises du secteur de l'énergie peuvent compter sur la plateforme intuitive et complète de protection contre les intrusions de Cynet pour résoudre leurs enjeux de sécurité, tout en sachant qu'elles bénéficient toujours d'une équipe d'experts en cybersécurité pour les appuyer.