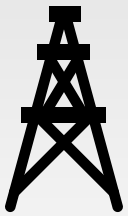
LIVRE BLANC

Les solutions Fortinet pour la cybersécurité du secteur du pétrole et du gaz

Une sécurité de bout-en-bout pour protéger les infrastructures et ressources stratégiques contre les menaces cyber et physiques

Synthèse

Les infrastructures IT des compagnies pétrolières et du gaz contribuent à la rentabilité de ces entreprises et à la stabilité économique et géopolitique du monde entier. Des sites de forage aux pipelines et aux raffineries, les processus de production pétrolière subissent des vulnérabilités que les assaillants ciblent avec des motivations et techniques multiples. Fortinet fournit des solutions de cybersécurité pour le secteur du pétrole et du gaz depuis plus d'une décennie, en intégrant de bout-en-bout la sécurité cyber et de la sécurité physique pour les réseaux distants. Pour les sites amont (upstream), intermédiaires (midstream) et aval (downstream) de la chaîne de production, les appliances renforcées de Fortinet résistent à des conditions environnementales extrêmes, tandis que leurs fonctions de sécurité protègent les sites distants vulnérables. La Security Fabric de Fortinet propose une approche globale de la sécurité sur le siège social des compagnies pétrolières et gazières. Cette architecture de sécurité s'étend jusqu'aux stations-service, fournissant ainsi un réseau sécurisé vers et au sein des sites.



60 % des acteurs du pétrole et du gaz ont récemment subi un incident majeur de cybersécurité.[1]

Les entreprises pétrolières et gazières possèdent et opèrent des éléments d'infrastructures critiques pour leur propre activité, mais aussi pour l'économie, voire la défense d'un pays. Les différents maillons de la chaîne de production sont des cibles privilégiées pour les assaillants dont les motivations sont multiples, allant du profit personnel à l'espionnage industriel et à la déstabilisation économique.[2] Comme le dit un auteur, « chaque maillon de la chaîne de valeur du pétrole et du gaz est actuellement exposé à des risques et les défenses conventionnelles ne suffisent plus. »[3]

Si cette affirmation peut paraître à première vue exagérée, le risque est pourtant bien réel. Une attaque sur le système de contrôle, de supervision et d'acquisition de données (SCADA) qui pilote une plate-forme offshore, un puits de pétrole, un oléoduc ou une raffinerie, ou sur les dispositifs IoT fournissant les données de surveillance à ces systèmes, peut avoir des conséquences dévastatrices.[4] Ceci peut aller de pertes financières conséquentes, à des interruptions de la chaîne de production, et, parfois, à des dommages corporels pour les collaborateurs et les communautés à proximité.

De telles attaques sur les infrastructures OT deviennent plus fréquentes[5]. Les infrastructures corporate des compagnies pétrolières et gazières sont également ciblées. Des attaques réussies peuvent divulguer des éléments de propriété intellectuelle, comme des relevés de données d'exploration, et compromettre des informations tant financières que personnelles. Outre les pertes financières résultant de ces attaques, celles-ci peuvent exposer les entreprises à un risque de non-conformité réglementaire.

Depuis plus d'une décennie, Fortinet fournit des solutions complètes de sécurité pour l'industrie pétrolière et gazière, pour les sites de forage sur terre comme en mer, les raffineries, les pipelines et même la station-service de quartier. Au cœur de l'offre Fortinet se trouve la Fortinet Security Fabric qui permet une intégration de bout en bout de la sécurité au sein des infrastructures étendues des entreprises de ce secteur.

Principaux défis de cybersécurité pour le secteur du pétrole et du gaz

Ces principaux défis sont les suivants :

Maîtrise des coûts

Les marchés pétroliers sont connus pour leurs fluctuations des cours de vente. Cette volatilité implique que des entreprises rentables peuvent subir, en quelques jours, une perte d'exploitation. La maîtrise des coûts reste donc une priorité pour optimiser leurs processus et ainsi surmonter les périodes déflationnistes.

Dans ces conditions, il est parfois impossible de remplacer des équipements coûteux ou obsolètes, même s'ils présentent des vulnérabilités. Il faut donc définir de nouvelles approches capables d'assurer la sécurité, mais sans impacter l'opérationnel. Beaucoup d'entreprises possèdent plusieurs composants d'infrastructure vulnérables, ce qui complique la tâche des équipes de sécurité.

La pénurie mondiale de compétences en matière de cybersécurité s'aggrave. Si 2,8 millions de spécialistes sont actuellement à la tâche, 4 millions manquent à l'appel.[6] La pénurie de spécialistes devient ainsi coûteuse et il est d'ailleurs parfois impossible de trouver certaines compétences spécifiques. Quoi qu'il en soit, embaucher ne résout pas le problème fondamental, à savoir que des processus manuels de sécurité sont inadaptés aux menaces qui se propagent de manière ultra-rapide.

Visibilité sur l'ensemble des systèmes IT et OT

Les objets connectés industriels IoT (IIoT) ont changé la donne en matière de sécurité des systèmes SCADA qui gèrent les forages, les pipelines et les raffineries. Les capteurs et dispositifs de contrôle connectés ont décloisonné les systèmes SCADA et les ont connectés à Internet, les rendant ainsi plus exposés aux cyberattaques.

Cela élargit bien sûr la surface d'attaque d'une entreprise. Cette problématique est exacerbée par le fait que de nombreux dispositifs de l'IIoT sont sans interface et ne peuvent être protégés par un logiciel de sécurité client, ni même recevoir de mises à jour de leur firmware. Pour pallier ces failles, les entreprises déploient souvent des solutions de sécurité distinctes et autonomes.[7] Le cloisonnement qui en résulte est source de complexité[8] et pèse sur la visibilité : de quoi retarder la détection, la prévention et la réponse aux menaces. Le risque de passer à côté d'une menace véloce est donc plus important.

Productivité opérationnelle

Cette fragmentation de l'architecture pèse sur la productivité des équipes de cybersécurité. L'automatisation des processus est impossible sans une intégration de bout en bout de toutes les composantes de sécurité. Sans cette automatisation, les processus manuels de sécurité mobilisent inutilement les ingénieurs en sécurité. D'autre part, c'est la complexité qui s'accentue, obligeant les professionnels à se former à de multiples produits de sécurité existants. À titre d'exemple, certaines équipes doivent mobiliser plusieurs collaborateurs dans les jours qui précèdent un audit pour que les rapports puissent être préparés manuellement.

Ces architectures cloisonnées génèrent également des redondances dans la gestion des applications, y compris dans les licences logicielles et matérielles, ce qui pèse sur les équipes des services juridiques, achats et finances qui gèrent ces licences. Les entreprises pourraient également constater une inflation de leur budget IT qui résulte d'un appel à plusieurs fournisseurs et de doublons entre les fonctionnalités de différents produits.

Expérience client

Les stations-service mettent à la disposition de la clientèle divers outils électroniques, notamment des pompes en libre-service, des applications mobiles et des cartes de fidélité. Toute transaction doit être conforme aux exigences de la norme PCI DSS, et cette conformité doit être prouvée grâce à un reporting. Les performances des capteurs IoT qui surveillent le niveau des réservoirs, les températures de réfrigération, etc. Ont également un impact sur l'expérience client. La protection de l'infrastructure d'un magasin contre les cybermenaces est primordiale, tant pour le respect des règles que pour la visibilité et l'image de la marque. Cette image de marque est véhiculée par les fournisseurs en amont, en milieu de chaîne et en aval, car ces détaillants portent généralement les logos des grands producteurs.

Reporting de conformité

Les entreprises du secteur de l'énergie sont soumises à un large éventail de réglementations et de normes, des exigences environnementales pour le forage et le raffinage, à celles de la cybersécurité. Malheureusement, une architecture de sécurité fragmentée et hétérogène rend la préparation des rapports difficile et fastidieuse. Qui plus est, l'incapacité à démontrer la conformité des procédures peut nuire à la réputation de marque et entraîner des pénalités substantielles.

Cas d'utilisation

Les cas d'utilisation de la cybersécurité pour les acteurs du pétrole et du gaz sont les suivants :

Sécuriser l'infrastructure amont

Les entreprises spécialisées dans l'extraction d'énergies fossiles doivent protéger une infrastructure complexe et multisite, sur terre et en mer. Ces sites constituent des cibles de choix pour les hackers dont l'objectif est de perturber l'opérationnel, causer des dommages environnementaux, voire s'en prendre à l'intégrité physique des collaborateurs ou des communautés avoisinantes.

Pour protéger ces sites, chaque volet de la sécurité, des systèmes de contrôle industriel à la sécurité physique, doit être pris en compte pour définir une visibilité et un contrôle centralisés. L'infrastructure de surveillance sur un forage de petite envergure doit être aussi importante qu'au siège social et à disposition des équipes opérationnelles de sécurité.

La **Fortinet Security Fabric** propose une sécurité cyber et physique intégrée et intégrale pour le secteur du pétrole et du gaz. Les pare-feu nouvelle-génération (NGFW) **FortiGate Rugged** et les points d'accès sans fil **FortiAP Outdoor** offrent une sécurité robuste et sont adaptés aux conditions extrêmes des plateformes de forage et d'exploration, en terre comme sur mer. Ces NGFW reçoivent des informations sur les menaces qui ciblent spécifiquement les systèmes de contrôle industriel

(ICS) et SCADA, des informations fournies par **FortiGuard Labs**. **FortiCamera** et **FortiRecorder** protègent contre les intrusions physiques, tandis que **Fortinet Secure SD-WAN** et **Fortinet SD-Branch** déploient un réseau sécurisé vers et au sein des sites distants. **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** et **FortiNAC**, généralement déployés au sein de l'infrastructure corporate sur le siège social, offrent des fonctions de sécurité pour ces sites distants les plus vulnérables.

Sécuriser l'infrastructure intermédiaire

L'infrastructure de transport d'hydrocarbures étend la surface d'attaque d'une entreprise sur des centaines, voire des milliers de kilomètres. Les pipelines peuvent subir des fuites accidentelles et des tentatives de sabotage, tandis que les systèmes SCADA et les dispositifs IIoT de surveillance sont souvent vulnérables.[9] Le bilan d'une attaque réussie peut être potentiellement catastrophique d'un point de vue environnemental et en termes de vies humaines.

Les opérateurs d'infrastructures intermédiaires ont adopté le modèle PERA (Purdue Enterprise Reference Architecture) en tant que référence pour concevoir leur infrastructure électronique.[10] Mais si PERA permet de définir la localisation de la sécurité dans sein de l'architecture, elle n'offre que peu de conseils sur la conception de l'architecture de cybersécurité.

La **Fortinet Security Fabric** permet d'élaborer une architecture qui intègre cybersécurité, sécurité physique et sécurité du réseau. Les pare-feu **FortiGate Rugged** et les points d'accès sans fil **FortiAP Outdoor** déploient une protection robuste et sont adaptés aux environnements distants et extérieurs parcourus par les pipelines. **FortiCamera** et **FortiRecorder** alertent sur les intrusions physiques, tandis que Fortinet **Secure SD-WAN** et **Fortinet SD-Branch** apportent un réseau sécurisé aux stations de pompage et autres sites distants. Différentes plateformes fournies depuis le siège social offrent des couches supplémentaires de protection : **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** et **FortiNAC**, pour ne citer qu'eux.

« Les systèmes OT utilisent souvent des technologies obsolètes et leur infrastructure de sécurité est moins développée. Deux raisons qui expliquent le plus fort taux de réussite des assaillants. »[11]

« Les états disposant de compétences cyber mènent souvent des opérations de reconnaissance ciblant des infrastructures critiques, pour ainsi se positionner et préparer des exactions plus dommageables. »[12]

Sécuriser l'infrastructure en aval

Les raffineries transforment le pétrole brut en différents combustibles et ce processus n'est pas sans danger physique. Les opérations en aval, tout comme celles en amont et intermédiaires, sont la cible d'attaques physiques et cyber. Ces attaques peuvent posent un danger physique aux collaborateurs et au grand public. Celles qui réussissent vont jusqu'à impacter l'économie d'un pays en causant des pénuries. Les menaces peuvent provenir de l'extérieur, de l'intérieur et de tiers. Et si certaines attaques internes sont délibérées, d'autres sont davantage fortuites.

Pour protéger des sites aussi versatiles, les équipes de sécurité doivent disposer d'une visibilité à partir d'une interface unique, et ce, sur l'ensemble du réseau et de l'infrastructure de surveillance. La **Fortinet Security Fabric** déploie une sécurité cyber et physique sur ces sites, de manière intégrée et globale. Les pare-feu **FortiGate Rugged** et les points d'accès dans fil **FortiAP Outdoor** sont adaptés à de nombreux défis environnementaux. **FortiCamera** et **FortiRecorder** intègrent la surveillance physique au sein de la Security Fabric. Différents outils de sécurité déploient des couches spécifiques de protection, parmi lesquels **FortiManager**, **FortiAnalyzer**, **FortiSIEM**, **FortiInsight**, **FortiClient**, **FortiEDR**, **FortiPresence** et **FortiNAC**.

Sécuriser l'infrastructure corporate

Les infrastructures corporate des entreprises du pétrole et du gaz hébergent de nombreuses données critiques : données de géolocalisation et d'exploration, informations financières et données personnelles de collaborateurs et de clients. La majorité de ces entreprises disposent de collaborateurs nomades, de partenaires externes accédant aux ressources corporate et de services fournis depuis de multiples clouds. Au-delà de protéger ces ressources contre des attaques externes, il est essentiel de prévenir le risque interne de divulguer fortuitement ou volontairement des données confidentielles.

Si une architecture fragmentée et la présence d'utilisateurs nomades pèsent sur la sécurité et sur la productivité opérationnelle, une visibilité à partir d'une interface unifiée et un contrôle centralisé améliorent ces deux domaines. Une infrastructure de sécurité étroitement intégrée automatise la détection et la prise en charge des menaces, ainsi que le reporting, libérant ainsi du temps parmi les équipes de sécurité.

La **Fortinet Security Fabric** fournit une architecture intégrée de sécurité qui rend cela possible. Fortinet couvre la totalité de la surface d'attaque, du data center aux environnements cloud multiples et à l'edge réseau, à l'aide d'une protection large, intégrée et automatisée. Les solutions **Fortinet Dynamic Cloud Security** lèvent les barrières entre les multiples clouds privés et publics, ce qui favorise une application cohérente des règles de sécurité. **FortiManager**, **FortiAnalyzer**, et **FortiSIEM** offrent l'ensemble des fonctions de gestion et de traitement analytique nécessaires. **FortiInsight** et **FortiDeceptor** assurent une protection contre les menaces internes. Les entreprises peuvent également protéger les dispositifs et applications à l'aide **FortiWeb**, **FortiMail**, **FortiClient** et **FortiEDR**. Enfin, en présence d'utilisateurs mobiles et de leurs dispositifs, **FortiAuthenticator** et **FortiToken** leur apportent un accès sécurisé au réseau corporate. Une segmentation de type intent-based, assurée par les pare-feu **FortiGate,** renforce le niveau de sécurité des utilisateurs distants et limite leur accès aux données et systèmes qui leur sont autorisés.

Seuls 17 % des professionnels de la sécurité dans le pétrole et le gaz estiment qu'il est fort probable qu'ils sachent repérer une cyberattaque sophistiquée.[13]

Sécuriser les points de vente d'essence et de gaz

Les stations d'essence et de gaz vendent généralement d'autres produits également et, à ce titre, opèrent de manière similaire aux magasins classiques. Elles doivent gérer de nombreux dispositifs IoT pour mesurer le niveau de leurs réservoirs, les températures des réfrigérateurs, ainsi que des caméras IP. La présence de réservoirs sur les points de vente implique des exigences supplémentaires en matière de sécurité et de conformité, tandis que les points de vente extérieurs en libre-service présentent également un risque. Ainsi, l'intégration de la sécurité cyber et physique devient essentielle, tout comme la conformité à la norme PCI et la nécessité d'offrir une expérience agréable en magasin.

Ces multiples besoins métier et de sécurité impliquent qu'une station-service doit bénéficier d'une architecture de sécurité étroitement intégrée. Cette infrastructure élimine tout processus manuel et de recherche de solution qui ralentit la réponse aux menaces et éloigne les équipes sur site de leur mission d'être au service du client.

Les solutions réseau et de sécurité de Fortinet permettent d'interconnecter différents sites, pour offrir une sécurité réseau robuste et automatiser le reporting de conformité. Les **pare-feu NGFW FortiGate** fournissent une protection robuste sur l'ensemble de la surface d'attaque. Le large panel de fonctionnalités intégrées en natif évite de devoir investir dans du matériel supplémentaire chez un autre éditeur. **Fortinet Secure SD-WAN** offre un réseau sécurisé à tous les points de vente sans avoir à déployer un réseau MPLS onéreux. Enfin, les solutions **Fortinet SD-Branch** , qui incluent **FortiAP**, **FortiSwitch** et **FortiNAC**, étendent la sécurité Fortinet vers les infrastructures de chaque point de vente.

Cette infrastructure permet de fournir des services de sécurité mutualisés à partir du siège social, via l'outil de gestion des accès et des identités **FortiAuthenticator**, les solutions de sécurité pour les terminaux **FortiClient** et **FortiEDR**, les fonctions analytiques UEBA par **FortiInsight** et la technologie de leurre **FortiDeceptor**. De plus, les outils de gestion et de traitement analytique **FortiManager**, **FortiAnalyzer** et **FortiSIEM** proposent une interface unifiée de visibilité et un reporting automatisé pour évaluer la conformité avec des référentiels comme PCI SSF (Software Security Framework).[14] Cette infrastructure est adossée à des fonctions d'intelligence artificielle (IA) et machine-learning (ML) pour détecter et traiter les menaces inconnues.

Les atouts de Fortinet

Voici les principaux facteurs de différenciation qui font de Fortinet un choix pertinent pour les acteurs du pétrole et du gaz :

Une architecture intégrée

La Fortinet Security Fabric propose une architecture de sécurité intégrée et fournie par un seul éditeur sur les environnements IT et OT, pour chaque phase du processus de production, de la protection à la détection et la prise en charge des menaces, pour davantage de visibilité et de contrôle.

Réseau, cybersécurité et sécurité physique

Fortinet permet de consolider les fonctions de réseau, de cybersécurité et de surveillance sur une interface unifiée, que ces fonctions soient actives sur le siège social, sur un site distant de forage ou sur la station-service de quartier.

Appliances de sécurité renforcées

Fortinet offre un large panel d'appliances renforcées, adaptées à différentes conditions environnementales, pour sécuriser toutes les phases du processus de production et de livraison.

« Pour défendre efficacement les systèmes SCADA, il s'agit de connaître les problématiques potentielles et de savoir planifier. Investir dans une ligne de défense efficace n'est plus une option, mais un impératif."[17]

Des performances optimales

Les pare-feu NGFW FortiGate savent opérer au sein d'environnements complexes et distants pour offrir des performances optimales, même en cas d'inspection du trafic chiffré sous SSL/TLS. Fortinet a été nommé en tant que Leader dans le Magic Quadrant de Gartner pour les pare-feu réseau[15] et a obtenu la meilleure note dans la NGFW Security Value Map de NSS Labs.[16]

Une veille pertinente sur les menaces

Au-delà d'identifier les menaces IT, FortiGuard Labs offre une veille sur les menaces spécifiques aux systèmes OT, le résultat de 15 années d'expérience sur le terrain. Pour détecter plus précisément les menaces zero-day, Fortinet analyse les fichiers à l'aide de technologies IA et ML éprouvées.

Un réseau étendu de partenaires

Le programme partenaires Fabric-Ready de Fortinet comprend le plus grand réseau de partenaires disposant d'une expérience dans l'OT et les systèmes industriels.

Une sécurité élargie avec un nombre restreint de dispositifs

Fortinet offre différentes fonctions de sécurité et réseau, à partir d'un seul équipement, alors que les outils concurrents exigent souvent de multiples dispositifs et licences pour le même périmètre fonctionnel.

Conclusion

Les acteurs du pétrole et du gaz opèrent des infrastructures parmi les plus critiques au monde. Toute attaque réussie induit de lourds dommages économiques, environnementaux et même sur l'intégrité physique des personnes. Fortinet offre une solution de sécurité cyber et physique large, intégrée et automatisée qui maîtrise les risques et protège les infrastructures en expansion.

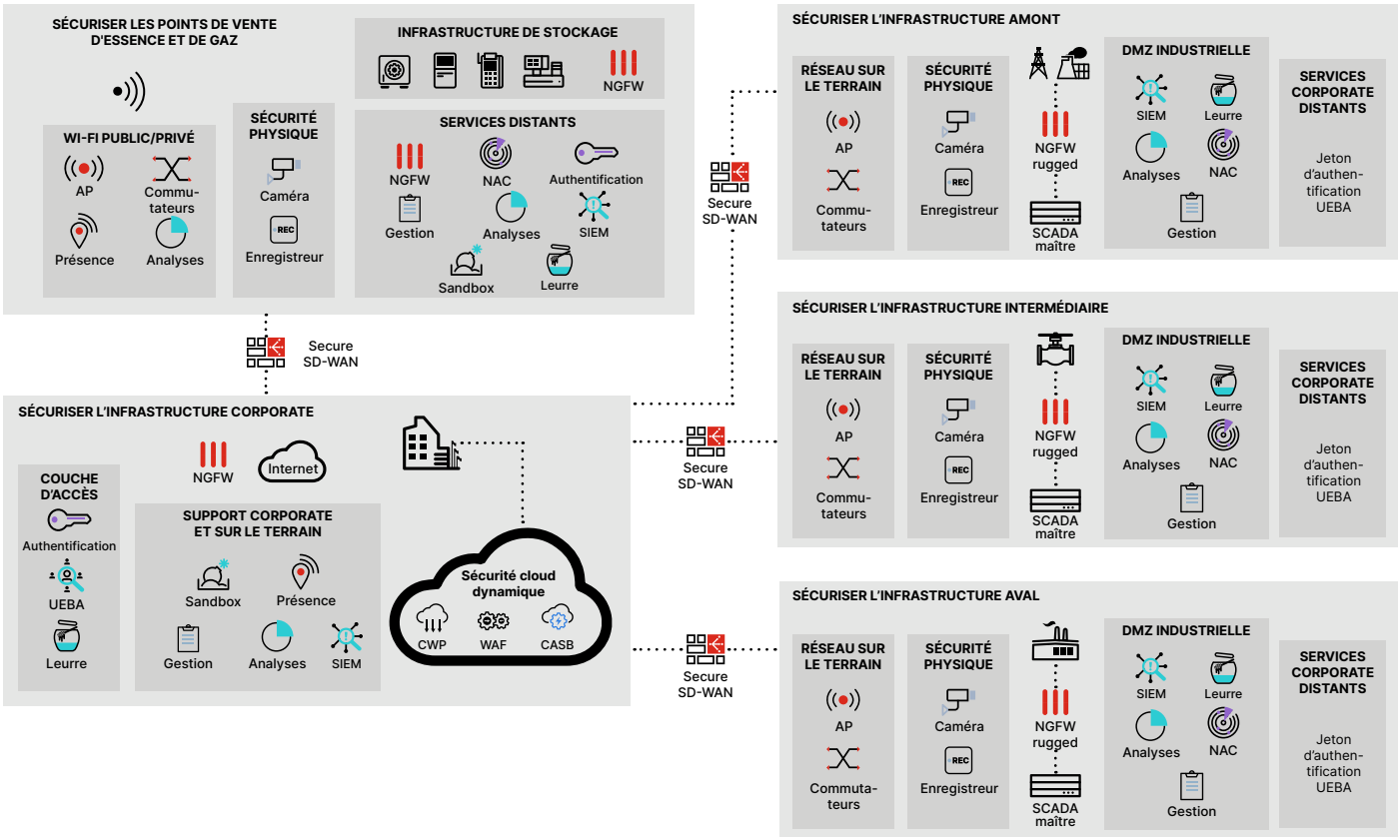


Schéma 1 : les solutions de cybersécurité de Fortinet pour les acteurs du pétrole et du gaz répondent à des cas d'utilisation qui couvrent la totalité du processus, de l'exploration à la distribution.

1 Jeff Williams, et al., « Six cybersecurity issues for oil and gas companies, » EY, 12 avril 2019.
2 « Independent Study Pinpoints Significant SCADA/ICS Security Risks, » Fortinet, 28 juin, 2019.
3 Aleksander Gorkowienko, « Ensuring Oil and Gas Critical Infrastructure Security, » Oil & Gas IQ, 26 juin 2019.
4 Idem.
5 Adlan Chaykin, « New systems, new cyber threats, » Petroleum Economist, 12 novembre 2019.
6 « Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019, » (ISC)², 2019.
7 John Maddison, « The Problem with Too Many Security Options, » Fortinet, 9 mai 2019.
8 « Strategies That Reduce Complexity and Simplify Security Operations, » Fortinet, 3 juillet 2019.
9 William T. Shaw, « SCADA System Vulnerabilities to Cyber Attack, » Electric Energy Online, consulté le 21 janvier 2020.
10 Gary Mintchell, « Purdue Enterprise Reference Architecture Meets IIoT, » The Manufacturing Connection, 16 mars 2016.
11 « Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems, » Fortinet, 16 mai 2019.
12 Adlan Chaykin, « New systems, new cyber threats, » Petroleum Economist, 12 novembre 2019.
13 Jeff Williams, et al., « Six cybersecurity issues for oil and gas companies, » EY, 12 avril 2019.
14 « Complying with PCI SSF Without Sacrificing Customer Experience: What to Look for in a Security Solution, » Fortinet, 24 août 2019.
15 « Gartner recognized Fortinet a Leader in the 2019 Magic Quadrant for Network Firewalls, » Fortinet, consulté le 15 janvier 2020.
16 « Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests, » Fortinet, janvier 2019.
17 Aleksander Gorkowienko, « Ensuring Oil and Gas Critical Infrastructure Security, » Oil & Gas IQ, 26 juin 2019.

FORTINET

www.fortinet.com/fr

3. juin 2022, 15:45
532367-A-1-FR