LIVRE BLANC

Les solutions de cybersécurité Fortinet pour la production industrielle

Une plateforme unifiée pour protéger les ressources IT et OT des sites industriels contre les menaces sophistiquées

Synthèse

Les industriels pilotent des équipements onéreux et sophistiqués au sein de leurs usines, tandis que les systèmes qui gèrent l'outil industriel sont de plus en plus connectés à Internet. Ce contexte a des conséquences directes en matière de cybersécurité, avec des menaces potentielles sur la sûreté physique, voire sur la sécurité d'un pays. Les industriels s'investissent pour protéger leurs systèmes tout en répondant aux exigences opérationnelles d'efficacité, de continuité des opérations, d'intégrité de leurs produits et de mise en conformité. La Fortinet Security Fabric offre une architecture de sécurité large, intégrée et automatisée qui couvre tous les aspects industriels, du back-office à la chaîne de production, des systèmes cloisonnés à ceux connectés en ligne, des utilisateurs internes aux prestataires externes.

L'exploitation de vulnérabilités a progressé en volume et prévalence sur l'année écoulée pour la majorité des fournisseurs de systèmes ICS et SCADA.[4]

Le secteur industriel opère aujourd'hui une convergence. Les acteurs qui, autrefois, fonctionnaient de manière indépendante disposent désormais d'un réseau de partenaires qui interviennent à différentes étapes du processus de fabrication.[1] Les systèmes électroniques qui gèrent le processus industriel, autrefois cloisonnés, sont désormais de plus en plus interconnectés avec les systèmes IT, et donc, avec Internet. Il en résulte que ces systèmes industriels (OT pour operational technology), et notamment les systèmes de contrôle industriel et SCADA, s'exposent à une surface d'attaque toujours plus large et deviennent la cible de cybercriminels impliqués dans des actions de terrorisme, d'espionnage ou de cyber-guerre.

Les systèmes OT, qui se décloisonnent progressivement, subissent désormais les cyber-risques IT classiques, ainsi que des exploits conçus sur mesure pour l'OT.[2] Une enquête pointe que 74 % des professionnels ont ainsi subi une attaque au cours des 12 mois passés.[3] Les attaques sur les infrastructures critiques du secteur industriel peuvent aboutir à des pertes financières, ternir la réputation de leur victimes, causer des pertes humaines, voire impacter la sécurité d'un pays.

Fortinet protège nombre d'environnements OT critiques dans l'énergie, la défense, la production industrielle, l'agroalimentaire et le transport depuis 2005. En tirant parti de la Fortinet Security Fabric pour sécuriser leurs infrastructures complexes, les entreprises peuvent déployer leur cybersécurité sur leurs environnements IT et OT, des chaînes de production aux data centers et à de multiples clouds.

Principaux défis de cybersécurité en milieu industriel

Sécurité des sites de production, des travailleurs et des communautés

Les sites industriels hébergent des machines susceptibles d'entraîner des blessures et des décès en cas de dysfonctionnement ou d'erreurs dans leurs opérations. Dans le contexte actuel des menaces, toute attaque, cyber ou physique, peut mettre à l'arrêt les activités et induire un risque de sécurité pour les télétravailleurs ou les communautés avoisinantes.[5] De plus, les attaques peuvent peser sur la sécurité des produits manufacturés, ce qui étend le risque à un périmètre géographique plus large.

Chez nombre d'industriels, les systèmes de sécurité IT, OT et physiques sont cloisonnés. L'intégration de l'architecture de sécurité IT entre le data center, les multiples clouds et l'edge est une tâche plutôt complexe. Face à des adversaires capables de coordonner attaques cyber et physiques de manière concomitante, l'intégration de toutes les composantes de sécurité dans une optique de visibilité centralisée est sans doute le seul moyen de protéger les vies humaines.

Productivité et haute disponibilité

Toute interruption fortuite d'activité induit de lourdes conséquences financières pour un industriel : un dysfonctionnement peut générer des problèmes en cascade, en amont (chaîne logistique) et en aval (canaux de distribution). Or, c'est précisément ce que visent certaines cyberattaques sur les industriels tandis que d'autres se propagent sur le réseau interne piraté, avec des conséquences sur l'opérationnel.

Historiquement cloisonnés et bénéficiant de mises à jour moins fréquentes, les systèmes OT sont souvent moins sécurisés que leurs homologues IT. Ils sont, aujourd'hui, régulièrement ciblés par les cybercriminels, sur des sites qu'il est plutôt simple d'infiltrer.[6] Même les systèmes OT cloisonnés peuvent être piratés, en infectant les mises à jour logicielles des éditeurs, avant leur installation.

Productivité opérationnelle
Les opérations de sécurité cloisonnées qui résultent d'une intégration aléatoire entre différents outils de sécurité entraînent des pertes de productivité opérationnelles. Sans une intégration étroite, les tâches manuelles (corrélation de logs provenant de différents systèmes, consolidation de multiples rapports de conformité, etc.) mobilisent fortement les professionnels de sécurité, au détriment de projets plus stratégiques.

Le cloisonnement de l'architecture induit une gestion redondante des applications. L'utilisation de produits spécifiques et distincts exige que les équipes de sécurité acquièrent davantage de compétences. Ceci peut également aboutir à des coûts de licence logicielle et matérielle plus importants et à une lourde charge de travail pour administrer de multiples licences. Autant de facteurs susceptibles de creuser les budgets opérationnels.

Expérience client
Que leurs produits soient grand public ou professionnels, les industriels s'engagent auprès de clients de manière très ciblée, en utilisant les réseaux sociaux et autres outils d'interaction, ainsi que leur présence sur le web. Ces efforts légitimes peuvent être contrés par les cybercriminels qui manipulent les réseaux sociaux dans un but lucratif. Une enquête révèle ainsi que plus de la moitié des comptes de réseaux sociaux seraient frauduleux.[7]

Pour les industriels, il devient essentiel de sécuriser leur présence sur le web et leurs interactions avec les réseaux sociaux : en effet, le détournement de données de clients potentiels lors d'une étape amont de leur cycle d'achat peut ternir la réputation de l'entreprise. D'autres facteurs, comme l'indisponibilité d'un site web ou une rupture sur certains produits pour cause de production défaillante, peuvent nuire à l'expérience des clients.

Intégrité du produit
Une qualité dégradée du produit, même temporaire, peut être désastreuse pour la réputation d'une marque. Par exemple, une cyberattaque peut cibler l'infrastructure OT d'un industriel de l'agroalimentaire, avec pour impact une légère modification de la température de conservation des aliments ou du temps de cuisson. Il peut en résulter un gaspillage ou une dégradation de la qualité d'un produit. Selon la nature de ce produit, c'est la santé du consommateur et sa sécurité qui peuvent être impactées.

Conformité
Selon le produit qu'ils fabriquent, les clients sont tenus de respecter différentes réglementations et normes. Les pénalités qui s'appliquent en cas de non-conformité sont parfois importantes. Mais le coût est encore plus élevé si la réputation de l'industriel est impactée suite à un piratage.[8]

Les entreprises doivent être capables de démontrer leur conformité avec différentes réglementations et normes, sans devoir affecter leurs équipes à des tâches d'audit et de reporting, ce qui mobilise de nombreuses heures de travail et augmente le risque d'erreurs humaines dans le reporting. La corrélation manuelle des données d'audit est généralement toujours nécessaire lorsque l'infrastructure de cybersécurité est fragmentée.

« Les attaques cybercriminelles sont présentées comme des menaces sérieuses depuis des années. Mais plus récemment, ces attaques sont passées de la théorie à la réalité. »[9]

53 % des identifiants de réseaux sociaux et 25 % des nouveaux comptes applicatifs sont frauduleux.[10]

Cas d'utilisation

Voici les principaux cas d'utilisation traités par les solutions de Fortinet :

45 % des opérateurs de systèmes ICS et SCADA n'utilisent pas un contrôle d'accès basé sur le rôle.[14]

Infrastructure corporate

Si la chaîne de production est au centre de l'outil industriel, les fabricants industriels présentent également des besoins similaires à ceux des autres entreprises. Le réseau corporate IT héberge des données financières, des éléments de propriété intellectuelle, des informations de support, etc. Comme dans d'autres secteurs d'activité, les industriels utilisent des applications et infrastructures cloud[11] tandis que les objets connectés se multiplient sur l'edge réseau.[12]

Que des données sensibles y soient hébergées ou pas, l'infrastructure corporate exige une solution de cybersécurité intégrée et automatisée. La Fortinet Security Fabric propose une telle solution, adossée aux pare-feux nouvelle-génération FortiGate et à la veille sur les menaces de FortiGuard Labs. Différents outils de cybersécurité de Fortinet sont intégrés en toute transparence au sein de la Security Fabric, ainsi que des dizaines d'autres solutions proposées par les partenaires Fabric-ready de Fortinet. D'autre part, un large éventail d'API rend l'intégration d'outils tiers possible.

Des systèmes de production cloisonnés

Si la majorité des systèmes OT est désormais connectée aux systèmes IT, des études récentes menées par Forrester indiquent que 40 % des systèmes OT sont toujours cloisonnés, et donc non connectés à un réseau.[13] On pourrait penser que ces systèmes sont à l'abri des cyberattaques. Cependant, ils utilisent des systèmes IP de contrôle tandis que les administrateurs continuent à installer des mises à jour logicielles fournies par les constructeurs. Il devient possible pour un assaillant de s'introduire dans un système en infectant les mises à jour via le réseau du constructeur. Même si les systèmes cloisonnés n'hébergent pas de données sensibles, toute intrusion peut aboutir à des perturbations coûteuses et à des problématiques de sécurité.

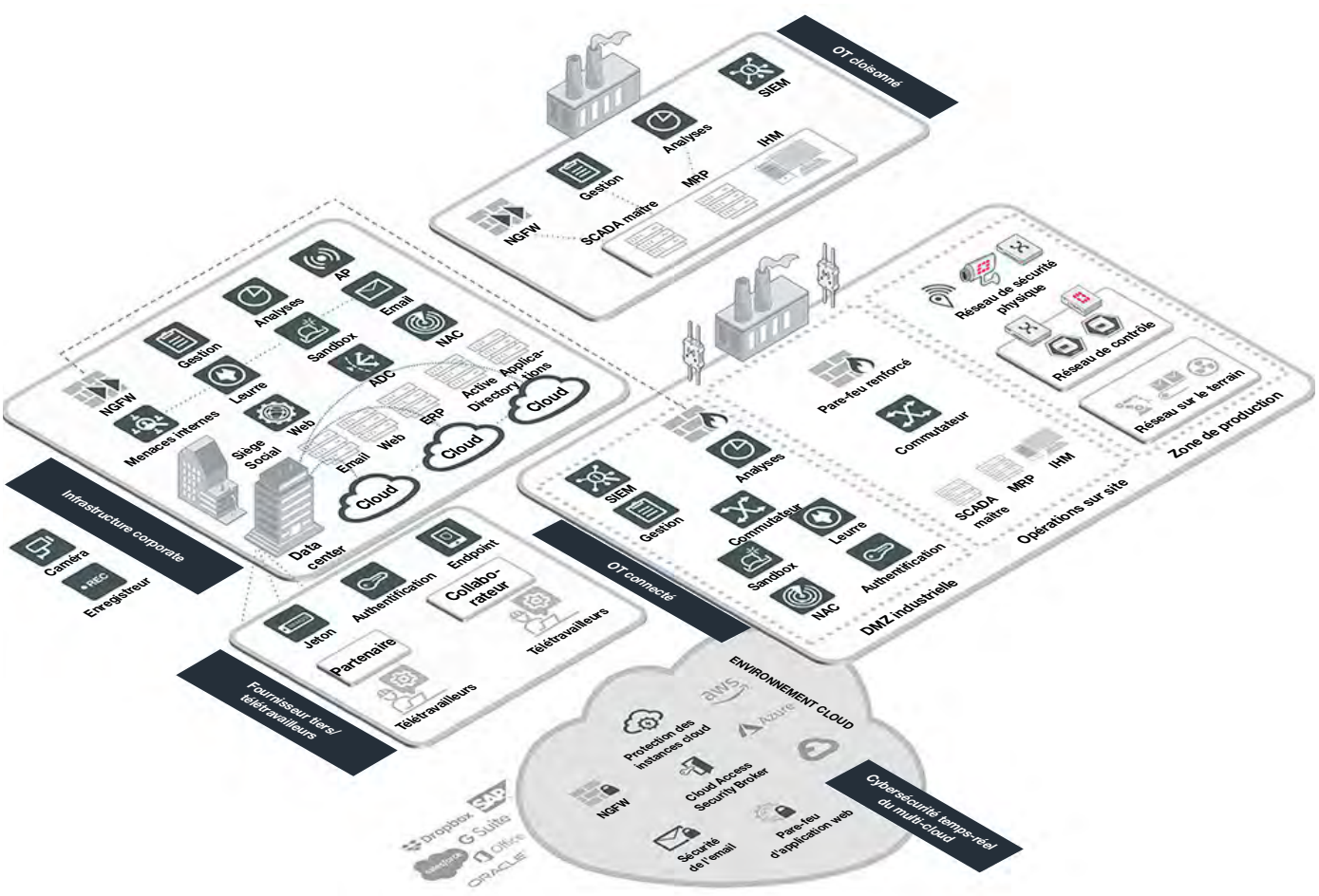
Il en résulte que la protection par pare-feu NGFW s'impose même pour les systèmes cloisonnés, et qu'elle doit être associée à un tracking et à un reporting intégral de cybersécurité. Les pare-feu FortiGate déploient une protection efficace et offrent des performances de tout premier rang pour inspecter le trafic en clair ou chiffré. FortiManager propose une interface unique de gestion et différents outils de reporting. De son côté, FortiAnalyzer déploie un traitement analytique des données de sécurité et une gestion des logs pour une visibilité optimale et une détection plus précise des incidents. Enfin, la plateforme FortiSIEM assure une prise en charge coordonnée et automatisée des attaques.

Des systèmes de production interconnectés

Comme nous l'avons vu, la transformation digitale et le besoin pour davantage d'agilité business favorisent la co-dépendance entre IT et OT. Des capteurs IoT industriels, qui surveillent les opérations de production, aux systèmes qui récupèrent des données publiques à partir d'Internet pour simplifier la prise de décision, les systèmes OT sont de moins en moins isolés. D'un point de vue cybersécurité, cette convergence favorise l'expansion de la surface d'attaque. D'autre part, les systèmes OT ne bénéficient pas de patchs réguliers, ce qui constitue un risque sur le court terme.

Si les problématiques de cybersécurité peuvent être résolues, il est surtout possible d'associer réseaux IT et fonctions d'automatisation, au sein d'un environnement unique, sécurisé, convergent et simple à gérer. Les équipes de cybersécurité doivent disposer d'une visibilité centralisée sur l'ensemble des systèmes, avec la possibilité de segmenter le réseau selon les besoins métiers, tout en contrôlant de manière centralisée les réseaux filaires et sans fil.

La Fortinet Security Fabric porte sur la totalité de la surface d'attaque, en offrant une visibilité élargie sur le réseau et sur son activité. Elle déploie également un contrôle sur chaque système pour assurer un fonctionnement pertinent. De plus, la Security Fabric permet une segmentation intelligente pour davantage de contrôle et une identification automatique des menaces connues et inconnues. En capitalisant sur les pare-feu NGFW FortiGate et sur la veille sur les menaces des FortiGuard Labs, la Security Fabric assure une intégration transparente avec des dizaines d'outils de cybersécurité de Fortinet et de ses partenaires.



Les solutions de cybersécurité Fortinet permettent aux industriels d'intégrer leur architecture de sécurité de bout en bout, pour couvrir la sécurité IT, OT et physique, du siège social aux sites de production, et protéger les utilisateurs internes et les prestataires externes.

Gestion des fournisseurs tiers

Alors que le modèle MaaS (Manufacturing-as-a-Service)[15] émerge, les tiers ont davantage accès aux réseaux corporate et systèmes OT. Ceci complique l'identification des utilisateurs de confiance et force les entreprises à évaluer en permanence leur protection face aux menaces internes, celles provenant de tiers notamment. Il est essentiel d'évaluer régulièrement la posture de cybersécurité de chaque partenaire. Les entreprises ont également besoin d'une protection pertinente contre les menaces internes, que ces dernières soient accidentelles ou volontaires, et qu'elles proviennent du périmètre interne de l'entreprise ou à partir du réseau d'un partenaire.

Les solutions intégrées de la Fortinet Security Fabric déploient une sécurité en profondeur contre ces menaces. Les pare-feu FortiGate permettent aux entreprises de segmenter leur réseau de manière intelligente, en mode intent-based. La solution de gestion des identités et des accès FortiAuthenticator, ainsi que les jetons FortiToken, tirent parti de cette segmentation pour valider l'accès des utilisateurs aux ressources qui leur sont autorisées. FortiInsight tire parti d'un traitement analytique du comportement des utilisateurs (UEBA) pour identifier les anomalies dans le comportement attendu des utilisateurs de confiance. Enfin, FortiDeceptor déploie une technologie de leurre pour identifier et neutraliser les attaques d'origine interne ou externe.

Cybersécurité du multi-cloud

Les industriels adoptent rapidement les services cloud.[16] Nombre d'entre eux utilisent des systèmes MRP (Manufacturing Resource Planning) et ERP (Enterprise Resource Planning) basés dans le cloud. Ces systèmes récupèrent des données à partir de systèmes IT et OT pour favoriser une prise de décision rapide et efficace. Les solutions cloud sont également utilisées pour les services qui impactent l'expérience utilisateur. La cybersécurité de ces ressources est critique : l'architecture intégrée de cybersécurité doit s'étendre du data center aux systèmes OT et aux clouds multiples.

La Fortinet Security Fabric protège intégralement les environnements multi-cloud, avec une gestion pertinente des règles, une gestion des configurations, ainsi que la détection et la réponse aux menaces, sur l'ensemble de la surface d'attaque. FortiGate VM est un pare-feu NGFW au format virtuel, parfaitement adapté aux environnements cloud, tandis que le pare-feu d'application web FortiWeb, disponible en différents formats, protège la couche applicative grâce à une veille sur les menaces bénéficiant de fonctions d'intelligence artificielle.

Le service CASB de FortiCASB offre une visibilité au cœur des ressources, utilisateurs, comportements et données stockées dans le cloud, via un reporting exhaustif. Ceci permet de définir des règles évoluées qui s'appliquent aux ressources IaaS (Infrastructure-as-a-Service) et aux applications SaaS (Software-as-a-Service). La protection des instances cloud qu'offre FortiCWP permet aux équipes de sécurité et DevOps d'évaluer la posture de sécurité de leur configuration cloud et d'identifier les éventuelles erreurs constituant des menaces.

Les atouts de Fortinet

Facteurs de différenciation de la cybersécurité de Fortinet pour la production industrielle

Les solutions Fortinet offrent aux industriels une protection intégrale de leurs réseaux OT et IT, avec des atouts majeurs à la clé :

- **Intégration**
  Les technologies Fortinet portent sur la sécurité IT et OT, la sécurité physique et cyber, ainsi que la protection des data centers, du siège social et des environnements cloud. Il devient possible d'automatiser cette sécurité et de coordonner les workflows de protection, de détection des menaces et de traitement de ces menaces.
- **Monitoring et management**
  Fortinet permet aux industriels de consolider les fonctions réseau, de cybersécurité et de monitoring au sein d'un seul système, pour bénéficier d'une visibilité et d'un contrôle intégral à partir d'une interface unique. Ceci prévient les cyberattaques et permet aux équipes de collaborer entre elles.
- **Matériel renforcé**
  Les solutions matérielles sont plus vulnérables au sein des environnements de production. Un dommage physique à un pare-feu peut entraîner un arrêt de la chaîne de production. Fortinet propose des appliances renforcées, adaptées aux risques inhérents des environnements industriels, pour favoriser la continuité des activités métiers.
- **Protection proactive contre les menaces internes**
  La gestion des risques internes devient plus complexe compte tenu du nombre plus important de fournisseurs et partenaires accédant au réseau. Fortinet propose des solutions pertinentes (segmentation intent-based, technologie de leurre, analyse UEBA) pour maîtriser les menaces d'origine interne.

Les intrusions en environnement de production[17] (sur les 12 derniers mois)

- Malware, 61 %
- Spyware, 45 %
- DDoS, 28 %
- Menaces internes, 26 %
- Phishing, 24 %
- Mobile, 21 %
- Ransomware, 21 %
- Attaques Man-in-the-middle, 18 %
- Attaques Zero-day, 17 %
- Injections SQL, 8 %

Impact des intrusions en environnement de production[17] (sur les 12 derniers mois)

- 45 % ont subi un arrêt opérationnel qui a grevé leur productivité
- 40 % ont constaté une dégradation de la réputation de leur marque
- 35 % ont connu des risques de sécurité physique résultant d'un arrêt opérationnel
- 32 % ont subi un arrêt opérationnel qui a freiné leur activité commerciale
- 26 % ont subi une perte de données critiques

- **Veille sur les menaces spécifique à l'OT**
  FortiGuard Labs propose une veille performante sur les menaces et spécifique aux systèmes OT, pour aider les industriels à améliorer leur prise de décision stratégique. Fortinet collabore étroitement avec ses clients industriels depuis plus de 15 ans.
- **Écosystème de la Security Fabric**
  Au-delà du large panel d'outils de sécurité Fortinet, des solutions spécifiques à l'OT peuvent être intégrées en toute transparence au sein de la Fortinet Security Fabric, via l'écosystème des partenaires Fabric. Ceci permet de simplifier et consolider les données pour faciliter la prise de décision.

Conclusion

Au sein d'un marché en évolution rapide et qui privilégie une production en flux tendus, les industriels ne peuvent se permettre de subir des incidents de cybersécurité. La Fortinet Security Fabric propose une plateforme unifiée pour la sécurité IT, OT et physique, avec une visibilité élargie et une gestion consolidée, à partir d'une interface unique.

"Les cadres dirigeants s'accordent à penser que les stratégies visant à accélérer le time-to-market, à améliorer la qualité des produits et à écouter les clients portent leurs fruits."[18]

"En dépit de variations saisonnières et de la diversité des cibles, les données indiquent clairement que les attaques IT menées sur les systèmes OT sont en progression."[19]

[1] Marco Annunziata, « Manufacturing-As-A-Service Platforms: The New Efficiency Revolution, » Forbes, 13 mai 2019.

[2] « Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems, » Fortinet, 8 mai 2019.

[3] « State of Operational Technology and Cybersecurity Report, » Fortinet, consulté le 7 novembre 2019.

[4] « Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems, » Fortinet, 8 mai 2019.

[5] « Cyber Physical Systems Security, » Department of Homeland Security, consulté le 7 novembre 2019.

[6] « Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems, » Fortinet, 8 mai 2019.

[7] « Q3 Fraud and Abuse Report, » Arkose Labs, 18 septembre 2019.

[8] « Ninth Annual Cost of Cybercrime Study, » Accenture et Pomenon Institute, 6 mars 2019.

[9] Elizabeth Montalbano, « Six Cyber-Physical Attacks the World Could Live Without, » The Security Ledger, 18 janvier 2017.

[10] « Q3 Fraud and Abuse Report, » Arkose Labs, 18 septembre 2019.

[11] Louis Columbus, « 10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018, » Manufacturing Business Technology, 23 février 2018.

[12] « Applications of IoT in Manufacturing Plants, » The Manufacturer, 12 avril 2018.

[13] « Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks », Fortinet, 16 avril 2019.

[14] Idem.

[15] Marco Annunziata, "Manufacturing-As-A-Service Platforms: The New Efficiency Revolution," Forbes, 13 mai 2019.

[16] Louis Columbus, « 10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018, » Manufacturing Business Technology, 3 février 2018.

[17] Sur la bases de différentes études menées par Fortinet sur des profils différents.

[18] Louis Columbus, « 10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018, » Manufacturing Business Technology, 3 février 2018.

[19] « Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems, » Fortinet, 8 mai 2019.

FORTINET

www.fortinet.com/fr

3. juin 2022, 16:18
517972-A-1-FR