cyberelements

eBook

SÉCURITÉ DES SYSTÈMES DE CONTRÔLE INDUSTRIEL

Table des matières

cyberelements

SECTION 1 :

HISTOIRE ET STATISTIQUES

Évolution des environnements industriels

- **Les Automates Programmables Industriels (API)** ont introduit pour la première fois l'électronique dans l'automatisation de la production, ce qui a révolutionné le processus en facilitant considérablement la création et la modification de la logique de contrôle.

- **Les systèmes de contrôle** sont créés à partir de boucles de contrôle composées de capteurs, de contrôleurs et d'actionneurs. Ils peuvent être utilisés pour modéliser des comportements complexes tels que les processus de fabrication en continu.

- **Systèmes de contrôle et d'acquisition de données (SCADA)** et systèmes de contrôle distribués (DCS - SNCC) : Les systèmes SCADA ont toujours intégré des capteurs, la transmission de données et un logiciel IHM pour une visibilité centralisée du système. Les DCS offrent des capacités similaires à l'échelle d'une usine, avec des réseaux et des communications généralement moins complexes.

- **Systèmes de contrôle industriel (ICS) :** Ils comprennent les SCADA, les DCS (SNCC) et les PLC (API) utilisés pour la gestion et l'automatisation des processus industriels.

- **Les systèmes OT versus les systèmes IT :** Les environnements industriels ont traditionnellement été dominés par la technologie opérationnelle (OT), axée sur les processus physiques. Avec la transformation numérique, nous avons constaté une interdépendance accrue entre les systèmes IT et OT.

- **Internet of Things (IoT) & Industrial Internet of Things (IIoT) :** désigne le réseau de dispositifs physiques, la communication entre machines et l'analyse des données.

1972

Présent

Principaux défis en matière de sécurité industrielle

90%

des responsables fédéraux en matière de systèmes OT signalent une augmentation de la priorité accordée par leur agence à la cybersécurité des systèmes OT au cours des deux dernières années.

68%

des organisations industrielles ont subi un incident de sécurité lié au système OT au cours de l'année dernière.

20%

des organisations industrielles s'attribuent un « A » en matière de préparation à la cyberprotection des systèmes OT.

EN ATTENDANT

Les principales lacunes du secteur industriel sont les suivantes :

Manque de visibilité du réseau

Gestion de la vulnérabilité et des risques

Sécurité des accès distants et surveillance

Besoins émergents

Après la quatrième révolution industrielle (Industrie 4.0), nous avons assisté à un changement de paradigme dans le monde de l'industrie. Les industries ne sont plus des usines isolées et déconnectées du reste du monde. Au contraire, les environnements informatiques sont désormais interconnectés avec les environnements OT puisque nous sommes désormais dans l'ère du big data, des machines intelligentes et de l'IoT/IIoT. Selon le rapport MeriTalk & CLAROTY « Guardians of Government : The State of Federal OT Security », 69% des équipes OT rendent compte désormais au RSSI - que ce soit de manière conjointe ou indépendamment de la sécurité IT.

Nous vivons aujourd'hui la cinquième révolution industrielle, qui met l'accent sur l'humain, la durabilité et l'intégration de technologies avancées pour améliorer le bien-être général. C'est pourquoi le télétravail a été largement adopté dans le monde entier. Il offre de la flexibilité, réduit l'empreinte carbone et maximise l'efficacité des ressources.

Ces changements technologiques et culturels ont entraîné une évolution substantielle du monde industriel, y compris de l'ensemble de son écosystème (fabricants et prestataires de services, par exemple), ce qui a fait naître de nouveaux besoins en matière de cybersécurité :

Besoins émergents

- **Sécuriser les accès à distance :** Autrefois, il fallait être physiquement présent dans l'usine pour se connecter à un appareil prouvant ainsi son identité. Cependant, la situation devient plus complexe lorsque les utilisateurs se connectent à distance à l'environnement OT, parfois à partir d'appareils personnels/non fiables.

- **L'utilisation de ressources cloud :** L'analyse des big data devenant essentielle pour les algorithmes d'apprentissage automatique et d'analyse prédictive, les industries s'appuient sur des solutions cloud qui traitent les données pour fournir divers tableaux de bord. Dans ce cas, les environnements OT sont ouverts au cloud et à Internet, d'où la nécessité d'une isolation appropriée.

- **Transferts de fichiers :** Étant donné le contexte du télétravail, les transferts de fichiers font partie des tâches quotidiennes des collaborateurs. Les industries sont tenues de fournir des méthodes de transfert de fichiers sécurisées à leurs utilisateurs afin de protéger les environnements OT du monde extérieur.

- **Segmentation IT/OT :** L'interconnexion IT/OT engendre la nécessité d'une segmentation appropriée. Cela signifie qu'il faut gérer à la fois les environnements IT et OT tout en maintenant une séparation claire entre les deux. En d'autres termes, il s'agit d'assurer l'isolement tout en maintenant l'interconnexion entre les deux.

- **Traçabilité :** Le besoin de traçabilité pour les environnements OT est considérablement élevé étant donné la sensibilité du secteur industriel. La plupart du temps, on ne peut se permettre d'interrompre une activité de fabrication. Il est donc important de pouvoir retracer toutes les actions en cas d'incident.

cyberelements

SECTION 2:

CONFORMITÉ DANS LE SECTEUR INDUSTRIEL

Conformité dans le secteur industriel

Compte tenu des changements émergents dans le secteur industriel, les cybermenaces se sont multipliées. En outre, une faille dans le secteur industriel peut avoir un impact catastrophique sur notre société. C'est pourquoi les gouvernements et les autorités chargées de la cybersécurité dans le monde entier s'emploient activement à élaborer et à mettre à jour leurs législations afin de renforcer la sécurité du secteur industriel.

NIS2

Nous pouvons considérer la directive NIS2 comme une continuité de NIS1. La principale différence entre les deux versions est que NIS2 s'applique désormais à un plus large éventail d'organisations, notamment les entreprises du secteur industriel spécialisées dans l'énergie, les transports, la fabrication et le traitement de l'eau. Ces organisations devront se mettre en conformité à une date qui sera fixée dans la transposition nationale de la directive d'ici octobre 2024.

Ces nouvelles mesures comprennent :

Article 18 2d & 21 1b
Sécurité de la chaîne d'approvisionnement

Article 21
Politiques de contrôle d'accès et gestion des actifs

Article 21 1b
Authentification multi-facteurs

Article 24 & 21 1e
Surveillance et audit

Conformité dans le secteur industriel

ISA/IEC 62443

ISA/IEC 62443 est une série de normes conçues pour fournir un cadre flexible permettant de traiter et d'atténuer les vulnérabilités actuelles et futures en matière de sécurité dans les systèmes industriels d'automatisation et de contrôle (IACS). Ces normes sont élaborées par la Société internationale d'automatisation (ISA) et la Commission électrotechnique internationale (IEC) et sont largement reconnues dans le domaine de la sécurité des technologies opérationnelles (OT).

Principaux éléments de la sécurité des accès couverts par la norme ISA/IEC 62443 :

IEC 62443-3-3 2013 SR 1.6:
Contrôle et politiques d'accès

IEC 62443-3-3 2013 SR 1.1:
Authentification et autorisation

IEC 62443-3- 3 2013 SR 1.3:
Principe du moindre privilège

IEC 62443-3-3 2013 SR 2.8 & SR 2.4:
Surveillance et audit

Conformité dans le secteur industriel

NIST 800-82, Révision 3

La publication spéciale 800-82, révision 3, du NIST, intitulée « Guide to Operational Technology (OT) Security » a été publiée le 28 septembre 2023. Elle fournit des lignes directrices et des recommandations complètes pour sécuriser les environnements OT, comprenant les systèmes de contrôle industriel (ICS), les systèmes de contrôle de surveillance et d'acquisition de données (SCADA) et d'autres systèmes de contrôle.

Principaux éléments de la sécurité des accès couverts par la norme NIST 800-82, révision 3 :

Section 5.2.6:
Contrôle d'accès

Section 5.3.4:
Gestion des comptes

Section 5.3.6:
Audit et responsabilité

cyberelements

SECTION 3:

SÉPARATION IT/OT ET SEGMENTATION DU RÉSEAU POUR UNE SÉCURITÉ INDUSTRIELLE AVANCÉE

Modèle Purdue pour la sécurité ICS

Malgré l'adoption croissante des technologies de pointe et de la connectivité directe au cloud, le modèle Purdue reste pertinent en matière de sécurité ICS.

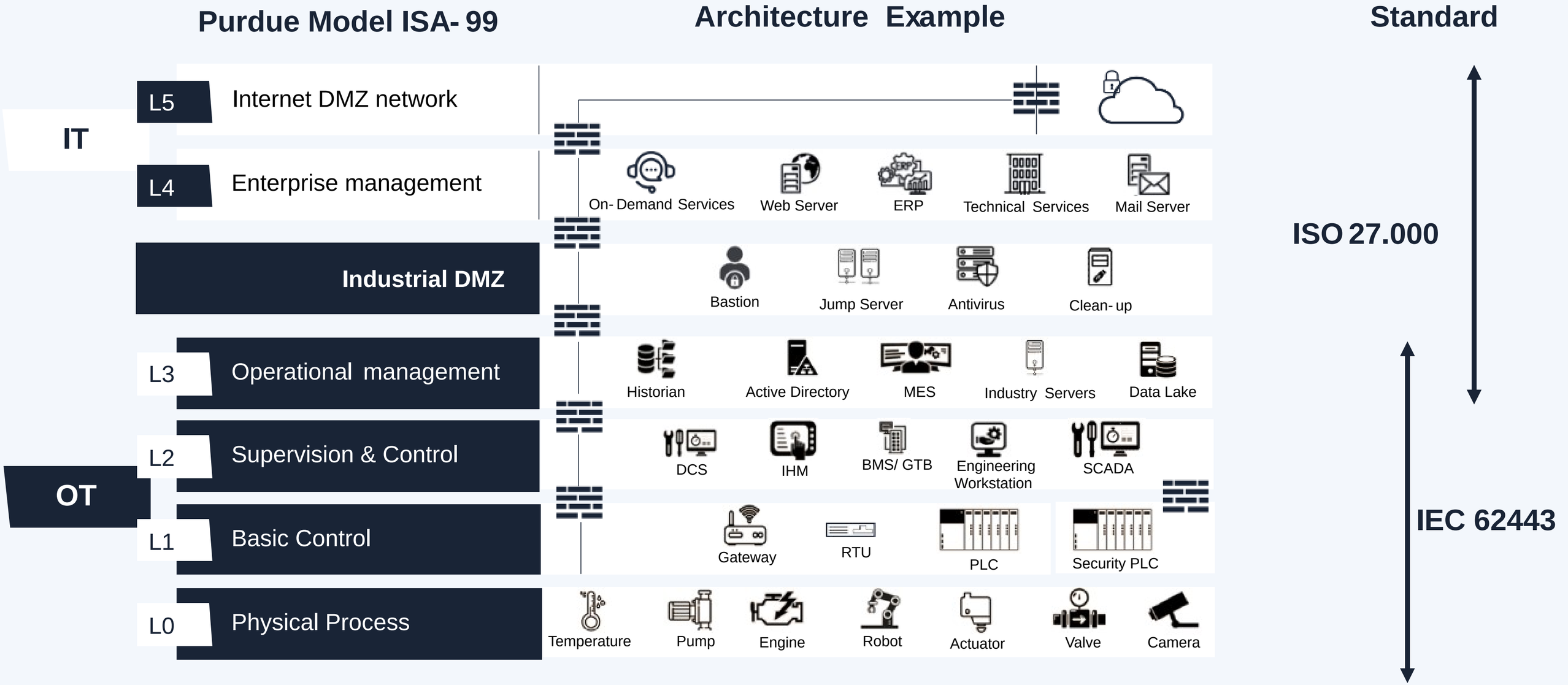
Qu'est-ce que le modèle Purdue ?

Le modèle Purdue est un cadre structurel pour la sécurité des systèmes de contrôle industriel (ICS) qui se concentre sur la segmentation des processus physiques, des capteurs, des contrôles de supervision, des opérations et de la logistique. Il est depuis longtemps considéré comme essentiel pour la segmentation du réseau ICS afin de protéger les systèmes OT contre les logiciels malveillants et d'autres menaces.

Comment sécuriser les ICS ?

Au cœur du modèle Purdue se trouve la technologie opérationnelle (OT), qui comprend les systèmes situés dans l'infrastructure critique utilisés pour surveiller et contrôler l'équipement physique. Au sommet de la zone OT se trouve la zone IT, séparée par une DMZ (zone démilitarisée) qui assure le contrôle d'accès entre les zones OT et IT.

Model of industrial architecture



Modèle Purdue pour la sécurité ICS

L0 - Capteurs / Actionneurs: Il s'agit de l'équipement physique qui effectue le travail et qui est connu sous le nom d'équipement sous contrôle. Il s'agit de vannes, de pompes, de capteurs, d'actionneurs, de compresseurs, etc.

L1 - Automatismes: Il s'agit des dispositifs de contrôle tels que les automates industriels programmables qui surveillent et contrôlent les équipements de L 0 et les systèmes de sécurité informatisés.

L2 - Supervision et contrôle : Logique de contrôle permettant d'analyser et d'agir sur les données de niveau 1. Les systèmes comprennent une interface homme-machine (IHM) et un logiciel de supervision et d'acquisition de données (SCADA).

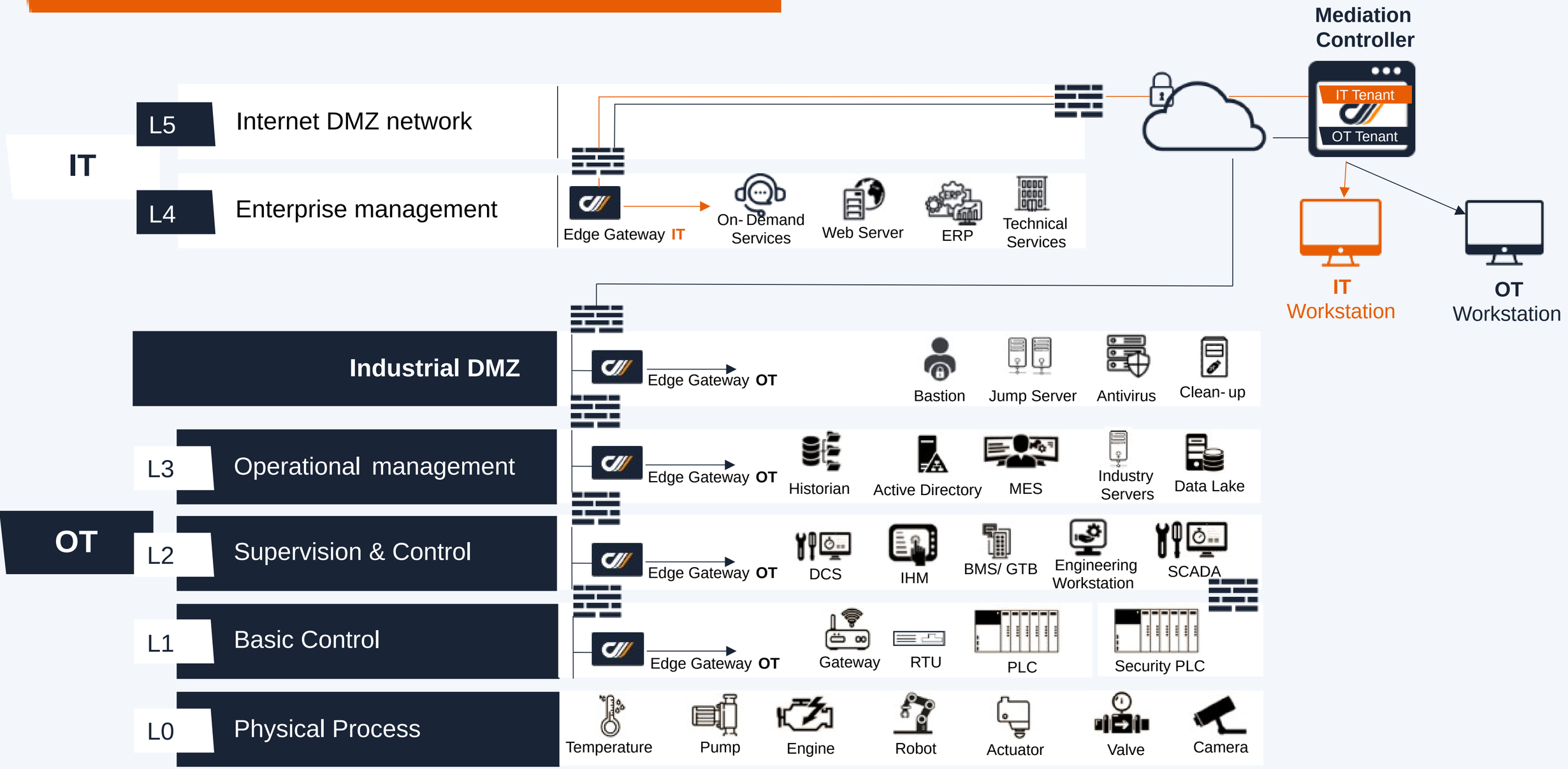
L3 - Gestion des opérations : Ce niveau comprend les systèmes qui prennent en charge les fonctions de contrôle et de surveillance de l'installation. Les systèmes de niveau 3 regroupent également les données de niveau inférieur qui doivent être transmises aux systèmes métiers de niveau supérieur.

DMZ industrielle (iDMZ) : barrière entre la zone IT et la zone OT, qui empêche toute propagation d'infection et bloque la contamination.

L4 - Gestion de l'entreprise : On y trouve les systèmes IT qui gèrent la logistique de fabrication, la communication et le stockage des données.

L5 - Réseau DMZ Internet: Ce niveau représente le réseau d'entreprise. Bien qu'il ne s'agisse pas d'un environnement ICS, il recueille des données provenant des systèmes ICS afin de faciliter la prise de décisions commerciales.

cyberelements PAM for OT



L'architecture cyberelements pour l'OT

L'architecture à double barrière de cyberelements est spécifiquement conçue pour ce type d'infrastructure. Elle comprend deux composants clés : Le contrôleur de médiation et la Edge Gateway, qui connectent en toute sécurité les utilisateurs uniquement aux ressources nécessaires à leurs tâches.

La Edge gateway :
Pour maintenir la séparation entre les différents niveaux, cyberelements fournit une gateway pour chaque niveau. Chaque niveau dispose d'une gayeway Edge connectée au contrôleur de médiation. De plus, cyberelements permet la segmentation de plusieurs (V)LAN si nécessaire, sans affecter l'expérience de l'utilisateur final. L'opérateur OT aura une visibilité sur toutes les ressources OT à travers une seule « fenêtre ».

Le contrôleur de médiation :
Le contrôleur de médiation comporte deux organisations distinctes : l'une pour la zone IT et l'autre pour la zone OT. Cette structure garantit que le personnel IT se connecte à la zone IT et le personnel OT à la zone OT.
Les tenants peuvent également être utilisés pour segmenter les systèmes OT réglementés (conformité NIS) et les systèmes OT non réglementés.

L'architecture cyberelements pour l'OT

Cette architecture unique garantit :

- Une architecture à double barrière avec un tunnel crypté de bout en bout entre le poste de l'utilisateur final et le réseau local OT
- Un cloisonnement organisationnel (multi-tenant) et réseau (gateways avec flux sortants sans ouverture de ports réseau)
- Protection contre les attaques grâce à des ports volatiles et aléatoires, à la réécriture d'url et à l'isolation des déports d'affichage.
- Technologie Zero Trust embarquée : least connection, JIT connection, zero standing connection.
- Accès sans client pour les prestataires avec rupture protocolaire et sans ouverture de port ni aucun flux entrant : seulement un flux sortant.

cyberelements

SECTION 4:

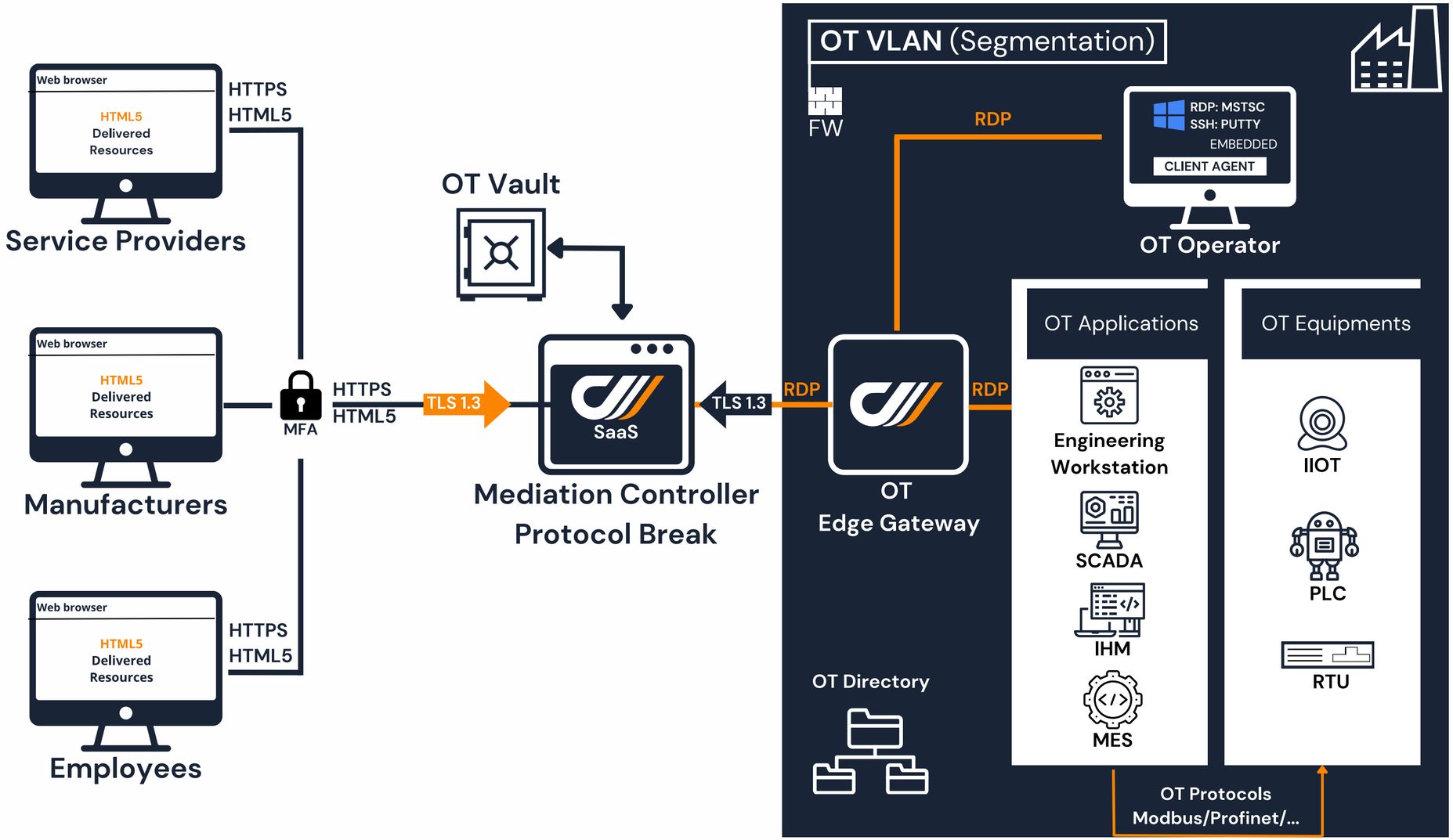
LES DIFFÉRENTS CAS D'USAGE

Les cas d'usage

Dans le monde industriel, il existe trois principaux cas d'usage de l'accès à distance. Les utilisateurs ont besoin de se connecter à distance à des ressources et des applications pour effectuer différents types d'actions : maintenance, mise à jour, surveillance, contrôle, etc.

Les utilisateurs peuvent provenir de sociétés prestataires, de fabricants industriels ou peuvent être des collaborateurs internes. Même s'il ne s'agit pas d'un accès privilégié ou nominal, il existe un besoin croissant de sécuriser ces accès à distance dans le secteur industriel. C'est pourquoi cyberelements propose une plateforme convergente qui couvre tous ces cas d'usage d'accès.

1er cas d'usage : Accès à distance sécurisé à une station d'ingenierie hébergeant une application ICS



1er cas d’usage : Accès à distance sécurisé à une station d’ingenierie hébergeant une application ICS

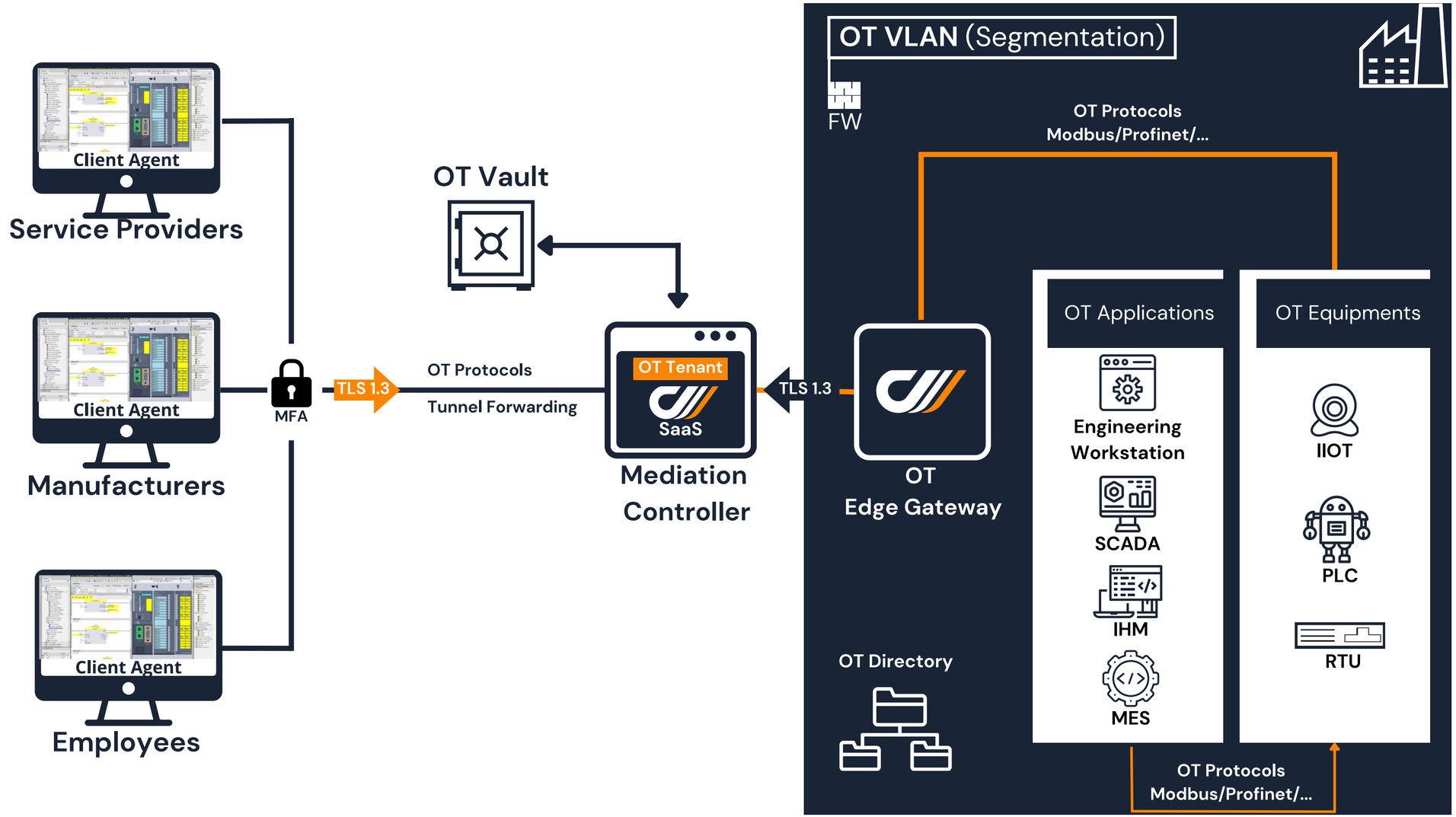
Dans ce cas précis, la station d’ingenierie est située dans le LAN OT et les utilisateurs ont besoin de se connecter depuis leurs appareils aux applications OT/ICS fonctionnant sur cette station d’ingenierie.

Le mode SaaS de cyberelements permet à vos utilisateurs de se connecter en toute sécurité à partir de n'importe quel navigateur web sans avoir à installer de client. Une fois que les utilisateurs sont connectés aux applications OT via cyberelements, ils peuvent effectuer les actions requises sur l'équipement OT en utilisant les protocoles industriels appropriés. Seules les images sont transmises sur le poste de l'utilisateur et seuls les flux du clavier et de la souris sont transmis depuis le poste de l'utilisateur.

Le mode SaaS limite l'interaction avec le poste de l'utilisateur, l'isolant ainsi des systèmes OT. cyberelements met en œuvre une technologie intégrée de rupture protocolaire couplée à une réécriture d'URL garantissant une protection OT complète contre toute possibilité de contamination par des postes infectés.

Par conséquent, la plateforme cyberelements vous permet de donner un accès entièrement sécurisé à tout type d'utilisateur situé n'importe où dans le monde, quel que soit le poste qu'il utilise, à condition qu'il dispose d'un navigateur web.

2ème cas d'usage : Utilisation à distance de l'application du constructeur via le bastion



2ème cas d’usage : Utilisation à distance de l'application du constructeur via le bastion

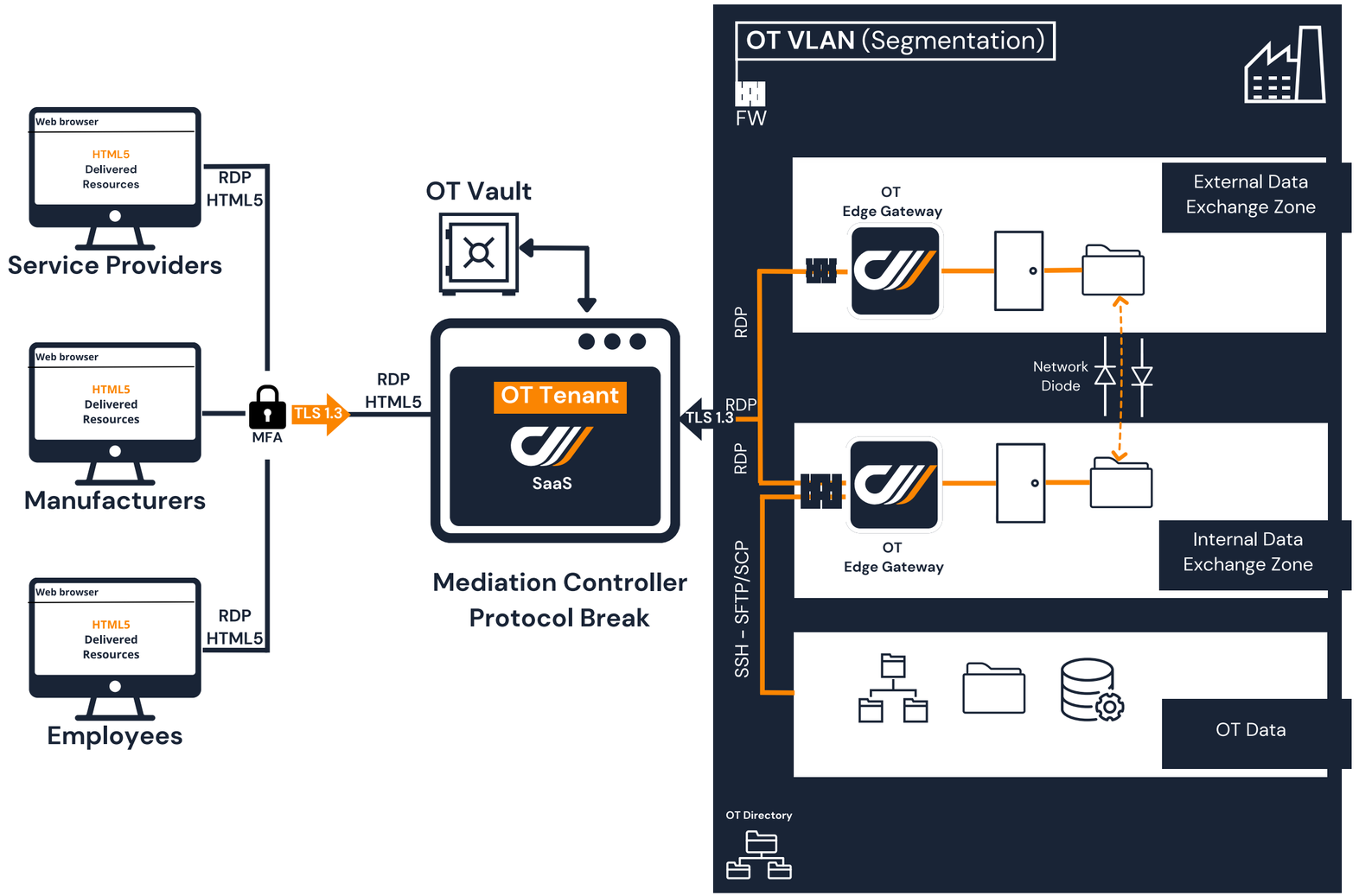
Dans ce second cas d'usage, les applications OT/ICS sont situées dans le datacenter d'un prestataire (prestataire de services, constructeur, ...), dont les utilisateurs se connectent à distance au réseau local OT de l'organisation, où se trouvent les équipements industriels. En d'autres termes, les utilisateurs sont connectés à partir d'un réseau externe non fiable. Dans ce cas, l'accès doit être sécurisé par une solution de gestion des accès à privilèges (PAM).

cyberelements est conçu pour offrir de telles capacités de Remote PAM. Dans ce cas, un tunnel est créé de bout en bout entre le poste de l'utilisateur et la Edge Gateway OT déployée dans le LAN OT, le tunnel entre la gateway et le contrôleur cyberelements étant sortant (uniquement des flux sortants, pas d'ouverture de port).

La solution permet alors de configurer une ressource de « port forwarding», qui permet d'acheminer les protocoles propriétaires OT tout au long du tunnel, jusqu'à ce qu'ils atteignent la gateway qui les achemine vers l'équipement industriel ciblé.

Le tunnel est crypté de bout en bout et il peut être crypté avec la propre clé de l'organisation, de sorte que personne d'autre - y compris cyberelements - ne puisse « voir » le flux entre les applications et l’API, par exemple.

3ème cas d'usage : Sécurité du transfert de fichiers



3ème cas d’usage : Sécurité du transfert de fichiers

Les entreprises industrielles traitent des données très sensibles qui doivent être protégées par une politique de sécurité solide. Dans le même temps, les infrastructures OT doivent être maintenues et mises à jour, ce qui ne peut se faire qu'en téléchargeant les fichiers des fournisseurs vers les LAN OT. Souvent, les données doivent être extraites des LAN OT vers un cloud où elles peuvent être traitées, afin d'exploiter la puissance de calcul du cloud et la capacité d'intelligence artificielle des outils d'analyse industrielle.

Le transfert de fichiers est donc inévitable dans le monde industriel. C'est là que la combinaison du PAM avec la technologie de transfert de fichiers « diode » (à sens unique) entre en jeu. La technologie diode est un dispositif de cybersécurité qui assure une isolation totale entre les différentes zones du réseau au niveau physique en garantissant un flux de données unidirectionnel.

cyberelements fournit une solution PAM intégrée avec les diodes pour sécuriser entièrement le transfert de données dans l'environnement OT : les utilisateurs devront se connecter à la zone d'échange de données externe où les données seront vérifiées avant d'être transférées vers la zone d'échange de données interne via la diode. Aucun autre moyen ne peut être utilisé pour effectuer le transfert de données.

De cette manière, cyberelements garantit une isolation et une segmentation totales des environnements OT par rapport au monde extérieur.

Inside the elements: Guide vidéo des cas d'usage du PAM dans cyberelements

Visionner la vidéo

cyberelements

SECTION 5:

TÉMOIGNAGES DU DOMAINE INDUSTRIEL

Centralisation de l'accès à distance aux systèmes IT et OT pour un leader de l'agro-alimentaire

Objectif : Centraliser et sécuriser l'accès interne et externe aux systèmes IT et OT tout en garantissant le cloisonnement total IT/OT.
4 000 collaborateurs I 15 sites de production

Enjeux :

› Mise en œuvre des principes du **Zero Trust**.
› **Centralisation et traçabilité des accès** aux infrastructures cibles selon les possibilités offertes par les constructeurs et les protocoles industriels : accès aux applications de contrôle sur une station d'ingénierie, accès aux équipements depuis la station d'ingénierie fonctionnant sur **le poste de travail du prestataire ou du constructeur**.
› Mise en place de **zones de contrôle totalement isolées** pour l'IT et l'OT.

La solution cyberelements

› Contrôle et traçabilité de tous les comptes et visibilité complète : qui a fait quoi, quand et sur quel système. Par conséquent, la responsabilité de tous les accès à l'infrastructure industrielle est garantie.
› La mise en œuvre des principes Zero Trust pour l'infrastructure industrielle et l'adoption du principe du moindre privilège.
› Centralisation de l'accès aux systèmes IT et OT à partir d'une plateforme convergente, tout en garantissant un cloisonnement total entre les deux. Les équipes opérationnelles peuvent ainsi déployer leurs outils d'administration (supervision, patch management, etc.) sur les réseaux de production.

Centralisation de l'accès à distance aux systèmes IT et OT pour un leader de l'agro-alimentaire

Caractéristiques principales :

› Logs d'accès détaillés

› Politiques d'accès granulaires

› Contrôle de conformité des postes (poste de travail)

› Accès just-in-time

› Authentification multi-facteurs

› Plateforme convergente

› Infrastructure unique pour la sécurité d'accès OT et IT

Sécuriser l'accès à distance pour un leader international de la Supply Chain

Objectif : Mise en place d'un bastion sécurisé, compatible avec les outils existants et offrant la meilleure expérience utilisateur, pour la télémaintenance.
1 000 collaborateurs I 50 pays

Enjeux :

›Améliorer et sécuriser la télémaintenance des logiciels et des systèmes déployés sur les sites des clients.
›Offrir une expérience utilisateur la plus fluide possible, permettant l'utilisation d'outils existants (RDM) et le SSO fédéré sur un coffre-fort de mots de passe existant.
›Se conformer à la norme ISO27001.

La solution cyberelements

› Accès sécurisé aux logiciels et API déployés sur les sites des clients : conçu pour l'accès à distance, cyberelements sécurise l'accès aux ressources IT & OT des clients pour l'organisation et ses prestataires.
› Une expérience utilisateur transparente et fluide permettant l'utilisation des outils existants : l'intégration de cyberelements et de RDM est donc « native », sans perturber l'expérience utilisateur : depuis RDM, les utilisateurs peuvent accéder (accès direct) à toutes leurs ressources, sans ré-authentification, tout en s'appuyant sur le coffre-fort de mots de passe existant.
› Un parfait cloisonnement entre les clients : permettant d'opérer à distance et en toute sécurité sur les différentes infrastructures des clients. En tant que fournisseur de services managés (MSP), les clients peuvent également utiliser la solution.
› Grâce à la capacité multi-tenant de la plateforme et à l'utilisation de gateways déployées dans des LAN distincts, les clients peuvent également utiliser la solution. Chaque gateway est connectée au contrôleur correspondant au client approprié. Un utilisateur n'accède et ne « voit » que les ressources de l'organisation qui lui en a donné les droits.

Sécuriser l'accès à distance pour un leader international de la Supply Chain

Caractéristiques principales :

› L'enregistrement des sessions lors de l'accès aux ressources RDP, SSH ou Web, sans avoir besoin d'un serveur de rebond.

› Les sessions enregistrées sont stockées dans les locaux du client et peuvent être consultées à la fois par le client et par l'entreprise de la chaîne d'approvisionnement.

› Les secrets d'authentification sont gérés sans qu'ils soient divulgués.

› Une architecture à double barrière empêche l'exposition des systèmes d'information des clients.

› Une interface web sans client, ce qui signifie qu'il n'est pas nécessaire d'installer ou de télécharger de client sur le poste de travail.

› La technologie de rupture protocolaire limite à la fois l'interaction avec le poste de travail et le risque de propagation de toute charge malveillante présente sur le poste de travail.

>Une solution multi-tenant avec un déploiement de gateway pour chaque LAN séparé.

Secteur de l'énergie : Se conformer à NIS2 en sécurisant l'accès des prestataires

Objectif : Remplacement de l'ancienne solution PAM pour sécuriser les accès prestataires conformément à la directive NIS2.
1000 collaborateurs I 21 sites I 100+ prestataires

Enjeux :

› Fournir aux prestataires de services externes un accès distant sécurisé aux systèmes IT et OT.
› Nécessité d'une solution pouvant être intégrée à une solution de sécurité pour le transfert de données.
› Se conformer à la directive NIS2.

La solution cyberelements

› Une solution sécurisée qui peut être opérationnelle de manière transparente en quelques minutes, sans aucun déploiement technique.
› Une approche de sécurité native Zero Trust grâce à une architecture à double barrière.
› Une expérience utilisateur avancée permettant aux prestataires d'accéder à leurs ressources de manière sécurisée via un portail web.

Secteur de l'énergie : Se conformer à NIS2 en sécurisant l'accès des prestataires

Caractéristiques principales :

› Architecture Zero Trust autorisant uniquement les flux sortants et garantissant l'absence d'ouverture de port.

› Enregistrement des sessions web sans client et sans serveur.

› Accès sans client des prestataires par l'intermédiaire d'un portail web.

› Rupture de protocole isolant le LAN OT de l'organisation des postes afin d'éviter toute contamination.

› Intégration transparente avec des solutions de transfert de données sécurisées (« diodes réseau »).

cyberelements

SECTION 6:

LES FONCTIONNALITES DE CYBERELEMENTS

L’authentification

En prenant en charge une gamme variée de méthodes d'authentification, cyberelements garantit la flexibilité et l'évolutivité des organisations de toutes tailles. Cette intégration permet aux utilisateurs d'accéder aux applications et aux services sans effort, tandis que des mesures de sécurité robustes les protègent contre les accès non autorisés et les violations de données. Grâce aux fonctions d'authentification avancées de cyberelements, les entreprises peuvent rendre la gestion des accès plus efficace et améliorer leur niveau de sécurité.

cyberelements intègre une technologie avancée d'authentification multi-facteurs (MFA) et de vérification biométrique pour protéger les données des utilisateurs et empêcher les accès non autorisés :

Azure AD

OTP (Mail, SMS)

TOTP FIDO2

Certificat

RSA/Radius

Neomia Pulse (biométrie comportementale)

cyberelements offre un système d'authentification qui s'intègre de manière transparente à diverses sources d'identité :

Annuaire local/intégré

AD d'entreprise

IDP tiers

cyberelments, grâce à sa fonction d'authentification unique (SSO/authentification secondaire), garantit l'accès aux prestataires sans qu'il soit nécessaire de partager avec eux des informations d'identification : aucune divulgation de secrets d’authentification.

Contrôle d'accès

Le contrôle d'accès est un élément fondamental de notre schéma de sécurité, conçu pour garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources critiques de votre organisation.

L'accès conditionnel garantit que l'accès aux ressources n'est accordé que dans des conditions sécurisées et prédéfinies. cyberelements renforce la sécurité en évaluant le contexte des demandes d'accès : poste, réseau, navigateur, système d'exploitation, anti-virus, EDR/XDR, lieu, présence d'un fichier, créneaux horaires.

cyberelements propose des politiques d'accès Zero-Trust basées sur l'approche "never trust, always verify" (ne jamais faire confiance, toujours vérifier).
-le moindre privilège, limitant l'accès à ce qui est nécessaire
-le privilège JIT (just-in-time), qui permet d'accorder des autorisations temporaires en cas de besoin
-le privilège Zero Standing, évitant les accès à privilèges permanents.
Cette approche minimise les risques de sécurité en validant continuellement l'accès et en évitant les autorisations permanentes inutiles.

Les politiques d'accès basées sur les rôles de cyberelements utilisent les groupes d'Active Directory (AD) pour gérer les autorisations en fonction des rôles des utilisateurs. Cela permet de s'assurer que les utilisateurs n'ont que les accès nécessaires à leurs tâches.

La gestion des demandes d'accès just-in-time (JIT) permet d'accorder des droits d'accès temporaires en fonction des besoins. Les utilisateurs demandent des autorisations élevées, qui sont examinées et approuvées avant d'être accordées. Il faut veiller à ce que les droits d'accès élevés soient automatiquement révoqués une fois les tâches accomplies.

L'élévation de privilèges de cyberelements accorde temporairement aux utilisateurs des droits d'accès plus élevés pour des tâches spécifiques. Gérée par le biais de demandes structurées et des workflows automatisés, elle permet aux utilisateurs d'effectuer des tâches nécessitant un accès élevé tout en maintenant la sécurité.

Gestion des comptes

Dans le domaine industriel (OT), la gestion des comptes joue un rôle crucial dans la sécurisation des systèmes critiques. cyberelements assure une gestion robuste des comptes en fournissant des fonctionnalités clés pour la gestion des comptes à privilèges, la création des comptes par les utilisateurs et l'application des politiques d'authentification.

L'application des politiques d'identification permet de s'assurer que toutes les informations d'identification des utilisateurs sont conformes à des normes de sécurité rigoureuses. cyberelements facilite la mise en œuvre d'une politique de rotation des secrets d'authentification, qui impose la mise à jour régulière des mots de passe et des méthodes d'authentification.

cyberelements fournit des comptes à privilèges aux utilisateurs qui ont besoin d'accéder aux ressources critiques OT. Ces comptes permettent au personnel autorisé d'effectuer des tâches de haut niveau telles que la configuration du système, le dépannage et la maintenance.

Les comptes pilotés par l'utilisateur de cyberelements introduisent de la flexibilité dans l'environnement OT grâce à des alias dynamiques et personnels. Ces comptes permettent aux utilisateurs de jouer leur rôle en accordant et en révoquant rapidement des droits conformément aux politiques de l'organisation et aux besoins de l'utilisateur.

Gestion des sessions

La gestion des sessions en cybersécurité fait référence au processus de gestion et de surveillance des interactions des utilisateurs avec un système, depuis leur connexion jusqu'à leur déconnexion. C'est un élément crucial pour garantir que les sessions des utilisateurs sont sécurisées, cohérentes et suivies tout au long de leur cycle de vie.

cyberelements prend également en charge le partage de session (à quatre mains), qui permet à plusieurs utilisateurs autorisés de collaborer au sein d'une session. Cette fonction garantit que les actions critiques sont effectuées avec les approbations et les vérifications nécessaires..

Un système d'audit détaillé, offrant une traçabilité avancée de toutes les activités de l'utilisateur. Cette fonction garantit que chaque action entreprise par les utilisateurs est enregistrée, ce qui permet une responsabilisation précise et un suivi facile des changements dans le système.

La fonction d'enregistrement de session permet de capturer toutes les interactions au cours d'une session à des fins d'analyse et de conformité. Les enregistrements sont sauvegardés dans un format vidéo avec des possibilités de recherche avancée pour une analyse juridique.

Des actions déclenchées par des alertes sur les sessions en cours permettent de réagir en temps réel aux comportements potentiellement dangereux : Les administrateurs sont avertis et la session est automatiquement interrompue.

Adaptation culturelle

Le secteur industriel est traditionnellement ancré dans les processus physiques, avec un accent sur les résultats tangibles. Cet état d'esprit opérationnel contraste souvent avec le monde abstrait des technologies de l'information. Par conséquent, l'intégration de solutions de cybersécurité peut s'avérer difficile. cyberelements propose une solution pour combler le fossé entre ces deux cultures.

cyberelements est une solution multi-tenant qui permet aux administrateurs de créer une instance dédiée aux utilisateurs OT. Grâce à une solution unique, il est possible de sécuriser à la fois les systèmes IT et OT.
Encapsuler les mesures de sécurité informatique complexes dans des dispositifs tangibles et physiques.

En fournissant un mécanisme d'authentification centralisé, le SSO élimine le besoin de connexions multiples, rationalisant ainsi l'accès aux différents systèmes et applications.
Cette simplification coïncide parfaitement avec la préférence des industriels pour l'efficacité et la simplicité des processus.

cyberelements est conçu en tenant compte de l'expérience de l'utilisateur et en privilégiant la simplicité et l'intuitivité. Reconnaissant la diversité des compétences au sein des environnements industriels, notre plateforme offre une interface propre et épurée, facilement accessible au personnel des environnements IT et OT.

cyberelements

cyberlements.io est la plateforme d'accès Zero Trust et Identity-First pour la performance de l'entreprise, permettant aux organisations d'être mieux assurées contre les cyberattaques sans compromettre la productivité du personnel.

Elle fournit des accès sécurisés et des capacités de gestion des identités, pour les collaborateurs à distance et sur site, les prestataires et les opérateurs industriels, afin d'accéder aux applications professionnelles et aux systèmes privilégiés de l'organisation.

Commencez maintenant Gratuitement