Cybersécurité pour les infrastructures sensibles

La cybersécurité dans les réseaux industriels (operational technology, OT) pose d'autres exigences que la sécurité informatique. Claroty, l'entreprise de logiciels spécialisée, fournit une plateforme de sécurité OT complète pour une visibilité à 100 %, un accès à distance sécurisé ainsi qu'une surveillance et une détection permanentes des menaces sur les réseaux OT.

Traditionnellement, les installations industrielles et les infrastructures critiques étaient isolées des réseaux informatiques de leurs organisations respectives. Avec la numérisation, les réseaux opérationnels (OT), jusqu'alors isolés, sont de plus en plus reliés aux réseaux informatiques. Cela pose de grands défis aux équipes de sécurité: les systèmes OT utilisent généralement des protocoles propriétaires ou spécifiques à l'OT et se composent d'appareils qui ne peuvent pas être saisis et gérés de manière adéquate avec les outils de sécurité traditionnels.

L'OT parle une autre langue que l'IT

Les différences entre l'OT et l'IT se manifestent déjà avec les protocoles utilisés pour la communication, la gestion et la surveillance, et plus précisément au premier niveau du modèle NIST de la cybersécurité ICT, à savoir l'identification des ressources et des risques existants: un outil d'inventaire traditionnel peut reconnaître qu'il y a un appareil, mais il ne peut pas fournir d'autres informations sans connaître les détails de l'environnement OT. C'est pourquoi les fournisseurs de cybersécurité du monde informatique ne disposent pas de la visibilité nécessaire sur les réseaux OT pour assurer la protection adéquate.
Par conséquent, les menaces ne sont pas détectées, notamment parce que l'on ne dispose pas d'informations sur les points faibles des systèmes OT. De plus, les systèmes OT sont conçus pour durer et fonctionner sans interruption. Les appareils OT ne peuvent pas être mis à jour ou remplacés par une nouvelle version sans mettre en péril la disponibilité de l'infrastructure ou entraîner des coûts énormes. En outre, les personnes responsables des réseaux OT sont souvent des chefs de production qui ne se sont pas encore focalisés sur la sécurité, ou alors des responsables de réseaux OT qui ne sont pas intégrés à l'équipe de sécurité informatique.

La spécialisation permet de combler les différences

C'est à ce genre de problèmes que sont confrontés les fournisseurs qui s'aventurent dans le nouveau domaine de la sécurité OT après avoir travaillé dans le domaine de la sécurité IT. La situation est différente pour les fournisseurs spécialisés comme Claroty, une entreprise fondée en Israël en 2015, dont le siège est à New York, qui emploie plus de 600 personnes et compte de nombreux clients de renom – également en Suisse (par exemple des entreprises publiques ou l'industrie alimentaire et chimique).
Fin 2021, Claroty a également acquis Medigate, le fournisseur de la plateforme de cybersécurité leader pour le milieu médical. Avec des acteurs mondiaux →

de l'environnement OT tels que Siemens, Schneider Electric ou Rockwell Automation comme investisseurs, Claroty a directement accès aux experts et au savoir-faire OT jusqu'au niveau des protocoles et des appareils. L'entreprise peut ainsi proposer une solution de cybersécurité complète pour les infrastructures sensibles, qui complète les plateformes de cybersécurité courantes avec des fonctionnalités spécifiques à l'OT et qui, grâce à des tableaux de bord clairs, met en évidence l'environnement OT de manière graphique à l'aide du modèle Purdue couramment utilisé dans le cadre des réseaux OT.

Visibilité, accès à distance et détection des menaces

La plateforme de Claroty comprend les trois technologies clés: Claroty Edge, Claroty Secure Remote Access (SRA) et Claroty Continuous Threat Detection (CTD). À cela s'ajoute un vaste écosystème d'intégrations, par exemple avec des solutions de cybersécurité du secteur informatique, des systèmes de contrôle industriels, des plateformes de gestion des services et SIEM sur la base d'une API robuste. Claroty Edge fonctionne comme un collecteur de données basé sur Windows, ne laisse pas d'empreinte physique dans l'environnement OT et ne nécessite aucune modification du réseau. En quelques minutes, un inventaire complet de toutes les ressources OT, y compris les détails spécifiques aux appareils, est créé, et ce sans charge notable sur le réseau OT.

Les solutions d'accès à distance conventionnelles sont trop complexes et centralisées pour les accès à distance OT. Claroty SRA a été spécialement conçu pour l'accès à distance aux environnements OT et optimisé pour les applications et les workflows OT. SRA gère des sites répartis dans le monde entier avec une gestion locale et centralisée et permet un contrôle complet des accès privilégiés. Claroty CTD fournit les données nécessaires à des fonctions telles que la segmentation du réseau, la détection des menaces et des anomalies, la gestion des ressources et des vulnérabilités, sur la base d'une connaissance intégrée des protocoles et des appareils spécifiques à l'OT, à l'aide d'une détection passive via des capteurs non intrusifs.

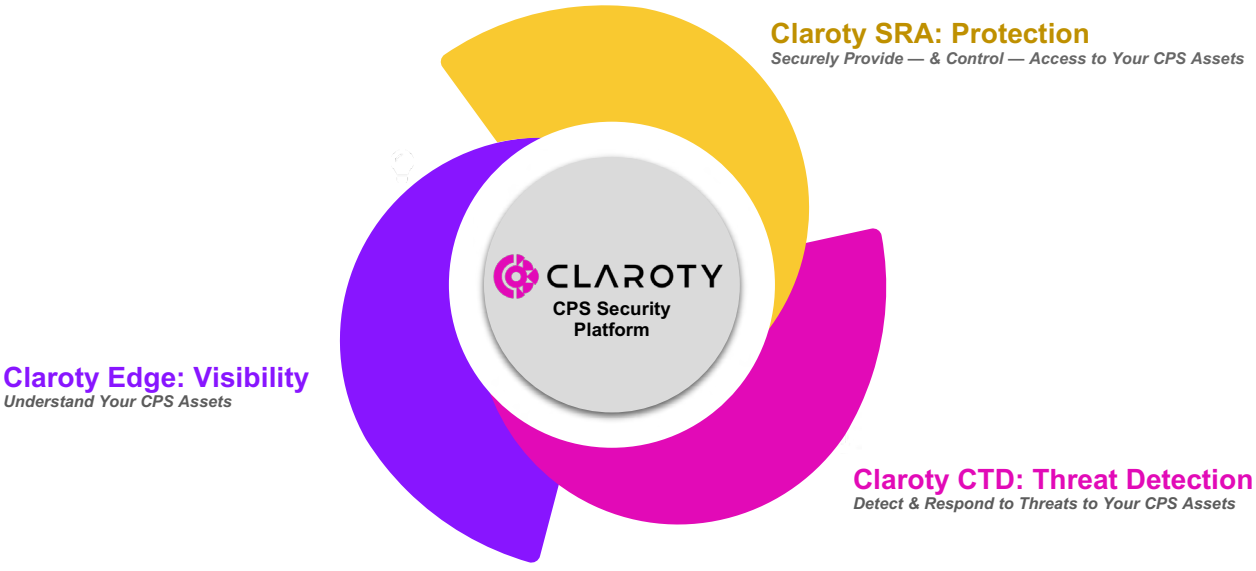
Claroty: les avantages

- Solution de cybersécurité complète pour l'industrie, les infrastructures sensibles et les soins de santé.
- Offre une visibilité à 100 % sur les réseaux OT (Claroty Edge)
- Etend le contrôle connu de l'IT à l'OT
- Ne surcharge pas les installations, les appareils et les réseaux OT
- Permet un accès à distance sécurisé de la gestion OT (Claroty SRA)
- Détecte en permanence les menaces ciblant les installations OT, IoMT et IoT (Claroty CTD)
- Mise en place au choix sur site ou dans le cloud

BOLL
IT Security Distribution

BOLL Engineering SA
En Budron H15
1052 Le Mont-sur-Lausanne

Tél. 021 533 01 60
vente@boll.ch
www.boll.ch



→ **boll.ch/claroty**