Gestion intégrée de l'exposition

Tenable se positionne comme un précurseur de la gestion des vulnérabilités, mais a bien plus à offrir avec sa plateforme de gestion des expositions, qui permet d'avoir une vue complète de tous les cyberrisques. Patrick Michel, principal consultant chez BOLL Engineering, nous livre dans cette interview des informations sur les solutions et leurs avantages.

Patrick Michel, principal consultant chez BOLL.

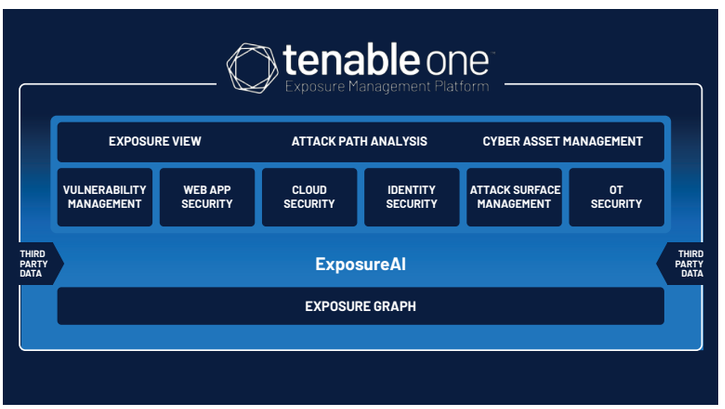
Tenable – qui est-ce?
Fondée en 2002, Tenable s'est d'abord consacrée à la gestion des vulnérabilités avec sa solution Nessus. Aujourd'hui, Tenable propose une plateforme complète de gestion de l'exposition, orientée vers l'analyse, qui couvre pratiquement tous les aspects de la cybersécurité et fournit une vue à la fois complète et détaillée des cyberrisques qui peuvent menacer une entreprise.

Qu'est-ce qui distingue Tenable des fournisseurs de solutions similaires?
Comme d'autres fournisseurs de cybersécurité, Tenable a acheté plusieurs produits et sociétés de cybersécurité au fil des ans. Cependant, Tenable a réussi de manière unique à intégrer ces différentes solutions pour former une plateforme unifiée qui offre une vue unique et unifiée de la surface d'attaque.

Quel est le nom de cette plateforme et comment est-elle structurée?
Elle s'appelle Tenable One. Outre une version spécialement adaptée de Nessus, trois composants clés permettent d'évaluer et de hiérarchiser tous les cyberrisques de manière étayée, afin de s'attaquer en premier lieu aux plus importants:

- «Asset Inventory» offre une visibilité centralisée de tous les assets du réseau de l'entreprise. Dans un contexte où de nombreuses entreprises ne savent même pas quels systèmes sont présents, c'est un aspect essentiel.
- «Lumin Exposure View» résume clairement les insights sur les risques.
- «Attack Path Analysis» permet de trouver les points faibles les plus importants et donc les plus dangereux au sein d'un chemin d'attaque. Cela aide à prioriser les vulnérabilités à éliminer.
- Le tout est soutenu par l'IA générative intégrée ExposureAI et par les informations d'exposition de l'équipe de recherche de Tenable. Sur cette base, la plateforme propose des solutions pour différents domaines techniques.

Quels sont les domaines couverts?
Tenable One maximise la sécurité informatique grâce à une gestion classique et générale des vulnérabilités, mais offre bien plus que cela. Ainsi, des composants dédiés assurent la sécurité des applications web ainsi que des environnements cloud et multicloud simples à complexes (y compris Kubernetes et les environnements de conteneurs). En outre, la solution soutient la sécurisation de l'authenticité des identités (par exemple dans Active Directory), permet la sécurisation des systèmes OT et assure une gestion globale de la surface d'attaque.



Comment utiliser Tenable One?
La plateforme est basée sur le cloud et peut donc être utilisée sans installation sur site. Elle est en outre multitenant et disponible en tant que service MSSP – ce qui est également intéressant pour les partenaires qui souhaitent offrir à leurs clients une plateforme de cybersécurité complète de première qualité avec le moins de frais possible.

La plateforme s'adresse à quelles entreprises?
Avec ses solutions, Tenable vise davantage le segment des grandes entreprises – comme la plupart des fournisseurs américains – et a des clients comptant jusqu'à 150 000 collaboratrices et collaborateurs. Tenable One est toutefois très évolutif et peut également faire valoir ses avantages dans des entreprises de taille moyenne, par exemple dans une PME de 100 ou 200 collaborateurs. Cela vaut tout particulièrement pour la variante Managed Service, qui peut être utilisée de manière très flexible.

Qu'est-ce qui distingue notamment Tenable?
L'excellent service d'assistance qui facilite la vie des partenaires et de leurs clients et qui s'occupe des problèmes de manière fondée et en temps voulu. L'expérience montre qu'une telle qualité de service n'existe pas chez tous les concurrents. Un autre avantage évident de la plateforme intégrée est la mise à disposition d'informations fiables sur les risques, indispensables pour le respect de la conformité et des directives réglementaires de l'entreprise.

BOLL
IT Security Distribution

BOLL Engineering AG

En Budron H15 I 1052 Le Mont-sur-Lausanne
021 533 01 60 I vente@boll.ch
www.boll.ch