

A knight in full plate armor, including a helmet with a visor and chainmail, is shown from the waist up. He holds a sword aloft in his right hand and a shield in his left. The shield is yellow with a grey unicorn emblem. The background is dark with a network graph of white nodes and lines, and some yellow nodes are visible on the left side.

**DTS**

# VULNERABILITY MANAGEMENT SERVICE

## VULNERABILITY MANAGEMENT SERVICE

Vulnerability Management – die Identifizierung und Priorisierung von IT-Schwachstellen – wird immer noch unterschätzt. Dabei sollte es höchste Priorität haben, Sicherheitslücken frühzeitig zu erkennen und anschließend zu beheben. Mit Tenable haben wir einen führenden Partner auf dem Gebiet der Schwachstellenerkennung an unserer Seite. In unserem gemeinsamen Service machen wir all Ihre IT-Assets und deren Sicherheitslücken sichtbar. Zudem werden sämtliche Problembereiche analysiert und priorisiert. Das Ergebnis: Wir helfen Ihnen maßgeblich, IT-Schwachstellen schnell und effektiv zu identifizieren, um diese anschließend beheben zu können – veredelt mit wichtigen DTS-Mehrwerten als Managed Service!

- Sichtbarkeit, Überblick & Darstellung von allen Assets & deren Schwachstellen
- Branchenweit umfangreichste Schwachstellen-Abdeckung
- Analyse, Bewertung & Priorisierung der Sicherheitslücken
- Intuitives Dashboard & Analysen sowie Visualisierungen
- DTS Managed Services
  - Einrichtung, Bereitstellung & Best-Practise-Beratung
  - Support
  - Tiefgreifendes Know-how – auch mittels vorgelagertes PoC

Sicherheitsrisiken sichtbar machen, Gefahren in der IT-Landschaft nachvollziehen und genau wissen, welche Schwachstellen zuerst geschlossen werden sollten – das alles liefert bestes Vulnerability Management. Unser cloudbasierter Service, natürlich nach deutschen Standards bereitgestellt, liefert Ihnen diese Aspekte, indem wir sämtliche Assets und Schwachstellen in Ihrem Unternehmen identifizieren. Das Besondere: Wir bieten zusätzlich die branchenweitumfangreichste Schwachstellen-Abdeckung und Priorisierung von Sicherheitsproblemen.

Aktives Scannen, Agents, passives Monitoring, Cloud-Connectoren sowie CMDB-Integrationen ermöglichen eine umfangreiche Sichtbarkeit und einen kontinuierlichen Überblick über alle Assets. Dabei spielt es keine Rolle, ob diese bereits bekannt sind oder bisher unbekannt waren. Außerdem erfolgen das Sammeln und Analysieren der Angriffsfläche durch die Vielzahl von Sensoren vollautomatisch.

Im nächsten Schritt können wir mit einer Abdeckung von mehr als 72.000 Schwachstellen und einer umfassenden Unterstützung für CVEs und Sicherheitskonfigurationen, sämtliche Risiken in diesen Assets nachvollziehen. Dies gilt selbst bei hochdynamischen Assets wie Mobilgeräten, virtuelle Maschinen, Containern und Cloud-Instanzen.

Die Kombination der Schwachstellendaten mit Threat-Intelligence und Datenwissenschaft, liefert die finale, leicht verständliche Risikobewertung. Auf dieser Grundlage erfahren Sie, wie bestimmte Risiken einzuschätzen und welche Schwachstellen mit welcher Priorität zu beheben sind. Das proaktive Identifizieren und Bewerten der Sicherheitslücken mit den größten Auswirkungen auf Ihr Unternehmen bezieht sich sogar auf vollkommen neuartige Bedrohungen. Sobald diese auftreten, erhalten Sie gezielte Warnmeldungen und können sofort reagieren.

Ganz allgemein zeigt das intuitive Dashboard verschiedenste Visualisierungen, Erkenntnisse und schnelle Analysen. Es bietet aber auch anpassbare Berichte, z. B. um Sicherheitsteams aktiv über kritische Probleme zu informieren.

## **DTS MANAGED SERVICES**

Wir stellen Ihnen das Vulnerability Management als echten Managed Service zur Verfügung. Das bedeutet, wir ergänzen die eigentliche Lösung durch zahlreiche Service-Mehrwerte, die Ihnen nicht nur wesentliche Ressourcen sparen, sondern auch wichtiges Know-how mit an die Hand geben. Vorab bieten wir eine Best-Practice-Beratung und machen gerne, gemeinsam mit Ihnen, einen Proof of Concept (PoC). Darin ist ein Kick-Off zu allen nötigen Abstimmungen inbegriffen, intensiver Austausch schon während des tatsächlichen PoC-Zeitraums sowie ein Abschlussgespräch zu den entsprechenden Ergebnissen. Selbstverständlich gehört auch die Einrichtung und Bereitstellung der Plattform für Sie mit zum Service. Außerdem übernehmen wir jeglichen Support.