



Tenable veröffentlicht die neueste Version von SecurityCenter 5.7

München, 27. August 2018 – [Tenable™](#), das Cyber Exposure-Unternehmen, veröffentlicht die neueste Version von SecurityCenter 5.7. Mit den neuen Erweiterungen können Kunden den Sicherheitsstatus mobiler Workspaces der Mitarbeiter besser bewerten und managen. Neben bestehenden Integrationen mit CyberArk und Thycotic hat Tenable nun auch neue Access-Management-Plattformen wie Bomgar und BeyondTrust ergänzt. So können Kunden kontinuierliche Schwachstellenbewertungen ihrer unternehmenskritischen Systeme durchführen, ohne die Privatsphäre der Mitarbeiter zu beeinträchtigen.

„In der modernen Arbeitswelt können sich IT-Verantwortliche nicht länger auf traditionelle Sicherheitsmethoden verlassen, um Informationen zu den Geräten zu sammeln. Das gilt vor allem, wenn diese selten mit der Unternehmensumgebung verbunden sind. Angreifer können über diese blinden Flecken Einblick in sensible Unternehmensdaten gewinnen“, erklärt Dave Cole, Chief Product Officer, Tenable. „Mit den neuesten Funktionen des Mobile Agent Workforce in SecurityCenter 5.7 können Kunden die Geräte und Assets im Unternehmensnetzwerk besser verstehen und managen. Unser Ziel ist es, den Kunden innovative Funktionen bereitzustellen und den Sicherheitsteams die richtigen Lösungen zu geben, mit denen sie moderne Computing-Umgebungen sichern können.“

Mit dem Support von Mobile Agent Workforce in SecurityCenter 5.7 erweitert Tenable die Funktionalitäten des Nessus® Agents. Sie unterstützen Unternehmen dabei, komplexe Infrastrukturen sowie gemeinsame, doppelte IP-Adressbereiche bereitzustellen, die häufig in Heimnetzwerken oder öffentlichen Hotspots verwendet werden. Mit der eindeutigen Tracking-Kennung pro Agent erhalten SecurityCenter-Kunden einen besseren Überblick über alle Geräte, die schwer identifizierbar sind, da sich mobile Mitarbeiter und Remote Büros häufig mit mehreren Netzwerken verbinden und trennen. Mit aktiviertem Tracking gewährt SecurityCenter Einblick in den vorherigen aber auch den aktuellen Gerätestatus, egal von welchem Netzwerk aus ein Agent kommuniziert.

SecurityCenter 5.7 unterstützt ab sofort auch Access Management-Plattformen wie Bomgar und BeyondTrust: Dadurch können Nutzer privilegierte Zugangsdaten in Passwort-Depots speichern und diese automatisch während des Scans abrufen. Das gibt ihnen umfassenden Einblick in die Sicherheitslage eines Assets und stellt gleichzeitig sicher, dass sensible

Passwörter kontrolliert, geprüft und in Scans einbezogen werden – ohne, dass sie dazu in SecurityCenter ergänzt oder gespeichert werden müssen.

„Es ist oft schwierig, die Zugriffsrechte zu erlangen, um ein System auf Schwachstellen zu überprüfen. Dies liegt daran, dass Sicherheits- oder Betriebsrichtlinien den Einsatz privilegierter Konten einschränken“, sagt David Cole. „SecurityCenter 5.7 unterstützt nun alle wichtigen Anbieter für privilegiertes Access-Management und kann zudem Agenten bereitstellen, die für tiefgehende Scans kein Benutzerkonto benötigen. So erfahren Sicherheitsteams die Details zu ihrem Gefährdungsgrad, ohne dafür die Berechtigungsnachweise umständlich managen zu müssen.“

Weitere Informationen zu SecurityCenter 5.7 auf der [Webseite](#) oder auf dem [Tenable-Blog](#).