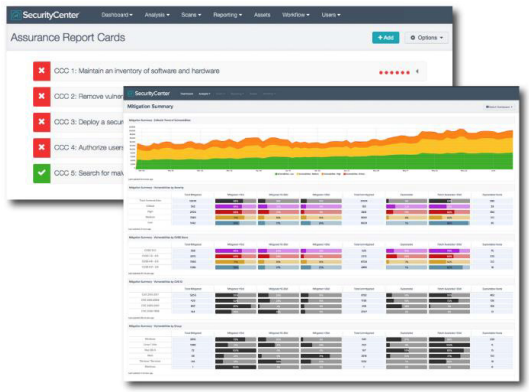
SecurityCenter CV
Continuous View

„Die ideale All-in-One-Lösung von Tenable, mit der ich Sicherheitsrisiken priorisieren und die Sicherheitslage meines Unternehmens jederzeit anhand der Unternehmensziele beurteilen kann.“ - Dienstleister im Gesundheitswesen

Marktführende Lösung für kontinuierliches Netzwerk-Monitoring

Angesichts einer sich verändernden IT-Landschaft (Virtualität, Mobilität, Cloud-Services) und ständig wachsender Cyberbedrohungen reichen periodische Scans und Compliance-Audits nicht mehr aus, um Unternehmen wirkungsvoll vor Cyberattacken zu schützen. Kontinuierliches Netzwerk-Monitoring ist ein neues Konzept für mehr Sicherheit und Compliance in Ihrem Unternehmen. Es verschafft Ihnen die Gewissheit, dass Ihre IT-Sicherheitssysteme korrekt konfiguriert sind, fehlerfrei arbeiten und zum richtigen Zeitpunkt aussagekräftige Daten zu den Unternehmensrelevanten Sicherheitsrisiken liefern.

SecurityCenter Continuous View® (SecurityCenter CV™) ist die marktführende Plattform für kontinuierliches Netzwerk-Monitoring. Sie bietet umfassende Informationen zum Sicherheits- und Compliance-Status Ihrer gesamten IT-Infrastruktur, aussagekräftige Daten zu priorisierten Schwachstellen und die Gewähr, dass Sicherheits- und Compliancestrukturen jederzeit auf die Organisationsziele abgestimmt sind. Als einzige am Markt verfügbare Lösung umfasst SecurityCenter CV das Monitoring von lokalen und cloudbasierten Assets, aktive und passive Schwachstellenanalyse, Konfigurationsüberprüfung, Änderungserkennung, Malware-Erkennung, Threat Intelligence sowie Analyse von Netzwerk- und Nutzeraktivitä ten.



Dashboards, Berichte, Workflows und Sicherheitsrichtlinien lassen sich individuell an Ihre spezifischen Anforderungen anpassen

SecurityCenter CV beinhaltet Assurance Report Cards® (ARCs), mit denen Sie die Effektivität Ihres Sicherheitsprogramms kontinuierlich visualisieren, messen und analysieren können. Sie basieren auf den von CISOs und der Unternehmensführung definierten Zielen sowie anpassbaren Richtlinien.

Tenable-Forschung

Das Tenable-Forschungsteam bietet allen SecurityCenter CV-Kunden regelmäßige Updates zu Schwachstellen- und Bedrohungsdaten, erweiterten Analysen, Sicherheits- / Compliance-Richtlinien, Dashboards, Berichten und Assurance Report Cards. Dieses vorkonfigurierte Material basiert auf von Tenable zusammengestellten Best Practices von Kunden und aus der Branche. Damit stellt Ihnen unser Security Research Team seine gesamte Kompetenz zur Verfügung. Die Inhalte sind Teil der SecurityCenter CV-Subscription.

Entscheidende Vorteile

- Sie werden immer informiert, wenn neue oder geänderte Assets auf Angriffsflächen zugreifen
- Sie erhalten umfassenden Überblick über Ihre IT-Infrastruktur mit Endgeräten, Servern, Datenbanken, Mobilgeräten, Domain Controllern, Netzwerkgeräten, virtuellen Anwendungen und der Cloud
- Sie erhalten einen Einblick in vorübergehend genutzte, schwer überprüfbare und nicht sicher zu scannende Systeme, der ohne kontinuierliches Netzwerk-Monitoring nicht möglich wäre
- Sie erhalten dank automatisierter Analyse von Schwachstellen- und Konfigurationsdaten detaillierte sicherheitsbezogene Informationen. Hinzu kommen Daten zu Patching-Status, bekannten Exploits und Bedrohungsanalyse sowie die Erfassung von verdächtigem Netzwerktraffic und Nutzerverhalten
- Sie können gefährliche Schwachstellen rasch identifizieren und sich somit auf die wirklich wichtigen Sicherheitsmaßnahmen konzentrieren
- Assurance Report Cards ermöglichen die Weiterleitung von Sicherheitsdaten
- Die Einhaltung von Branchennormen und Vorschriften wird dokumentiert
- Immer auf dem neuesten Stand mit den von Tenable bereitgestellten Daten

Wichtigste Merkmale und Funktionen

- Assurance Report Cards: kontinuierliche Analyse der Effektivität von kundendefinierten, unternehmenszielbasierten Sicherheits- und Compliance-Richtlinien zur Identifikation und Schließung von Sicherheitslücken.
- Umfassend anpassbare Dashboards/Berichte: Eine HTML5-basierte Benutzeroberfläche erfüllt die spezifischen Anforderungen von CISOs, Sicherheitsmanagement, Analysten und Anwendern.
- Breite Asset-Abdeckung: Server, Endgeräte, Netzwerkgeräte, Betriebssysteme, Datenbanken und Anwendungen in physischen, virtuellen und Cloud-Infrastrukturen.
- Kontinuierliche Asset-Erkennung: Erfassung aller Mobilgeräte sowie physischer, virtueller und cloudbasierter Instanzen im Netzwerk, einschließlich unautorisierter Assets.
- Dynamische Asset-Klassifizierung: Gruppierung von Assets auf der Grundlage von Richtlinien und Kriterien (z. B. mehr als 30 Tage alte Windows 7-Assets mit Schwachstellen).
- Schwachstellenmanagement: verschiedene Scanning-Optionen wie passives Netzwerk-Monitoring sowie credentialed und non-credentialed Scanning zur umfassenden Analyse und Konfigurationsüberprüfung.
- Agent-basiertes Scanning: zum leichteren Scanning von Mobilgeräten und schwer zu erfassenden Assets.
- Malware-Erkennung: Integrierte Threat Intelligence-Feeds (Malware-Indikatoren, schwarze Listen) identifizieren komplexe Malware.
- Analyse des Netzwerkzustands: kontinuierliches Monitoring des Netzwerkverkehrs auf verdächtigen Traffic von und zu verwundbaren Systemen/Services, unbekannten Geräten, Botnets und Command-/Control-Servern.
- Erkennung von Anomalien: Einsatz von Statistiken und Analysen anormalen Verhaltens bei der Überwachung externer Log-Quellen zur automatischen Erkennung von Aktivitäten, die von der Regel abweichen.
- Umfassende Analyse/Trenderkennung: kontextbezogene Daten und umsetzbare Informationen zur Priorisierung von Sicherheitsproblemen im Zusammenhang mit sämtlichen Assets des Unternehmens.
- Benachrichtigung: konfigurierbare Warnmeldungen für Administratoren zur Einleitung manueller (E-Mail, Mitteilungen, Trouble Tickets) oder automatischer Aktionen über APIs.
- Automatisierte Compliance: vordefinierte Kontrollen bezüglich Branchenstandards und gesetzlichen Vorgaben wie CERT, DISA STIG, DHS CDM, FISMA, PCI DSS und HIPAA/HITECH.
- Integration: vorkonfigurierte Integration mit Patch-Management, Mobilgeräte-Management, Threat Intelligence und anderen Drittanbieter-Produkten oder Nutzung von SecurityCenter-APIs zur Entwicklung eigener Integrationen.

SecurityCenter CV – Vorteile

Kunden profitieren von SecurityCenter CV durch

- **Beseitigung von Schwachstellen** aufgrund von nicht verwalteter Assets und Schwachstellen, die das Risikoprofil erhöhen und häufig Ursache von Sicherheitsproblemen sind.
- **Erhöhte Effizienz**: Die Verfügbarkeit kompletter Kontexte ermöglicht die schnelle Analyse und Priorisierung von Schwachstellen.
- **Nachweis von Sicherheit und Compliance** gegenüber allen Stakeholdern anhand spezifischer Kennzahlen, aus denen der Sicherheitsstatus eindeutig hervorgeht.

SecurityCenter-Editionen

SecurityCenter

SecurityCenter® ist die innovative Lösung zur Analyse von Schwachstellen und arbeitet mit Nessus®-Scannern, der weltweit am häufigsten eingesetzten Technologie zur Schwachstellenerkennung. SecurityCenter ermöglicht lückenlosen Einblick in die Sicherheitssituation verteilter und komplexer IT-Infrastrukturen.

SecurityCenter Continuous View

SecurityCenter Continuous View ist die marktführende Lösung für kontinuierliches Netzwerk-Monitoring. Sie verbindet SecurityCenter, Passive Vulnerability Scanner® (PVS™)-Netzwerksensoren und die Log Correlation Engine® (LCE®) zu einer umfassenden Infrastruktur für kontinuierliches Netzwerk-Monitoring.

tenable™

Für weitere Informationen: Besuchen Sie tenable.com
Kontakt: Bitte senden Sie eine E-Mail an sales@tenable.com oder besuchen Sie tenable.com/contact