# tenable.sc™

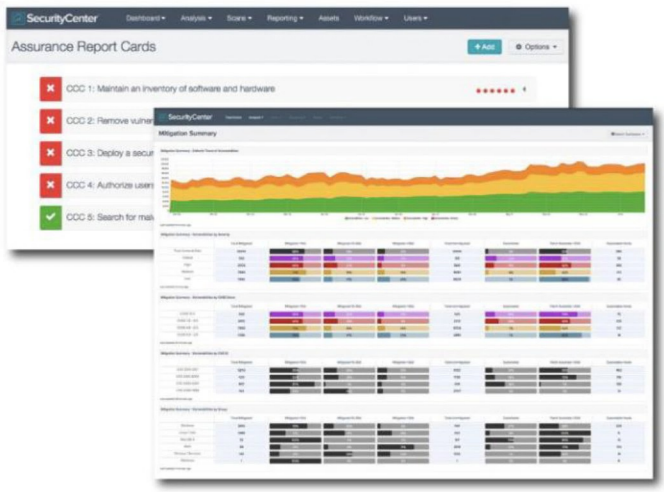
پلتفرم Tenable.sc™ یک دیدگاه جامع و یکپارچه از وضعیت امنیتی سازمان ارائه می‌دهد تا ریسک‌های کسب‌وکار کاهش یابد و انطباق به‌صورت مؤثر تضمین شود.

## مدیریت آسیب‌پذیری - استقرار مدیریت‌شده در محل سازمان

Tenable.sc با ارائه دید کامل از سطح حمله (Attack Surface)، به شما کمک می‌کند تا ریسک سایبری را مدیریت و اندازه‌گیری کنید.
این راه‌حل از طریق تحلیل‌های پیشرفته، داشبوردها و گزارش‌های قابل سفارشی‌سازی و گردش‌های کاری (Workflows) نقاط ضعف دارایی‌های متصل به شبکه را شناسایی می‌کند، شامل آسیب‌پذیری‌ها، پیکربندی‌های نادرست و بدافزارها.

Tenable.sc، مبتنی بر فناوری پیشروی Nessus، داده‌های آسیب‌پذیری را از مجموعه‌ای از اسکنرهای Nessus® در سراسر سازمان جمع‌آوری و تحلیل می کند. این پلتفرم با نمایش روندهای آسیب‌پذیری در طول زمان، امکان ارزیابی دقیق ریسک و اولویت‌بندی هوشمند اصلاحات را فراهم می‌سازد.
Tenable.sc مجهز به یک موتور گردش‌کار قابل پیکربندی است که فرآیند پاسخ و اصلاح (Remediation) را سرعت می‌بخشد، ریسک کلی را کاهش می‌دهد و انطباق را بهینه می‌کند.

همچنین این پلتفرم دارای کارت‌های گزارش تضمین (Assurance Report Cards® ،ARCs) است که اثربخشی برنامه امنیتی سازمان را به‌صورت مستمر اندازه‌گیری، تحلیل و بصری‌سازی کرده و بینش لازم را برای مدیران ارشد امنیت اطلاعات و تیم مدیریت ارائه می‌دهد.




## تیم تحقیقاتی Tenable

تیم تحقیقاتی Tenable به‌طور مستمر به‌روزرسانی‌های مرتبط با اطلاعات آسیب‌پذیری و تهدید، تحلیل‌های پیشرفته، سیاست‌های امنیتی و انطباق، داشبوردها، گزارش‌ها و کارت‌های گزارش تضمین (ARC) را در اختیار کاربران Tenable.sc قرار می‌دهد.

این محتوای آماده استفاده، بر پایه بهترین شیوه‌های صنعت توسعه یافته و بخشی از اشتراک Tenable.sc است؛ به شما امکان می‌دهد از تخصص و دانش روز تیم تحقیقاتی Tenable برای ارتقای برنامه امنیتی خود بهره‌مند شوید.

## مزایای کلیدی

- شناسایی نقاط ضعف: اسکن کامل دارایی‌های متصل به شبکه برای کشف آسیب‌پذیری‌های شناخته‌شده، پیکربندی‌های نادرست و بدافزارها.
- اولویت‌بندی هوشمند آسیب‌پذیری‌ها: تمرکز بر آسیب‌پذیری‌های با بیشترین ریسک و تحلیل احتمال سوءاستفاده طی 28 روز آینده.
- ارزیابی مدیریت پچ: تحلیل روند آسیب‌پذیری‌ها برای سنجش اثربخشی فرایندهای Patch Management.
- پاسخ‌دهی سریع به تغییرات: استفاده از هشدارها، اعلان‌ها و اقدامات خودکار برای واکنش سریع‌تر.
- اندازه‌گیری وضعیت امنیتی: سنجش مستمر سطح امنیت بر اساس سیاست‌هایی همسو با اهداف کلان کسب‌وکار.

**Tenable.sc مجموعه‌ای انعطاف‌پذیر از قابلیت‌های تحلیل آسیب پذیری، پایش روندها، گزارش‌دهی و گردش‌کار ارائه می‌دهد که می‌تواند کاملاً متناسب با نیازهای برنامه امنیتی سازمان شما سفارشی‌سازی شود.**

## ویژگی‌های کلیدی

- کارت‌های گزارش تضمین (Assurance Report Cards): پایش مستمر اثربخشی سیاست‌های امنیتی و شناسایی سریع شکاف‌های احتمالی.
- امتیازدهی اولویت آسیب‌پذیری (VPR): ترکیب تهدیدهای روز و یادگیری ماشینی برای تعیین احتمال سوءاستفاده در محیط واقعی سازمان.
- داشبوردها و گزارش‌های قابل سفارشی‌سازی: رابط HTML5 با انعطاف بالا برای نیازهای مدیران امنیت، کارشناسان و تحلیل‌گران.
- پوشش گسترده دارایی‌ها: ارزیابی جامع سرورها، کلاینت‌ها، دستگاه های شبکه، دیتابیس‌ها و برنامه‌ها در محیط‌های فیزیکی، مجازی و ابری.
- طبقه‌بندی پویای دارایی‌ها: گروه‌بندی هوشمند براساس سیاست‌های ازپیش‌تعریف‌شده؛ مثال: شناسایی دارایی‌های Windows 7 با آسیب‌پذیری های قدیمی‌تر از 30 روز.
- مدیریت آسیب‌پذیری: پشتیبانی از اسکن با/بدون احراز هویت برای تحلیل عمیق، کشف ضعف‌ها و بررسی تنظیمات امنیتی.
- اسکن مبتنی بر عامل (Agent-based): مناسب برای موبایل و دارایی هایی با دسترسی دشوار.
- وضعیت امنیتی مدیریت‌شده: اسکن قابل زمان‌بندی برای میزبان‌ها، دستگاه‌های مجازی و موبایل جهت شناسایی آسیب‌پذیری، بدافزار و misconfiguration.
- نتایج اسکن تجمیعی: تجمیع داده از چندین اسکنر و ارائه روندهای اصلاح امنیتی.
- تحلیل و روندهای پیشرفته: تولید بینش زمینه‌ای برای اولویت‌بندی دقیق‌تر ریسک‌ها در سطح سازمان

# tenable.sc

- تحلیل و روندهای پیشرفته: تولید بینش زمینه‌ای برای اولویت بندی دقیق‌تر ریسک‌ها در سطح سازمان.

- پاسخ به رخداد / گردش‌کاری: هشدارها و Workflowهای قابل تنظیم برای اقدامات دستی یا خودکار.

- مدل مدیریتی لایه‌ای: پشتیبانی از ساختارهای چندتیمی و چندمنطقه‌ای با کنترل دسترسی مبتنی بر نقش.

- توزیع بار خودکار: افزایش سرعت اسکن از طریق موازی‌سازی عملیات در محیط‌های توزیع‌شده.

- یکپارچه‌سازی‌های گسترده: اتصال آماده با Patch Management، Threat Intel، MDM و ... یا توسعه Integration اختصاصی از طریق APIها.

- انطباق پیشرفته: بررسی آماده برای استانداردهای امنیتی و الزامات نظارتی مانند PCI DSS، HIPAA، FISMA، SCADA، DISA STIG و موارد دیگر.

## نسخه‌های Tenable.sc

- Tenable.sc

نسخه اصلی و جامع پلتفرم تحلیل آسیب‌پذیری Tenable که با استفاده از چندین اسکنر Nessus–به‌عنوان پرکاربردترین اسکنر آسیب‌پذیری جهان–دید کامل و عمیقی از وضعیت امنیتی زیرساخت‌های بزرگ، پیچیده و توزیع‌شده ارائه می‌دهد.

این نسخه برای سازمان‌هایی مناسب است که نیاز به تحلیل دوره‌ای یا برنامه‌ریزی‌شده آسیب‌پذیری‌ها و مدیریت کامل چرخه اصلاح دارند.

- Tenable.sc Continuous View™

نسخه پیشرفته‌تر برای نظارت مداوم (Continuous Monitoring) بر شبکه.

این نسخه با ترکیب Tenable.sc، حسگرهای (Nessus Network Monitor (NNM و تحلیل رویدادها و ترافیک شبکه، دید بی‌درنگ (Real-time) از تهدیدات، آسیب‌پذیری‌ها و تغییرات محیطی فراهم می‌کند.

برای سازمان‌هایی ایده‌آل است که نیاز به مشاهده‌پذیری لحظه‌ای، کشف سریع تهدیدات و پایش 24/7 دارند.

| قابلیت‌ها | Tenable.sc | Tenable.sc Continuous View |
|---|---|---|
| مدیریت متمرکز آسیب‌پذیری با چندین اسکنر | ☐ | ☐ |
| طبقه‌بندی پویای دارایی‌ها (مانند سرور ایمیل، سرور وب و غیره) | ☐ | ☐ |
| حسابرسی پیکربندی مبتنی بر سیاست | ☐ | ☐ |
| شناسایی بدافزار (Malware Detection) با اطلاعات تهدید داخلی | ☐ | ☐ |
| داشبوردها و گزارش‌های از پیش تعریف‌شده با فیدهای خودکار Tenable | ☐ | ☐ |
| پاسخ به رخداد با هشدارها، اعلان‌ها و تیکتینگ قابل پیکربندی | ☐ | ☐ |
| کارت‌های گزارش تضمین (ARCs) | ☐ | ☐ |
| امتیازدهی اولویت آسیب‌پذیری (VPR) | ☐ | ☐ |
| کشف مستمر دارایی‌ها (مجازی، موبایل و ابری) | | ☐ |
| شناسایی غیرفعال آسیب‌پذیری دارایی‌های جدید و غیرقابل اسکن | | ☐ |
| شناسایی بلادرنگ ترافیک بات‌نت و فرمان و کنترل | | ☐ |
| شناسایی ناهنجاری با تکنیک‌های آماری و رفتاری | | ☐ |
| انطباق بهینه با هشدارهای پیشگیرانه درباره تخلفات | | ☐ |