ME Bank
ME Bank Uses Tenable SecurityCenter To Maintain CIS Compliance

Overview

ME Bank is the only bank that is 100 percent owned by Australia's leading industry super funds. ME Bank provides industry super fund, union and employer association members with a genuinely fairer banking alternative.

From the beginning, ME Bank's philosophy has been to deliver exceptional customer service, with a no-nonsense approach to borrowing. It offers products that are simple, fair and transparent, with low fees, low interest rates and higher returns, for industry super fund and union members.

- Key Business Needs: ME Bank needed a robust solution for conducting CIS-based best practice audits on its infrastructure and generating reader-friendly reports to support decision makers.
- Tenable Products Selected: ME Bank implemented Tenable SecurityCenter with Nessus® Vulnerability Scanner, Tenable Passive Vulnerability Scanner and Tenable Log Correlation Engine.

Top Benefits: SecurityCenter provides ME Bank with CIS-certified auditing and reporting using a scalable, agent-less architecture that minimizes performance impact.

Business Needs

Compliance with the CIS Framework

The Center for Internet Security (CIS) publishes benchmarks with recommended security settings to harden servers and applications from attack while maintaining operational ease of use. ME Bank wanted a solution that would help it maintain compliance with the CIS-based best practice audit framework, while providing easy-to-use reports for IT and management alike.

Performance and Cost

To protect the performance of its existing information systems, ME Bank required an agent-less architecture that would not tax the resources of its existing servers. And of course the bank was looking for a good return on its investment.

The Tenable Solution

Together with Content Security, a Tenable authorized reseller in ANZ, ME Bank selected Tenable's Unified Security Monitoring solution using Tenable SecurityCenter.

SecurityCenter puts everything you need to know about the security of your network at your fingertips, including vulnerability assessment, missing patches, intrusion events, configuration audits and anomalies. Tenable SecurityCenter centralizes and integrates information from the complete Tenable solution suite, including:

- Nessus® Vulnerability Scanner, which leverages the world's largest vulnerability and exposure database, including botnet detection
- Tenable Passive Vulnerability Scanner, which monitors network traffic for client-side vulnerabilities
- Tenable Log Correlation Engine, which collects and analyzes logs from thousands of data.

Using this data, SecurityCenter creates a central network security repository with advanced analysis, reporting and alerting on a role-by-role basis.

The Results

Using Tenable SecurityCenter, ME Bank is able to meet its CIS compliance objectives. Tenable Network Security has been certified by the Center for Internet Security to perform a wide variety of Unix, Windows and application audits based on the best practice consensus benchmarks developed by CIS. Tenable SecurityCenter includes CIS compliance templates for ready-to-use reports that can be shared with the IT team as well as management.

Because SecurityCenter is completely customizable, ME Bank is able to fine-tune the solution for its specific needs. A web-based interface provides easy access to the console panel. As a scalable, agent-less solution, Tenable SecurityCenter helps ME Bank protect its network while planning for the future.

For More Information
Questions, purchasing, or evaluation:

Content Security
Securing Networks