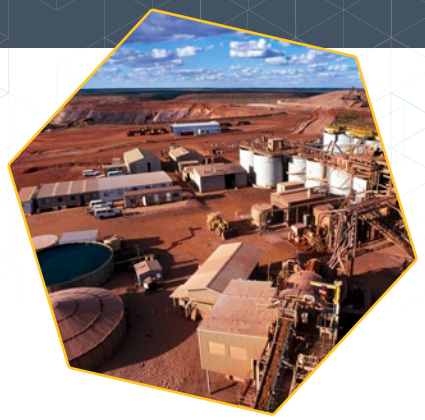
tenable network security

# Industrias Peñoles

## Mining for Vulnerabilities



## Overview

Based in Mexico City, Mexico, Industrias Peñoles S.A. de C.V. is one of the largest mining concerns in Mexico, and a major silver producer worldwide. The IT administrators at the organization's main Plata site are responsible for providing computing services to 4,000 employees and protecting the security of mining operations.

- **Key Business Needs**: Peñoles needed to replace manual network security scanning and analysis with an automated system that supported fast threat identification and mitigation.
- **Tenable Products Selected**: Peñoles selected Tenable Nessus for vulnerability scanning and Tenable SecurityCenter for scanning automation, analysis, real-time dashboards and constant vulnerability updates.
- **Top Benefits**: SecurityCenter automates vulnerability detection, accelerates threat mitigation, and finds vulnerabilities that previous manual systems did not uncover. With SecurityCenter dashboards, the IT team has constant insight into potential vulnerabilities.

## Business Needs

### Manual Processes Were Time-Consuming

As the mining industry increases its dependence on networked technologies, the risk from cyberthreats grows. Peñoles' IT team is tasked with protecting the security of the mining information systems as well as computing systems supporting business operations and processes.

For many years the IT team used manual processes to find vulnerabilities in its network. Security administrators ran network scans using nmap, used the resulting information to populate a database, then ran queries to produce reports and analyze the results.

This labor-intensive system consumed more than 50 percent of a security administrator's time, and limited the amount of scans that the team could perform and analyze. As a result, the scans and reports appeared approximately once per quarter. In addition, keeping the system up-to-date with the threat environment was a constant challenge.

### The Need for Fast Threat Mitigation

The IT team at the company's main site in Plata wanted a faster, more efficient way to discover any vulnerabilities in its networks, without the 'lag time' of the current processes. They looked for a vulnerability scanning solution that could meet the following requirements:

- **Automated vulnerability scanning processes:** Peñoles needed to automate the process of running and analyzing scans so they could do them more frequently than once per quarter.
- **Up-to-date threat information:** The IT organization wanted to stay current with the threat environment, without a great deal of manual investigation.
- **Support for a heterogeneous IT environment:** The team needed a solution that would work with a wide variety of platforms and devices.

## The Tenable Solution

Peñoles turned to Tenable Nessus® and SecurityCenter™ to implement high-performance, automated scanning with flexible dashboards and analysis.

Nessus is the industry's most widely used vulnerability scanner, offering high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis. Tenable SecurityCenter adds scan automation as well as centralized reporting, analysis, and visualization for vulnerability information from throughout the network.

PEÑOLES®

## Business Needs

- Find and remediate vulnerabilities quickly to protect information systems
- Reduce the time spent running and analyzing scans
- Maintain up-to-date information about vulnerabilities and fixes

> "Previously we had a "snapshot" of our status once every three months. With SecurityCenter, we are able to obtain that snapshot on a daily basis. The dashboards help us make fast decisions about which vulnerabilities to tackle first."
>
> ***Sergio Arizpe Mora***
>
> Security Administrator, Peñoles

Using Nessus and SecurityCenter, Peñoles schedules regular, automated scans and uses SecurityCenter's flexible dashboards to analyze the results. Tenable automatically updates SecurityCenter with the latest threat and compliance information on a daily basis if needed. This means that Peñoles always has the most up-to-date threat information at hand.

## Results: Fast Time to Remediation

Rather than waiting three months for the next vulnerability snapshot, the Peñoles IT team now has continuous insight into potential vulnerabilities using SecurityCenter dashboards, which offer a variety of views appropriate for different roles. The reports also include recommended fixes and solutions for vulnerabilities. With up-to-date dashboards and recommendations, the team can find and mitigate vulnerabilities very quickly.

"Previously we had a "snapshot" of our status once every three months. With SecurityCenter, we are able to obtain that snapshot on a daily basis. The dashboards help us make fast decisions about which vulnerabilities to tackle first," said Sergio Arizpe Mora, Security Administrator at Peñoles.

Using Nessus and SecurityCenter, Peñoles discovered a vulnerability that manual processes missed, present in almost 70 servers. According to Mora, "By finding and fixing this vulnerability, we greatly reduced the potential for unauthorized access to the affected servers"

## Next Steps and Bottom Line

Peñoles now uses Tenable SecurityCenter and Nessus at its corporate headquarters as well as its main Plata site. By automating scanning and eliminating the manual processes around gathering, analyzing, and reporting on data, Peñoles has freed up administrator time for other projects, including penetration testing.

According to Mora, "Since automating the process of vulnerability administration with Tenable, we have more time to focus on other tasks such as perimeter security and new security projects."

> "Since automating the process of vulnerability administration with Tenable, we have more time to focus on other tasks such as perimeter security and new projects."
>
> ***Sergio Arizpe Mora***
>
> Security Administrator, Peñoles

### For More Information

**Questions, purchasing, or evaluation:**
sales@tenable.com or 410.872.0555, x500
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable™ network security