Oil and Gas Manufacturer Reduces Critical Vulnerabilities in Under Thirty Days

The Company

A global design, manufacturing, and service organization specializing in flow control applications for the oil and gas industry.

Their environment consists of multiple physical locations with network connected embedded devices, machinery, and technologies.

☑ ISO 9001 and API Q1 quality standards

☑ Equipment meets the requirements of the American Petroleum Institute Specification 6A and/or 16C

The Situation

Cybersecurity threats to organizations within critical infrastructure are one of the most significant strategic risks within the United States, threatening our national security, economic prosperity, and public health and safety. This manufacturing company within the oil and gas industry knew that they were a target and that they needed to establish a vulnerability management program.

With no CISO in place, the Vice President of Technology was responsible for managing the cybersecurity needs of the company. The organization had secured their cybersecurity services from a well-known managed security service provider who offered many cybersecurity solutions, but didn't make a positive difference towards the company's security. The organization was now seeking a solution that provided coverage, context, and peace-of-mind.

The goal was to find a vulnerability management solution which would reduce risk as well as support compliance and adherence to an information security program.

The Solution

In researching solutions, other solution providers required individual integration and management as well as required an extensive skillset and domain knowledge to prioritize and contextualize issues that were identified. Since there were limited security resources within the organization, it would be difficult to manage a complex security system while remediating vulnerabilities across the infrastructure. The VPT was seeking a managed solution which would help address his staffing needs. He reached out to VULNERA to learn more.

The demo helped the VPT understand how VULNERA's Continuous Assessments fit into their cybersecurity program and to determine the level of effort required from their staff. This solution offered a turnkey approach to vulnerability management, 24x7x365 coverage, and real-time analytics via the dashboard.

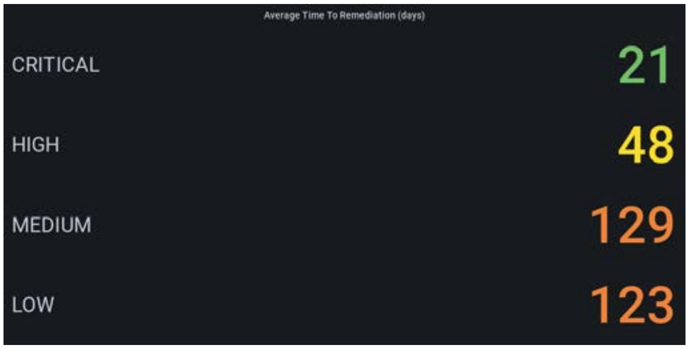
The Results

The organization immediately saw results from their selection. Within 1 month of implementation, the critical risk exposure was reduced 90% (Figure 1). This allowed them to next focus on high severity and other issues which reduced their risk exposure over time.

The first scan of the environment identified upwards of 220 critical issues (Figure 3). Within the first week, open issues were reduced to 40. Over the course of 45 days, the company was able to remediate 219 identified issues.

The real-time dashboard allows the organization to easily observe the status of open issues as well as those items which have been remediated. The robust reporting provides them with data and graphs needed to support their KPIs which are reported to the board.

> **In just two short months, we have decreased our overall security vulnerability score by over 60 percent. Just our critical score alone has decreased by over 82 percent.**
>
> CISO
> Oil and Gas Manufacturer



Average Time To Remediation (days)

CRITICAL	21
HIGH	48
MEDIUM	129
LOW	123

Figure 1: *Average Time to Remediate Issues by Severity (days)*

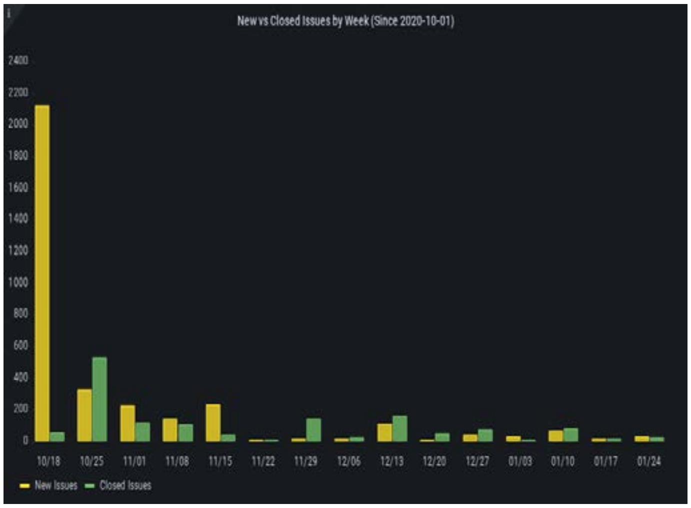


Figure 2: *Open vs. Closed Issues by Week*

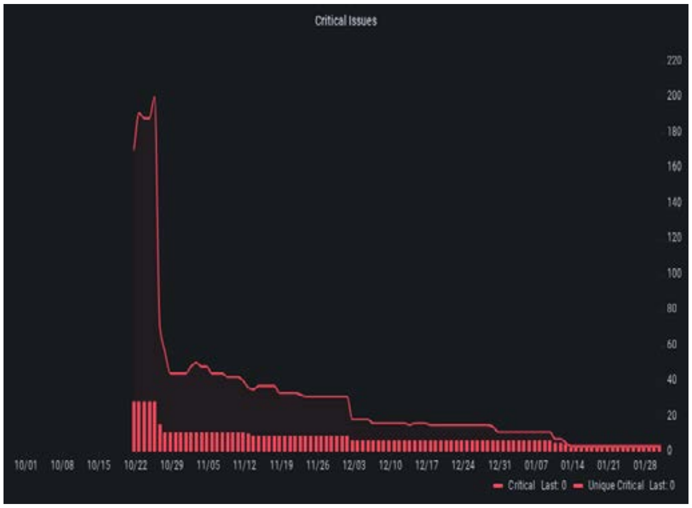


Figure 3: *Number of Open Critical Issues*

+1 626.515.5523
www.vulnera.com | info@vulnera.com