Customer Case Study: Oil Company Strengthens Cyber Resilience

Industry: Oil & Gas

Engagement Type: Vulnerability Management On Prem Tool Health Check

Delivery Format: Remote

Engagement Duration: 2 days

Client Overview

Oil Company is one of North Americas' leading oil infrastructure and logistics companies, responsible for managing critical Oil assets across the country. With significant exposure across operational technology (OT) environments and IT infrastructure, the company relies on its Vulnerability Management On Prem tool to provide continuous visibility into cyber risk and vulnerabilities.

To ensure the tool's deployment continued to meet performance, visibility, and governance expectations, Oil Company engaged our team for a strategic Health Check. This service was designed to validate the platform's configuration, identify inefficiencies, and prepare the environment for scalability and future security initiatives.

Engagement Objectives

- Assess the current configuration, health, and scalability of Oil Company's Vulnerability Management On Prem tool instance and its connected components.
- Identify gaps in scan performance, asset coverage, user access, tagging, and reporting workflows.
- Provide best-practice guidance to optimize scan policies, asset management, and role-based access controls (RBAC).
- Deliver a prioritized roadmap of improvements with quick wins and long-term strategies to improve vulnerability lifecycle management.
- Ensure platform readiness for future upgrades, including migration to Oracle Linux 8.

Strategic Priorities

- **Optimize Scanner Deployment Across Segmented Environments:** Oil Company operates a hybrid infrastructure aligned to the Purdue Model, with defined OT (Level 3) and IT (Level 4)

zones. Ensuring optimal scanner placement, scan zones, and policy segmentation was crucial to reduce scan conflicts and enhance performance.

- **Platform Modernization:** The existing deployment included legacy CentOS-based appliances. The team wanted strategic guidance to migrate to Oracle Linux 8, align resources with modern architecture, and expand data retention for trend analysis.
- **Credentialed Scanning & Compliance Readiness:** While several scan types were in use, there was limited credential validation and no compliance scanning. Oil Company needed advice on audit file usage, asset-targeted compliance templates, and credential configuration.
- **Governance, Access, and Operational Clarity:** The environment had accumulated numerous users, asset lists, and scan policies—many of which were outdated or unused. Streamlining this complexity was key to strengthening governance and ensuring sustainable operations.
- **Visibility and Reporting Optimization:** With limited use of dashboards, saved queries, and asset tagging logic, Oil Company's teams were struggling to derive actionable insights from Security Center's data. Enhancing these outputs was a major objective for the InfoSec team.

Approach

The engagement was delivered via Zoom across two days, following a standard methodology adapted to Oil Company's operational realities:

1. Installation and Licensing Review

- Validated the active license capacity: 3000 IPs licensed for Vulnerability Management On Prem tool and 1000 for Operational Technology Security tool.
- Reviewed current scan volume (~2358 active IPs), system storage, and license utilization.
- Identified the need to expand disk storage for improved retention and trending as the platform scales.

2. Version Control and Component Audit

- Assessed the versioning of all deployed scanners and the Vulnerability Management On Prem tool core platform.
- Noted one scanner in the Operational Technology zone was outdated and assisted with a live upgrade to v10.8.3 on Oracle Linux 8.
- Recommended full migration to Vulnerability Management On Prem tool Core for all appliances to benefit from automated OS and app updates.

3. Operational Configuration and Governance

- Reviewed scan zone configuration and identified unnecessary overlap. Recommended removing obsolete zones such as "Host Discovery."
- Analyzed repository utilization: 7 repositories were active, but several were unused. Suggested consolidation with refined IP scope management.
- Detected use of an all-inclusive asset list (0.0.0.0/0), which risked poor targeting. Advised segmentation and targeted list creation instead.

4. Access Control and User Management

- Audited 19 organizational users, with many dormant or assigned inappropriate roles.
- Flagged legacy service accounts with elevated permissions that had never logged in.
- Recommended deleting or disabling inactive accounts and aligning roles with functional responsibilities using Security Center's RBAC model.

5. Scan Policy and Credential Review

- Evaluated existing scan policies. Found policies with default concurrency limits (30 hosts per scan) that could be increased to improve scan efficiency.
- Identified 30+ stored credentials—many of which were unused or misconfigured. Provided a framework for credential testing and validation tied to specific asset lists.
- Oil Company was not yet running compliance scans; we introduced audit file configuration and asset-aligned policy building as a future step.

6. Asset Management and Tagging

- Observed that of 143 asset lists, 43 contained zero hosts, creating unnecessary clutter.
- Recommended purging unused lists and implementing dynamic asset lists based on OS, location, and scan result metadata.
- Emphasized tagging as a key strategy for targeting scans and simplifying dashboards.

7. Reporting and Dashboard Enhancement

- Found underutilization of dashboards and saved queries.
- Introduced the team to pre-built dashboards such as Worst of the Worst, CISA KEV, and CMMC views.
- Demonstrated the use of saved queries using VPR, CVSSv3, plugin families, and patch availability filters.

- Guided creation of custom reports aligned with stakeholder needs (e.g., management summary vs. technical remediation plans).

Results & Impact

- **Streamlined Platform Footprint:** Cleanup recommendations for users, scan zones, asset lists, and credentials simplified the operating environment and reduced administrative overhead.
- **Improved Scan Performance:** Adjusted concurrency settings and clarified scan scopes to reduce unnecessary load and improve scan times.
- **Operational Governance Strengthened:** RBAC realignment, credential scoping, and group-based access enhanced visibility and accountability across teams.
- **Enhanced Reporting Readiness:** Dashboards and saved queries now better support Oil Company's risk management, vulnerability triage, and stakeholder reporting.
- **Migration Path Identified:** A clear plan was delivered to upgrade to Oracle Linux 8, modernize the appliance architecture, and scale trend data collection.

Customer Feedback

"This health check gave us clarity and helped us refocus on what matters in our scanning and reporting. It's the kind of reset we needed before taking the next step in our maturity."
— **Security Operations Lead**, Oil Company