Customer Case Study: Energy Company Strengthens Vulnerability Management

Industry: Energy

Engagement Type: Vulnerability Management Tool Health Check

Delivery Format: Remote (Zoom)

Engagement Duration: 2 days

Client Overview

Energy Company, a global technology leader in sustainable energy infrastructure, maintains a vast hybrid IT environment encompassing cloud workloads in Azure and traditional on-premise networks. With a mature deployment supporting tens of thousands of assets and a history of proactive security practices, Energy Company engaged our team to conduct a comprehensive Vulnerability Management Tool Health Check. The goal was to validate their platform architecture, resolve emerging issues, and ensure continued alignment with operational and compliance priorities.

Engagement Objectives

- Assess the architecture and configuration of the Vulnerability Management Tool and related scanning components.
- Review and optimize scan strategy, including sensor placement, scan scheduling, credentialed scan success, and template design.
- Evaluate asset management and tagging practices to improve clarity, reduce duplication, and support compliance use cases.
- Review role-based access controls (RBAC) and governance configurations to ensure secure and scalable operational ownership.
- Deliver prioritized recommendations to guide future improvements and platform sustainability.

Strategic Priorities

- **Consolidate Hybrid Infrastructure Visibility:** The Vulnerability Management Tool was deployed in both Azure and on-prem environments, but conflicting network assignments and connector behaviors had begun to create asset duplication, especially around Azure's Connector and scanner group settings.

- **Enhance Scan Performance and Cadence:** With 16 Nessus scanners supporting over 82,000 assets across multiple zones, the organization sought recommendations to optimize plugin use, schedule frequency, and policy reuse across both discovery and credentialed scans.
- **Credentialed Scan Tuning and Coverage Expansion:** While the team had already implemented authenticated scanning across Windows and Linux, they needed help improving scan consistency, failure handling, and audit trail reliability.
- **RBAC & Access Governance Reinforcement:** User groups and role mappings were in place, but a secondary review was requested to validate user permissions and identify opportunities to enhance delegation for regional or zone-based administration.
- **Streamline Reporting and Compliance Workflows:** The customer had invested in detailed tagging hierarchies and was exporting reports in JSON and CSV formats but wanted to better align dashboards with business risk and compliance KPIs, and integrate with Power BI.

Approach

Our consultants followed a structured Health Check methodology, tailored to Energy Company's mature deployment and specific goals:

1. Planning and Discovery

- Worked with platform owners and key stakeholders to:
    - Identify immediate pain points (e.g., asset duplication, scan delays, recast rule conflicts)
    - Review platform topology, scanner layout, and current tagging/segmentation models
    - Align on success criteria and prioritize short-term wins vs. long-term strategy

2. Assessment and Review

- **Scan Engine & Network Architecture:** Evaluated the configuration of 16 deployed Nessus scanners across cloud and on-prem zones. Reviewed high-volume discovery scans (covering ~1.8 million IPs) and assessed scanner group behavior, IP segmentation, and scan distribution.
- **Connector Analysis:** Found Azure Connector was generating asset duplication due to overlapping default and custom scan networks. Explored three resolution paths: isolating connector-managed agents, restructuring scan networks, or consolidating scan targets under a unified default network.
- **Scan Policy Tuning:** Reviewed discovery, credentialed, and compliance scans. Provided tuning recommendations, including:
    - ICMP-only for basic discovery scans with host type exclusion toggles
    - Credential reuse guidance and scan separation by asset type

- Decoupling compliance scans from vulnerability scans to support policy flexibility

- **RBAC and Access Groups:** Confirmed current use of Administrator, Scan Operator, Standard, and Web App Reader roles. Suggested refinements in how access groups and user roles were mapped to geography, site, and business unit to enhance decentralized management.
- **Tagging Framework Review:** Validated robust use of API-based tagging and Azure subscription-derived dynamic tags. Assessed effectiveness in reporting, dashboard filtering, and scan targeting. Discussed tag consolidation for improved dashboard performance.
- **Reporting and Dashboarding:** Reviewed existing report exports (CSV/JSON) and demonstrated native TVM dashboards with filter options aligned to KPIs. Outlined next steps for integrating Vulnerability Management Tool data with Power BI using APIs and scripts to centralize reporting.

Results & Impact

- **Clarity Around Architecture and Network Behavior:** The engagement helped the customer understand how connector configuration and scanner network assignments can impact asset duplication and scan targeting. They now have a path forward to address duplication without disrupting scan coverage.
- **Improved Scan Efficiency:** Policy tuning guidance led to better separation of compliance and vulnerability scanning, improved resource usage, and more accurate scan duration expectations.
- **Credentialed Coverage Optimization:** Recommendations around policy design, credential handling, and error recovery improved the reliability and audit traceability of Windows and Linux credentialed scans.
- **Stronger Governance and Ownership:** The RBAC and access group reviews gave the customer confidence in their current model and surfaced new ideas for regional access delegation and role refinement.
- **Enhanced Reporting Strategy:** The team received practical steps to align scan outputs with compliance KPIs and executive metrics, and to streamline reporting through API integrations and dashboard use.

Customer Feedback

“The Health Check was invaluable. It brought both strategic insights and technical depth that we can apply right away—and gave us a roadmap to scale vulnerability management intelligently.”
— **Security Program Lead**, Energy Company