Enhancing Asset Visibility & Compliance in Tenable

As part of my role, I spearheaded an initiative to identify, track, and optimize asset visibility within our vulnerability management platform, Tenable. This project aimed to ensure accurate asset monitoring and classification, improve monitoring capabilities, and enhance security compliance across various teams.

Phase 0: Planning & Coordination

- Collaborated with Network Services, Windows, and Application teams to gain a comprehensive understanding of asset ownership and distribution.
- Established a strategy to systematically track assets across multiple platforms while ensuring proper tagging and integration into Tenable dashboards.

Phase 1: Data Collection & Integration

- Aggregated asset inventories from multiple stakeholders, including Network Services, Windows and Application teams.
- Integrated assets into Tenable, ensuring they were correctly categorized, tagged, and integrated into operational dashboards. This process involved close collaboration with the Security Operations Center (SOC) to determine what was already being tracked.
- Designed and optimized security dashboards to provide actionable insights by displaying:
    - Vulnerability counts categorized by severity.
    - Compliance status (pass, fail, and warning metrics).
    - Most affected systems, enabling prioritization of remediation efforts.
    - Most common vulnerabilities, allowing for targeted security improvements.
- Collected and consolidated asset lists from Active Directory, Microsoft Intune, Tenable Vulnerability Management, Zscaler, SolarWinds, and Crowdstrike.
-

Phase 2: Automation & Data Processing

- Developed Python scripts utilizing the pyTenable API and Pandas to programmatically extract, cross-reference, and validate asset data from Tenable, Zscaler, SolarWinds, Active Directory, and Crowdstrike.
- Conducted data correlation across various security platforms to identify discrepancies, missing assets, and gaps in monitoring.

Phase 3: Validation & Compliance

- Conducted root cause analysis on untracked assets, identifying the reasons behind discrepancies.
- Verified asset visibility using:
    - Crowdstrike to determine whether Nessus Agents were properly installed on Windows assets.
    - SolarWinds to validate IP address integrity and scanning accuracy for network devices.
- Identified asset owners and assigned ServiceNow tickets to ensure proper remediation and accountability.

Key Accomplishments & Impact

- Successfully identified and remediated tracking gaps for 30 previously unmonitored assets
- Enhanced security compliance by ensuring all assets were properly scanned and categorized.

This initiative improved our organization's asset visibility, ensuring that Tenable accurately reflects our infrastructure while enhancing security monitoring and compliance efforts.