PCI SSC Community Meeting Workshop Summary

Vulnerability Management and Penetration Testing Best Practices

Workshop Objective: Support peer learning through sharing of key practices in vulnerability management and penetration testing.

Workshop Discussion Questions
How would you describe your organization’s current vulnerability mgt and pen testing maturity?
Which processes/tools are most effective at identifying, prioritizing and remediating vulnerabilities?
What are the biggest gaps or difficulties you face? (e.g., authenticated scans, tracking acceptable risks, remediation prioritization, etc.)
What recent changes in requirements or your business practices have had the biggest impact?
Looking ahead, what would a mature, effective vulnerability mgmt. and pen testing program look like in your organization and what collaboration would you like to see from the industry?

Industry Insights:

- ➕ Automation is increasingly being adopted (asset identification, ticketing, etc.); but manual review and human verification remain essential.
- ➕ There is a shift from annual assessment-driven activities to integrating security into business-as-usual processes.
- ➕ Partnerships with third party vendors for penetration testing are common and necessary.
- ➕ Executive sponsorship and leadership buy-in are critical for program success.
- ➖ Authenticated scans are a significant challenge, especially for legacy systems and credential management.
- ➖ Cloud and containerized environments may introduce new complexities in scope and responsibility.
- ➖ False positives and manual review of findings can result in increased overhead costs, especially in response to enhanced automation.
- ➖ With the increased number of vulnerabilities being detected, remediation prioritization and tracking are becoming more complex to manage.

Ongoing Industry Opportunities
Facilitated peer discussions and workshops for information sharing are considered high-value.
Industry interest in more practical implementation guidance for penetration testing in cloud environments.
Need for continued pen testing and vulnerability management process education.