APPLICATION SECURITY PROGRAM CHECKLIST

AN APPLICATION SECURITY MANAGER'S STEP-BY-STEP REFERENCE TO IMPLEMENTING AN ADVANCED APPLICATION SECURITY PROGRAM

Phase 1: Pilot Program

- ☐ Conduct maturity assessments
  - ☐ Leverage the OpenSAMM framework
  - ☐ Identify most critical gaps in application security efforts
- ☐ Discover your web perimeter: Use a discovery solution to identify all public-facing applications
  - ☐ Patch vulnerable sites
  - ☐ Eliminate unnecessary or unused sites
- ☐ Assess most critical vulnerabilities: Identify your organization's 5 to 20 most business-critical applications
  - ☐ Evaluate and partner with automated application security solution
  - ☐ Scan for critical code-level vulnerabilities and fix
- ☐ Create report to demonstrate success and suggest next steps
  - ☐ Present to C-Level to win program expansion support

Phase 2: Set Program Policies and Metrics

- ☐ Identify external compliance drivers
  - ☐ Determine internal success metrics
  - ☐ Leverage the OWASP Top 10

Phase 3: Scale Program to Legacy Applications and SDLC

- ☐ Leverage automated code scanning technology to scale application coverage
  - ☐ Prioritize by flaw severity
- ☐ Meet with development team, address concerns and gain buy-in
- ☐ Identify opportunities for automation and streamlining processes
- ☐ Leverage APIs to enable seamless testing in development process

Phase 4: Create a Strategy for Third-Party Applications and Components

- ☐ Create an inventory of software component usage
  - ☐ Compare inventory to the National Vulnerability Database
- ☐ Create third-party software assessment policy
  - ☐ Strive to match in-house standards
  - ☐ Receive feedback from legal and procurement teams

Do you know how many web applications your organization has?

Get an estimate of your web application perimeter

For information on how to talk to the board, watch:

A CISO's Perspective on Talking to the Board About Cybersecurity

- ☐ Work with vendors to ensure compliance with policies

- ☐ Identify groups in the organization that purchase the most technology
  - ☐ Educate and enable internal purchasers on software attestation steps

- ☐ Reach out to existing providers about attestation

Be Ready to Answer These Questions

Any successful application security program requires collaboration with various departments of an organization. Be ahead of the curve by knowing the answer to these questions before meeting with each respective group.

C-Suite

- ☐ What does our risk posture look like now?
- ☐ Why should we invest in application security as opposed to other forms of cybersecurity?
- ☐ What metrics will you use to demonstrate progress?

Development Teams and DevOps

- ☐ How will the assessment process fit into the current development lifecycle?
- ☐ How will this impact the development teams' productivity?
- ☐ What training programs will be put in place to help the development team?

Software Purchasers

- ☐ Why are we assessing the security of the software we are buying?
- ☐ From whom should I get approval for software purchases?
- ☐ What is the process for purchasing software?
- ☐ What about software we already purchased?

For more information on creating an application security program, read the:

Ultimate Guide to Getting Started with Application Security