GETTING STARTED ON YOUR APPLICATION SECURITY PROGRAM

NABIL HANNAN

July 2020

NETSPI™

COMMON MYTHS AROUND APPLICATION SECURITY PROGRAMS

In order for an organization to have a successful Application Security Program, there needs to be a centralized governing Application Security team that's responsible for Application Security efforts. In practice, we hear many reasons why organizations struggle with application security, and here are four of the most common myths that need to be dispelled:

1

An Application Security Team is Optional

Just like everything else, there needs to be dedicated effort and responsibility assigned for Application Security in order for an Application Security Program to be successful. Based on our experience and evidence of successful Application Security Programs, all of them have a dedicated Application Security team focused on managing Application Security efforts based on the organization's business needs.

2

My Organization is Too Small to Have an Application Security Team

A small organization is no excuse to avoid doing Application Security activities. Application security cannot be an after-thought or something that's bolted on when needed. It needs to be an inherent property of your software and having focus and responsibility for Application Security in the organization will help prevent and remediate security vulnerabilities.

3

I Cannot Have an Application Security Team Because We Are a DevOps/Agile/Special Snowflake Shop

Just because your business or your development processes are different from others, doesn't mean that you don't have a need for Application Security, nor does it mean that you cannot adopt certain application security practices. There are many opportunities in any type of an SDLC to inject application security touchpoints to ensure that business objectives or development efforts are not hindered by security, but rather are enhanced by security practices.

4

An Application Security Team Will Hinder Our Ability to Deliver/Conduct Business

In our experience, we have seen that more secure applications are typically better in all perspectives – performance, quality, scalability, etc. Application Security activities, if adopted correctly will not hinder your organization or team's ability to conduct business but will in fact provide a competitive advantage within your business vertical.

WHY DO YOU NEED AN APPLICATION SECURITY PROGRAM?

Defect Discovery

Organizations typically start their application security journey in defect discovery efforts. The two most common discovery techniques used are Penetration Testing and Secure Code Review to get started discovering security vulnerabilities and remediating them appropriately.

Defect Prevention

An Application Security Program's goal is not only to help proactively identify and remediate security issues, but also to avoid security issues from being introduced.

Understanding Risk

In order to identify an organization's risk posture, it's necessary to identify what defects exist, and then determine the likelihood of these defects being exploited and the resulting business impact from successful exploitation. Organizations need to understand how the defects identified actually work and determine what components of the organization and business are affected by the identified defects.

GETTING STARTED WITH DEFECT DISCOVERY

There are many different techniques of defect discovery, and each has its own set of strengths, weaknesses, and limitations in what they can identify. Certain techniques are also prone to higher levels of false positives than others. There's also factors such as speed at which these techniques can be implemented and how quickly results can be made available to the appropriate stakeholders which need to be considered when implementing a particular defect discovery technique in an organization. Ultimately, all of the techniques do have certain areas of overlap in terms of the types of defects that they can identify, and all the techniques do complement each other.

1. Penetration Testing
2. Secure Code Review

DISCOVERY TECHNIQUE #1
PENETRATION TESTING

Penetration Testing is the most popular defect discovery technique used by organizations and is a great way to get started if you have had no focus towards Application Security in the past. Pentesting allows an organization to get a baseline of the types of vulnerabilities that their applications are most likely to contain. There's a plethora of published materials on known attacks that work and it's easy to determine what to try. When performing penetration testing, the type of testing varies significantly based on the attributes of the system being tested (web application, thick client, mobile application, embedded application, etc.).

EXECUTION METHODS	
Technology/Tool Driven	• Multiple commercial and open source tools available • DAST tools are widely available while IAST tools are maturing and gaining adoption • Cost, tool capability, customizability, deployment options, features, etc. are factors to consider
Outsourced Manual Penetration Testing (Third-Party Vendor)	• Many options available • NetSPI provides a wide range of Penetration Testing services at varying levels of depth • Available on-demand and easy to scale • Driving factors to consider – cost, scalability, quality, scheduling logistics, trust, delivery model maturity, etc.
In-House Manual Penetration Testing	• Hard to find good talent • Harder to retain good talent long-term • Impossible to scale

DISCOVERY TECHNIQUE #2
SECURE CODE REVIEW

Secure Code Review is often mistaken for Code Review that development teams typically do in a peer review process. Secure Code Review is an activity where source code is reviewed in an effort to identify security defects that may be exploitable. There are plenty of checklists on common patterns to look for or certain coding practices to avoid (hard-coded passwords, usage of dangerous APIs, buffer overflow, etc.). There are also various development frameworks that publish secure coding guidelines that are readily available. Some organizations with more mature Secure Code Review practices have implemented secure by design frameworks or adopted hardened libraries to ensure that their developers are able to avoid common security defects by enforcing the usage of the organization's pre-approved frameworks and libraries in their development efforts.

EXECUTION METHODS	
Technology/Tool Driven	• Multiple commercial and open source SAST tools available • Cost, tool capability, customizability, false positive rates, deployment options, features, etc. are factors to consider • Triaging scan results can be costly and time consuming given the nature of SAST scanning and the high false positive rates
Outsourced Manual Secure Code Review (Third-Party Vendor)	• Many options available • NetSPI provides a wide range of Secure Code Review services at varying levels of depth • Available on-demand and easy to scale • Driving factors to consider – cost, scalability, quality, scheduling logistics, trust, delivery model maturity, etc.
In-House Manual Secure Code Review	• Hard to find good talent • Harder to retain good talent long term • Impossible to scale • Inconsistent results – even if it's the same person on a different day • Checklists help, but results vary significantly based on the reviewer's capabilities

DEFECT DISCOVERY IS JUST THE BEGINNING

It's important to remember that defect discovery is more than just the two techniques discussed here. In the scheme of your Application Security Program, the effort towards defect discovery is just a part of your application security program. In addition to defect discovery, you need to consider the following (and much more):

- What does it mean for your organization to have a Secure SDLC from a governance perspective?
- How are you going to create awareness and outreach for your SDLC to ensure the appropriate stakeholders know what their roles and responsibilities are towards application security?
- What key processes and technology do you need to put in place to ensure everyone is capable of performing the application security activity that they're responsible for?
- How are you going to manage software that's developed (and/or managed) by a third party (augmenting vendor management to reduce risk)?

APPLICATION SECURITY GOVERNANCE AND STRATEGY

Application security governance is a blueprint that is comprised of standards and policies layered on processes that an organization can leverage in their decision-making processes in their application security journey.

Organizations have started adopting a Secure SDLC (S-SDLC) process as part of their software development efforts, and this tends to vary greatly between organizations. Ultimately, the focus of the S-SDLC is to ensure that vulnerabilities are detected and remediated (or prevented) as early as possible.

Many organizations unfortunately have not defined their application security governance model, and as a result, lack a proper S-SDLC. Without the proper processes in place, it's challenging, if not impossible to have oversight of the application security risks posed to all the applications in an organization's application inventory.

Ultimately, we've observed that regardless of where the governance function is implemented (software engineering, centralized application security team, or somewhere else), there needs to be dedicated focus on application security to get started on the journey to reducing risk faced from an application security perspective.

THE TRIFECTA OF PEOPLE, PROCESS, AND TECHNOLOGY

1 Application Security Team (People)

Organizations need to assign responsibility for application security. In order to do this, it's important to establish an application security team that is a dedicated group of people who are focused on making constant improvements to an organization's overall application security posture and as a result, protect against any potential attacks. Organizations that have a dedicated application security team are known to have a better application security posture overall.

2 Secure SDLC/ Governance (Process)

Clear definition of standards, policies, and business processes are key to having a successful application security strategy. The S-SDLC ensures that applications aren't created with vulnerabilities or risk areas that are unacceptable to the organization's business objectives.

3 Application Security Tools and Technology

There's a plethora of open source and commercial technologies available today that all leverage different defect discovery techniques to identify vulnerabilities in applications. DAST, SAST, IAST, SCA, and RASP are some of the more common types of technologies available today. Based on the business goals, objectives, and the software development culture, the appropriate tool (or combination of tools) needs to be implemented to automate and expedite detection of vulnerabilities as accurately and early as possible in the SDLC.

TAKING A STRATEGIC APPROACH TO APPLICATION SECURITY

In order to grow and improve, organizations need to have an objective way to measure their current state, and then work on defining a path forward. Leveraging the appropriate application security framework to benchmark the current state of the application security program allows organizations to use real data and drive their application security efforts more strategically towards realistic application security goals.

Standard frameworks also allow for re-measurements over time to objectively measure progress of the application security program and determine how effective the time, effort, and budget being put towards the application security program are.

As the application security capabilities mature, so does the amount and quality of data that is at the organization's disposal. It's important to ensure that the data collection is automated and proper application security metrics are captured to determine the effectiveness of different application security efforts, and also measure progress while being able to intelligently answer the appropriate questions from executive leadership and board members.

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest health care companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.
Follow us on LinkedIn, Twitter, and Facebook.

NETSPI'S STRATEGIC ADVISORY SERVICES

NetSPI offers a range of Strategic Advisory Services to help organizations in their application security journey.

Regardless of where you are in your application security goals and aspirations, NetSPI provides:

- **Application Security Benchmarking** – Measure the current state of your application security program and understand how your organization compares to other similar organizations within the same business vertical.
- **Application Security Roadmap** – Understand the organization's application security goals and build a realistic roadmap with key timely milestones.
- **Application Security Metrics** – Based on the organization's application security program, understand what data is available for collection and automation, allowing for definition of metrics that allow the application security team to answer the appropriate questions to help drive their application security efforts.