TENTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

THE RIPPLE EFFECT

The Cascading Impacts of Cyber Security

OCTOBER 26–28, 2020

cybersecuritysummit.org

10 YEAR ANNIVERSARY

NETSPI™

Getting Started on Application Security

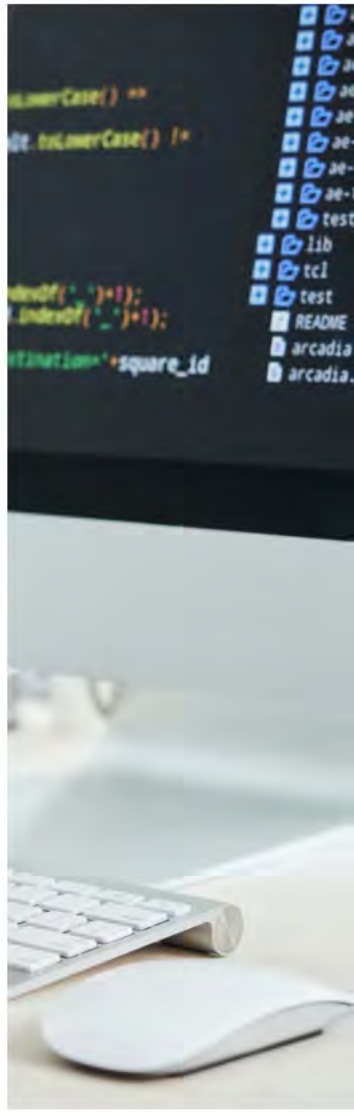
Nabil Hannan / Managing Director / NetSPI

Application Security is a Key Component of Your Cyber Security Strategy

COMMON MYTHS AROUND APPLICATION SECURITY PROGRAMS

MYTH #1:
An Application Security Team is Optional

- Someone has to “own” responsibility for Application Security
- You don’t need a big Application Security team to have an impact
- Consider building a Security Champions program



MYTH #2:

My Organization is Too Small to Have an Application Security Team

- You're never too small
- Start by defining governance and processes
- Plan on how to implement a Secure-SDLC

MYTH #3:

We Love DevOps/Agile so We Cannot Have an Application Security Team

- DevSecOps is the cool new kid on the block
- Identify opportunities to introduce security touchpoints throughout development processes
- Integrate tooling and automation into CI/CD workflows

MYTH #4:

Application Security Team Will Slow Us Down

- Application Security needs to be an inherent property of software
- Security should be an “ility”, like reliability, scalability, availability, etc.
- Build a culture of security

Defining a Secure SDLC

PLAN

Governance and Compliance Pressures | Security Requirements
AppSec Benchmarking | Roadmap | AppSec Metrics

DESIGN

Mis-use & Abuse Cases | Security Requirements
Secure Design Review | Threat Modeling

CODE

SAST | SCR | IAST | SCA

TEST

Manual Pentesting | DAST | IAST | SCA
Risk-Based Security Testing | Mis-use & Abuse Cases

DEPLOY

Security Operations | Manual Pentesting | Continuous Scanning
RASP | Red Teaming | SCA

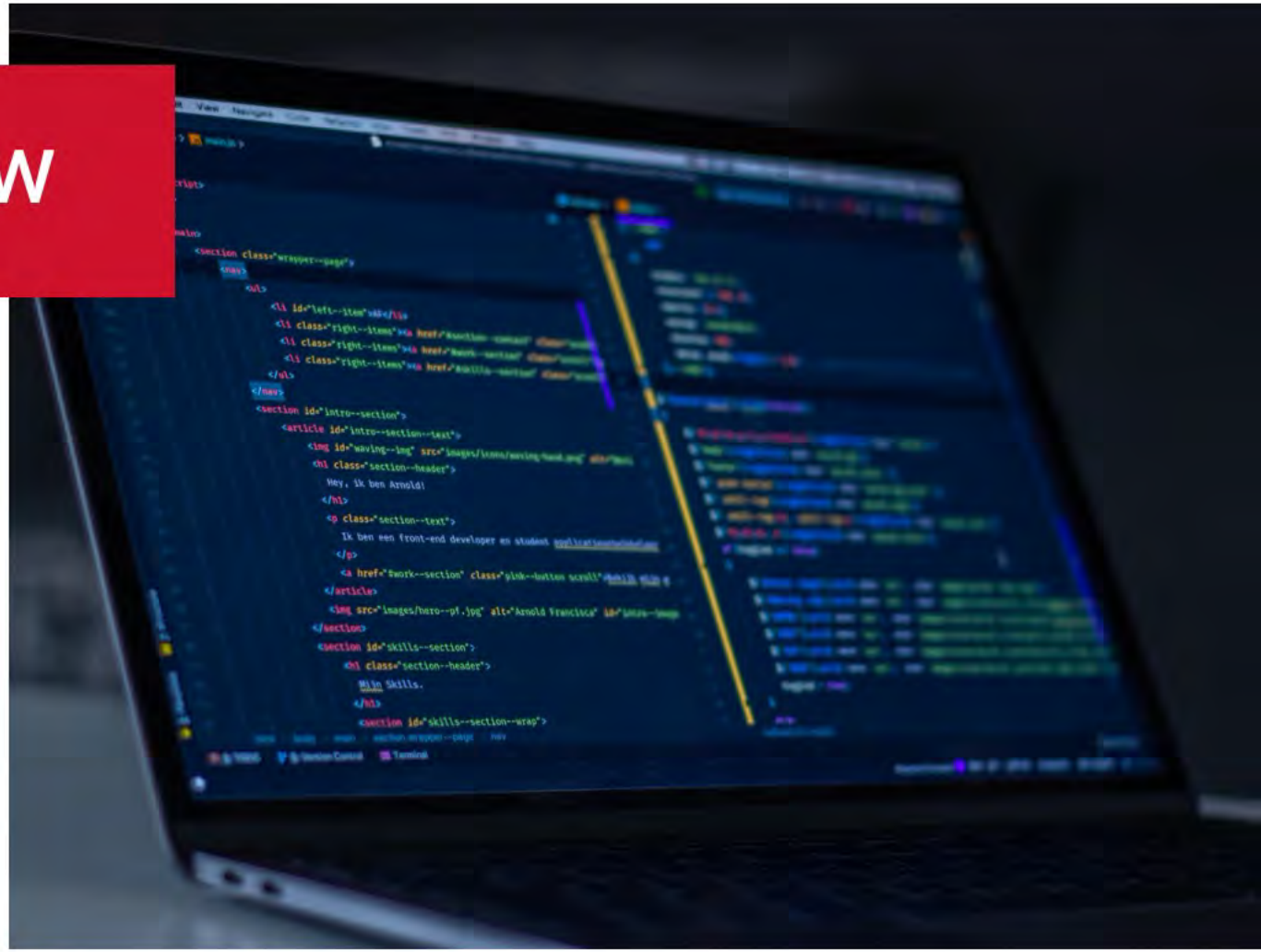
POPULAR APPLICATION SECURITY ACTIVITIES

S-SDLC Governance Definition

- Consider incorporating security gates
- Gather evidence of security activities and results with automation
- Communicate security activities with development organization

Secure Design Review

- Incorporate review focused on security as part of the design phase
- Consider building “secure-by-design” frameworks/library to be used consistently
- Identify opportunities to create re-usable security features



Penetration Testing

- Use experts / vendors to perform regular penetration testing
- Leverage penetration testing to identify effectiveness of S-SDLC

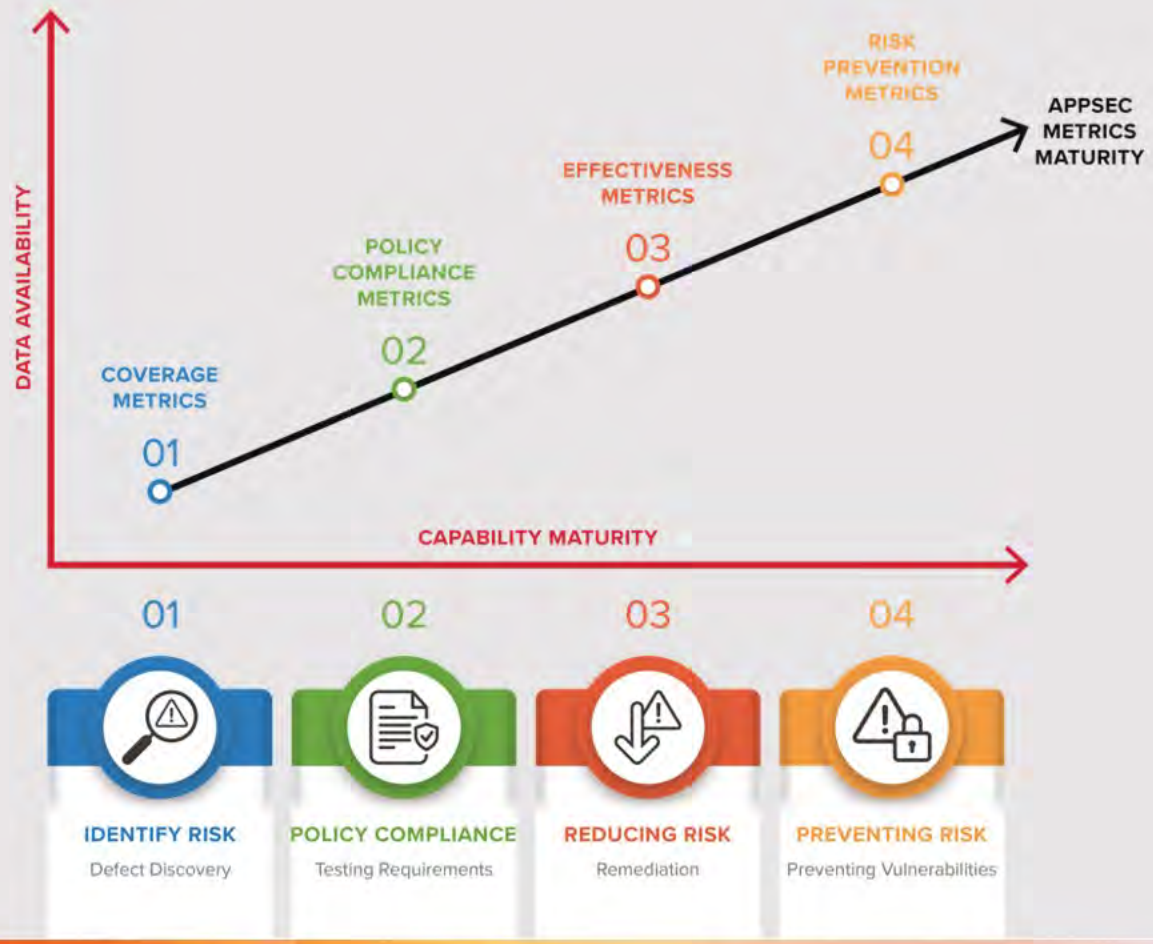
Security Testing as Part of QA

- Formalizing edge/boundary test case creation is a good start
- Determine where basic security tests can be automated as part of QA testing
- IAST is gaining popularity as part of the testing phase

Create a Threat and Vulnerability Management Process

- Build a centralized system to manage vulnerabilities
- Develop KPIs and KRIs based on business risk
- Measure efficacy of Application Security Program over time
- Create mature security metrics over time as your AppSec program matures

HOW MATURE ARE YOUR PROGRAM'S CAPABILITIES?

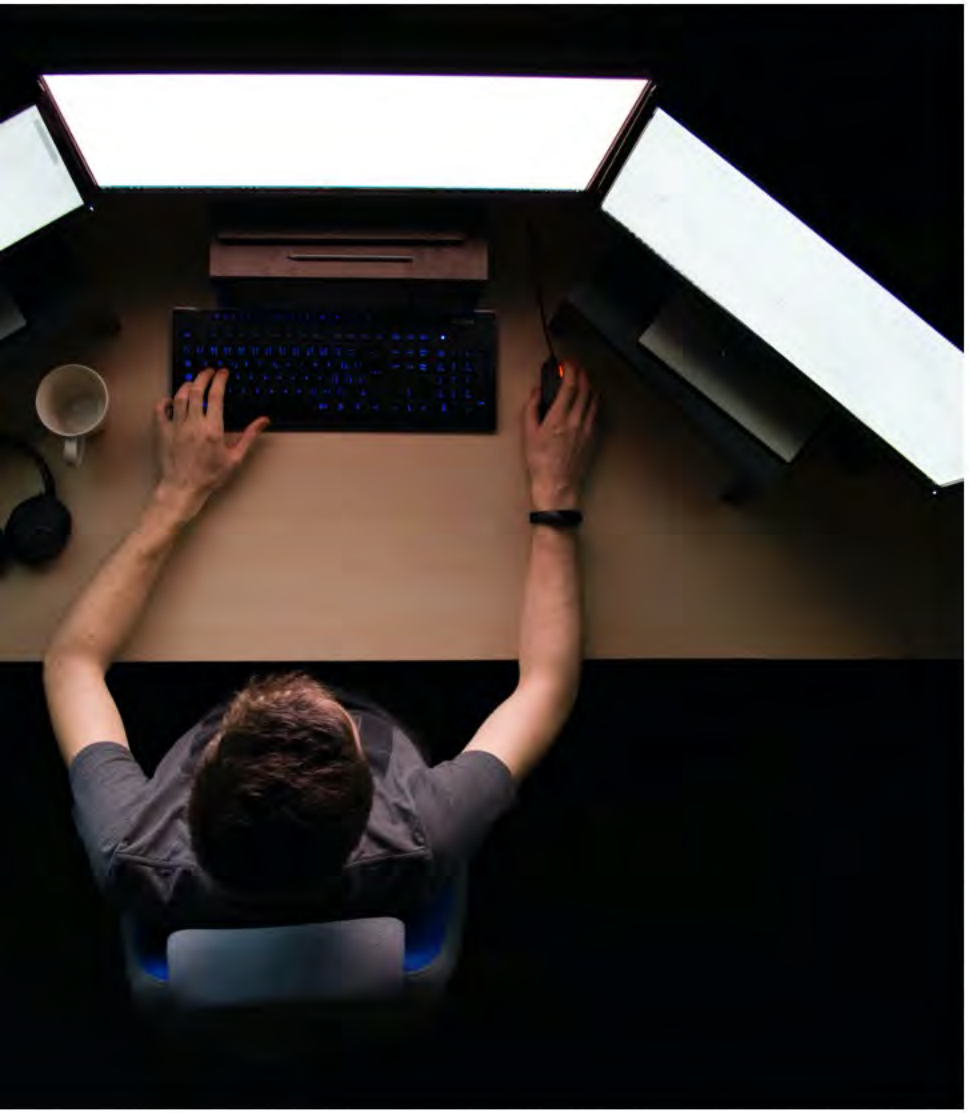


Develop Application Security Standards

- Build standards based on security policies that apply to your business
- Communicate and enforce standards through automation (SAST/DAST)

Use Security Tools as Part of SDLC

1. SAST
2. DAST
3. IAST
4. RASP
5. SCA



Identify and Inventory Open Source Risk

- Identify open source usage
- Track known vulnerabilities
- Identify license compliance conflicts

NETSPI™

Thank You!

QUESTIONS?

Website: www.netspi.com

Blog: blog.netspi.com

Executive Blog: www.netspi.com/executive-blog

Tools: www.netspi.com/research/netspi-open-source-tools

Podcast: www.netspi.com/agentofinfluence

Email: nabil.hannan@netspi.com