RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: ASEC-T07

EFFICACY OF LAYERED APPLICATION SECURITY THROUGH THE LENS OF HACKER

Gyan Prakash

Chief Security Architect
VISA Inc.

Bill Yue Chen

Chief Security Architect
VISA Inc.

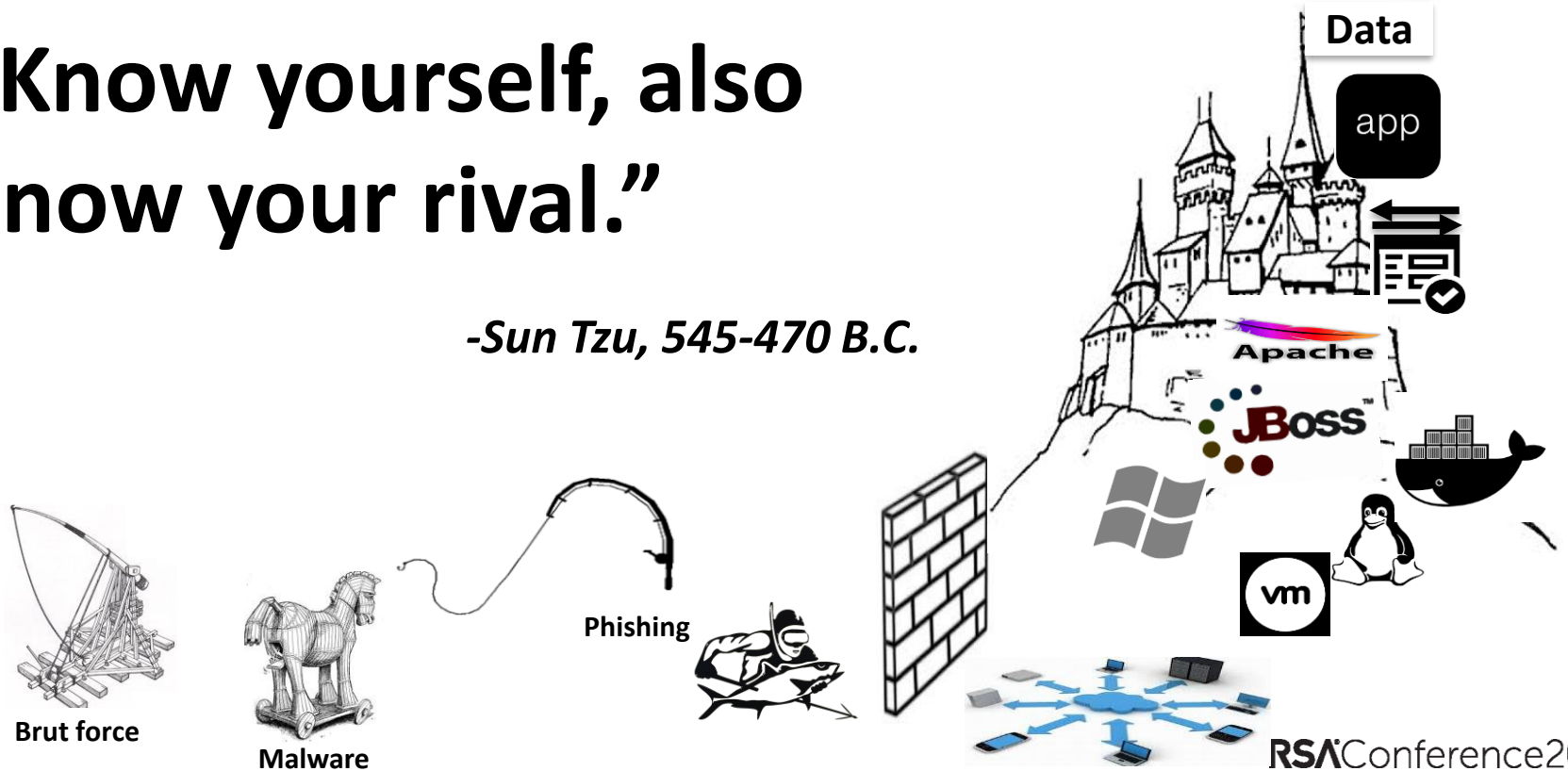
Agenda

- Threat Model
- Observations
- Optimizing App Security Life-Cycle Controls
- Agility with Security
- What Pen Test Should Focus on
- Recommendations

A Tight Race

“Know yourself, also know your rival.”

-Sun Tzu, 545-470 B.C.



Threat Model Over The Kill Chain

Scans, DNS, Asset discovery, Social Eng., etc.

Malware, Open Source Poisoning, Faked Web, etc.

Passive Traps & Proactive Attacks

Network, Infra, OWASP Vuln IAM Issues, etc.

Camouflaged Actions, APT, Outbound control exploit

Recon. → **Weaponizing** → **Delivery** → **Exploit** → **Installation** → **C & C** → **Act. & Obj.**

ML Assisted Social Engineering

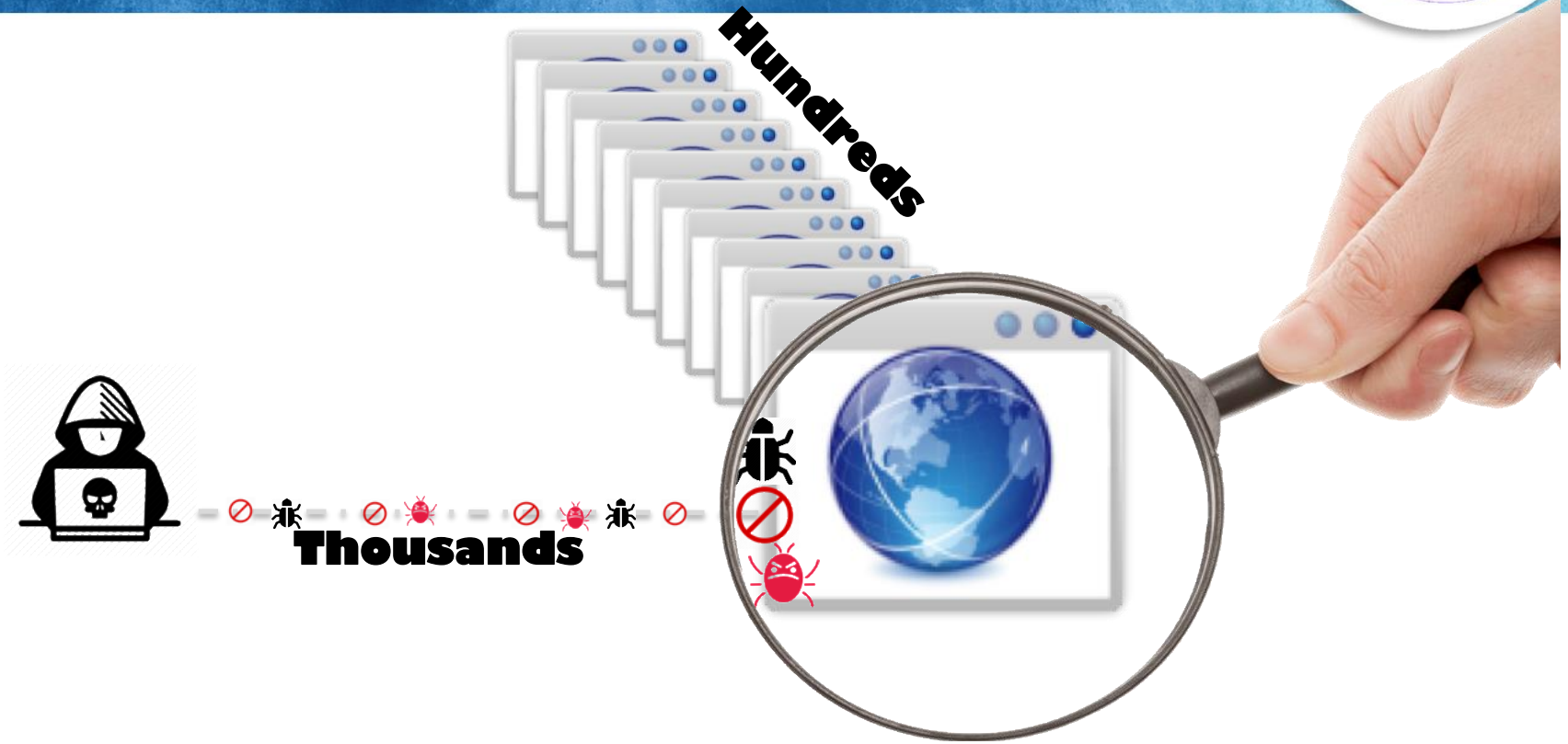
Advanced Spearphishing (e.g. SNAP_R)

Automated CAPTCHA Reader

Advanced PW Guessing (e.g. PassGAN)


Web Vul. Scanner
Binary Composition
App Vul. Monitoring
RASP
SAST
Pen Test
WAF
DAST
IAST

Observations



Observations: Application Vulnerabilities

- **Flawed Authentication**
- **Security Misconfigurations**
- **Sensitive Data Exposure**
- **Insecure TLS/SSL usage**
- **Cross-Site scripting**
- **Injection**
- **Using vulnerable components**
- **Inappropriate error handling**
- **CSRF**

Optimizing App Security Coverage

More Than One Third

- Injections
- Sensitive Data Exposure
- XML External Entities (XXE)
- Cross-Site Scripting
- Insecure Deserialization

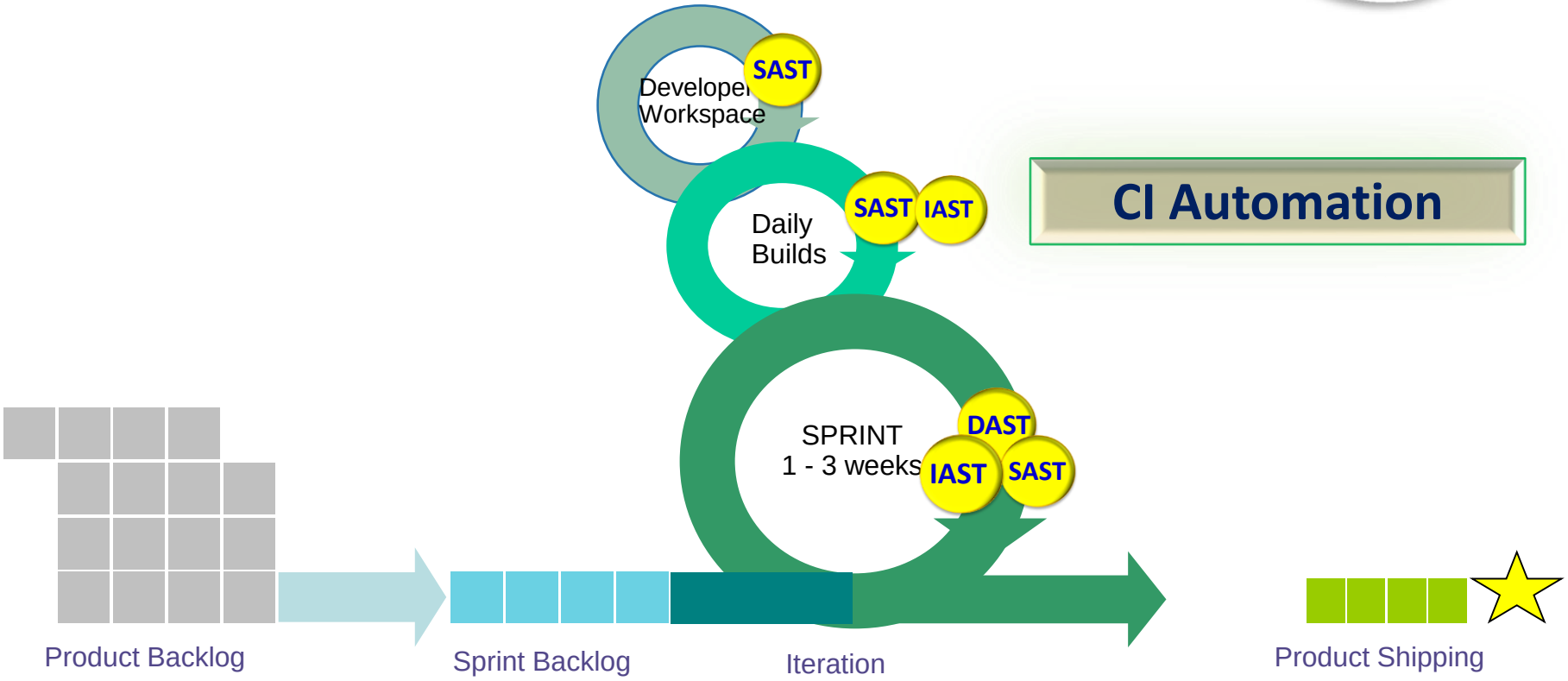
Around Two Third

- Injections
- Sensitive Data Exposure
- XML External Entities (XXE)
- Cross-Site Scripting
- Insecure Deserialization
- Security Misconfigurations
- 3rd Party Vulnerable Lib

Around One Third

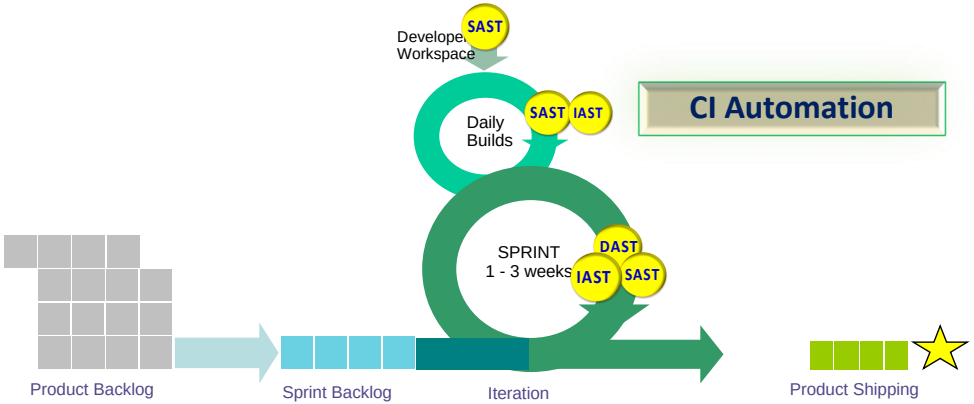
- Injections
- Sensitive Data Exposure
- XML External Entities (XXE)
- Cross-Site Scripting
- Security Misconfigurations

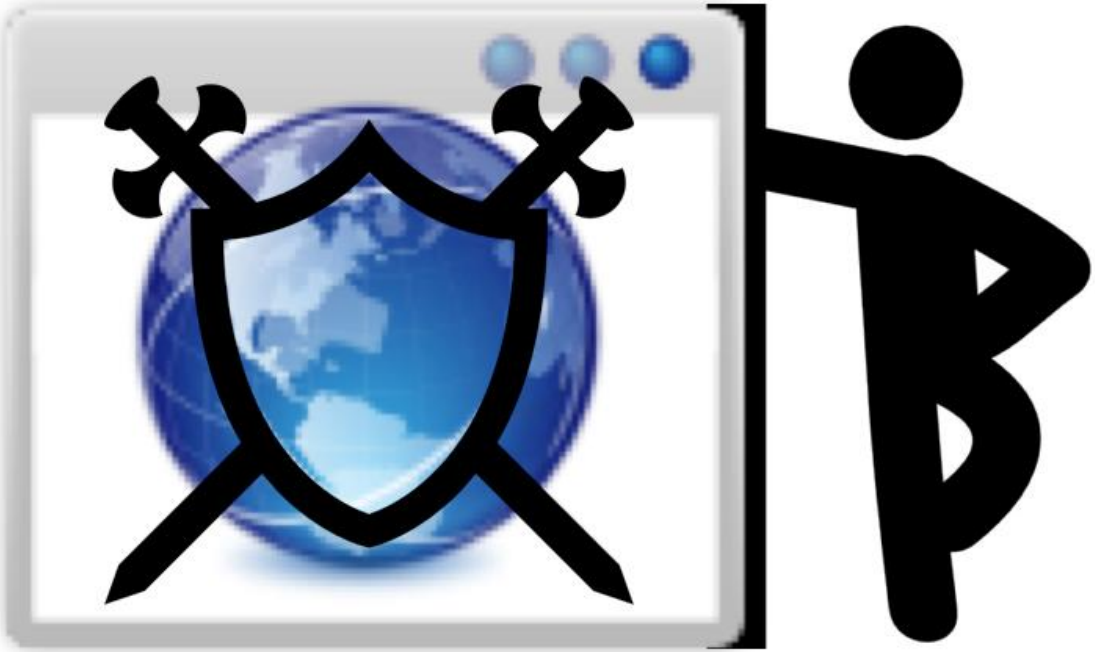
Security Embedded with Agile



Security Embedded with Agile

> 80 % with <<

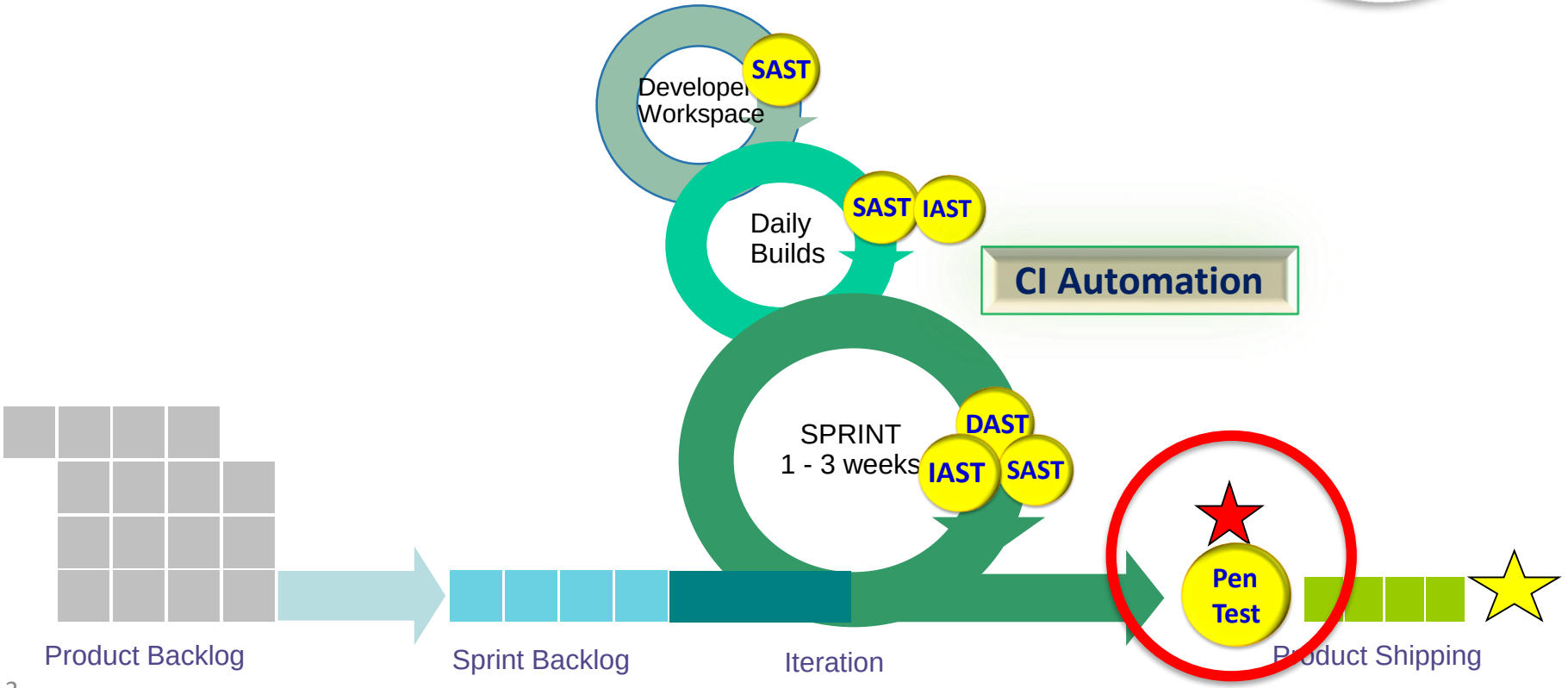




What Pen Test should focus on?

- Authentication & Authorization
  - Authentication flow and design, Passwords, 2FA, Security questions, Access Control
- Session management
- Business Logic
- All possible bypassing issues
- Data flows that are not covered by scanners, such as email, SSH, SAML etc.
- Examine Attack surface
- Sampling test Injection, XSS, to validate SAST/IAST/DAST controls
- Last but not the least, Infrastructure

Completing the Puzzle



Recommendations

- **Shift Left** – Train and Empower Developers to Security Champions
- **Automation** - Empower engineers with SAST, IAST, OSS, and WVS
- **Pen test smartly** – Focus on the limitation area of tools
- **Implement multi-factor authentication**
- **Check password blacklist**
- **Phishing/social engineering awareness training**

Questions & Answers