



Application Security Processes



Kürşat Oğuzhan Akıncı
@KOAkinci



#Agenda

- What is Application Security?
- How do we design application security processes?
 - Secure Development Partnership
 - Secure Development Standards
 - Manageability: Automation & Integration
 - Manageability: Secure Pipeline
 - Tools: Exclusion of Code Qualification Vulnerabilities
- Security Library Development
- Threat Modeling
- Developer Benchmark
- Security Training
- Security Tests
- Bug Bounty



#What is Application Security?

Application security is defined as the set of steps a developer takes to identify, fix, and prevent security vulnerabilities in applications at multiple stages of the software development lifecycle (SDLC). It involves several steps to keep security vulnerabilities at bay, from development to testing and post-deployment reviews, keeping in mind the application deployment environment. These steps span right from application design to code review and post-deployment.

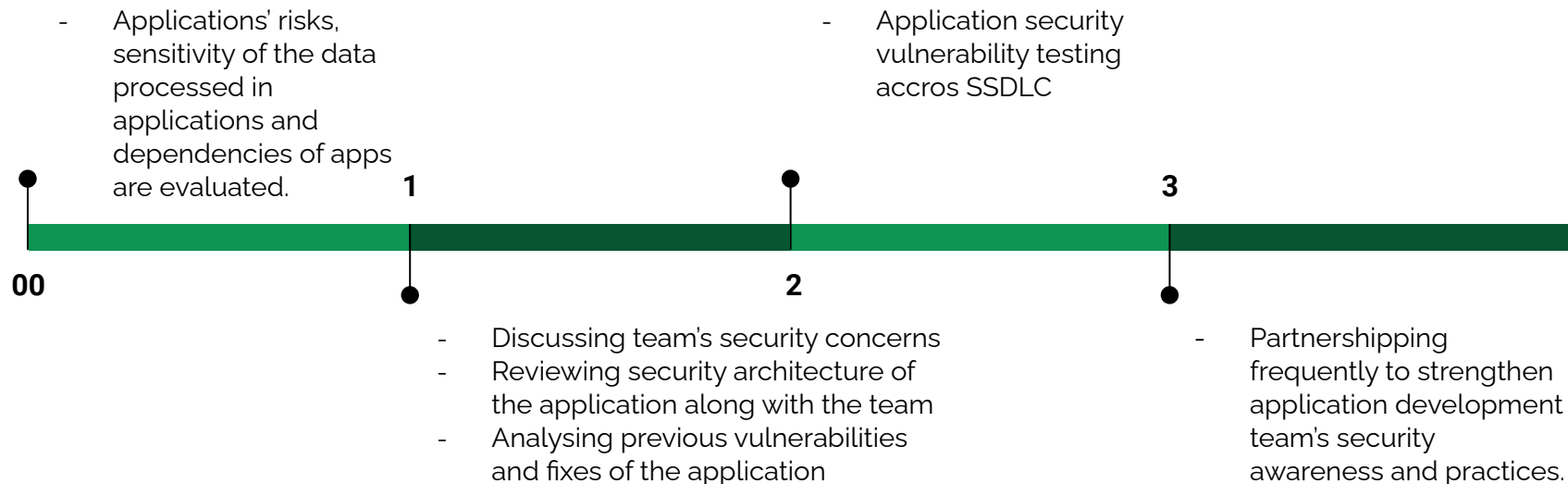


#Security Teams : Partnership

Today	Secure By Default	Self Service	Security Partnership
Mid Term	Secure By Default	Self Service	Security Partnership
Long Term	Secure By Default	Self Service	Security Partnership



#Secure Development: Partnership





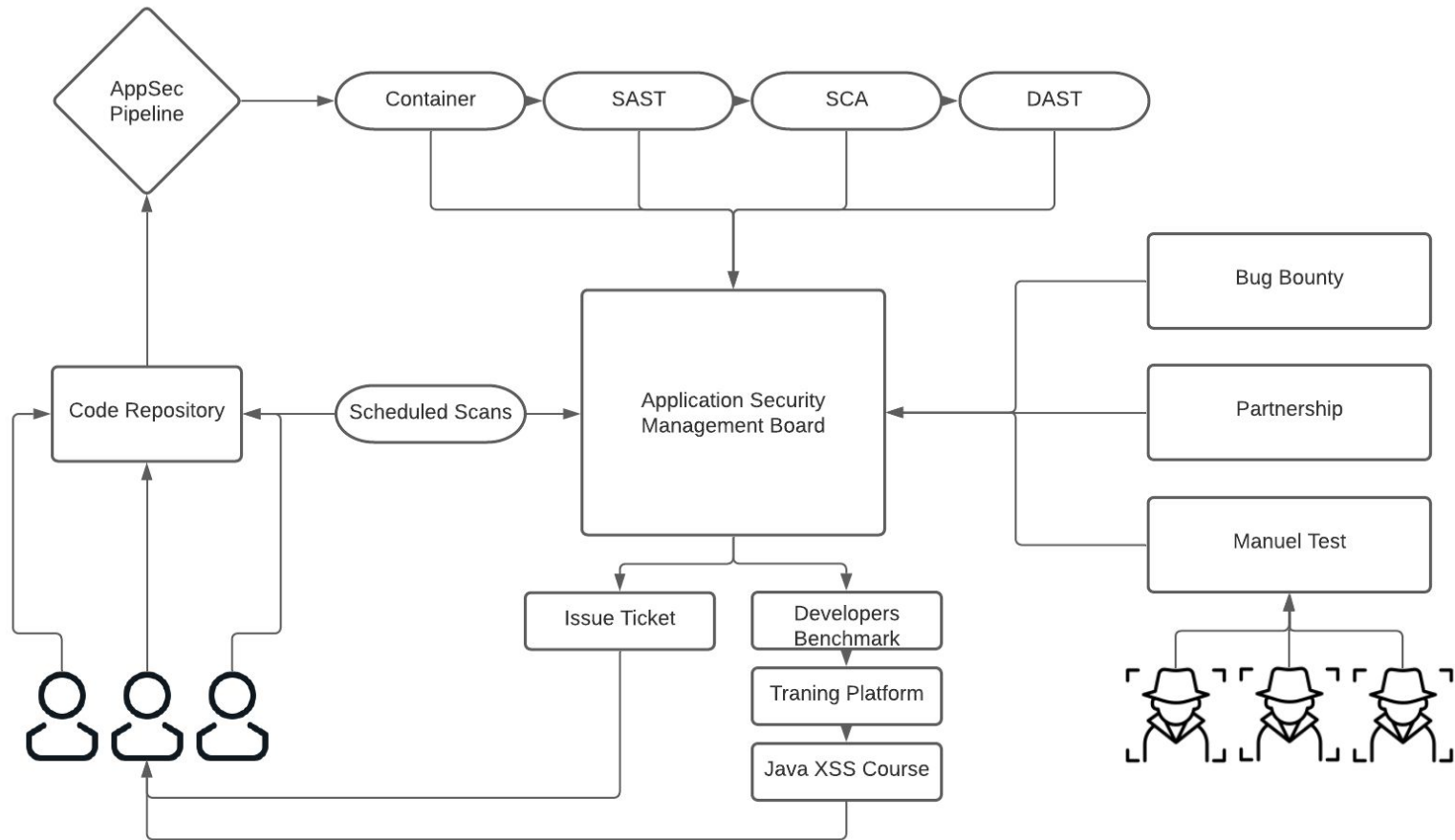
#Secure Development: Standards





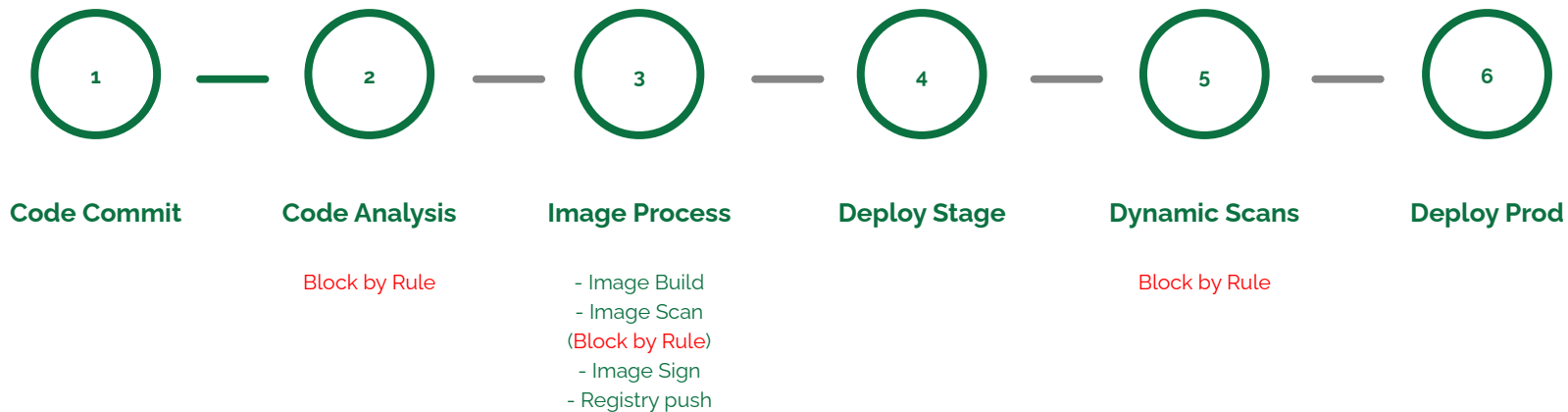
#Manageability: Automation & Integration

- AppSec Pipeline (Container, SAST, SCA, DAST)
- Scheduled Scans
- Issue Ticket
- Vulnerability Management
- Mail, Slack, other Communication Apps





#Manageability: Secure Pipeline



#Tools: Exclusion of Code Qualification Vulnerabilities



Example:

- Dead Code: Unused Field
- Dead Code: Unused Method
- Dead Code: Unused Parameter
- Dead Code: Expression is Always true
- Dead Code: Expression is Always false
- Dead Code: Empty Try Block



#Security Library Development





#Threat Modeling

The process of identifying potential security risks of applications is called **Threat Modeling**.

- **STRIDE** (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege)
- **DREAD** (Damage, Reproducibility, Exploitability, Affected users)



















































- Identification of security risks
- As the design of the applications changes, the potential risks that may arise in the future will also change, so checklists and controls need to be changed
- Listing of possible threats to the system
- Listing of actions to be taken for each threat

...



Node Properties		
Critical		
<id>	623	
authentication control	true	
authorization control	true	
callcount	300086	
dbaccessread	true	
dbaccesswrite	true	
exceptionhandling	true	
gitlabURL	https://gitlab.delivery.apigee.com	
guid	bmsunbveip	
kvkk	true	
kvkksensitive	true	
labeled	true	
name	moon-delivery-firstmile-package-api	
owner	Gökhan	
projectID	4105	
risk_score	6.1964640000000001	
servicetosevice communication	true	
severity	Critical	
sox	true	
team	firstmile	
tribe	delivery	
type	API	
internal	true	

#Developer Benchmark

	example-developer1@trendyol.com Link	 10	 5	 63	 17	Score : 336
	example-developer2@trendyol.com Link	 5	 1	 17	 4	Score : 86
	example-developer3@trendyol.com Link	 8	 0	 7	 8	Score : 44
	example-developer4@trendyol.com Link	 0	 0	 10	 2	Score : 44
	example-developer5@trendyol.com Link	 0	 2	 2	 6	Score : 40
	example-developer6@trendyol.com Link	 4	 0	 8	 3	Score : 38
	example-developer7@trendyol.com Link	 0	 0	 6	 6	Score : 36
	example-developer8@trendyol.com Link	 0	 0	 7	 3	Score : 34
	example-developer9@trendyol.com Link	 0	 0	 8	 0	Score : 32
	example-developer10@trendyol.com Link	 0	 3	 0	 0	Score : 30

#Developer Benchmark

Developer Benchmark Details



Developer

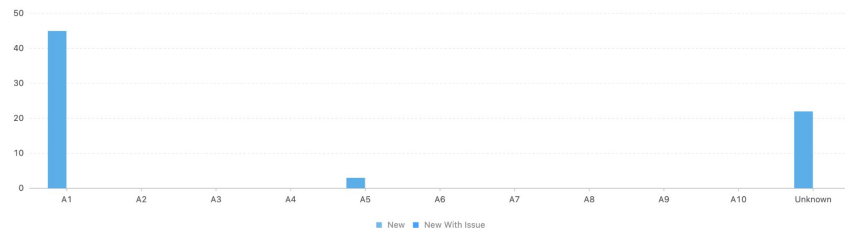
Name : example-developer999@trendyol.com

Date Range : 01 May 2021 – 25 Nov 2021



> [Python Icon] Python Total : 52

Owasp Top Ten



#AppSec Training

Committer Benchmark Details

Committer

Name : example-developer1000@trendyol.com

Date Range : 01 May 2021 ~ 25 Nov 2021

Training

Language : Python
Score : 385000



Python

Total : 467

Compiler Optimization Removal or Modification of Security-cr ...	337
Improper Handling of Exceptional Conditions	31
Use of Potentially Dangerous Function	9 1 14
Improper Neutralization of Special Elements used in an OS Co ...	7 17
Insufficient Encapsulation	15
Improper Control of Generation Code (Code Injection)	1
Use of Cryptographically Weak Pseudo-Random Number Generator ...	9
Use of Internally Dangerous Function	5
Use of a Broken or Risky Cryptographic Algorithm	5
Deserialization of Untrusted Data	2
XML Injection (aka Blind XPath Injection)	1
Improper Input Validation	1
Improper Authorization in Handler for Custom URL Scheme	1
Improper Enforcement of Message Integrity During Transmissio ...	1



#Bug Bounty

- Platform Quality
- Researchers Quality
- Ease of Operation

Triage Team Quality
Program Manager Quality
Cost

bugcrowd

hackerone

 **Synack**

 **zerocoaster**

 **Cobalt**



#Bug Bounty

Preparation

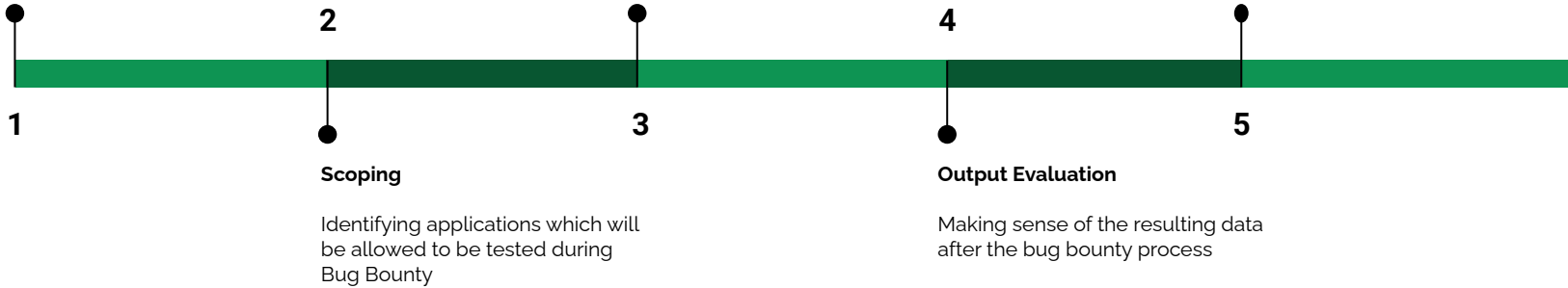
Determination of processes and requirements before the program

Private Bug Bounty Process

Starting Bug Bounty only with the hackers who are privately invited

Public Bug Bounty

Starting Bug Bounty publicly after all processes are completed and matured





Data Security: Application Security Processes



Kürşat Oğuzhan Akıncı
KOAkinci