SAMM

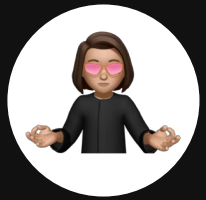
What is maturity in application security and how build wellness process?

2022
ALMATY
KAZAKHSTAN

TOLTARYS
KAZHACKSTAN

02 —— Whoami

- 7 years experience of working in information security
- 5 years experience of working in application security
- Lead of application security team of fintech company



Olga Sviridova / turbobarsuchiha

03 —— Application security process

Goals

To help integrate security themes early in the development process. To reduce the number of vulnerabilities released over the long term.

Tasks

to train staff on application security and to embed security practices in SDLC

Results

maintaining the CIA triad on the security side of the application

04 —— Security SDLC aka SDL

05 —— Our retrospective

We had been implementing activates simultaneously for 6Qs by 2 people

- Implement SAST with taint analysis
- Implement SCA with different feeds
- Implement enterprise DAST
- Implement different courses
- Design reviews
- Manage Bug Bounty program

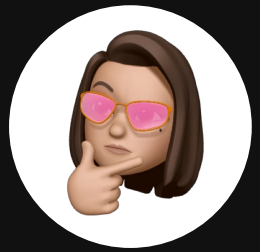
As result
Our team had burn out


DAST
CI/CD
SCA
Business logic
Vulnerability
Code review
Bug Report
API
Credentials
OWASP
Fuzzing
BurpSuite
Checkmarx
Awareness
Education
Response
Pipelines
SAST

Okay, how could we structure this?

SAMM stands for Software Assurance Maturity Model by OWASP foundation.

owaspsamm.org



WTF is maturity of security?

11 —— Maturity of application security

In business development, a maturity model is a common way **to distinguish the capabilities and needs of different companies**. The maturity of your security provides a context which, in turn, helps when determining your needs.

Measurable

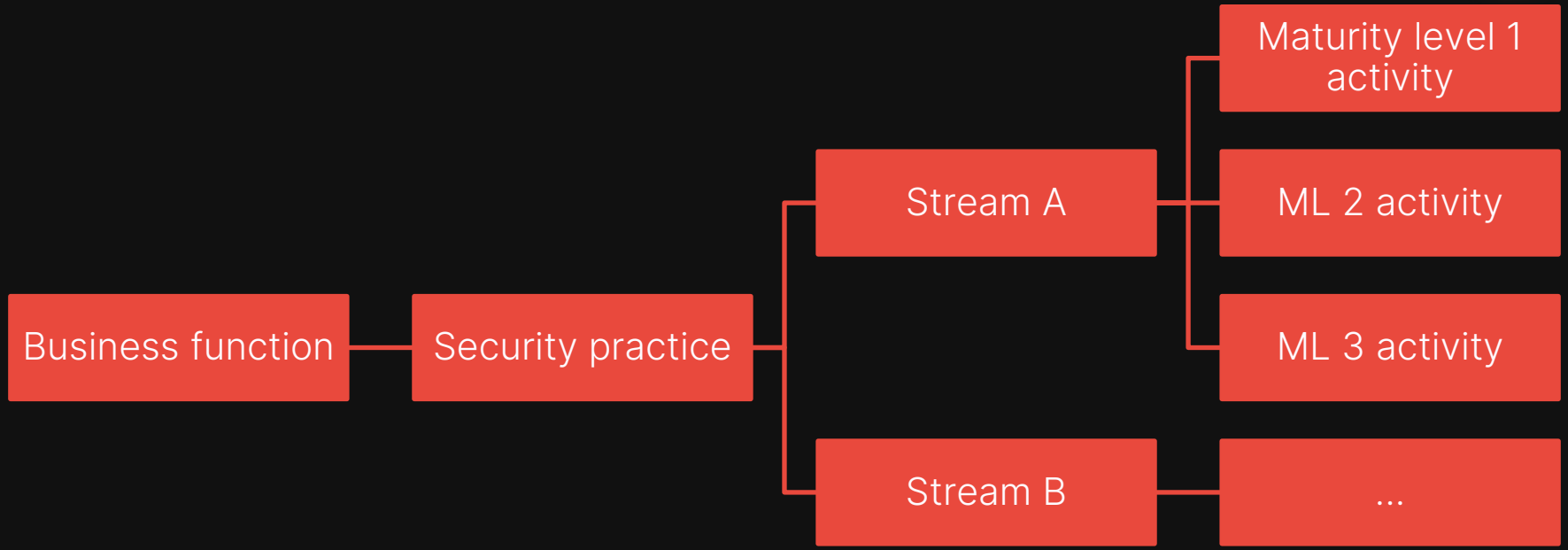
Defined maturity levels across security practices

Actionable

Clear pathways for improving maturity levels

Versatile

Technology, process, and organization agnostic


Business function
Security practice
Stream A
Stream B
Maturity level 1 activity
ML 2 activity
ML 3 activity
...

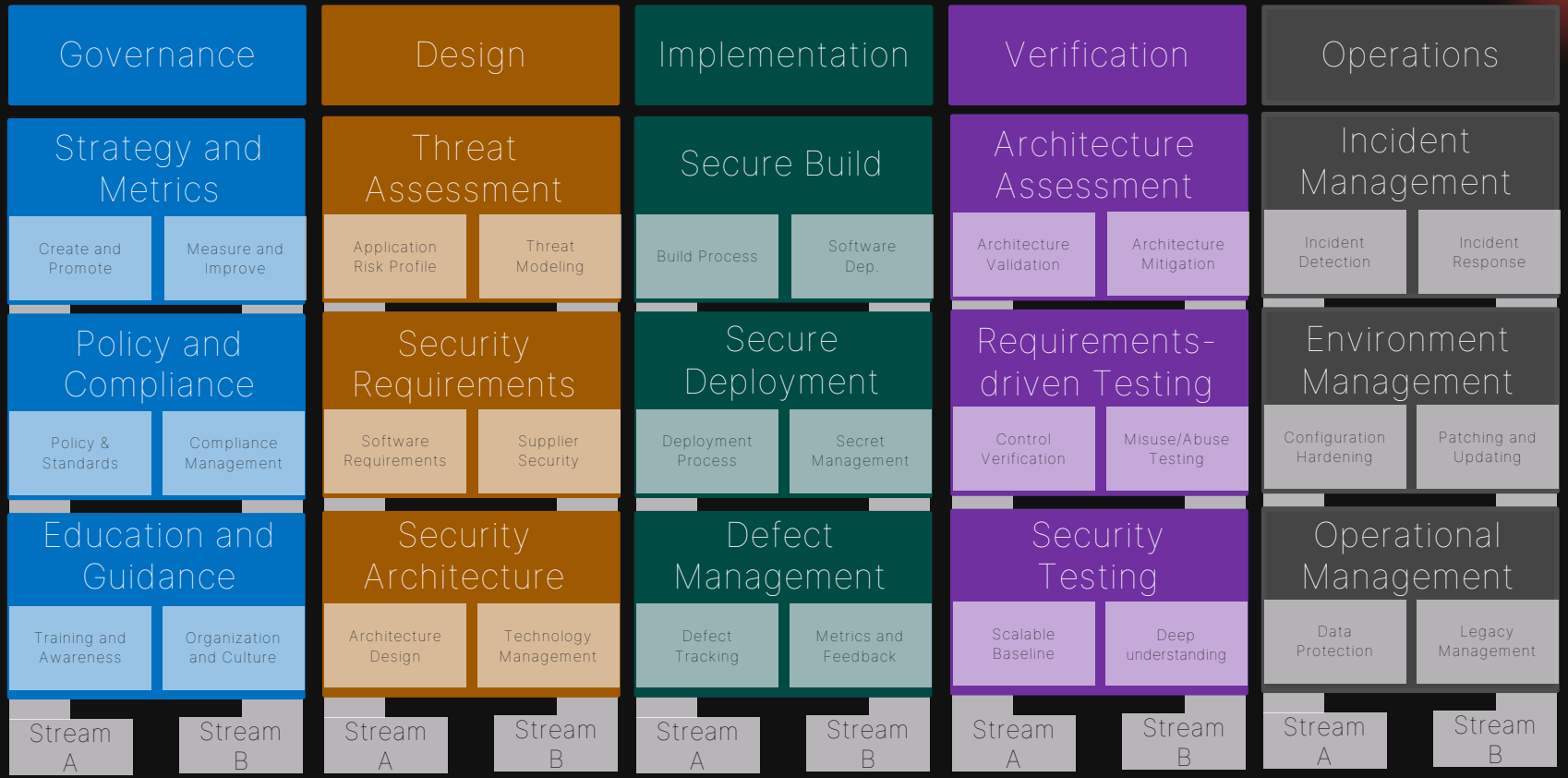
5
Business functions

15
Security practices

30
Streams

90
Activities

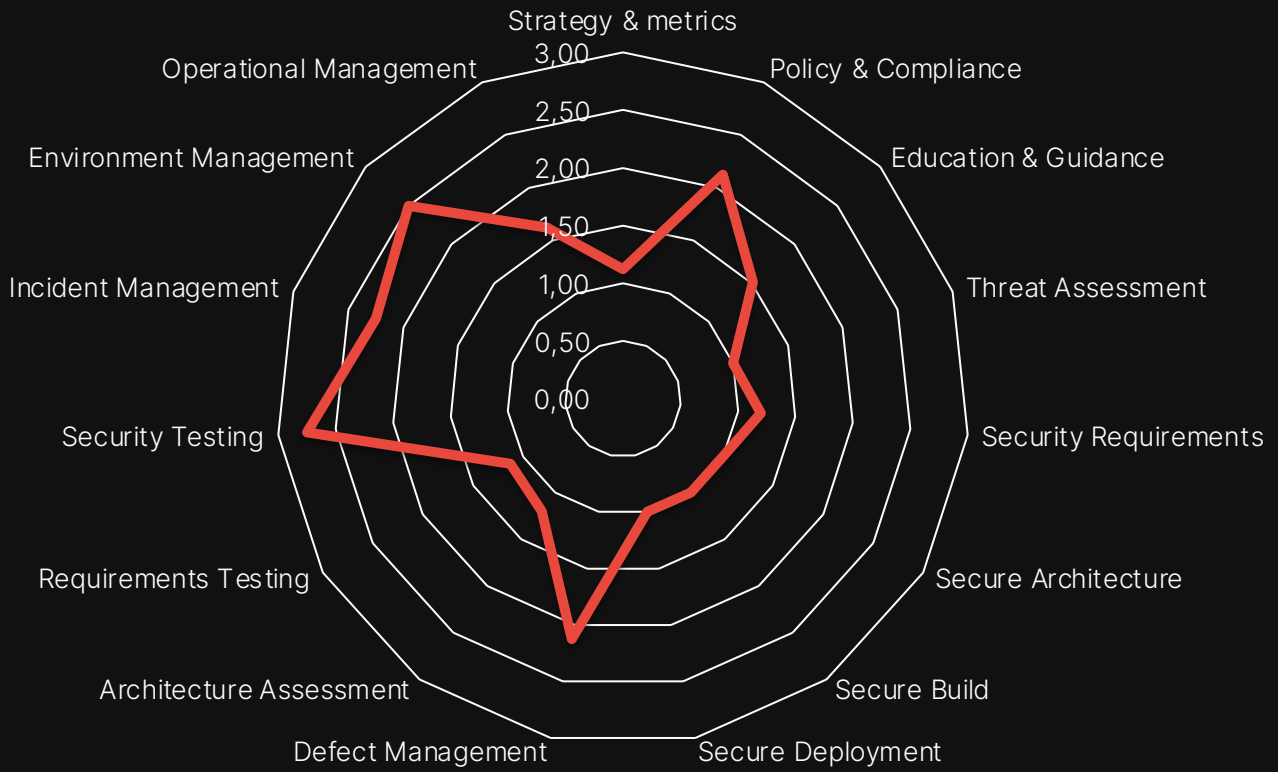
15 —— SAMM


Governance
Strategy and Metrics
Create and Promote
Measure and Improve
Policy and Compliance
Policy & Standards
Compliance Management
Education and Guidance
Training and Awareness
Organization and Culture
Stream A
Stream B
Design
Threat Assessment
Application Risk Profile
Threat Modeling
Security Requirements
Software Requirements
Supplier Security
Security Architecture
Architecture Design
Technology Management
Stream A
Stream B
Implementation
Secure Build
Build Process
Software Dep.
Secure Deployment
Deployment Process
Secret Management
Defect Management
Defect Tracking
Metrics and Feedback
Stream A
Stream B
Verification
Architecture Assessment
Architecture Validation
Architecture Mitigation
Requirements-driven Testing
Control Verification
Misuse/Abuse Testing
Security Testing
Scalable Baseline
Deep understanding
Stream A
Stream B
Operations
Incident Management
Incident Detection
Incident Response
Environment Management
Configuration Hardening
Patching and Updating
Operational Management
Data Protection
Legacy Management
Stream A
Stream B

16 —— SAMM

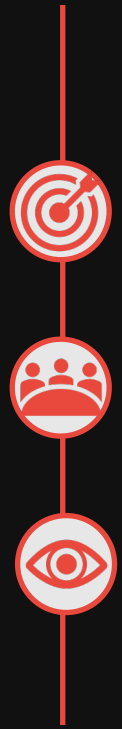
stream	ML	questions relating to activities	answer options
Software Dependencies	1	Do you have solid knowledge about dependencies you're relying on?	No Yes, for some applications Yes, for at least half of the applications Yes, for most or all of the applications
	2	Do you handle 3rd party dependency risk by a formal process?	
	3	Do you prevent build of software if it's affected by vulnerabilities in dependencies?	

17 —— SAMM


Strategy & metrics
Policy & Compliance
Education & Guidance
Threat Assessment
Security Requirements
Secure Architecture
Secure Build
Secure Deployment
Defect Management
Architecture Assessment
Requirements Testing
Security Testing
Incident Management
Environment Management
Operational Management
3,00
2,50
2,00
1,50
1,00
0,50
0,00

How it works in practice?

19 —— SAMM (First step)

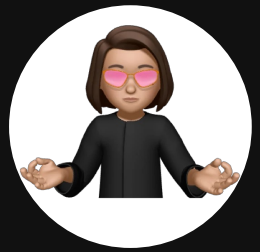


Define targets

Support for the security department and other departments of the company

Have realistic expectations and time

20 —— SAMM (First step | Our practice)



Entire self-developed application enterprise

CISO and lead of other security domains

Expecting to find gaps in the processes

21 —— SAMM (Set your goals)

Understand your resources

Set your goals for 1 years

Chose 2-4 activities for 1Q

Do assessment again

Do a self-assessment of the team's skills. Determine the involvement of other teams.

Chouse few practices for years

A few activities for a sprint of ~3-4 months

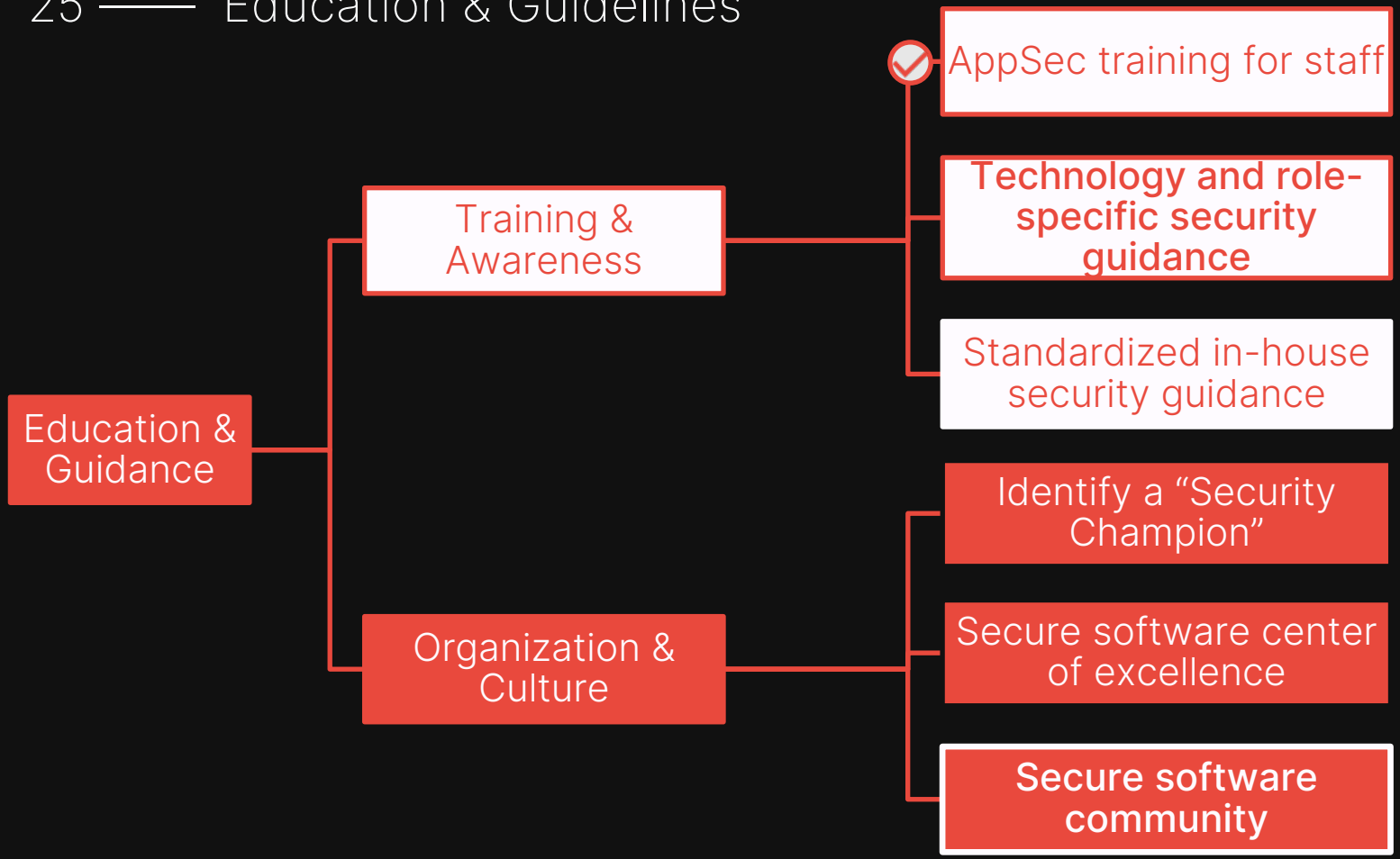
What about examples?

23 —— SAMM processes

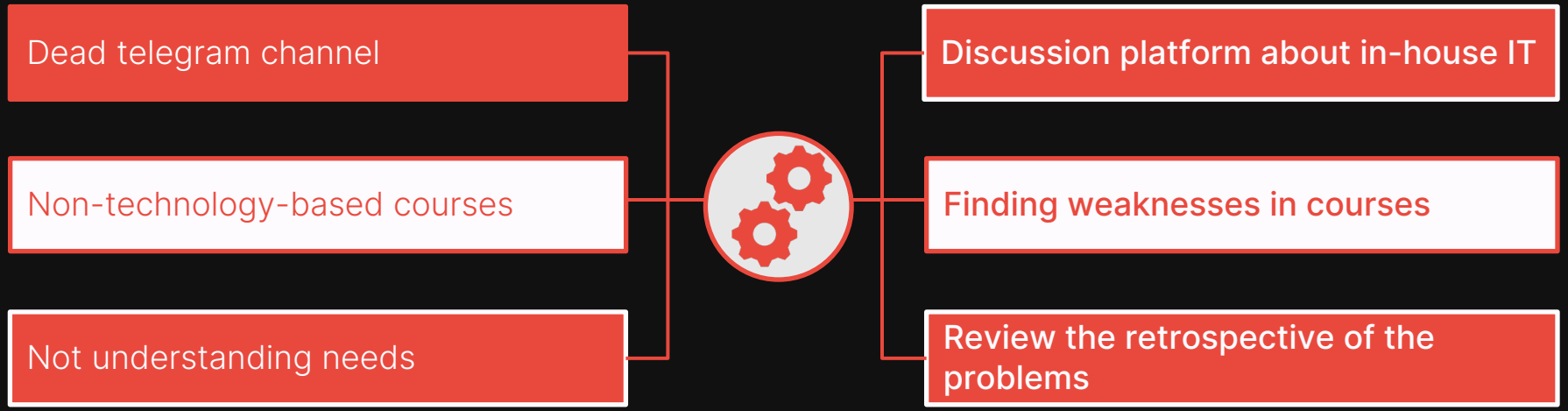
- Fix the education processes
- Fix the security build processes
- ...

Governance

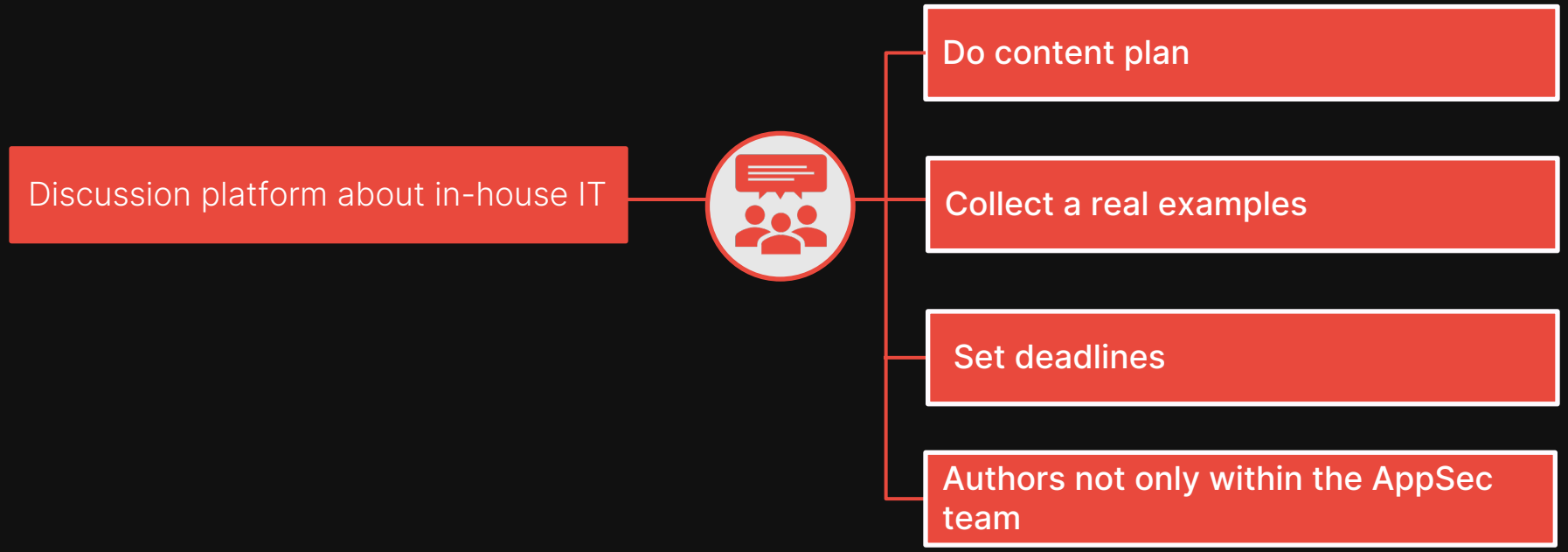
25 —— Education & Guidelines



26 —— Secure software community



27 —— Discussion platform about in-house IT



28 —— Writing an article

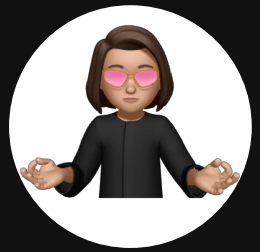
Understand problem

Collect examples of your company

Keep a call to action in the article

Publish and distribute

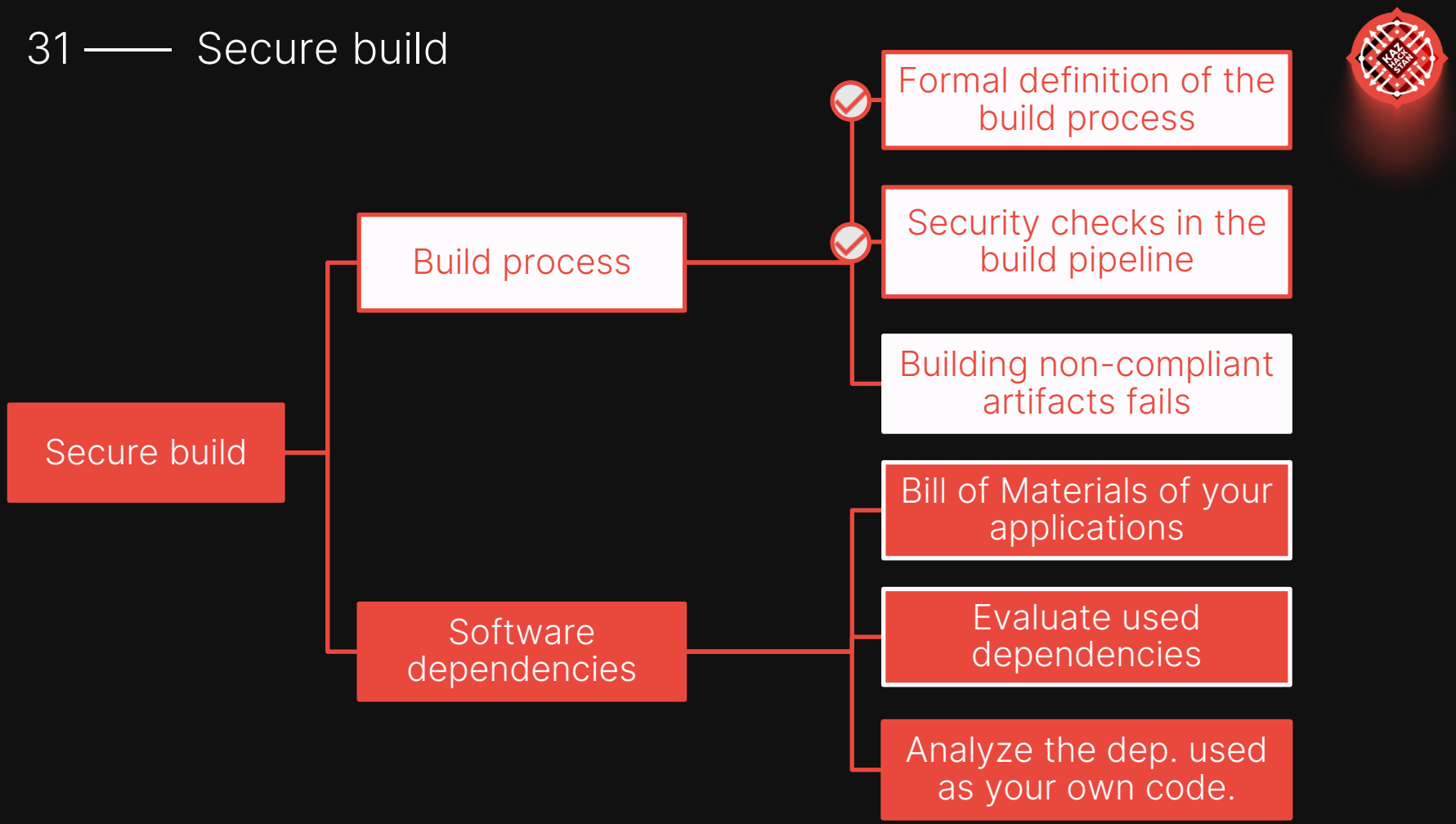
29 —— Writing the article (vulnerable dependencies)



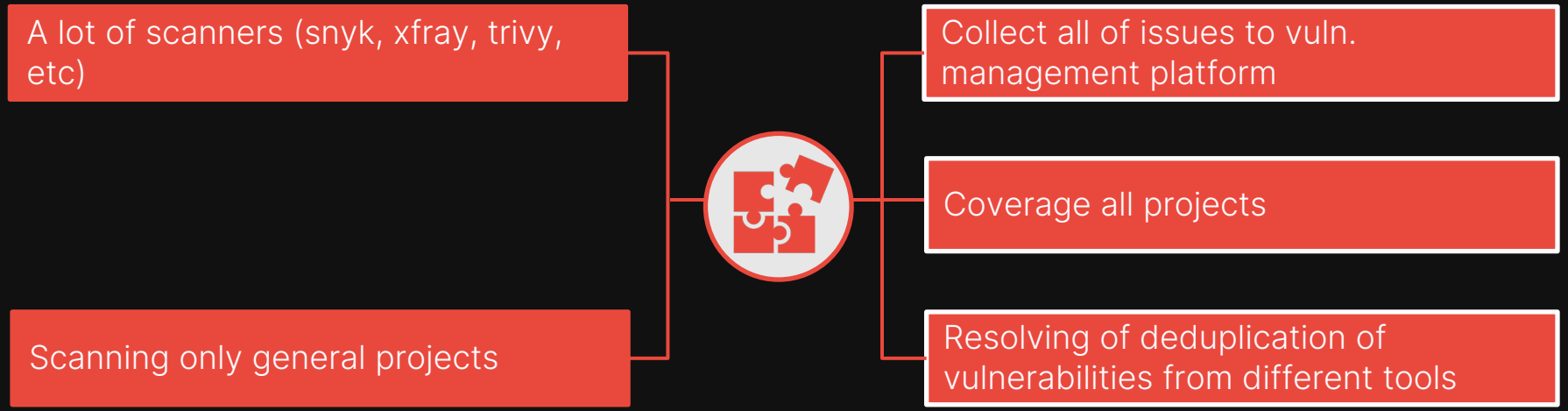
- What is dependency?
- What is the SCA?
- What our company use to prevent security problems with dependency?
- Real reports on problems within the company (ex. pen.tests, internal audits, bugbounty)
- What can we provide to the development team to improve the security experience within the team?

Implementation

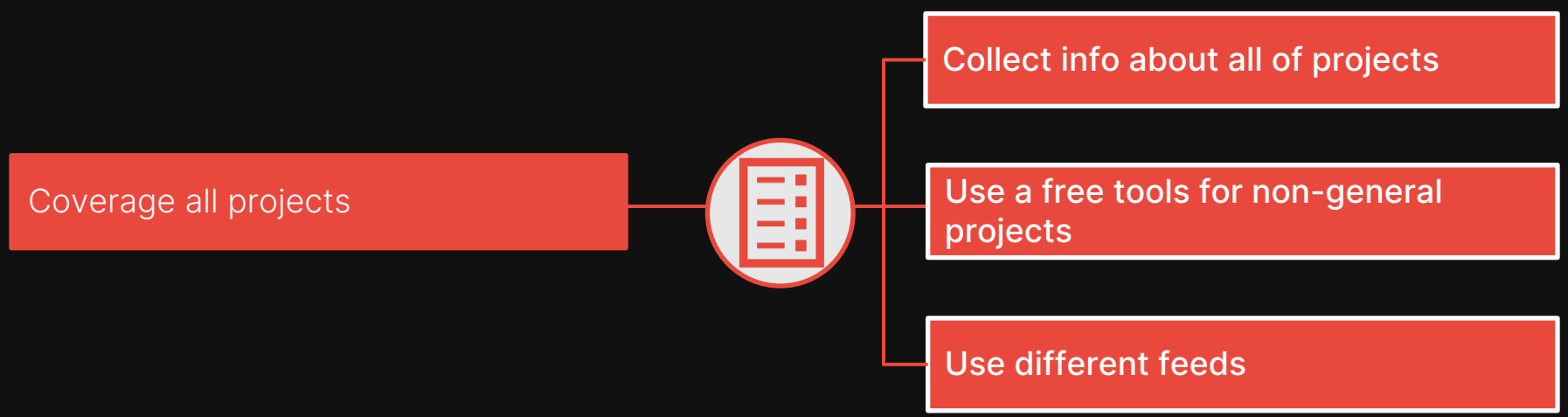
31 —— Secure build



32 —— Evaluate used dependencies



33 —— Coverage all projects

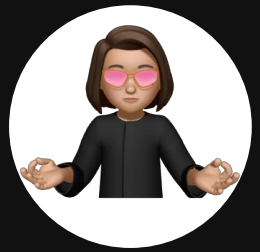


Check chart

35 —— SAMM chart after next phase

Conclusions

37 —— Conclusions

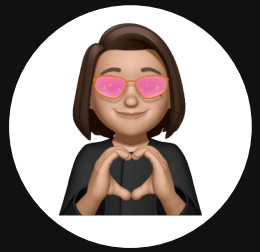


- Be honest with yourself and your team
- Adapt activities to your needs and resources
- Don't try to close all activities at once
- Take notes on your observations
- Keep calm and do SAMM

38 —— Links

OWASP SAMM: owaspsamm.org

github.com/owaspsamm/core/releases/tag/v2.0.6



Thank you for attention