CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Sneak Peak into the Security Assessment with the community

Ragashree M C, CISSP
Graduate Student, Carnegie Mellon University
Technical Lead, CNCF TAG Security

What a wonderful world..

- We are more connected now, that ever
- Innovation everywhere!

What a wonderful world..

- Huge number of connected devices, services..
- Larger attack surface that ever
- How secure really is it?

Meanwhile,


For the security we said we'd hire someone to...
Hold on, that's not the priority. Let's get the project started first, we'll see about that later...
Hey the project is nearly done, we should do a security audit to...
Too late man, we don't have the time or the budget for that
The site's been online for 10 days, and we haven't done any security testing, I'm nervous...
Don't worry, we'll take care of it later...
LATER...
DOWN! THE SITE IS DOWN! WE'VE BEEN HACKED!
How could you let this happen!?
CommitStrip.com

Agenda

- What is a security assessment?
- How is it different from audits?
- How to perform a security review?
- What are the resources available?
  - Announcement!
- How to get a TAG-security security assessment?
- What’s next?

What is a security assessment?

How is it different from audits?

How to perform a security review?

What are the resources available?

..Announcement!

How to get a TAG-security security assessment?

What’s next?

Security Assessments

- Dives into Systemic/design
- Subjective
- Longer validity

What is a security assessment?

How is it different from audits?

How to perform a security review?

What are the resources available?

..Announcement!

How to get a TAG-security security assessment?

What’s next?

Security Assessments vs Security Audits

- Longer validity vs Single point in time
- Systemic/design issues vs process/implementation issues
- Subjective vs objective

What is a security assessment?

How is it different from audits?

How to perform a security review?

What are the resources available?

..Announcement!

How to get a TAG-security security assessment?

What’s next?

Actors

The good, the neutral, the bad

Source: AliExpress, Marvel Chinese Brand Name Creation | Labbrand

Disclaimer All characters represented in this artwork belongs to the respective owner.

System goals

- Confidentiality
- Integrity
- Availability
- … Non-repudiation, Secrecy, Privacy…..

Source: AliExpress, Marvel Chinese Brand Name Creation | Labbrand

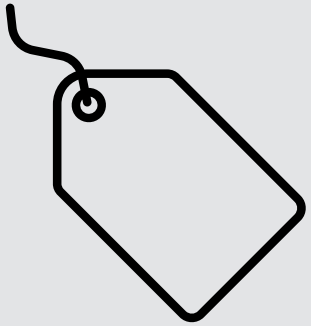
Attacker goals

- Disclosure
- Alteration
- Destruction

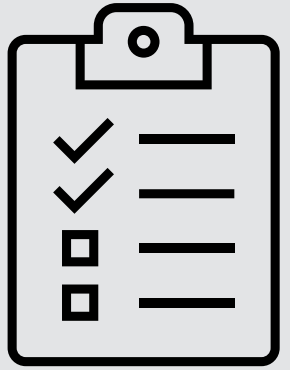
Source: AliExpress, Marvel Chinese Brand Name Creation | Labbrand

Security assessment goals

Identify



Categorize



Respond

Identification

- Goal: identify what are the threats and possible attack scenarios
- Requirement: service architecture
- Methodology & Frameworks
  - STRIDE
  - Attack graphs

Special mention:
Light weight threat modelling framework; GitHub - https://github.com/cncf/tag-security/issues/903
Presentation @ Cloud Native Security Con NA ’23 - Security Threat Modeling Live from Scratch Session - Andrew Martin, Control Plane

STRIDE Framework

- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service
- Elevation of privilege

Categorization

- Goal: Identify the impact
- Requirement: Identified risks
- Methodology
  - Quantitative
  - Qualitative
- Frameworks
  - DREAD
  - LINDDUN
  - .. etc

DREAD Framework

- Damage caused
- Reproducibility
- Exploitability
- Affected users
- Discoverability

Response

- Goal: Reduce the impact!
- Options
  - Prevention
  - Recover
  - Detection with traceability
  - Detection
  - Traceability

Prevention > Recover > Detection with traceability > Detection > Traceability

What is a security assessment?

How is it different from audits?

How to perform a security review?

What are the resources available?

..Announcement!

How to get a TAG-security security assessment?

What’s next?

Resources, from TAG Security

Guidelines

- Cloud native security whitepapers
  * Translation:
    - Chinese
    - Portuguese
    - Italian (on the way)
  * Audio recordings
- Supply chain security whitepapers
- Cloud native security controls mappings

Tools

- Cloud native use-cases and personas
- Cloud native 8
- Cloud native security map
- Cloud native controls
- Cloud native security lexicon

Assessments & Reviews

- Self-assessments
- Joint reviews
- Security assessment book

Special mention:
All the resources are available at TAG Security GitHub - tag-security/PUBLICATIONS.md at main · cncf/tag-security (github.com)
Presentation @ Cloud Native Security Con NA '23 - TAG Security Cloud Native Security Whitepapers Overview - Shlomo Zalman Heigh, CyberArk

What is a security assessment?

How is it different from audits?

How to perform a security review?

What are the resources available?

..Announcement!

How to get a TAG-security security assessment?

What’s next?

TAG Security Assessments Process

Special Mention:
- Justin Cappos
- Matthew Giassa

Phase 1: Self Assessment

Step 1: Self Assessment	Step 2: Present the project and self assessment	Step 3: Conclude self assessment
Complete self assessment as per cncf/tag-security (github.com)	Create presentation issue in GitHub - New Issue · cncf/tag-security	Incorporate TAG security feedback into self assessment
	Present the project & self assessment to TAG Security community	Create a PR and add the self-assessment in TAG Security repo

Phase 2: Joint Assessment

Step 4: Initiate Joint reviews	Step 5: Conflict of interest statement and review	Step 6: Questions & Clarifications	Step 7: Hands-on review (optional)	Step 8: presentation & final summary
Create tracking issue New Issue · cncf/tag-security (github.com)	TAG Security review team provides the statement of conflict of interest	Lead security reviewer or their designee will perform initial, clarifying review	Security reviewers may perform a hands-on review	Create a presentation issue at New Issue · cncf/tag-security (github.com)
				Present the project and self assessment to the CNCF TAG Security community

Owner(s)

Lead Security reviewer

Project Lead

Introducing, Security Assessments book..!!!

- Draft

  Security Assessment Book Draft - Google Docs
- GitHub Issue:

  [Suggestion] Should we write a Linux Foundation guide / course on how to do a security assessment? · Issue #999 · cncf/tag-security (github.com)
- Primary author: Justin Cappos

What is a security assessment?

How is it different from audits?

How to perform a security review?

What are the resources available?

..Announcement!

How to get a TAG-security security assessment?

What’s next?

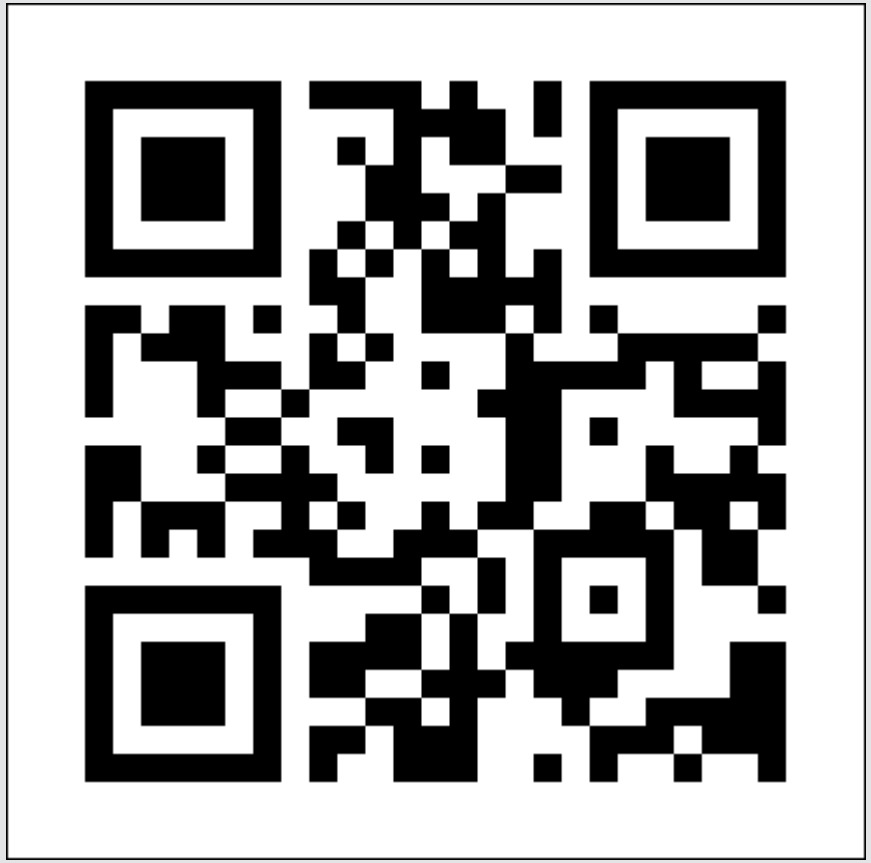
So… What's next?

- Have a feedback?
- Want to get involved?
- Want to get a security assessment?

Slack Us! CNCF Workspace
- #tag-security (General discussions)
- #security-assessments-book (Security assessment book discussions)

GitHub
- Tag-security (for requesting security assessments)

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023



Please scan the QR Code above to leave feedback on this session


CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023