From Elbrus to Kali
Reference Model Security Updates

Karine Sevilla, Walter Kozlowski

June 9, 2021

Security, a major concern

- Build a trusted Cloud Infrastructure is key
  - Within virtualised and containerised environments, security concerns are multiple and complex. All the layers must be secured

- Beyond best practices
  - Security must be taken into account earlier in Cloud Infrastructure and workloads life cycle
  - Integrate Security by Design
  - Align with recent security standards
  - Test continously

Collaboration with GSMA FASG

- Cross collaboration with GSMA FASG (Fraud And Security Group)
  - Shared interest on Cloud Infrastructure, 5G services, O-RAN
- Starting point with GSMA documents:
  - **FS.40** 5G Security Guide, version 1.0, Sept. 2020, draft v1.10 Feb 2021
  - **FS.33** Network Function Virtualisation(NFV) Threats Analysis, v1.0, March 2020
  - **White Paper** Open Networking & the Security of Open Source Software Deployment, Jan. 2021
  - **FS.31** Baseline Security controls v2.0, Feb 2020
- Reference Model and Anuket work mentioned in GSMA FS.40 and white paper Open Networking & the Security of Open Source Software Deployment

Additional security standards

- Security standards pointed out by FASG members and mentioned in RM:
  - The Six Pillars of DevSecOps: Automation(2020), Cloud Security Alliance and SAFECode joint publication
  - Fundamental Practices for Secure Software Development, SAFECode publication
  - Managing Security Risks Inherent in the Use of Third-party Components, SAFECode publication
  - Tactical Threat Modeling, SAFECode publication

From Elbrus to Kali

- Reference Model Security enhancements – Chapter 7
  - Section 7.3.3 Common Security Standards, addition:

    Description of GSMA FASG work on security including references to FS.31, FS.40 and Open Networking white paper
  - Section 7.7 Open Source Software Security, new section
  - Section 7.4.4 Infrastructure as a code and DevSecOps, new section
  - Section 7.6.6 Zero Trust Architecture, new section
  - Section 7.6.4 Volume Encryption, addition: sensitive data encryption
  - Section 7.9 Consolidated Security Requirements: related requirements added

Open Source Software security, section 7.7

- For Cloud Infrastructure and workloads, new challenges coming with the increasing part of open source code into software
- Open source code present in Cloud Infrastructure software from host Operating System to virtualisation layer components
- Security risks: poor quality code, obsolete code with known vulnerabilities, code from inactive open source community branch
- Risks mitigated by:
  - Code inspection by tools: static analysis (without execution) and dynamic analysis (during runtime)
  - Continuous vulnerabilities identification using CVE, scanning tools
  - Use of an isolated and dedicated internal repository to inspect and validate software
  - Identification of software components, Software Bill of Materials

Open Source Software security, section 7.9

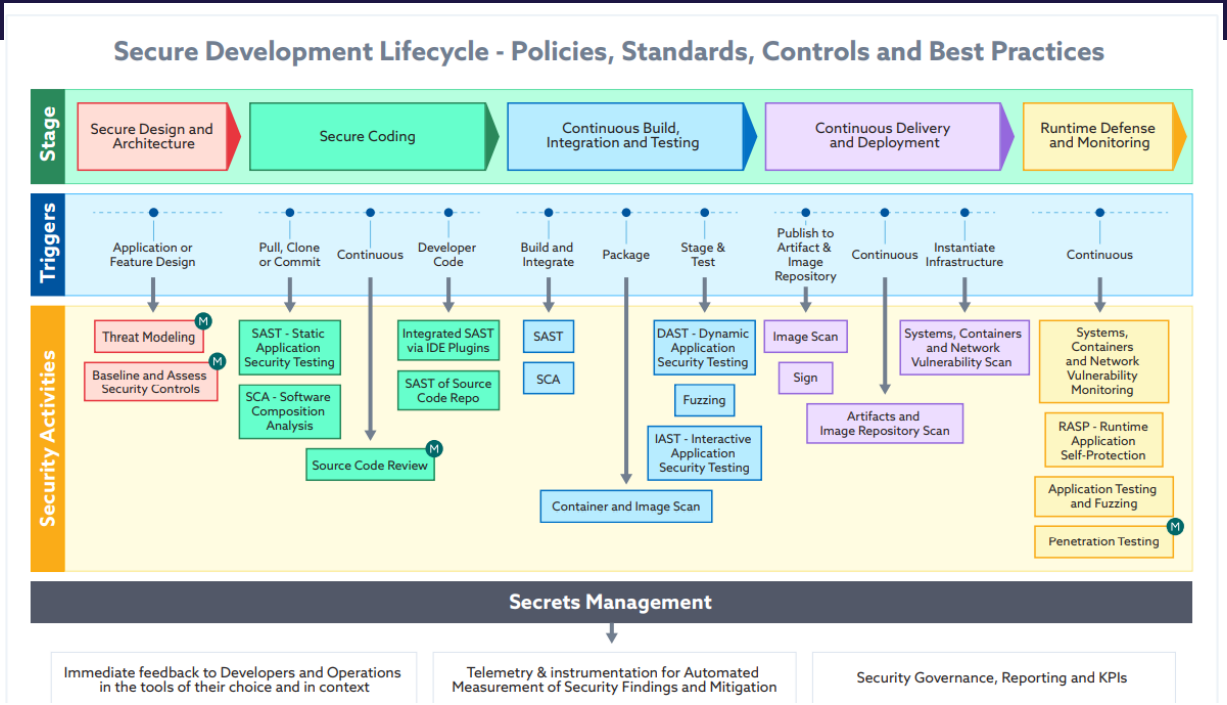
- Open source software security requirements

Reference	Description
req.sec.oss.001	Open source code **must be** inspected by tools with various capabilities for static and dynamic code analysis.
req.sec.oss.002	The CVE(Common Vulnerabilities and Exposures) **must** be used to identify vulnerabilities and their severity rating for open source code part of Cloud Infrastructure and workloads software.
req.sec.oss.003	A dedicated internal isolated repository separated from the production environment **must** be used to store vetted open source content.
req.sec.oss.004	A Software Bill of Materials (SBOM) **should** be provided or build, and maintained to identify the software components and their origins.

IaaC and DevSecOps

- Infrastructure as a Code (IaaC) = software used for the declarative management of cloud infrastructure resources
- IaaC requires secure lifecycle DevSecOps best practices adapted to infrastructure code development/LCM specifics
- Security aspects of this best practice were missing in Anuket Reference Model
- Anuket Kali release of RM adds the best practice requirements, adapting the framework introduced in Cloud Security Alliance (CSA) and SAFECode, "The Six Pillars of DevSecOps: Automation (2020)". The document utilises the base definitions and constructs from ISO 27000, and CSA's Information Security Management through Reflexive Security.

IaaC and DevSecOps framework



Reprinted from "The Six Pillars of DevSecOps: Automation" (2020) https://safecode.org/the-six-pillars-of-devsecops-automation

Anuket Requirements in: [CNTT/chapter07.md at master · cntt-n/CNTT (github.com)]

Zero Trust Architecture

- NIST 800-207:

Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.

- ZTA for Cloud Infrastructure:
  - Adopt least privilege configurations
  - Authentication and authorization required for each entity, service, or session
  - Fine grained segmentation
  - Separation of control plane and data plane
  - Secure internal and external communications
  - Monitor, test, and analyse security continuously

Zero Trust Architecture and Sensitive Data Storage Requirements

- ZTA, NIST 800-207: Trust never granted implicitly, it must be evaluated continuously

req.sec.sys.020	The Cloud Infrastructure architecture **should** rely on Zero Trust principles to build a secure by design environment.

- Sensitive Data Storage FS.40: external HSM to be integrated for cryptographic keys protection. GSMA FASG recommendations for the storage of UICC (Universal Integrated Circuit Card) credentials

req.sec.ci.009	For sensitive data encryption, the key management service **should** leverage a Hardware Security Module to manage and protect cryptographic keys.

And for Lakelse…

- Develop on multi-cloud security in RM
- Integrate security in RAs, RCs, RIs per RM requirements
- Identify the appropriate tools to include security tests into conformance test suites

Security Testing

- What are the most used and interesting tools for security testing?
  - OWASP tools
  - Clair
  - Trivy
  - Falco
  - …
- Feedbacks needed on these tools


Anuket