Nephio Security SIG

Proposal
General Philosophy

- Holistic: Secure all stages [dev, release, deploy, runtime]
- Focus on security intent than on tooling
- Zero Trust Enablement
- Policy based framework
- Frictionless Security
  - Fail the build not the release

Opportunity: Differentiate Nephio as a “Secure Telco Automation Framework”
Dev stage: Project/Repo/Code security

- OSSF checklist/score
- Security automation for new repos
  - Using org-level common github actions
- Security Review Checklist
  - Approving CI execution for PRs from external contributors
- SAST/DAST tools integration
  - Check LF for access to licensed tools (FOSSA, Synk)
- Security Advisories/Policy in place
  - Provide external folks to report a security issue
Release stage: Supply Chain Security

- Adhere to SLSA framework
  - Processes need to be set with automation
- Image signing & verification
- Automate release workflows with signed images
- Vulnerability scans in release pipelines
Deploy Stage: Deployment Security

- **Deployment best practices**
  - Use of non-privileged workloads
  - Process for defining how to enable privileged workload if need be
  - Mandatory resource request specification
- **Use of Admission Controllers and CD best practices**
- **Policy Framework**
Runtime Security

● Implications of Identity in multi-cluster deployments
  ○ Why would it be important? Consider ZTNA for NFs
  ○ What solution to use? SPIFFE?
● Automating hardening controls
  ○ ENISA
  ○ MITRE FiGHT
● API Security
● Secrets Management
● Risk assessment tools
● Zero Trust Enablement
● Preparing blueprints and automating deployment
  ○ Policy Framework
5G specific security

- 3GPP TS 33.501
- ENISA
- MITRE FiGHT
- Securing RIC
- Network Slice Security
Multi-cluster security orchestration

- Use of security operator
- K8s native policy framework
Security Committee

- Manage Security policies and advisories
- Managing Incident Responses
TODOs

- Consider compliance, auditing requirements
- Zero Trust enablement
- Observability & Monitoring
- 5G specific threat vectors
- Identities & Entitlements management
- Performing Threat Modelling