Edge/IoT/5G Security
AccuKnox Introduction for Akraino community
Briefly about AccuKnox

- Zero Trust Enterprise CNAPP
- Lead maintainer for CNCF Project **KubeArmor**
  - First preemptive mitigation solution leveraging BPF-LSM
  - KubeArmor/k8tls
    - Check TLS/Certs best practices
    - FIPS 140-3, NIST 800-52 best practices compliance
- Member of **SE-RAN**
  - NSF-DOD project
- TSC Member & SIG-Security Chair for LFN Nephio
- TSC member for LF Edge Open Horizon
Briefly about KubeArmor

- Leverages LSMs
  - (BPF-LSM, AppArmor, SELinux) for workload hardening
- Preemptive Mitigation
Our work with Nephio Community

- Executing SIG-Security charter with the community
- Currently working with Nephio O-RAN WG
  - Identity Provisioning for Nephio Workload Clusters
  - Identity provisioning for SMO/O-Cloud entities
- Security deliverables for Nephio R3 release
Nimbus: Intent Driven Security Automation

- User specifies the security intent and the k8s operator figures out the best implementation method available given the deployment
- Security Intents store
- Nimbus k8s operator
Our work with LF Edge Open Horizon

- **Management Hub**: 192.168.1.49
  - System processes
  - Anax agent
  - other processes

- **Docker Containers**
  - agbot
  - sdo-owner-services
  - css-api
  - Vault
  - exchange-api
  - postgres
  - mongo

- **Edge**: 192.168.1.46
  - Anax agent
  - hzn cli
  - karmor cli

- **Kubernetes Cluster**

- **Process**
  - TCP, UDP, Raw
    - curl
    - python3.10
    - busybox
    - S6-svscan
    - S6-supervise
    - S6-svlisten1
    - ...
  - /config/
    - home-assistant_v2.db

- **Network**
  - TCP, UDP, Raw
    - protocol
    - Ingress, egress

- **File**
  - dir: /etc/
    - fromSource
    - /bin/bash
    - path: /usr/bin/mysql
  - matchDirectories:
    - - dir: /sbin/
      - readOnly: true

- **Browser**

- **✅** App Behaviour Visibility & Network Graph
- **✅** Workload Hardening based on Standard best practices
- **✅** Zero Trust Least Permissive Posture
Demonstrate 5G SBP Use Case
- Remote Attestation Use Case
- IoT Device Security and Authn, where SEDIMENT RA Verifier and Relying Party are containerized and deployed with KubeArmor providing visibility and protection policies.
Summary & Questions

- Why are we here?
- Any other similar efforts in LF Edge/Akraino in security?
- Community testbed efforts?
References

- NSF & DOD
  - 5gsec.com
  - 5G Security Award to AccuKnox
  - Projects
    - Nimbus
    - Security Blueprints/Intents store
- LF Edge Open Horizon
  - Integration details, service integration
  - Runtime Security Demo details
- 5G SBP work