Digital Forensics and Incident Response (DFIR) in O-RAN Implementations

Henrik Wittemeier (TH Köln)
Thomas Karl (PROCYDE GmbH)

Technology
Arts Sciences
TH Köln

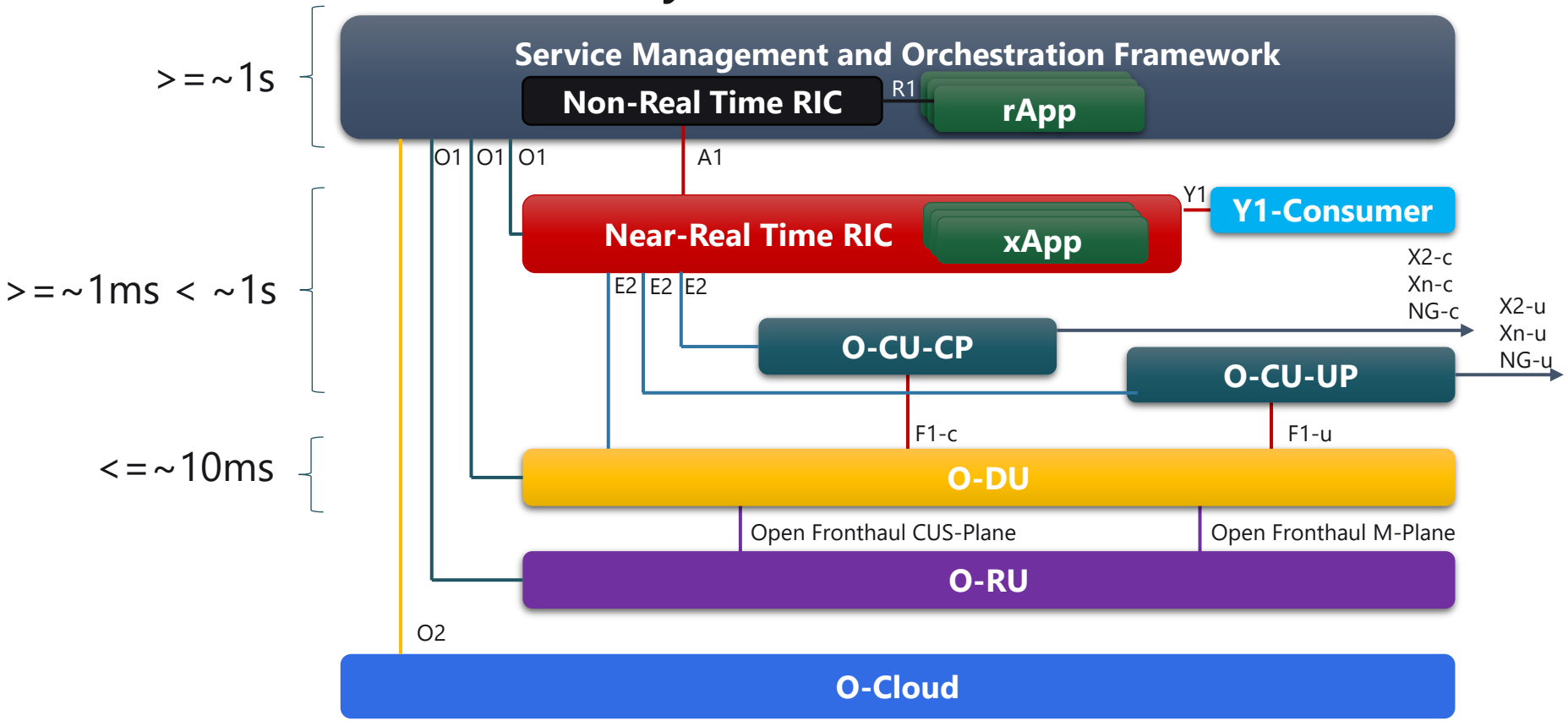
PROCYDE

Bundesamt
für Sicherheit in der
Informationstechnik

28. VDE/ITG Fachtagung Mobilkommunikation
15. - 16. Mai 2024, Osnabrück

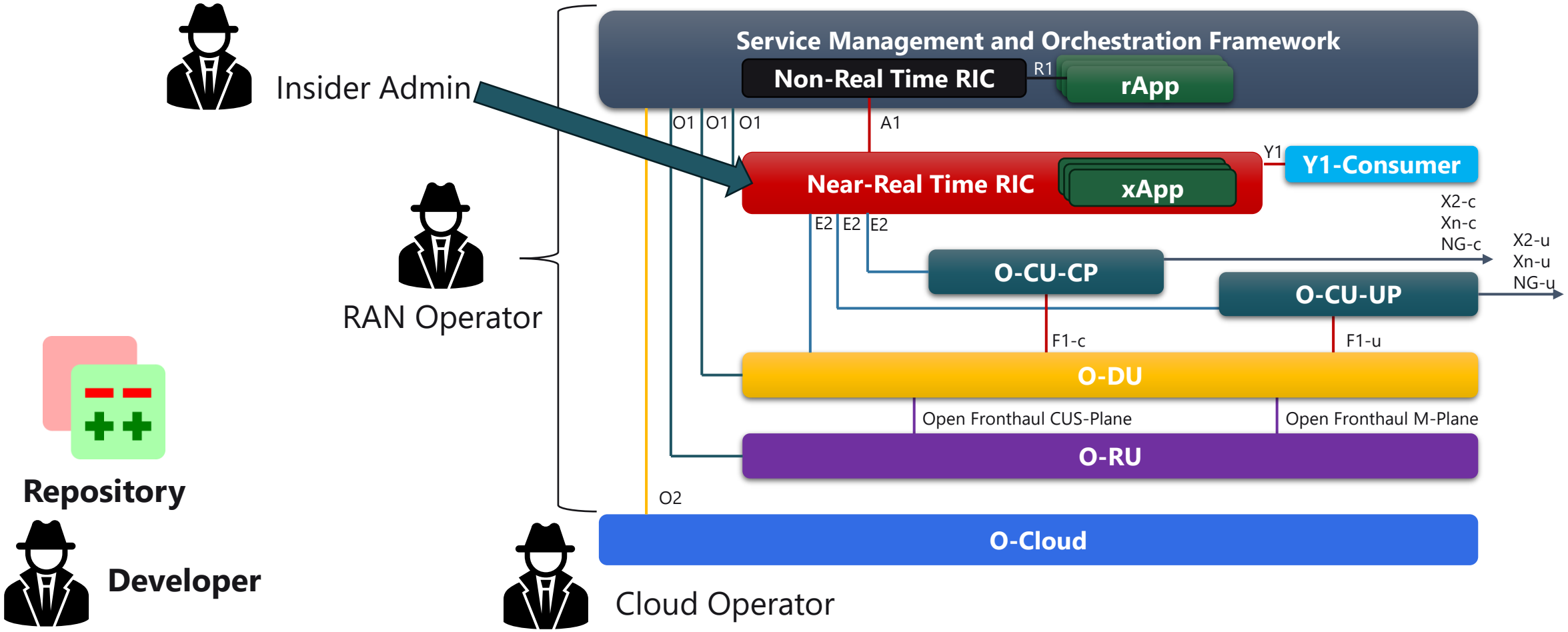
O-RAN Architecture and Implementation

O-RAN Software Community I-Release Architecture



O-RAN Architecture and Implementation

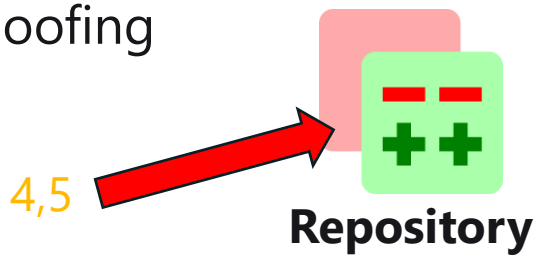
Central Threat Actors

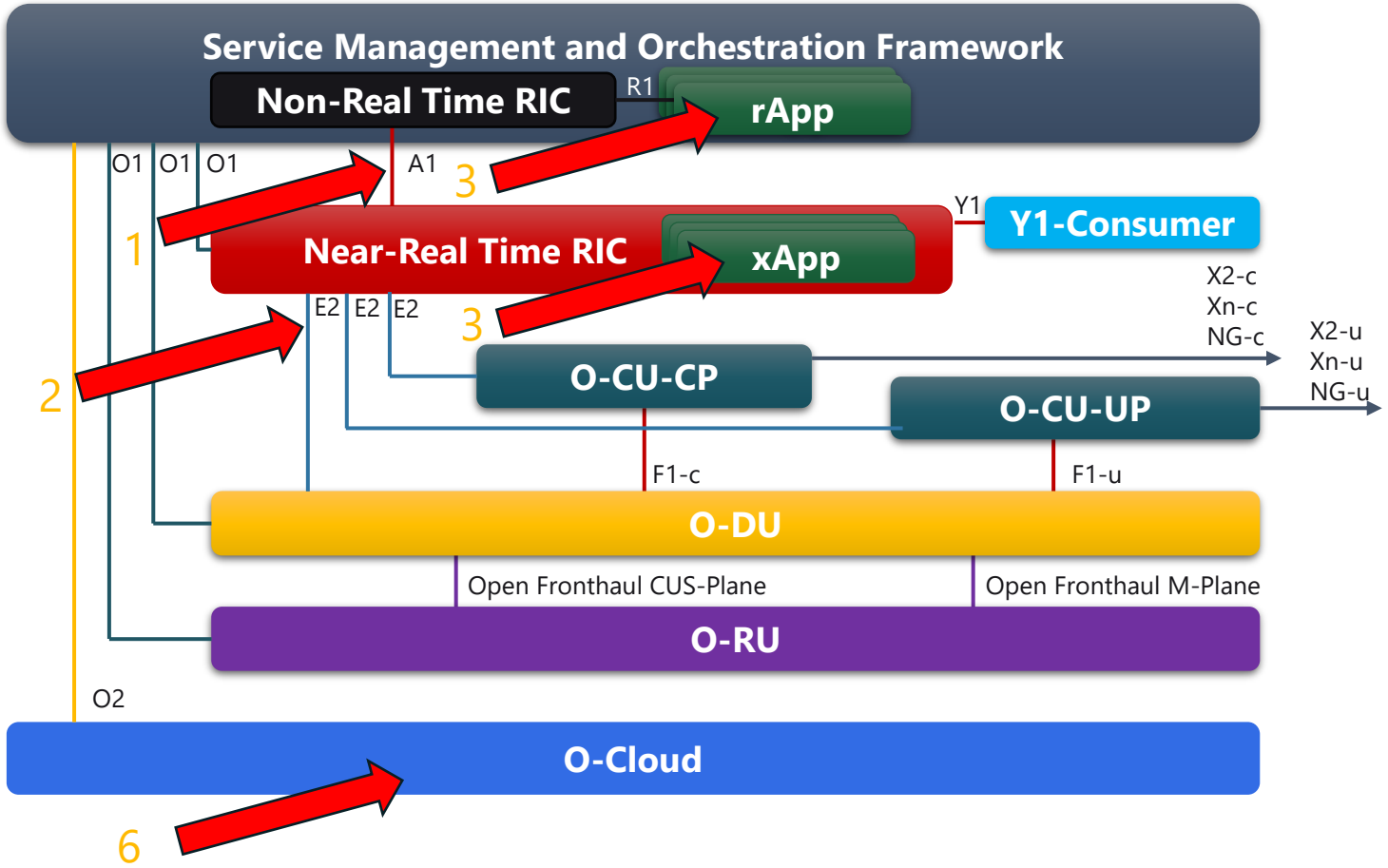


O-RAN Architecture and Implementation

Identified Threats

1. Unencrypted A1 Interface
2. Unencrypted E2 Interface
3. No Principle of least privilege
4. Hardcoded Credentials and Certificates
5. Insufficient merge restrictions
6. ARP spoofing





O-RAN Architecture and Implementation

Identified Threats

Component	Vulnerability	Reference	Source
E2 Interface	Unencrypted E2AP	CWE 284	O-RAN WG11
A1 Interface	Unencrypted HTTP	CWE 284	O-RAN WG11
A1 Interface	Unauthenticated A1-Interface	CWE 284	O-RAN WG11
R1 Interface	No Principle of least privilege	CWE 269	O-RAN WG11
Near-RT RIC	Outdated Kubernetes Version	CWE 1104	O-RAN WG11
Non-RT RIC repository	Hardcoded Credentials and Certificates	CWE 798	5G-FORAN
Non-RT RIC repository	Insufficient merge restrictions		5G-FORAN
Internal network (K8s)	ARP spoofing	CVE 1999-0667	NVD

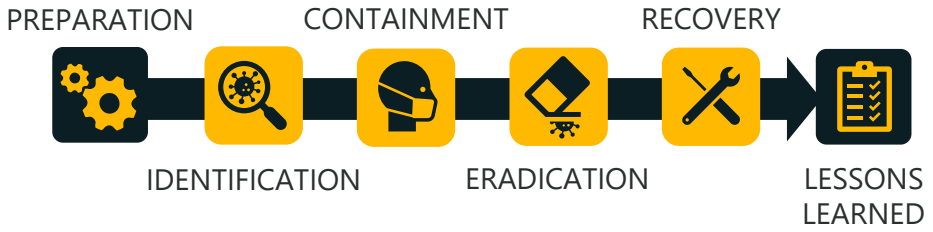
Digital Forensics and Incident Response in Open RAN

Visibility and Security Observability

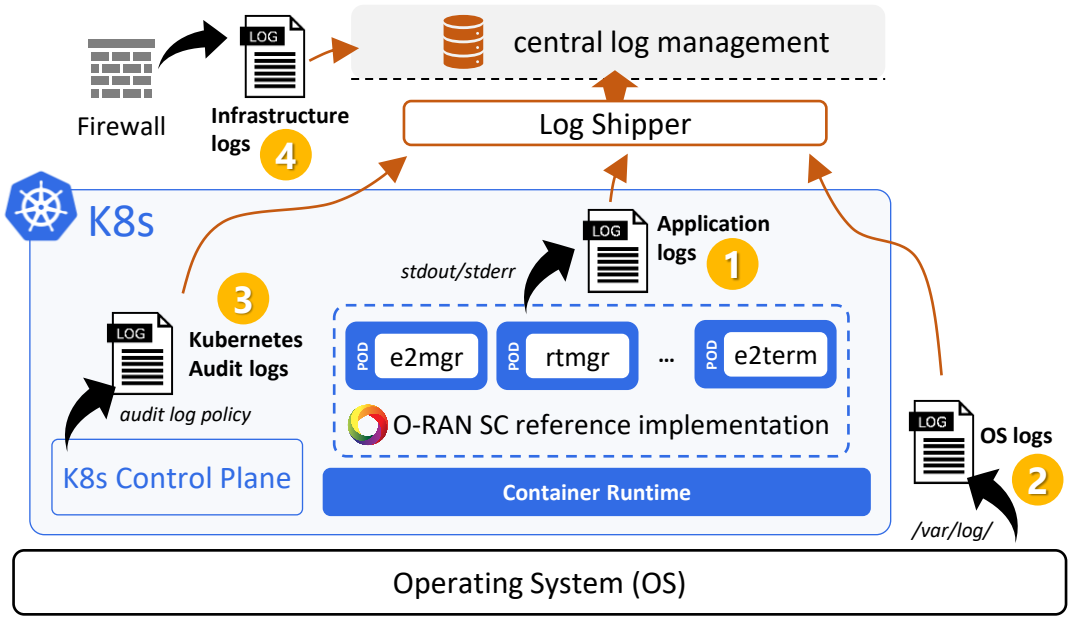
- During security incidents, the CSIRT[1)] needs to understand:

  what happened, where and when?

- Incident Response process[2)]



- Visibility by different log sources in O-RAN SC reference implementation:

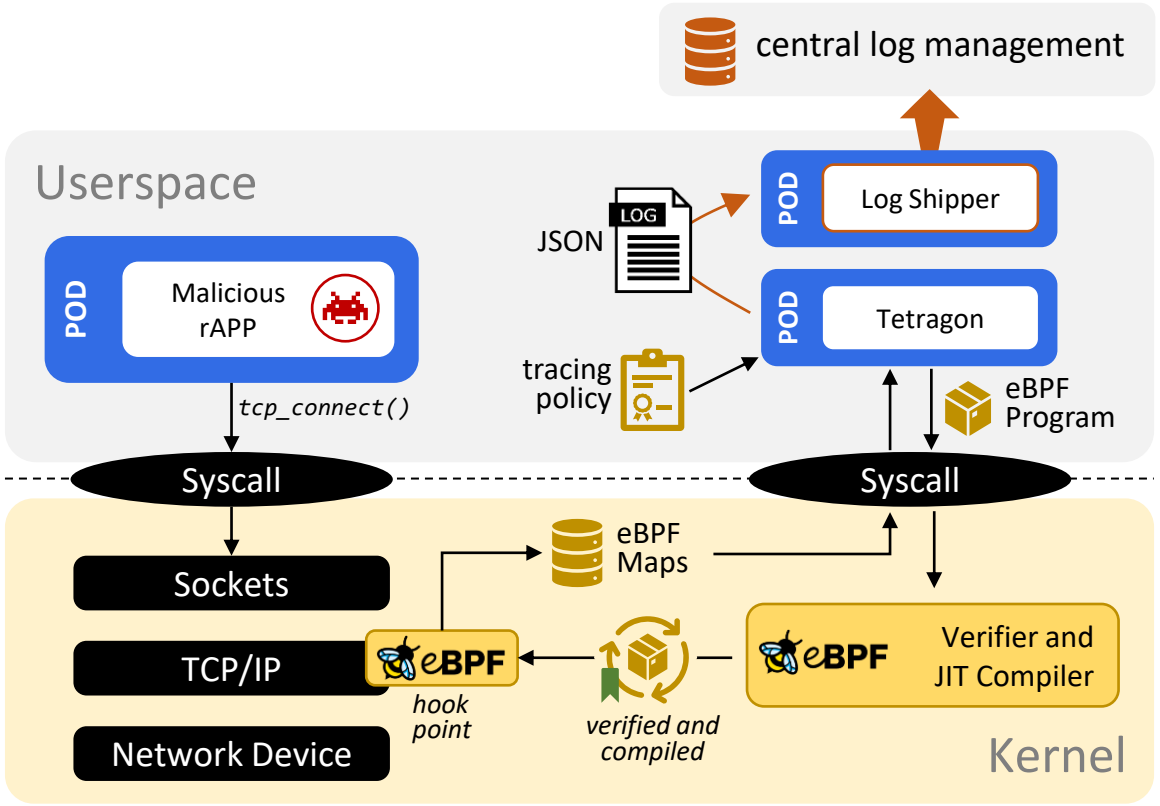


1) Computer Security Incident Response Team (CSIRT)
2) SANS 6-step IR process

Digital Forensics and Incident Response in Open RAN

Visibility and Security Observability

- Extended Berkeley Packet Filter (eBPF) adds additional security observability capabilities
  - From Kubernetes host to specific container
  - Beyond traditional packet filters: Read/write (sensitive) files on filesystem, mount filesystem from container, inter-process communication, etc.
- Security tools like Tetragon or Falco[1)] offer Kubernetes-aware event collection in near real time



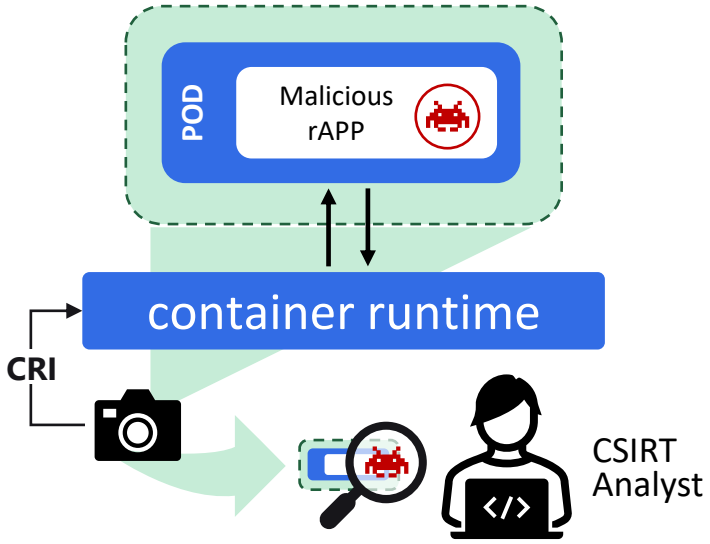
1) https://tetragon.io/ and https://falco.org/

Digital Forensics and Incident Response in Open RAN

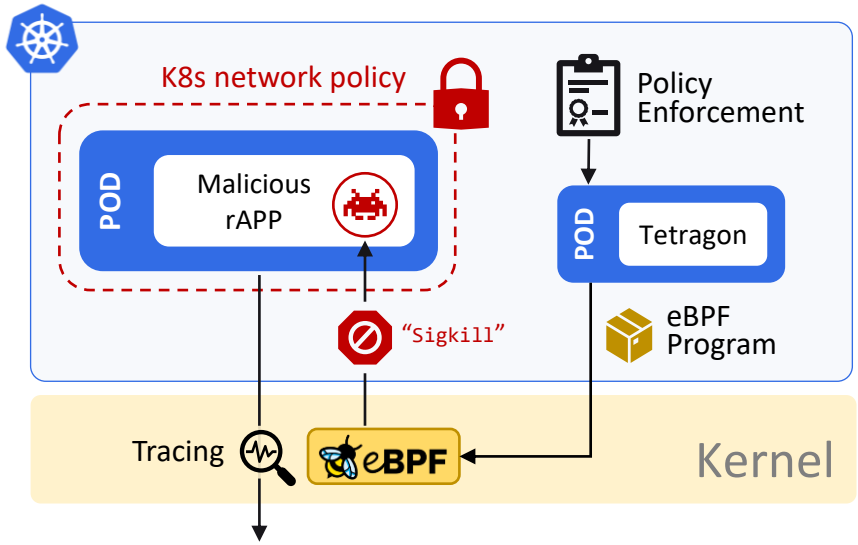
Incident Scoping and Response Measures

- After a reasonable initial suspicion, further evidence collection and the initiation of response measures must be initiated quickly:

Forensic Container Checkpointing



Containment/Eradication Measures



Vielen Dank für Ihre Aufmerksamkeit

Henrik Wittemeier
Technische Hochschule Köln

Email: henrik.wittemeier@th-koeln.de

Thomas Karl
PROCYDE GmbH

Email: thomas.karl@procyde.com
Phone: +49 2682 50696 03