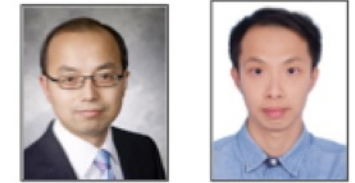




SRI International



Ohio State University



AccuKnox, Inc.



# Security Enhanced Open-RANs




## For Mission Critical 5G Networks

Phillip.Porras@sri.com



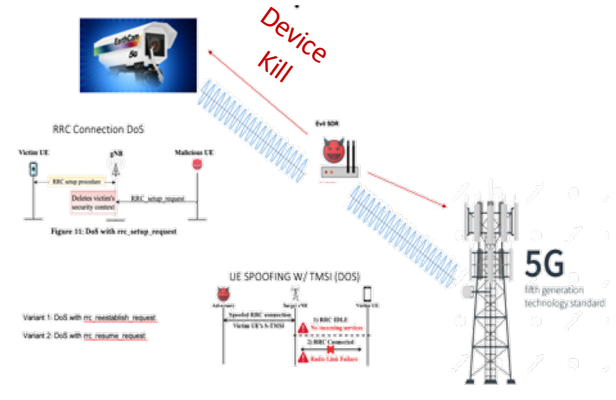
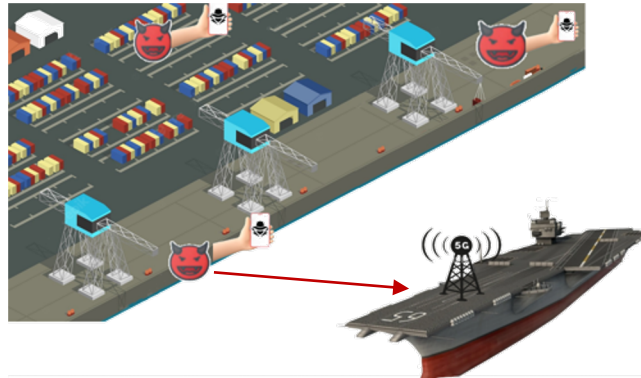
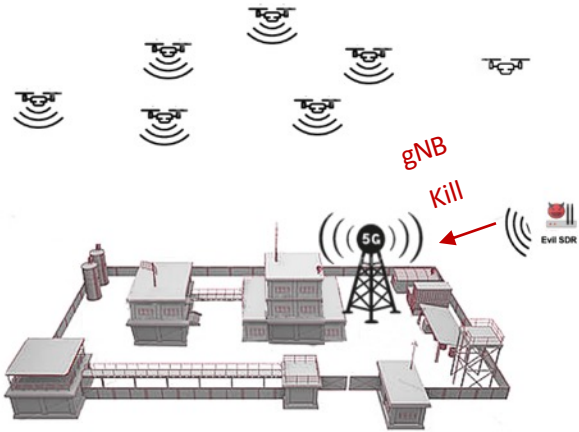
# Overview

## -RAN Compliant Software Security Services

Our Tech	What it is	Who Cares	Platforms	Threat Coverage	
<b>5G-L3 IDS</b>	First 5G-IDS to combat Layer-3 Attacks	Mission Critical 5G-Operators  & 5G Open-Source Stakeholders	 OAI srsRAN	Sophisticated SDR Savvy Adversaries	SE-RAN Future G
<b>5G-KubeArmor</b>	SD-RAN runtime security enforcement system			K8s / Cloud Exploits and Insiders	
<b>RILDefender</b>	SMS Exploit Prevention System	5G users who operate through hostile networks		SMS Exploits	Operating Through



# Layer-3 attacks are not new to 5G... but the ability to integrate a solution *IS*



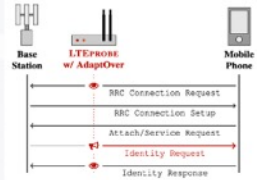
## WE HAVE IMPLEMENTED ADVERSARIAL MODELS IN RIAB!

- o **SigOver** LTE (USENIX Sec 19), **SigUnder** 5G (Wisec 21)
- o **AdaptOver** (MobiCom 21), **LTRACK** (USENIX Sec 22)
  - Apply overshadowing attacks for DoS, extracting IMSI

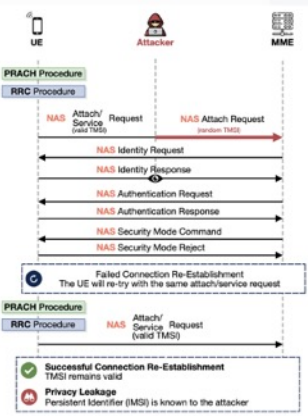
- o BTS resource depletion attack in the **LTEFuzz** paper

### LTRACK

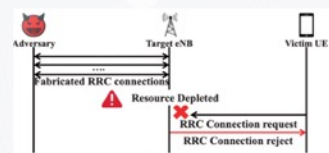
#### Downlink overshadowing



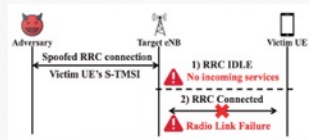
### ADAPTOVER UPLINK OVERTHROWING



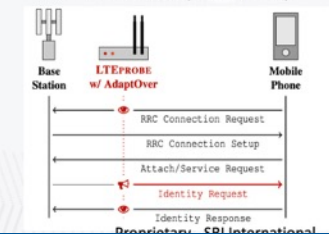
### RRC Connection DoS



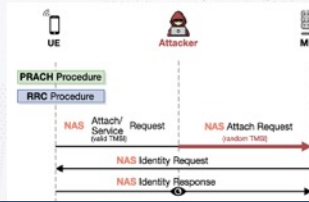
### UE SPOOFING W/ TMSI (DOS)



### IMSI EXTRACTOR (DOWNLINK)



### IMSI EXTRACTOR (UPLINK)



## Layer-3 Exploit Methods

## Impact

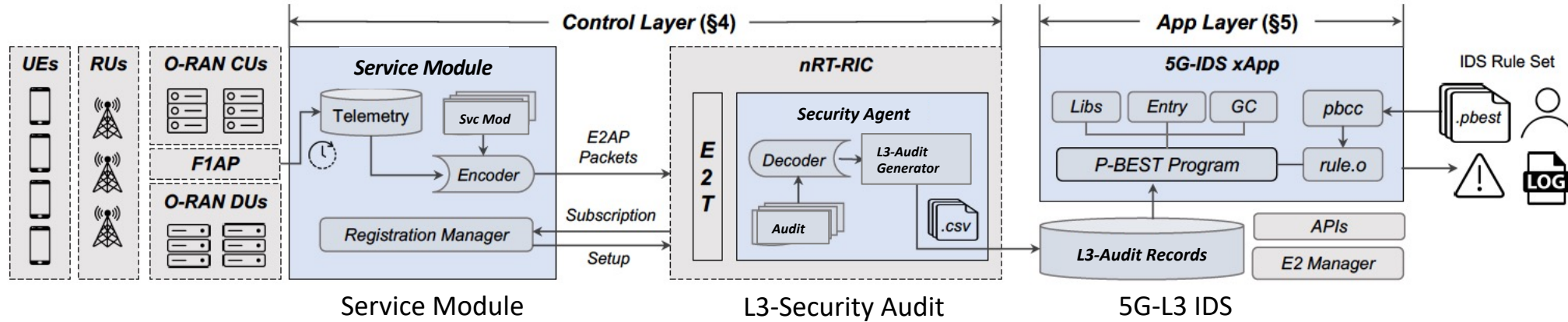
Blind Connection Flood	DoS
BTS DoS Resource Depletion	DoS
Re-establishment DoS	DoS
Resume Request DoS	DoS
Downlink IMSI Extractor	Geo-Track
Downlink IMEI Extractor	Geo-Track
Downlink TMSI Extractor	Geo-Track
SUCI Catcher Attack	Geo-Track
Uplink IMSI Extractor	Geo-Track
Signal Injection	Infiltration
Authentication Synchronization Failure	DoS
Downlink DoS Signal Infection	Downgrade
Null Cipher/Signature gNB complete	Downgrade
Null Cipher/Signature gNB reject	DoS
Uplink DoS using invalid MAC	DoS
Uplink Dos using blocked IMSI	DoS
Downlink DoS Signal Injection	DoS
Remote Deregistration	DoS



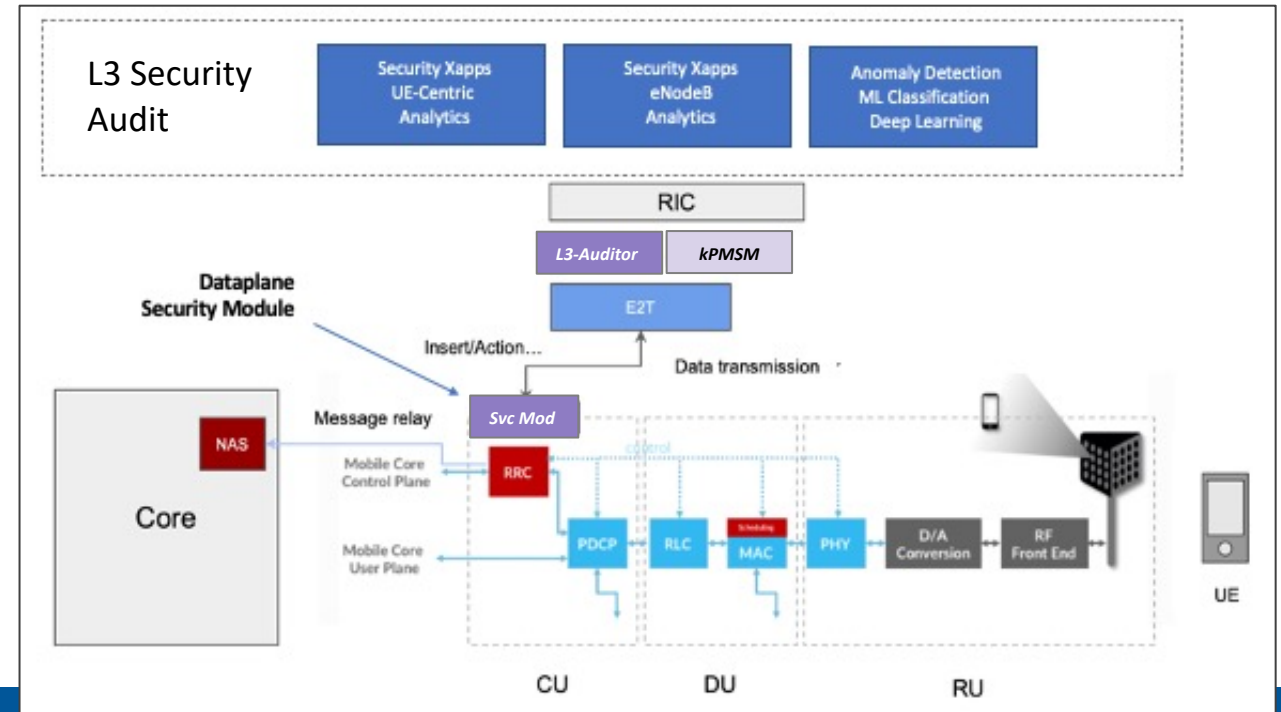
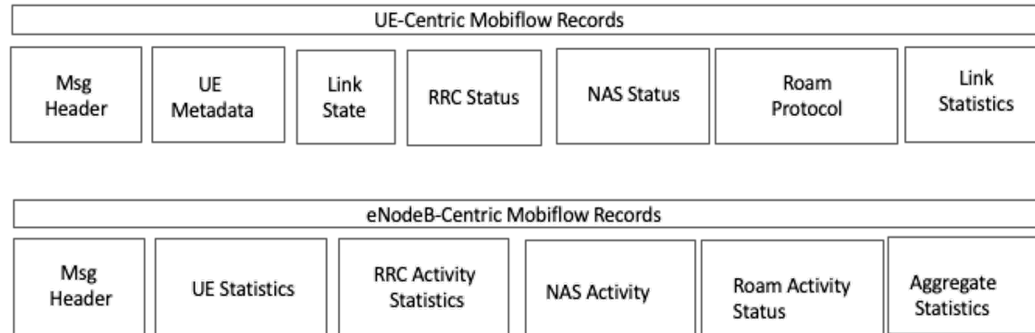
Sec.Com

For Mission Critical 5G Networks

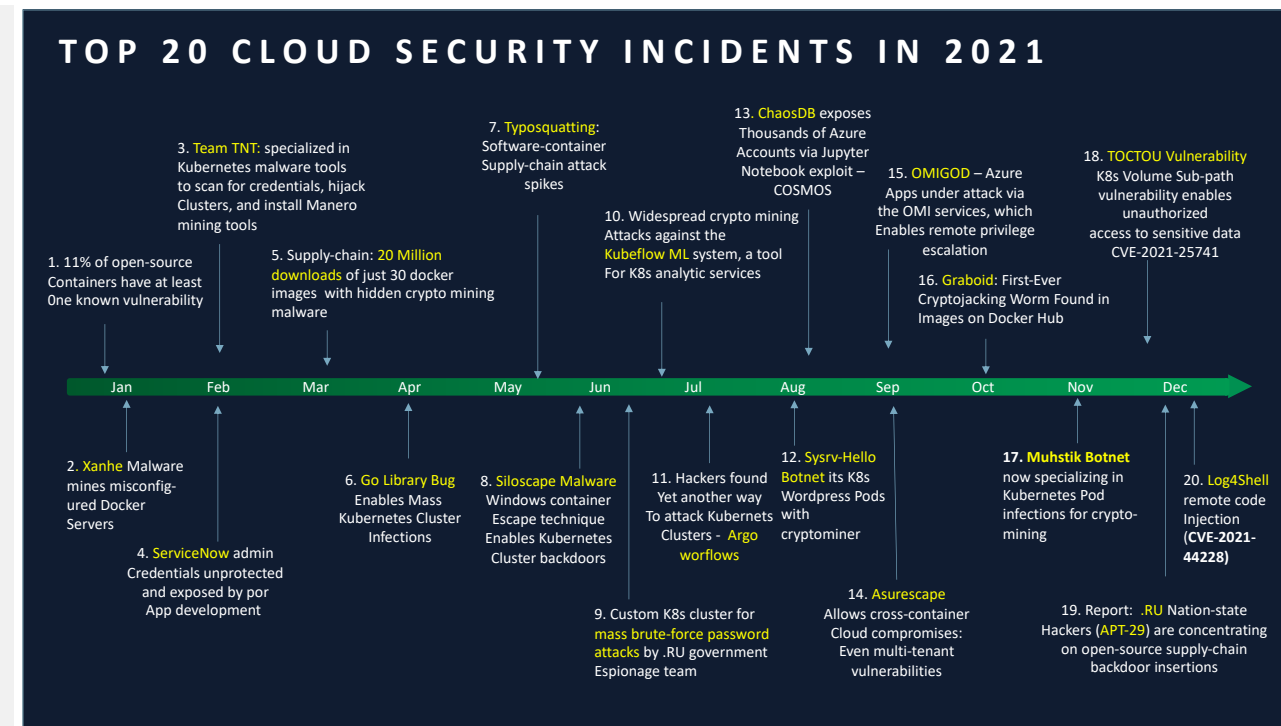
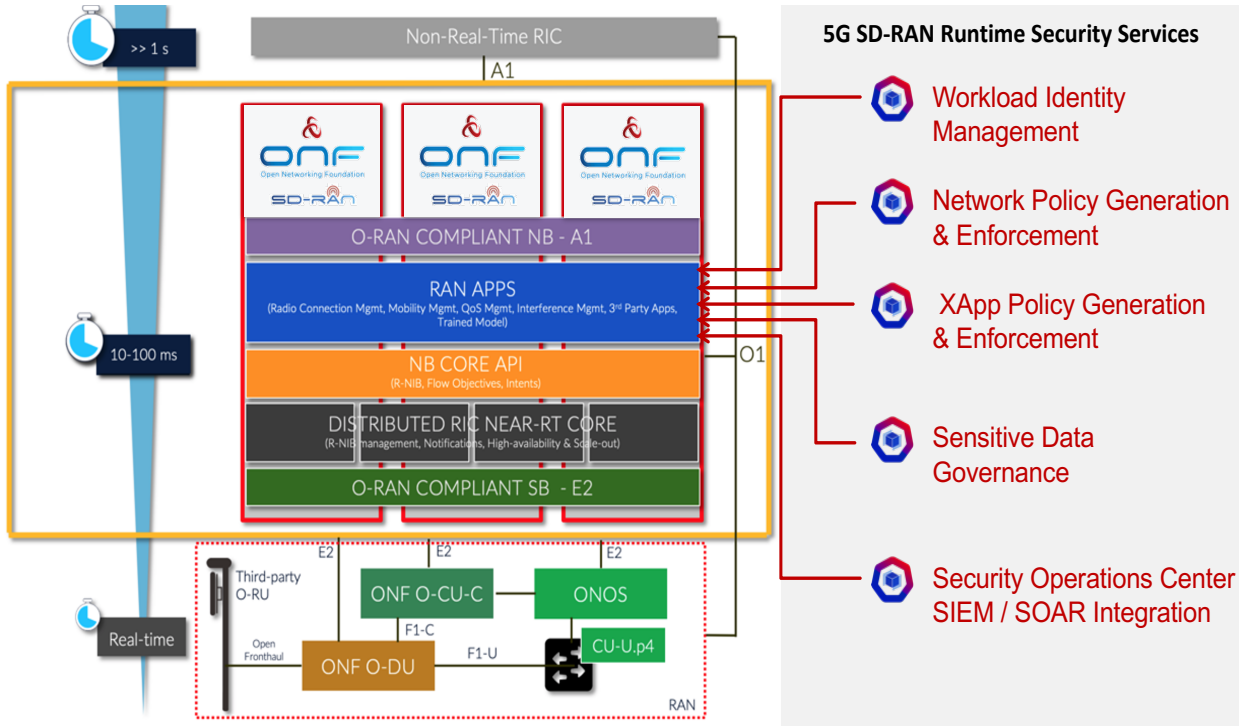
# 5G-L3 IDS - a xApp for Live Detection of Malicious SDRs



## L3 Security-Audit Definition



# 5G-KubeArmor - for 5G Control Plane Policy Enforcement



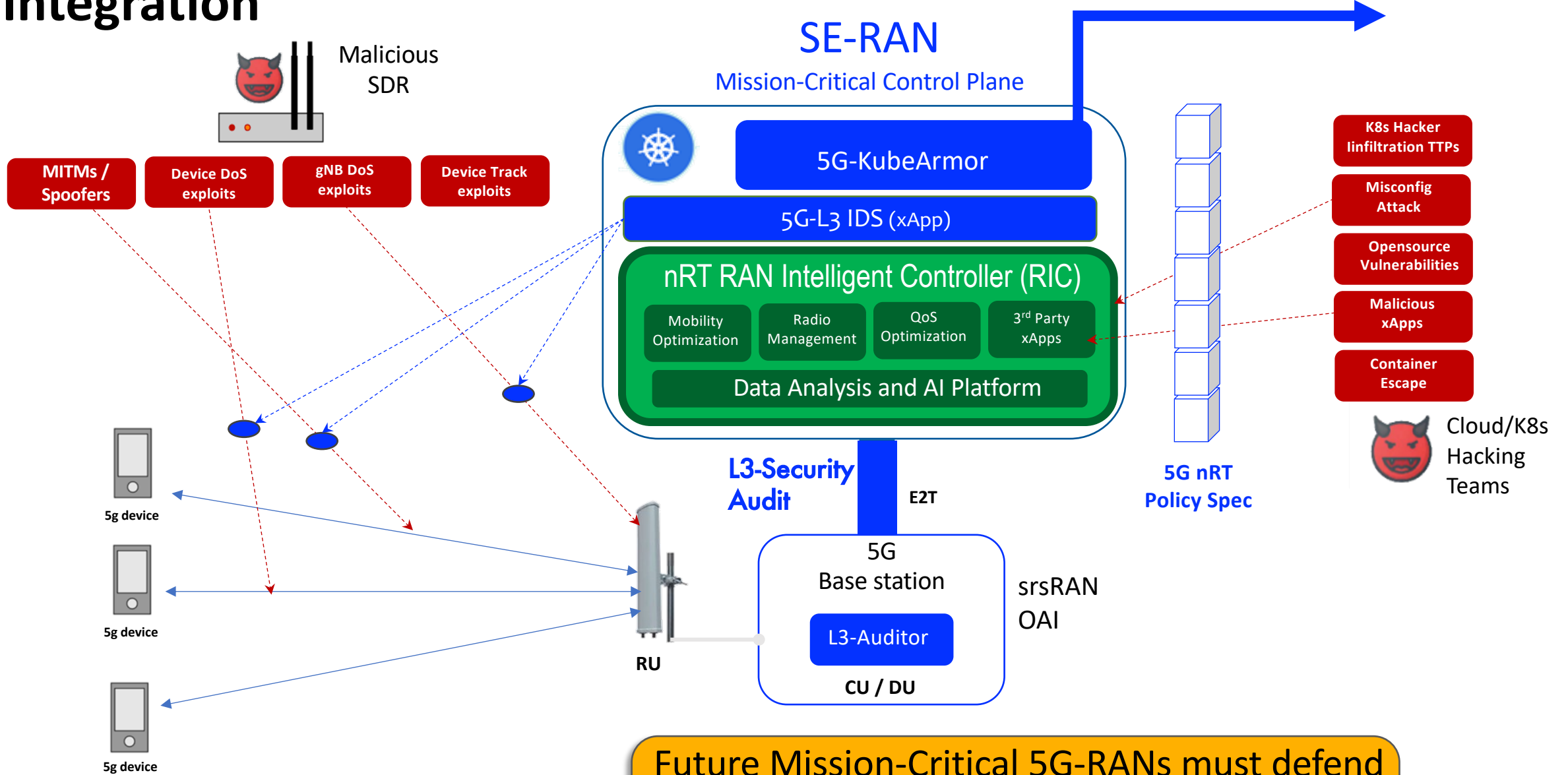
- An nRT-RIC customization for SD-RAN. Include auto-policy generation for xApp DevOps operations.
- 5G-KubeArmor will be based on the most modern Cloud Native, Open-Source led Cloud Security Platforms.



Sec.Com

For Mission Critical 5G Networks

# Integration



Future Mission-Critical 5G-RANs must defend their protocols, base stations, and control functions from sophisticated adversaries



Sec.Com

For Mission Critical 5G Networks

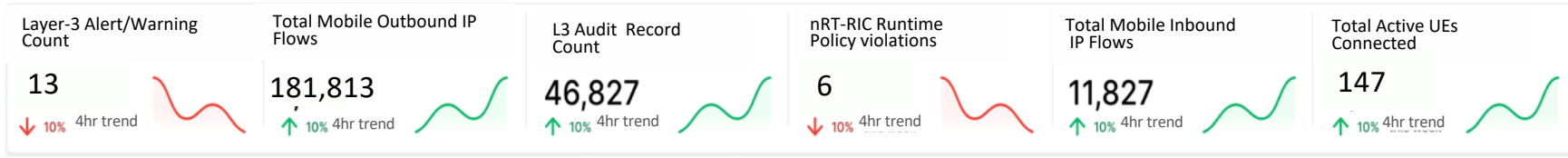
# Managing a Secure Open-RAN

5Gsec.Com

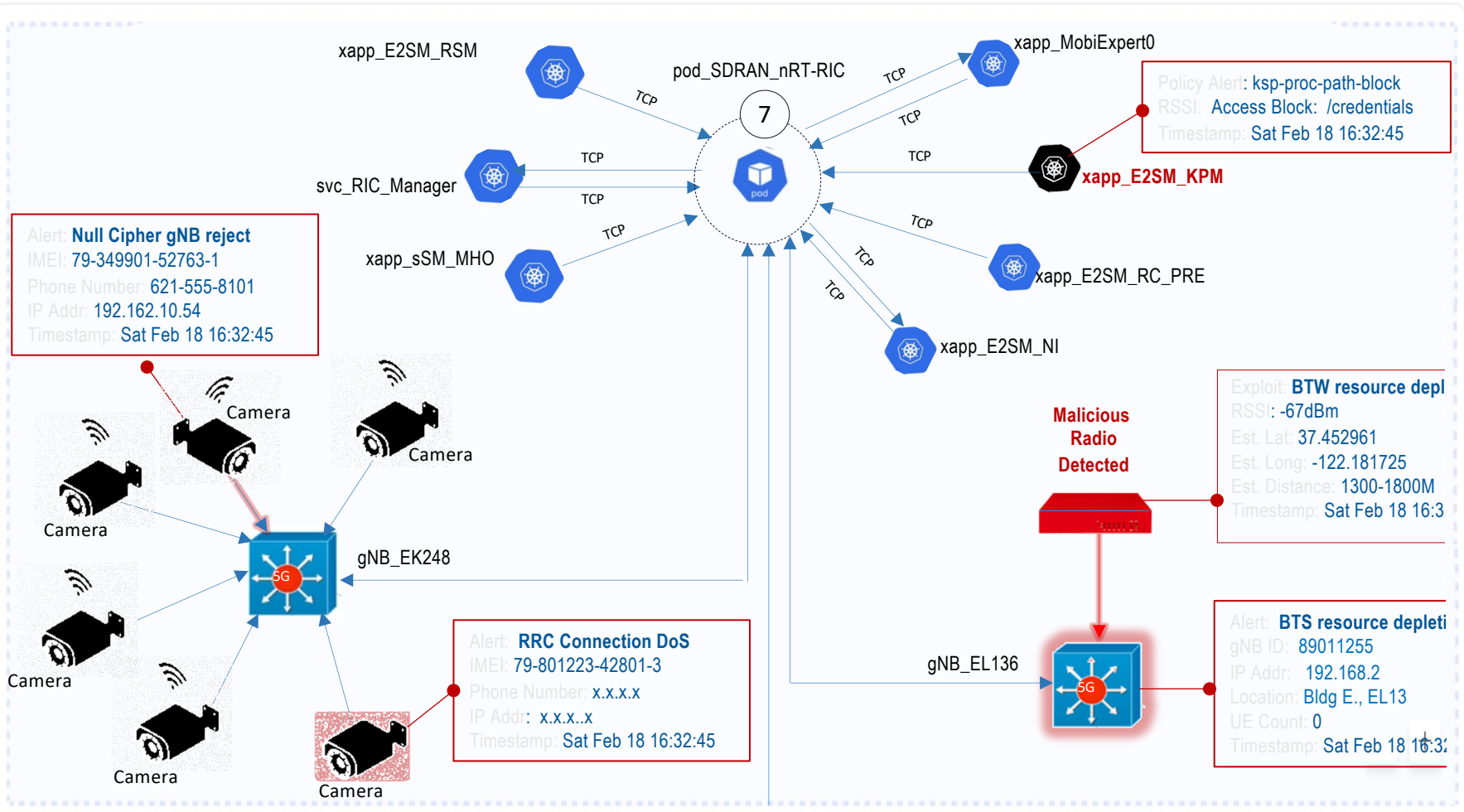
- Dashboard
- Inventory
- Issues
- Compliance
- Runtime Protection
- CWPP Dashboard
- App Behavior
- Policies
- Remediation
- Monitors / Logging
- Settings
- Logout

5G Security: *You cannot secure what you cannot see.*

List Graph



Network Observability Services: ● 5G-KubeArmor ● 5G-L3 IDS ● L3 Auditor



- ## 5G-SPM
- (Security Posture Management)
- Configuration Validation
  - Least-permissive xApp/RIC policy generation
  - Compliance Enforcement
  - Runtime Monitoring
  - Threat Response
  - Audit Governance

# Learn More

## 5GSec.Com

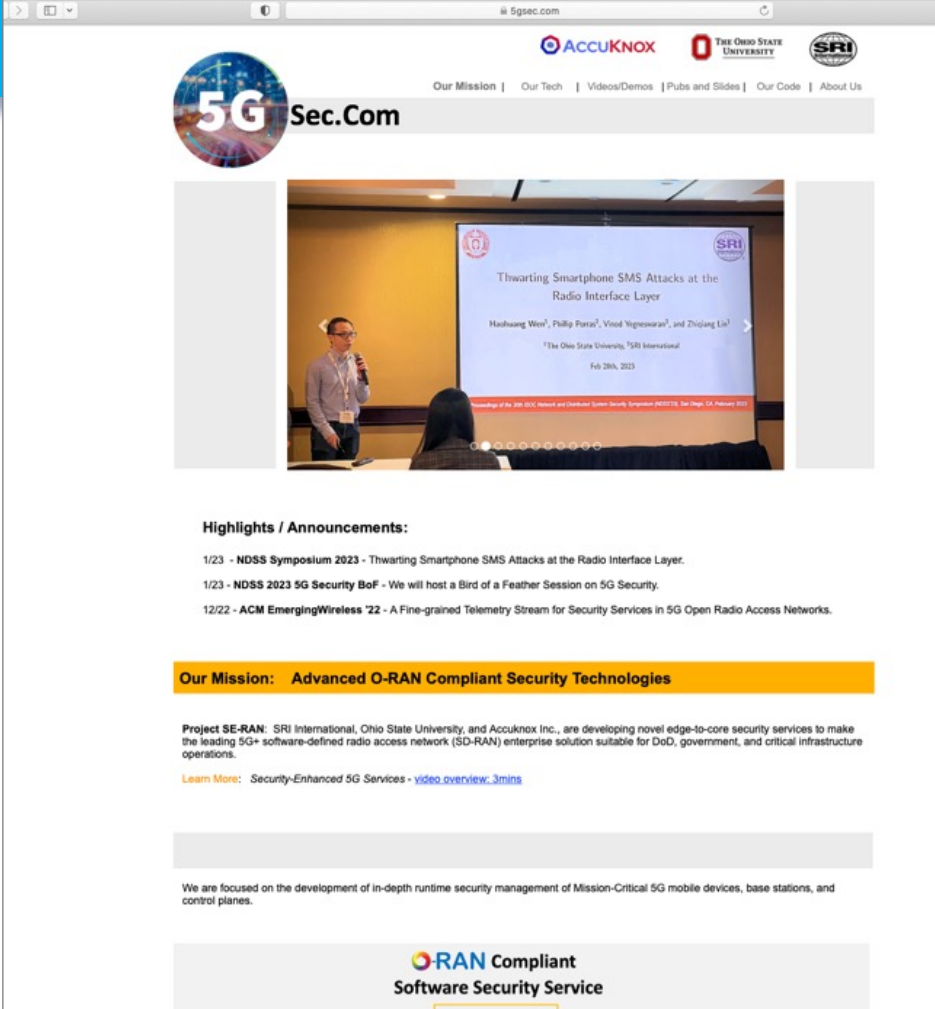
(our papers, slides, demos, and code)

RILDefender

"Thwarting smartphone SMS attacks at the Radio Interface Layer," in Proceeding of the ISOC Network and Distributed System Security Symposium (NDSS), San Diego, CA, U.S.A., February 2023.

5G-IDS

"A fine-grained telemetry stream for security services in 5G open radio access networks," in Proceedings of the 1st International Workshop on Emerging Topics in Wireless (EmergingWireless '22).



The screenshot shows the 5GSec.Com website. At the top, there are logos for ACCUKNOX, THE OHIO STATE UNIVERSITY, and SRI. Below the logos is a navigation menu with links: Our Mission | Our Tech | Videos/Demos | Pubs and Slides | Our Code | About Us. The main content area features a large image of a presentation slide. The slide title is "Thwarting Smartphone SMS Attacks at the Radio Interface Layer". Below the title, the authors are listed: "Haochang Weng<sup>1</sup>, Philip Porra<sup>2</sup>, Vinod Vignেশwaran<sup>3</sup>, and Zhijiang Lin<sup>3</sup>". The affiliations are "1The Ohio State University, 2SRI International, 3The Ohio State University". The date is "Feb 28th, 2023". Below the image, there is a "Highlights / Announcements:" section with three items: "1/23 - NDSS Symposium 2023 - Thwarting Smartphone SMS Attacks at the Radio Interface Layer.", "1/23 - NDSS 2023 5G Security BoF - We will host a Bird of a Feather Session on 5G Security.", and "12/22 - ACM EmergingWireless '22 - A Fine-grained Telemetry Stream for Security Services in 5G Open Radio Access Networks.". Below this is a yellow banner with the text "Our Mission: Advanced O-RAN Compliant Security Technologies". At the bottom, there is a section for "Project SE-RAN" which states: "SRI International, Ohio State University, and Accuknox Inc., are developing novel edge-to-core security services to make the leading 5G+ software-defined radio access network (SD-RAN) enterprise solution suitable for DoD, government, and critical infrastructure operations." and a link "Learn More: Security-Enhanced 5G Services - video overview\_3mins". At the very bottom, there is a logo for "O-RAN Compliant Software Security Service".



5GSec.Com

For Mission Critical 5G Networks