Presentation to LFN Developer & Testing Forum

Security Call Data Records (SCDR) Use Case development

13-16 February 2023 – Virtual Conference

David Armbrust – MITRE

darmbrust@mitre.org

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Agenda ~20 min presentation with 5 min Q&A/feedback

- SCDR refresher
  - Security roles of DCAE, NWDAF, and SCDR - Differentiated Security Focus in network slicing
  - Security Call Data Record – Desired artifacts
- Security Use cases enabled by SCDR
  - Compatible with 3GPP specifications and architecture
  - Security use cases leverage physical and logical properties to detect anomalies
  - Roles of network providers and analytics for visibility and anomalous NS behavior detection
- Summary of benefits
  - Mutual benefits to Carriers, CSPs, and Enterprise subscribers

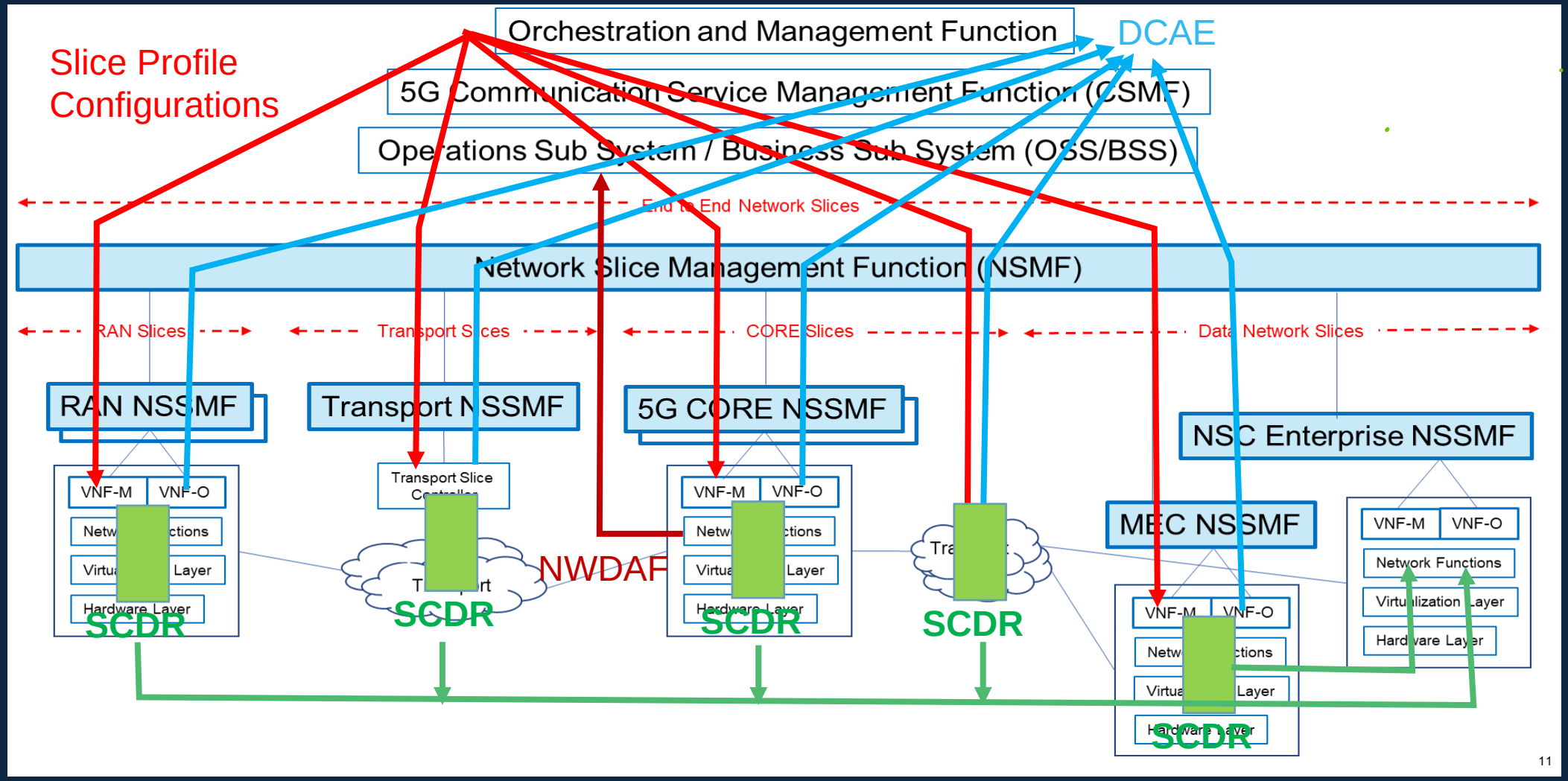
MITRE

Overview of SCDR

Security Call Data Record

- 5G Network Slicing (NS) will be a key enabler for companies and enterprise verticals.
- Therefore, Network Slice enterprise Consumers (NSC) will demand *security visibility* and *operational transparency* for every NS instantiation.
- Enhanced security for enterprise verticals (ex. financial, manufacturing, government, etc.) can be achieved by combining operational *data from network slices* and *knowledge from the enterprise*.
- MNOs cannot access internal enterprise knowledge to use this information in MNO security analytics; however, the enterprise can and should receive evidence about the MNO's security posture and operations concerning their purchased network slice instantiation.
- Security Call Data Record (SCDR) is a framework to make this MNO and CSP end-to-end data available and make possible the detection of nuanced and advanced persistent threats using tailored enterprise analytics for assessing their own network slice behaviors.

Security focus of DCAE, NWDAF, and SCDR



SCDR security context – record details (preliminary)

Subscriber Network Slice Profile configurations →

PLMNs and CSPs Software Bill of Materials (SBOMs) →

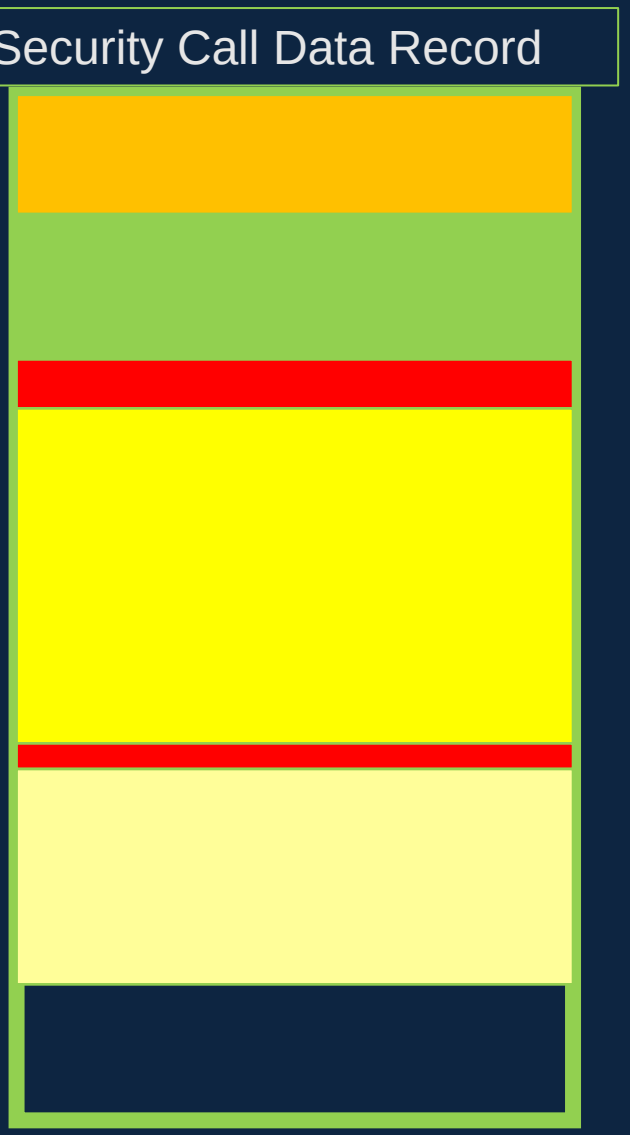
PLMNs and CSPs – Security Posture / Versions / Patch History →

Network Slice UE Connection attributes, etc. →
- Admitted connections
- Dynamic Changes to configurations

CSP detected Network Slice security anomalies →

Network slice operational measurements and statistics →

Customization - TBD selected attributes →
specific to subscriber's cyber threats



MITRE

Key analytic benefits of SCDR framework

Enterprise verticals can use information exposed by multi-domain SCDR records to enhance their security by identifying suspicious behavior in their network slice.

- Cross Correlating artifacts from different CSPs' SCDRs exposes inconsistencies across the end-to-end Network slice.
- Correlating Enterprise private facts & knowledge against current artifacts in SCDRs utilizes dynamic information not publicity available nor predictable limiting malicious options
- Historical SCDRs allows tracking NS Configuration changes over time
- Enterprise partners can provide SCDRs enabling a stronger security collective among enterprise verticals, partners, vendors, suppliers, and their customers
- Mutual security benefit for Carriers, MNOs, CSPs, with their Enterprise consumers. Together combining each domains unique knowledge to detect and track nuanced malicious behaviors and persistent threats in network slices.

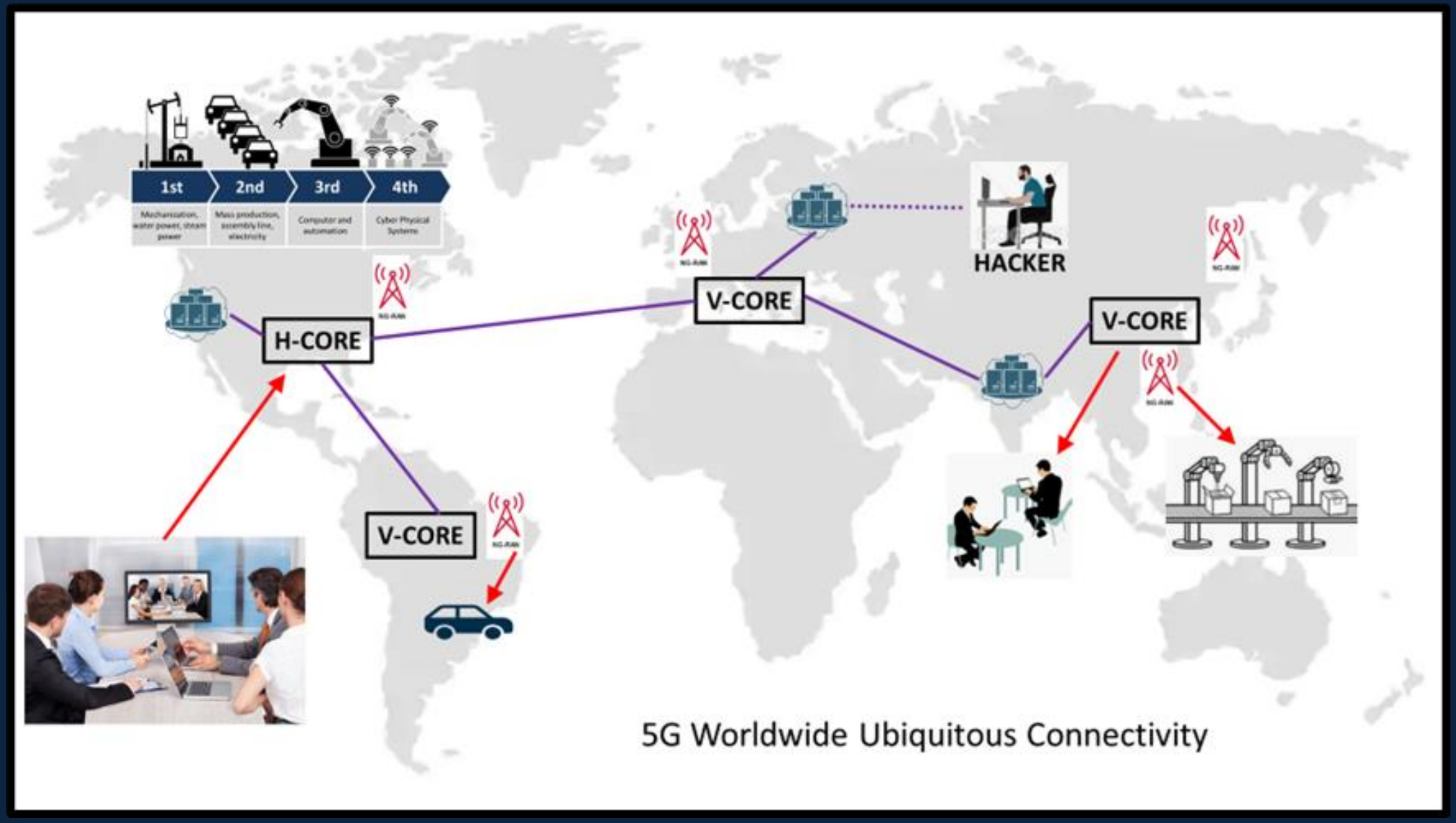
MITRE

Security use cases enabled by SCDR

-- detecting and resolving anomalies --

MITRE

5G global enterprise network slice(s)



Security Use Cases

Security use cases leverage the physical properties (time, latency, connection location, distance) and logical properties (access tokens, configuration profiles, security options) to achieve visibility on *NS behaviors* including isolation, status of optional security settings, critical configurations, dynamic connectivity, etc.

- ❑ 5G enterprise asset(s) - detect geographic *location* inconsistencies?
- ❑ 5G distributed protocols - detect anomalous *latency* issues?
- ❑ 5G NS – detect *Isolation* issues?
- ❑ 5G CSP – detect possible NS *routing and connections* manipulation?
- ❑ 5G protocols - detect possible *race conditions* on a distributed network?

MITRE

Security Use Cases - detect geographic *location* inconsistencies

Security issue: Artifacts from multiple SCDRs are inconsistent for enterprise's UE 5G NS attachments, used to join a network slice from MNO authorized but suspicious 5G connection locations. The analytics will expose anomalous connectivity in the network slice, inconsistent with enterprise knowledge, indicating malicious activity from potentially compromised credentials

Artifacts in SCDRs

For UE registration events, SCDR will collect and record the timestamp, NS identifier (NS ID), and New Radio Cell Global Identifier (NCGI) (consisting of Mobile Country Code (MCC), Mobile Network Code (MNC), and NR Cell ID).

- ❑ 3GPP 5G Network Function (NF) information exposure APIs.
- ❑ Artifacts collected via NWDAF (TS23.288) diagnostic subscriptions in the 5G CORE(s).

MITRE

Security Use Cases - detect anomalous ***latency*** issues

SCDRs would contain artifact messages with time-stamped headers to resolutions of a microsecond from the ONAP DCAE diagnostics

Security Issue: 5G distributed connections across known physical distances

- Whole class of malicious spoofing activities on connection setups by returning a response before the legitimate endpoint responds, which can produce undesired effects such as man-in-the-middle hi-jacking, redirects, etc.
  - Violates the physics of minimum response time possible from distant legitimate endpoint locations.
- Whole class of obfuscating connection location endpoints through TOR produces detectable longer latencies on bi-directional communications
  - Exceeds expected and previously measured response times from endpoint locations

MITRE

Security Use Cases – detect weakened *isolation issues*

Security issue: malicious privilege escalation of network functions servicing an enterprise network slice in violation of NS profile configurations

- Rogue VNFs get access to enterprise network slice
- NS crosstalk through a shared VNF resource(s) between multiple slices
- Access tokens are manipulated for malicious privilege escalation

3GPP defines three types of access tokens for NF service producer(s) – TR33.318 Security Aspects of NS enhancement – TS23-501 System Architecture for 5GS – Stage 2

- PLMN Level - Global access across all network slices
- Shared-slice level - Local access across a specific list of network slices
- slice-specific level - Singular access belonging to a S-NSSAI

MITRE

Security Use Cases – detect NS *routing and connections* manipulation

Security issue: Network Operators reroute connections to support mobility and CSPs undergoing congestion reroute connections to support mobility and balance loads. Compromised NFs in either case can possibly manipulate connections for data exfiltration purposes

- SCDR would contain artifacts of rerouting connections dynamically

- See TS23.502 Procedures for the 5G System (5GS) – Stage 2
  - Handover of PDU session between 3GPP and non-3GPP access
  - Handover between EPS and 5GC-N3IWF
  - Handover between EPC/ePDG and 5GS
- Variations on handovers include 9 non-roaming and 16 roaming 3GPP architectures with further variations on whether home routed or visiting local roaming data UPF breakout

MITRE

Security Use Cases – detect protocol *race conditions* on a distributed network

Security issue: protocol *race conditions* on a distributed network – due to message propagation delays from the MANO to the VNF functions at the distributed network boundary.

- Malicious actor in a compromised VNF does not terminate connections on command
  - Retrieves data in memory and exfils
- Ties up local resources and injects malicious payload into temporary open connections
- Malicious actor sends “connection terminated” message to MANO to restart connections that can be highjacked, or produce DOS effects

MITRE

Summary of SCDR benefits

SCDR Benefits

- SCDR enables enhanced security visibility and operational transparency for the enterprise vertical NS consumer
- SCDR enhances security for the Network Operators (NOPs) and Communications Service Providers (CSPs) from their enterprise subscriptions
  - Market differentiator (trust) for service providers and potential source of revenue
  - Leverages expertise sourced from (enterprise IT SOCs) experience, skill, and cyber analysis for anomaly detection, provided through enterprise feedback to NOPs and CSPs
- SCDR may help reduce overall telecom fraud (~ $33B US / year) by discovering and fixing vulnerabilities quicker through customer feedback

Questions? or Comments!

scdr-list@mitre.org

MITRE