**3GPP TSG-SA3 6G Workshop**

**Conference Calls, 6 - 7 August 2025**

**Source: T-Mobile**

**Title: 6G Work Tasks proposal**

**Document for: Approval**

**Agenda Item:**

# 1 Justification

The security capabilities within the SA3 specifications need to be updated so that the operators have greater visibility, control, alerting, and remediation of threats in the 6G system – including the study of using AI/ML for anomalous behaviour detection. Additionally, studies on M2M communications, network segmentation, micro-perimeters, IAM with dynamic access controls, and integration with the Operator Security Functions (e.g., SIEM/SOAR).

In a highly HW disaggregated network, the operators are challenged with the standardization of security specifications specific to these topics that make it harder to prevent, detect, and respond to the ever increasing number of cyber attacks.

# 2 Work Tasks

**WT#1:** Study on continuous security monitoring, logging, and alerting capabilities that should be integrated into the security architecture (embedded) for the integration with the Operator Security Function (Security Monitoring Entity).

* 1. Study of a unified observability plane with the Operator Security Function (aka Security Monitoring Entity for security monitoring integration across all domains of the 6G system (e.g., radio, core, management).
	2. Study of a unified observability plane integrated with the Operator Security Function (e.g., SIEM/SOAR) for all APIs, interfaces, and flows of the 6G system (radio, core, management).

**WT#2:** Study on IAM, including dynamic access control policies and the principle of least privilege.

* 1. Study the concept of a trust anchor, an implicitly trusted component, that is tamper proof for validating the authenticity of subscriber and UE identities that can be used for both SIM based and SIMless devices internally within the operator’s network and with 3rd parties.
	2. Study of the 6G system to support and enforce dynamic policy-based resource authentication and authorization before access is granted to the Access Stratum (UE), Non-Access Stratum (UE and NB), and SBI/SBA (UE, NB, NF, Non-3GPP).
	3. Study the integration of a policy enforcement capability using real-time context (e.g., location, device health, network behaviour) to dynamically grant/deny/revoke access to resources (e.g., NFs, slices).
	4. Study the ability for the 6G network to support service access restrictions including the ability to dynamically modify/revoke service access on a per user basis (e.g., UE).
	5. Study the ability for the 6G network to support service access restrictions including the ability to dynamically modify/revoke service access on a per Network Function basis.
	6. Study the ability for the 6G network to support continuous re-authentication and re-authorization of network functions and user equipment (UE) as needed, based on behavioral, contextual, and device posture metrics.
	7. Study the ability and methods for the 6G system to support short-lived access tokens and session-specific access to APIs to reduce the threats associated with long-lived tokens and API access grants.
	8. Study the methods that the 6G system can support dynamic security posture integration so source NFs can make the appropriate access/engagement decisions based upon the security posture of a target NF.
* For example, several key infrastructure vendors are already delivering a type of security score capability for each network function. This scoring can be based upon any identified vulnerabilities in the NF via a vulnerability scanner, security misconfigurations (alignment with SCAS 33.117 and any specific NF SCAS), etc. Much of this today is at the platform layer and not at the application layer. 3GPP should support a parallel type of scoring matrix for compliance with the SCAS so this can be used by the operators as well.
	1. Study the methods required so that each network slice could have its own policy set, auth/authz logic, telemetry, and visibility — reducing lateral movement, cross-slice traffic interception, etc.
* For example, network slices use shared infrastructure, do not have isolated resources, access control is coarse grained (OAuth2 and mTLS is used at the NF interface level and not per transaction or per data object, logging data is weak and not all state information is collectable and there are no robust mechanisms to prevent or audit communications between slices. PCF enforces QoS and access control via policies but enforcement is per-session and not per packet or behavior based.

**WT#3:** Study on Anomalous Behaviour Detection using AI/ML

* 1. Considering the recent Salt Typhoon attack, study the methods that the 6G network can use automated anomalous behavior detection for monitoring for non-human, human, and UE devices including real-time telemetry from all layers (radio to app), integrated with threat intelligence and SOC visibility.
* As a result of the ever increasing cyber attacks against the mobile networks, 3GPP needs to take a more proactive approach to embedding detection and defense capabilities into the NFs and RAN for the operators. Beyond Salt Typhoon, Sandworm, published ransomware attacks, etc. Per Nokia’s Threat Intelligence Report (June 2023 – June 2024), telecom networks have experienced a dramatic spike in **DDoS attacks**—from a few per day to over **100 per day** in many regions, especially **North America**, driven by automation and generative AI tools.
	1. Study the ability for the 6G network to support closed-loop threat mitigation within the security monitoring capabilities.
	2. Study the ability for the 6G network to leverage standard interfaces for a policy decisions that uses AI/ML driven insights and dynamic context for access decisions which will allow Behavior-Based policy enforcement.

**WT#4:** Study on the requirement to mandate PKI-based mutual authentication for machine-to-machine communications

* 1. Study the impacts of mandating that all M2M communications use mTLS with PKI for all SBA and RAN interfaces.

**WT#5:** Study on the further requirements pertaining to Network Segmentation and Micro-Perimeters

* 1. Study the ability for the 6G network to support native micro-segmentation across all domains (NFs, RAN, UEs, Slices, NPN, NTN, etc.) with granular policy management/enforcement.
* If an operator defines a network slice, for example, the UEs associated with that network slice should be logically segmented from other UEs associated with other slices – no shared data plane slices.
* NFs should not be shared across slices – each specific slice should have its own NFs in their own containers/VMs so that all processing, data, services, etc. are isolated from other slices.
	1. Study the ability for the 6G network to support robust and scalable policy decision and policy enforcement mechanisms.
	2. Study the ability for the 6G network to require relevant fine grain access control for network slices and UE to mitigate cross-domain threats.
* Today, access control is on a per-session basis versus a per-flow basis. Leveraging policies, an operator could support per-flow policies which can be used for access control (policy enforcement) decisions.

**WT#6:** Study on integration of 6G network with the Operator Security Function, including SIEM/SOAR platforms

* 1. Study the integration of the Operator Security Function, including the methods to implement closed-loop automation to adjust access permissions, network slice bandwidth, or service quality based on threat intelligence and behaviour monitoring.