**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, alerting and remediation capabilities that should be integrated into the security architecture (embedded) for the integration with a Security Monitoring Entity.

* 1. Study of a unified observability plane with the Security Monitoring Entity for security monitoring integration across all domains of the 6G system (e.g., radio, core, management).
	2. Study to integrate with the Security Monitoring Entity with the 6G system (e.g., SIEM/SOAR) for all APIs, interfaces, and flows of the 6G system (e.g. radio, core, management).
	3. Study the identification of potential security threats to communication and network elements.
	4. Study on enforcement of real time security policy changes in response to an identified/confirmed security attack or event to minimize the service disruption and recover the network and services.

**WT#2:** Study on Identity and Access Management 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 party network (e.g. NPN, NTN).
	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 RAN), and SBI/SBA (UE, RAN, 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 user 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 NF security posture integration and security control interaction.
	9. Study the methods required to allow and monitor each network slice based on a policy set, auth/authz logic, telemetry, and visibility to reduce lateral movement, cross-slice traffic interception, etc.

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

* 1. Study methods/requirements toautomate 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 security operation visibility.
	2. Study methods/requirements to support AI based closed-loop threat mitigation within the security monitoring capabilities.
	3. Study methods/requirements to leverage standard interfaces for dynamic policy decisions using 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 mutual authentication for machine-to-machine communications

* 1. Study the impacts of mandating that all M2M communications use mutual authentication (e.g. mTLS with PKI) for all SBA and RAN interfaces.

**WT#5:** Study on security architecture and management when supporting 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 UE requested network slices to mitigate cross-domain threats.

**WT#6:** Study on integration of 6G network with the Security Monitoring Entity

* 1. Study the integration of the Security Monitoring Entity, including the methods to implement closed-loop automation to adjust access permissions, device bandwidth, or service quality based on threat intelligence and behaviour monitoring across the 6G system (e.g., radio, core, management).