**3GPP TSG-SA3 Meeting #116** ***draft\_S3-242428-r1***

Jeju, South Korea, 20th - 24th May 2024

**Source: Ericsson**

**Title: Adding solution to KI#1 "Data exposure for security evaluation and monitoring"**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***Approve the pCR to TR 33.794 [1] below.***

# 2 References

[1] 3GPP TR 33.794 "Study on enablers for Zero Trust Security"

# 3 Rationale

This contribution proposes a solution to KI#1 "Data exposure for security evaluation and monitoring".

# 4 Detailed proposal

\*\*\* BEGIN CHANGES \*\*\*

## 7.X Solution #X: Security log events collection for evaluation and monitoring.

### 7.X.1 Introduction

This solution is addressing Key Issue #1: Data exposure for security evaluation and monitoring, aspect (2) "Architecture to be used for exposure of data collected for security evaluation and monitoring of the 5G SBA". It provides the means to facilitate collection of different security log events, either existing or new, and to facilitate export of log data to external security monitoring function as input.

The motivation for this solution is to use the existing practice of security monitoring as baseline for the study of standardization efforts. Current security monitoring in practice is based on the export of security log events.

### 7.X.2 Solution details

Figure 7.x.2-1: Generic procedure of NF security events exporting to external monitoring function.

External Security Management Function

NF

Log events exchange

The NF and the external security management function set up secure communication channel. The NF exports security log event to the external security monitoring function.The External Security Monitoring Function itself does not belong to the 5G Service-Based Architecture. Therefore, the interface between NF and External Security Monitoring Function is also not an interface of the 5G Service-Based Architecture.

Editor's Note: The interface between a NF and the External Monitoring Function is FFS.

Security events need to be logged separately from normal logs, e.g., there should be own stream for security events as typically security operations are separate from normal network operations.

Optionally, the system can be configured so that to set up what events to be logged / to be sent to external system.

### 7.X.3 Evaluation

TBD

\*\*\* END CHANGES \*\*\*