**Offline Call - SA3#117 FS\_eZTS Preparations**

# 1. Call Information

**Date:** 1 July 2024, Monday

**Time:** 15:00-16:30 CET

**Venue:** Microsoft Team Meeting (Online)

**Organizer:** Rapporteur, Lenovo (Sheeba Backia Mary Baskaran)

# 2. Call Participants:

|  |  |
| --- | --- |
| **Name** | **Company** |
| Achari Kakinada - Charter | Charter |
| Andreas Kunz | Lenovo |
| Candace Carducci | JHU/APL |
| David Gabay | MITRE |
| Denisha Jackson | US NSA |
| DJEMAI Tanissia | irt-saintexupery |
| Dusty Hoffpauir | Charter |
| Elizabeth Koser | US NSA |
| German Peinado | Nokia |
| Grewal, Rajpreet | NTIA |
| Imran Saleem | Huawei |
| Johannes Doerr | BMWK |
| Michael Bilca | Trideaworks |
| Rakshesh P Bhatt | Nokia |
| Sedjelmaci Hichem | Huawei |
| Sheeba Baskaran | Lenovo |
| Tim Woodward | MSI |
| Tyler Hawbaker | OTD\_US |
| Warren Kim | JHU/APL |
| X Lee | CISA ECD |

# 3. Agenda and Minutes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Agenda** | **Discussion Topic** | | **Meeting Minutes** |
| 1 | Overview of FS\_eZTS work plan | Work Plan Document  (10 mins) | | # Lenovo (Sheeba): presented the work plan.  Takeaway: We have limited TUs available and got only 2 more meetings for completing the study. The primary focus in SA3#117 meeting is to stabilize the solutions, evaluations along with cleanup & initial conclusions. |
| 2 | Open aspects discussions and alignment (for KI#1 solutions consolidation) | Handling security log e.g., factors to consider from NIST SP 800-92  (15 mins)  (Indirect case) EN: *The security risk of handling security data together with non-security related data needs to be evaluated against best practice of handling security logs, e.g., in NIST SP 800-92* | | Aspects to discuss:   1. *SP 800-92. Guide to computer Security Log management (predominantly discuss about log security and protection such as confidentiality, integrity e.g., Clause 2.3.2 Log Protection and 5.1.3 Log Security). What factor(s) in specific to this EN need to be considered from SP 800-92? What is seen as handling security data together with non-security data?*   # Nokia (Rakshesh): Strict security requirements need to be in place (such as dedicated data collection agent – i.e., a separate and dedicated one; collect data in a secure channel; also store data in a secure manner; TLS could be mandatory but optional use).  # Lenovo (Sheeba): Okay, similar recommendations are also listed in NIST SP 800-92 e.g., to use TLS for log security.  # Huawei: classification of logs itself we will not discuss; There is no 3rd party agent on the NFs; OSF can rely on both security event data and it can also rely on other data available external to 3GPP.  # Nokia (German): SCAS 33.117 doesn’t address about log/data classification, and it is bit generic in nature, right?  # Huawei (Imran): OSF may not rely on classification. Classification itself would create more complexity. Currently data classification is not done and it is generic.  # Lenovo (Sheeba): Actually, behind this EN there is no intension to classify data. Current security event related data collection involves both new abnormal behaviour related data and some existing data e.g., such as NF load and performance, while adding this EN, our understanding was ‘may be this security event data means new data and non-security data means existing data’; As none of the text in 33.794 describes to handle these data together, EN is bit ambiguous. May be if we get the clarity on what is seen as handling security data together with non-security data’, it will be helpful to appropriately resolve the EN.   1. *Security events if logged separately (e.g., like one of direct data collection type sol#5 where it is mentions, ‘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.’, can it address this open aspect?*   # Lenovo (Sheeba): Do we have Ericsson colleagues in the call? If not, as sol #5 is from them, it’s okay we can discuss these aspects in the later discussions when the contributor is available. |
| The extent of reusing existing data collection framework (along with need, merits vs de-merits (if any))  (15 mins) | | Aspects to discuss:   1. *There are solutions which additionally have concept of Data Collection Coordination Function (DCCF) as well as repository functions. As the data need to be provided to operator’s security function, here following discussion would help in understanding:* 2. *what is the merit/need of storing the collected data within 3GPP network?*   #Lenovo (Sheeba): As the security evaluation/analytics itself is going to be done by OSF outside 3GPP, do we still need a repository function inside 3GPP network? or can the collected data be stored by OSF by operator implementation means?  #Nokia (Rakshesh): Historical data helps in AI model training; If an external consumer is consuming the data, then we should take care privacy of data; there should be a 3GPP repository in place. External consumer should have limitations in access e.g., external exposure related security requirements, authorization.  #MITRE (David): Have the same view as Nokia but will think about it further.  #Charter Communication (Dusty): If we store internally, it would come with some cost. While data collection and storage, certain factors need to be taken case (such as localities, regulation, retention period, policies).  #OTD\_US(Tyler): OSF will set the policy.  #Charter Communication (Dusty): Should not be a borderless storage. Basically data storage is expensive.  #OTD\_US (Tyler): Would be based on certain principles e.g., 4 hours or so.  #MITRE (David): For previous comment, Dusty mentioned internal not external.  #Lenovo (Sheeba): Okay, fixed it as internal.  #Charter Communication (Dusty): Consider the hybrid case, where the data is stored with cloud service provider storage. Storing endless data will come with a cost. Having the flexibility on storage is important. Most of the log data that is been stored isn’t value. So have to specific about the data to be stored.  #MITRE (David): May be a verbose logging, specifies what is to be logged.  #Lenovo (Sheeba): So far, the main take way from Nokia and charter comments are: Nokia recommends internal storage for security reasons; Charter asked to take into account factors such as: while storing the data to make sure only necessary data is stored and to take into account regulatory aspects. Further added that Exposure to external data repository need to be secured, should be taken care not to expose any privacy info as well.   1. *if an abnormal event happens, why a co-ordinated data collection needed like DCCF?*   #Lenovo (Sheeba): If there is a means to collect the data, do we additionally need a collection coordination function? Because here the scope is to collect the necessary data and provide it to the OSF. In certain case only DCCF is implemented in the network, in some case, even it is hosted as part of NWDAF or it may not be implemented.  # Nokia (Rakshesh): DCCF is just one example, so the conceptual proposal is that we can reuse the collection agent.  # Charter Communication (Achari): Do we inherit existing functionality from DCCF or do we need new functionalities.  # Nokia (Rakshesh): Can be implementation specific. If the same data can be inherited, and if the solution works fine, then to resolve the EN, for security specific data to ensure security we may need a dedicated collection agent.  # Charter Communication (Achari): Do we need to state certain requirements for the DCCF or the dedicated agent.  # Nokia (Rakshesh): Yes, as expressed previously there should be security requirements for the collection agent. |
| Interface to use for security event exposure to Operator’s Security function  (15 mins) | | Aspects to discuss:   1. *What type of interface is used to provide the security event data to the operator’s security function?*   # Huawei (Imran): Better wait for the meeting, as it may need a larger audience.  # Lenovo (Sheeba): This is to discuss and understand the different perspectives. The larger audience’s feedback when available can be considered. Then I would suggest the contributors to take into account the different case of interface possibility to use for this scenario (to be discussed in their solutions to avoid endless ENs) as it may determine the workability of the solution as well as the principle may also impact the KI#2 solutions. |
| 3 | KI#2 | solution consideration highlights/discussions (if any)  (15 mins) | | Aspects to consider:   1. 2 more meetings to complete the study, so a complete evaluation for the input contributions is essential.   No further discussions. |
| 4 | Any other business | New Use case proposal for data exposure related to attacks on network slices (IRT, Nokia)  (15 mins) | | #IRT (Djemai Tanissia) presented the draft.  Huawei (Imran): Have 2 comments one is the context of reference listed can have different execution scenario. We need to understand the execution scenario to have the relevant data. The other comment is the study work plan as presented is focusing on solution discussion and completion for KI#1 and #2, how long are we going to bring/discuss new usecases.  IRT (Djemai Tanissia): It is generic, and we do not have specific explanation on how the attack could happen. Actually, it is a question we put to Nokia, we should classify different usecases where attack can happen in slice. Yes, we were thinking how to present the different data relative to different attack case, but not sure.  Lenovo (Sheeba): For the second comment, I can address once discussion on 1st comment is over.  Nokia (Rakshesh): Considering attack on network slice is a common aspect. There could be different KIs for the different slice related attacks. There may be some data which can be specific to certain attack scenarios, but there can also be data which are general and applicable to multiple attack scenario.  Huawei (Imran): This information if made available to performance management system, in the context of security we want to understand if the harm to slice is intended. We might need to describe more granular data to understand the attack specific information.  IRT (Djemai Tanissia): The information in clause 5.1.X.3, helps to identify the attack source.  Huawei (Imran): To identify the abnormal behaviour, we should know the normal behaviour. It is not clear in the current text.  Lenovo (Sheeba): Thanks for the discussing the draft. On technical aspects content needs refinements, i.e., a long list of reference has been provided, but what is the justification or take away from the related reference which backs this use case is not described. This clarification can be added in the rationale and in the description clause too... for the better understanding of the use case. Then on the list of data, kindly cite the existing reference wherever existing data is listed, it can help to see what is the specific new data that is needed for this use case on top. On the 2nd comment, really the time unit is very limited, so the author(s) of this contribution need to work offline with the involved companies to collect the feedback and possibly address before hand, as the discussion time during the f2f meeting may be very limited. Nevertheless, if we manage the time efficiently during the meeting, we can do our best to open/discuss new contributions soon after KI#1 and 2 doc handling during the f2f meeting. |
| Any other aspect  (5 mins) | | No discussion |
|  | | | Call is closed at 16:21 CET | |