 O-RAN.WG11.TR.ZTA-R004-v02.00

Technical Report

O-RAN Work Group 11 (Security Work Group)

Study on Zero Trust Architecture for O-RAN

Copyright © 2025 by the O-RAN ALLIANCE e.V.

The copying or incorporation into any other work of part or all of the material available in this document in any form without the prior written permission of O-RAN ALLIANCE e.V. is prohibited, save that you may print or download extracts of the material of this document for your personal use, or copy the material of this document for the purpose of sending to individual third parties for their information provided that you acknowledge O-RAN ALLIANCE as the source of the material and that you inform the third party that these conditions apply to them and that they must comply with them.

O-RAN ALLIANCE e.V., Buschkauler Weg 27, 53347 Alfter, Germany

Register of Associations, Bonn VR 11238, VAT ID DE321720189

Contents

List of figures 4

List of tables 5

Foreword 7

Modal verbs terminology 7

Introduction 7

1 Scope 8

2 References 9

2.1 Normative references 9

2.2 Informative references 9

3 Definition of terms, symbols and abbreviations 10

3.1 Terms 10

3.2 Symbols 11

3.3 Abbreviations 11

4 NIST Zero Trust Tenet Applicability 13

4.1 NIST ZT Tenets overview 13

4.2 NIST ZT Tenets applicability study 13

4.2.1 ZT Tenet 1 Applicability Study 13

4.2.2 ZT Tenet 2 Applicability Study 14

4.2.3 ZT Tenet 3 Applicability Study 15

4.2.4 ZT Tenet 4 Applicability Study 16

4.2.5 ZT Tenet 5 Applicability Study 17

4.2.6 ZT Tenet 6 Applicability Study 18

4.2.7 ZT Tenet 7 Applicability Study 19

4.3 NIST ZT Tenets applicability summary 20

5 ZTA Assets 22

5.1 Asset Categories 22

5.2 Defined Assets 23

5.3 New Assets 23

5.3.1 New Assets in the SMO 23

5.3.2 O-Cloud Assets 25

5.3.3 New Assets in the Open Fronthaul 26

5.3.4 New Assets in F1 (Midhaul) 26

6 Reference ZTA Security Requirements 28

6.1 ZTA Framework 28

6.1.1 Introduction 28

6.1.2 CISA's Zero Trust Maturity Model (ZTMM) 28

6.1.3 DoD Zero Trust Strategy and Reference Architecture 28

6.1.4 Comparison of ZTMM models 30

6.1.5 Selection of CISA ZTMM Model 30

6.2 Target ZTA Security Requirements 31

6.2.1 Introduction 31

6.2.2 Identity 31

6.2.3 Devices 33

6.2.4 Networks 35

6.2.5 Applications and Workloads 37

6.2.6 Data 40

6.2.7 Cross-Cutting Capabilities 43

7 Alignment to Target ZTA Requirements 50

7.1 Introduction 50

7.2 Current O-RAN Security Requirements and Controls 50

7.3 Gap Analysis 51

7.3.1 Gap Analysis Methodology 51

7.3.2 Transversal Functions 53

7.3.3 xApp and Near-RT RIC Gap Analysis 53

7.3.4 E2 Interface Gap Analysis 62

7.3.5 Y1 Interface Gap Analysis 64

7.3.6 rApp and Non-RT RIC Gap Analysis 66

7.3.7 A1 Interface Gap Analysis 72

7.3.8 R1 Interface Gap Analysis 74

7.3.9 SMO Gap Analysis 75

7.3.10 O1 Interface Gap Analysis 75

7.3.11 O-Cloud Gap Analysis 79

7.3.12 O2 Interface Gap Analysis 86

7.3.13 O-CU Gap Analysis 88

7.3.14 O-DU Gap Analysis 94

7.3.15 O-RU Gap Analysis 100

7.3.16 Open Fronthaul Gap Analysis 106

7.4 WG11 Considerations for Mapping Security Controls to CISA ZTMM 108

7.4.1 Introduction 108

7.4.2 Mapping to CISA ZTMM 109

8 ZTA Threats 110

8.1 Introduction 110

8.2 Mapping of the existing Security Principles to ZT Tenets 110

8.3 Existing defined threats 111

8.4 New threats 111

9 Threat analysis 112

10 Risk assessment 113

11 Recommendations 114

Annex: Change history/Change request (history) 115

# List of figures

Figure 6.1‑1: CISA Zero Trust Maturity Model 28

Figure 6.1‑2: DoD ZT Capabilities 29

Figure 6.1‑3: Comparison of US CISA and DoD ZTMM 30

Figure 7.3‑1 Gap Analysis Workflow 52

# List of tables

[Table 4.3‑1: NIST ZT Tenet Applicability Summary 21](#_Toc182904677)

[Table 5.2‑1: High Level ZTA Assets for O-RAN 23](#_Toc182904678)

[Table 5.3‑1: SMO Assets 23](#_Toc182904679)

[Table 5.3‑2: O-Cloud Assets 25](#_Toc182904680)

[Table 5.3‑3: Open Fronthaul Assets 26](#_Toc182904681)

[Table 5.3‑4: F1 Assets 26](#_Toc182904682)

[Table 7.2‑1: Mandatory O-RAN interface security controls (See NOTE for 802.1X1 and PDCP2) 50](#_Toc182904683)

[Table 7.2‑2: O-RAN Cross-Platform Security Requirements 51](#_Toc182904684)

[Table 7.3‑1 Mapping of O-RAN Assets and Other Components to Different Pillars 52](#_Toc182904685)

[Table 7.3‑2: xApp and Near-RT RIC Data Pillar Gap Analysis 54](#_Toc182904686)

[Table 7.3‑3: xApp and Near-RT RIC Applications and Workloads Pillar Gap Analysis 58](#_Toc182904687)

[Table 7.3‑4: xApp and Near-RT RIC Identity Pillar Gap Analysis 60](#_Toc182904688)

[Table 7.3‑5: xApp and Near-RT RIC Networks Pillar Gap Analysis 62](#_Toc182904689)

[Table 7.3‑6: E2 Interface Data Pillar Gap Analysis 63](#_Toc182904690)

[Table 7.3‑7: E2 Interface Networks Pillar Gap Analysis 64](#_Toc182904691)

[Table 7.3‑8: Y1 Interface Data Pillar Gap Analysis 65](#_Toc182904692)

[Table 7.3‑9: Y1 Interface Networks Pillar Gap Analysis 66](#_Toc182904693)

[Table 7.3‑10: rApp and Non-RT RIC Data Pillar Gap Analysis 67](#_Toc182904694)

[Table 7.3‑11: rApp and Non-RT RIC Applications and Workloads Pillar Gap Analysis 69](#_Toc182904695)

[Table 7.3‑12: rApp and Non-RT RIC Identity Pillar Gap Analysis 70](#_Toc182904696)

[Table 7.3‑13: A1 Interface Data Pillar Gap Analysis 72](#_Toc182904697)

[Table 7.3‑14: A1 Interface Networks Pillar Gap Analysis 74](#_Toc182904698)

[Table 7.3‑15: R1 Interface Data Pillar Gap Analysis 74](#_Toc182904699)

[Table 7.3‑16: R1 Interface Networks Pillar Gap Analysis 75](#_Toc182904700)

[Table 7.3‑17: O1 Interface Data Pillar Gap Analysis 76](#_Toc182904701)

[Table 7.3‑18: O1 Interface Networks Pillar Gap Analysis 78](#_Toc182904702)

[Table 7.3‑19: O-Cloud Data Pillar Gap Analysis 79](#_Toc182904703)

[Table 7.3‑20: O-Cloud Applications and Workloads Pillar Gap Analysis 82](#_Toc182904704)

[Table 7.3‑21: O-Cloud Identity Pillar Gap Analysis 84](#_Toc182904705)

[Table 7.3‑22: O-Cloud Networks Pillar Gap Analysis 85](#_Toc182904706)

[Table 7.3‑23: O-Cloud Devices Pillar Gap Analysis 86](#_Toc182904707)

[Table 7.3‑24: O2 Interface Data Pillar Gap Analysis 86](#_Toc182904708)

[Table 7.3‑25: O2 Interface Networks Pillar Gap Analysis 88](#_Toc182904709)

[Table 7.3‑26: O-CU Data Pillar Gap Analysis 89](#_Toc182904710)

[Table 7.3‑27: O-CU Application and Workloads Pillar Gap Analysis 91](#_Toc182904711)

[Table 7.3‑28: O-CU Identity Pillar Gap Analysis 93](#_Toc182904712)

[Table 7.3‑29: O-CU Devices Pillar Gap Analysis 94](#_Toc182904713)

[Table 7.3‑30: O-DU Data Pillar Gap Analysis 95](#_Toc182904714)

[Table 7.3‑31: O-DU Applications and Workloads Pillar Gap Analysis 97](#_Toc182904715)

[Table 7.3‑32: O-DU Identity Pillar Gap Analysis 99](#_Toc182904716)

[Table 7.3‑33: O-DU Devices Pillar Gap Analysis 100](#_Toc182904717)

[Table 7.3‑34: O-RU Data Pillar Gap Analysis 101](#_Toc182904718)

[Table 7.3‑35: O-RU Applications and Workloads Pillar Gap Analysis 103](#_Toc182904719)

[Table 7.3‑36: O-RU Identity Pillar Gap Analysis 104](#_Toc182904720)

[Table 7.3‑37: O-RU Devices Pillar Gap Analysis 105](#_Toc182904721)

[Table 7.3‑38: Open Fronthaul Data Pillar Gap Analysis 106](#_Toc182904722)

[Table 7.3‑39: Open Fronthaul Networks Pillar Gap Analysis 107](#_Toc182904723)

[Table 7.4‑1: CISA ZTMM Mapping of O-RAN security controls 109](#_Toc182904724)

[Table 8.2‑1: Mapping of security principles to ZT tenets1 110](#_Toc182904730)

# Foreword

This Technical Report (TR) has been produced by O-RAN Alliance.

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the O-RAN Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in O-RAN deliverables except when used in direct citation.

# Introduction

In today's era of digital transformation, the complexity of a typical enterprise's infrastructure—encompassing multiple internal networks, remote offices, mobile users, and cloud services—has outstripped legacy perimeter-based network security methods, as there is no longer a single, easily identifiable perimeter for the enterprise [i.6]. The majority of cyber-attacks targeting applications and workloads stem from inadequate access control. Poor management of user, service, and device identities and credentials, along with the use of weak authentication mechanisms such as passwords, are often the underlying causes of security breaches.

This complexity has led to the development of a new model for cybersecurity known as "Zero trust" (ZT). Zero trust responds to enterprise network trends such as remote users, bring your own device (BYOD) policies, and cloud-based assets not located within an enterprise-owned network boundary, which is a typical use case for O-RAN. Preventing lateral movement is crucial for protecting O-RAN from attackers who typically attempt lateral movement after initially exploiting the network. Traditional remote access solutions, such as VPNs, lack control over insider attacks and grant access to all on-site data, applications, and resources. Mitigating the risk of insider threats, breaches, and data exposure is essential to protecting O-RAN assets and resources.

Zero trust is an evolving set of cybersecurity paradigms that shifts defenses from static, network-based perimeters to focus on users, assets, and resources. It assumes no implicit trust is granted to assets or user accounts based solely on their physical or network location or asset ownership. Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least-privilege per-request access decisions in information systems and services, even in a network viewed as compromised. The approach focuses on authentication, authorization, and shrinking implicit trust zones while maintaining availability and minimizing temporal delays in authentication mechanisms. Access rules are made as granular as possible to enforce the least privileges needed to perform the action in the request [i.6].

# Scope

The contents of the present document are subject to continuing work within O-RAN and may change following formal O-RAN approval. Should the O-RAN Alliance modify the contents of the present document, it will be re-released by O-RAN with an identifying change of version date and an increase in version number as follows:

version xx.yy.zz

where:

xx: the first digit-group is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc. (the initial approved document will have xx=01). Always 2 digits with leading zero if needed.

yy: the second digit-group is incremented when editorial only changes have been incorporated in the document. Always 2 digits with leading zero if needed.

zz: the third digit-group included only in working versions of the document indicating incremental changes during the editing process. External versions never include the third digit-group. Always 2 digits with leading zero if needed.

Zero Trust Architecture (ZTA) is applicable to protect O-RAN architecture elements, interfaces, and data. This technical report studies the state of O-RAN's Zero Trust security posture with respect to the NIST publications [i.6] [i.7] and their seven tenets of zero trust. This report identifies new zero trust assets, threats, risks, and security controls in pursuit of a ZTA while considering those already existing in WG11 specifications.

This technical report includes the following activities:

* Applicability study of NIST seven tenets of zero trust to O-RAN Security Architecture
* Identification of Zero Trust assets
* Identification of ZTA threats using STRIDE
* ZTA risk assessment
* Determination of ZTA security controls
* Gap analysis between target ZTA security controls and existing security controls
* Proposal of new ZTA recommendations, requirements, and security controls

This technical report makes the following considerations:

* The technical report takes into consideration existing WG11 technical reports and specifications and may inform of the associated assets, threats, risks, and security controls.
* The O-RAN ALLIANCE is pursuing a zero-trust architecture (ZTA) for its specifications based upon NIST SP 800-207 [i.6].

# References

## Normative references

Normative references are not applicable in the present document.

## Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies. In the case of a reference to a 3GPP document, a non-specific reference implicitly refers to the latest version of that document in Release 18, or the latest 3GPP release prior to Release 18 that includes that document.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, O-RAN cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

1. O-RAN ALLIANCE TS: "O-RAN Architecture Description"
2. O-RAN ALLIANCE TS: "O-RAN Security Requirements and Controls Specifications"
3. O-RAN ALLIANCE TS: "O-RAN Security Protocols Specifications"
4. O-RAN ALLIANCE TR: "O-RAN Security Threat Modeling and Risk Assessment"
5. O-RAN ALLIANCE TS: "O-RAN Security Test Specification"
6. NIST Special Publication 800-207, "Zero Trust Architecture", August 2020, <https://doi.org/10.6028/NIST.SP.800-207>
7. NIST Special Publication 800-207A, "A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments", September 2023 <https://doi.org/10.6028/NIST.SP.800-207A>
8. Enhanced Zero Trust and 5G, ATIS, July 2023, [Enhanced Zero Trust and 5G | ATIS](https://www.atis.org/resources/enhanced-zero-trust-and-5g/).
9. Zero Trust Maturity Model, v2.0, US DHS CISA, April 2023. <https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf>
10. 3GPP TR 33.894: "3GPP Study on applicability of the zero trust security principles in mobile networks"
11. "Security guidance for 5g cloud infrastructures", <https://www.cisa.gov/sites/default/files/2023-02/security_guidance_for_5g_cloud_infrastructures_part_i_508_compliant.pdf>
12. O-RAN ALLIANCE TS: "Xhaul Packet Switched Architectures and Solutions"
13. Embracing a Zero Trust Security Model, US National Security Agency, February 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI\_EMBRACING\_ZT\_SECURITY\_MODEL\_UOO115131-21.PDF
14. DoD Zero Trust Reference Architecture, US Department of Defense, July 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT\_RA\_v2.0(U)\_Sep22.pdf .
15. NSTAC Report to the President on Zero Trust and Trusted Identity Management, NSTAC, 2022.
16. IEEE Std 802.1X-2020: "IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control", (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018), 28 Feb. 2020, doi: 10.1109/IEEESTD.2020.9018454.
17. 3GPP TS 33.501: "Security architecture and procedures for 5G System"
18. DoD Zero Trust Strategy, US Department of Defense, October 2022. <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>
19. DoD Zero Trust Capability Execution Roadmap (COA 1), DOD CIO, ZT PfMO, January 2023.  <https://dodcio.defense.gov/Portals/0/Documents/Library/ZTCapabilityExecutionRoadmap.pdf>
20. NIST Special Publication 800-95 "Guide to Secure Web Services", August 2007, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf>
21. O-RAN ALLIANCE TS: "Non-RT RIC: Architecture"
22. "Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar", US National Security Agency, May 2024. <https://media.defense.gov/2024/May/30/2003475230/-1/-1/0/CSI-VISIBILITY-AND-ANALYTICS-PILLAR.PDF>
23. O-RAN ALLIANCE TS: “Near-RT RIC Architecture”
24. 3GPP TS 33.511 “Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class”
25. 3GPP TS 33.117 “Technical Specification Group Services and System Aspects; Catalogue of general security assurance requirements”
26. O-RAN ALLIANCE TS: “O-RAN Management Plane Specification”
27. O-RAN ALLIANCE TR: "O-RAN Study on Security for Fronthaul CUS-Plane"
28. O-RAN ALLIANCE TS: "O-RAN Management interfaces for Transport Network Elements"
29. O-RAN ALLIANCE TS: "O-RAN Synchronization Architecture and Solution Specification"
30. "Advancing Zero Trust Maturity Throughout the Network and Environment Pillar", <https://media.defense.gov/2024/Mar/05/2003405462/-1/-1/0/CSI-ZERO-TRUST-NETWORK-ENVIRONMENT-PILLAR.PDF>

# Definition of terms, symbols and abbreviations

## Terms

For the purposes of the present document, the following terms apply:

**A1:** Interface between non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications/functions, and support AI/ML workflow.

**E2:** Interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs.

**Microsegmentation:** Microsegmentation is a security practice of partitioning networks and assets into small, isolated segments based on various attributes such as communication requirements and risk profiles. Fine grained access control mechanisms are used to minimize the permissible communication paths both within and between disjoint segments.

NOTE: Microsegmentation is commonly used in zero trust architecture to minimize the threat of attacks from disjoint segments.

**Near-RT RIC:** O-RAN near-real-time RAN Intelligent Controller: a logical function that enables real-time control and optimization of RAN elements and resources via fine-grained data collection and actions over E2 interface.

**Non-Person Entity (NPE):** An entity with a digital identity that acts in cyberspace, but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts as defined in [i.6].

**Non-RT RIC:** O-RAN non-real-time RAN Intelligent Controller: a logical function that enables non-real-time control and optimization of RAN elements and resources, AI/ML workflow including model training and updates, and policy-based guidance of applications/features in Near-RT RIC.

**O-CU:** O-RAN Central Unit: a logical node hosting O-CU-CP and O-CU-UP

**O-CU-CP:** O-RAN Central Unit – Control Plane: a logical node hosting the RRC and the control plane part of the PDCP protocol.

**O-CU-UP:** O-RAN Central Unit – User Plane: a logical node hosting the user plane part of the PDCP protocol and the SDAP protocol.

**O-DU:** O-RAN Distributed Unit: a logical node hosting RLC/MAC/High-PHY layers based on a lower layer functional split.

**O-RU:** O-RAN Radio Unit: a logical node hosting Low-PHY layer and RF processing based on a lower layer functional split.

**O1:** Interface between management entities (NMS/EMS/MANO) and O-RAN managed elements, for operation and management.

**O2:** Interface between SMO and the O-Cloud to provide cloud resources management and workload management for supporting O-RAN cloudified network functions.

**O2dms:** Interface between the SMO and the O-Cloud that is responsible for the deployment management services of the NF Deployment.

**O2ims:** Interface between the SMO and the O-Cloud that is responsible for the infrastructure management services of the NF Deployment.

**Open Fronthaul:** The interface between O-DU and O-RU logical nodes, including the CUS (Control User Synchronization) Plane and M (Management) Plane, as defined in O-RAN Architecture Description [i.1].

**R1:** Interface between rApps and Non-RT RIC Framework via which R1 Services can be produced and consumed.

**rApps:** Non-RT RIC application: an application designed to consume and/or produce R1 services.

**Service Management and Orchestration (SMO):** The O-RAN Service Management and Orchestration system as specified in the O-RAN Architecture Description (OAD) document [i.1], clause 5.3.1.

**xApps:** Near-RT RIC application.

**Y1:** An interface between Near-RT RIC and Y1 consumers, as defined in O-RAN Architecture Description [i.1], clause 5.4.18. The interface enables RAN analytics information exposure from Near-RT RIC.

## Symbols

None

## Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI/ML Artificial Intelligence/Machine Learning

CM RAN NF Configuration Management

DME Data Management and Exposure

DMS O-Cloud Deployment Management Services

FHGW Fronthaul Gateway

FHM Fronthaul Multiplexor

FM Fault Management

FOCOM Federated O-Cloud Orchestration and Management

GM Grand Master

IMS O-Cloud Infrastructure Management Services

JEA Just-Enough-Administration

JIT Just-In-Time

NFO Network Function Orchestrator

NPE Non-Person Entity

O-CU-CP O-RAN Centralized Unit – Control Plane

O-CU- UP O-RAN Centralized Unit – User Plane

O-DU O-RAN Distributed Unit

O-RU O-RAN Radio Unit

PM RAN NF Performance Management

RAN Radio Access Network

RIC O-RAN RAN Intelligent Controller

SME Service Management and Exposure

SMO Service Management and Orchestration

SMOS SMO Service

TE&IM Topology Exposure and Inventory Management

TNE Transport Node Equipment

UE User Equipment

UEBA User and Entity Behaviour Analytics

ZT Zero Trust

ZTA Zero Trust Architecture

ZTMM Zero Trust Maturity Model

# NIST Zero Trust Tenet Applicability

## NIST ZT Tenets overview

Numerous interpretations and discussions of ZT emphasize the imperative of eliminating wide-area perimeter defences. They define ZT as a transformative shift from a location-centric paradigm to an identity, context, and data-centric approach with fine-grained security controls between users, systems, applications, data, and assets that change over time. NIST Special Publication 800-207 [i.6] defines ZT through a set of basic tenets that should be involved in zero trust architectures. While acknowledging the ideal nature of these tenets, NIST recognizes that these tenets practical application may differ based on specific strategic considerations. The basic tenets, essential for a comprehensive Zero Trust Architecture, are detailed below:

1. **All data sources and computing services are considered resources.** This tenet emphasizes that all classes of devices, ranging from large devices to sensors, and all types of computing services, should be considered as resources that need protection within the Zero Trust Architecture (ZTA), whether they are personally owned or enterprise-owned resources.
2. **All Communication is secured regardless of network location.** This means that trust should not be automatically granted based on the device being on the enterprise network infrastructure. Instead, all communication should be conducted in the most secure manner available, protecting confidentiality and integrity, and providing source authentication.
3. **Access to individual enterprise resources is granted on a per-session basis.** Trust in the requester is evaluated before access is granted. Moreover, access should be granted with the least privileges needed to complete the task.
4. **Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioural and environmental attributes.** These rules and attributes are based on the needs of the business process and an acceptable level of risk. Resource access and action permission policies can vary based on the sensitivity of the resource/data. Least privilege principles are applied to restrict both visibility and accessibility.
5. **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.** No asset is inherently trusted. The security posture of the asset needs to be evaluated and considered when evaluating a resource request. An enterprise implementing a ZTA should establish a continuous diagnostics and mitigation (CDM) or a similar system to monitor the state of devices and applications and should apply patches/fixes as needed.
6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.** This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually reevaluating trust in ongoing communication as defined and enforced by policy, striving to achieve a balance of security, availability, usability, and cost-efficiency.
7. **The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.** This data should be utilized to improve policy creation and enforcement, and to support contextual access control decisions.

## NIST ZT Tenets applicability study

### ZT Tenet 1 Applicability Study

#### Introduction

**ZT tenet 1: All data sources and computing services are considered resources.**

This tenet underscores the importance of safeguarding all forms of data sources and computing services within the framework of ZTA. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.

#### Applicability Study

This tenet addresses the dynamic shifts in enterprise network trends, encompassing various internal networks, remote offices with distinct local infrastructures, remote individuals, and cloud-based assets existing beyond enterprise-owned network boundaries—common scenarios encountered in Open RAN deployments. The increasing complexity surpasses traditional perimeter-based network security methods, given the absence of a single, easily identifiable enterprise perimeter.

The ZTA approach primarily concentrates on safeguarding data and services but should extend its coverage to include all enterprise assets (devices, infrastructure components, applications, virtual and cloud components) and subjects (end users, applications, and other non-human entities seeking information from resources) [i.6]. Consequently, ZT security models operate on the assumption that an attacker is present in the environment, and no enterprise-owned environment is inherently more trustworthy than a non-enterprise-owned one. Addressing this tenet becomes imperative for establishing robust security measures within such contexts.

In the context of a ZT-based O-RAN architecture adhering to ZT tenet 1, each data source and computing service in the O-RAN system should be considered a resource. As depicted in [i.8], this tenet necessitates the system owner to identify resources within the 5GS, enabling the construction of the ZTA around these resources. In the 5G landscape, network assets, including UEs, RAN, transport, Core, applications, and services, are acknowledged as assets and data sources with distinct system owners. Computer resources running NFs and applications are also recognized as assets.

#### Conclusion

The significance of Zero Trust Architecture's first tenet is notably pronounced in the context of O-RAN deployments. By emphasizing the safeguarding of data sources and computing services, the tenet addresses the unique challenges posed by diverse network assets in O-RAN architectures. This approach ensures that each component, whether locally owned or part of a broader ecosystem, is considered a valuable resource within the zero trust framework, thereby enhancing security measures tailored to the specific demands of O-RAN environments.

### ZT Tenet 2 Applicability Study

#### Introduction

**ZT Tenet 2: All Communication is secured regardless of network location.**

This tenet highlights the importance of not automatically granting trust solely based on a device's presence within the enterprise network infrastructure. Access requests from assets within enterprise-owned network infrastructure, such as those inside a legacy network perimeter, must adhere to the same security requirements as requests from non-enterprise-owned networks. All communication should prioritize the most secure methods available, ensuring confidentiality, integrity, and source authentication.

#### Applicability study

The relevance of this tenet is particularly evident in the context of Radio Access Network (RAN) considerations for several compelling reasons. O-RAN introduces elements like disaggregation, open interfaces, and diverse deployment models, expanding the potential attack surface. Components such as the O-RAN Service Management and Orchestration (SMO), Radio Intelligent Controller (RICs), and RIC Apps within the Open RAN framework are susceptible to exploitation for confidentiality, integrity, and availability attacks from both external and internal threats [i.8]. Therefore, addressing tenet 2 is crucial within the Open RAN architecture to effectively mitigate these security vulnerabilities.

In the context of a ZT-based O-RAN architecture adhering to ZT tenet 2, all network communications should prioritize confidentiality, integrity, and source authentication. In 5G, encryption, integrity protection, authentication schemes, and security protocols are employed to secure communication among participating entities in the network.

#### Conclusion

In summary, this tenet holds significant importance for O-RAN by stressing the necessity of robust security standards across all communications, regardless of their network location. With O-RAN's distinctive features like disaggregation, open interfaces, and third parties' applications, tenet 2 becomes essential for preventing security issues. By prioritizing confidentiality, integrity, and source authentication in network communications, Tenet 2 stands as a fundamental element in establishing a secure O-RAN framework, offering protection against potential threats both internal and external.

### ZT Tenet 3 Applicability Study

#### Introduction

**ZT tenet 3: Access to individual enterprise resources is granted on a per-session basis.**

According to ZT tenet 3 as stated in NIST SP 800-207 [i.6], each access request should be evaluated for trustworthiness before being granted. This tenet enforces the need to authenticate and authorize every subject requesting access to a protected resource and assess all permissions before granting access with the least privileges that is required to complete the task. This tenet enforces that successful authentication and authorization to one resource by a given subject will not automatically grant access to a different resource.

#### Applicability Study

For a zero trust based O-RAN architecture, each access request to O-RAN resources must adapt the principle of ZT tenet 3 with strong authentication, and fine-grained access control at every point of access.

In the O-RAN architecture there are multiple Points Of Access (POA) that have been considered for the applicability of ZT tenet 3 study.

1. **User Access to SMO:** User Access to internet facing SMO services and applications.
2. **User Access to the O-Cloud Orchestration layer:** User Access to VMs and containers via the O-Cloud Management Plane (EXAMPLE: Kubernetes API server).
3. **User Access to O-Cloud Host OS Access**: User Access via SSH to Host OS.
4. **User Access to O-Cloud Hardware Infrastructure:** User authentication and authorization for accessing the network storage, and compute resources.
5. **Network Function to Network Function Access:** NF to NF communication over O-RAN defined interfaces.
6. **User access to TNE:** User Access to Transport Network Elements, such as switches, routers, or other network devices.
7. **Device access to the network (Open FH):** Device access to open fronthaul resources like O-DU, O-RU FHM, Grandmasters etc.
8. **User Reauthentication:** Ensuring that a user accessing a protected resource is the same user who initially authenticated at the start of the session.

O-RAN ALLIANCE WG11 follows the principle of ZT tenet 3 while defining security controls and measures in the "O‑RAN Security Requirements and Controls Specifications" [i.2]. WG11 has specified security requirements and security controls for the following points of access - [2], [5] and [7].

- The current access control security mechanism specified are mTLS, IPsec, OAuth2.0, IEEE 802.1X, and NACM that ensures granular access control for O-RAN fronthaul and non-fronthaul interfaces.

- Communication between Network Functions over O-RAN defined interfaces has been secured based on the principles of zero trust.

- Security controls and measures have been defined for the access control for certain O-RAN components like access of O-Cloud using SMO via the **O2** interface and access of NFs using SMO via the **O1** interface.

Access control for the following points of access is not specified currently- user access to internet facing SMO services, user access to O-Cloud orchestration layer, O-Cloud Host OS, User Access of NFs from Host/O-Cloud node of SMO or other hosts. Access control mechanisms to these need to be evaluated for defining specific security recommendations that align to the ZT tenet 3 principle. This will ensure that the identity of the subject that is requesting access to a specific O-RAN resource identity is always verified, the subject possesses the necessary rights and meets the environment specific requirements to access the requested resource.

#### Conclusion

Human users, services, and applications request access to specific O-RAN network components. It is essential to authenticate every subject based on its unique identity and use RBAC rules to authorize and enforce least privilege access to the requested resources. By implementing Access Control Policies based on the Principle of Least Privilege (POLP), operators can effectively prevent attackers from moving laterally within the network.

WG11 should expand on the ZT tenet 3 principle of session-based access control to encompass the user access scenarios identified in [1],[3],[4],[6]. This will allow to define additional security controls and measures for granular categorization of access policies considering Just-in-time access, Least privileges and Just enough access for each subject identity and their rights to access the destination O-RAN assets.

### ZT Tenet 4 Applicability Study

#### Introduction

**ZT tenet 4: Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioural and environmental attributes.**

According to ZT tenet 4 as stated in NIST SP 800-207[i.6], access requests are evaluated not solely based on the outcome of subject authentication but also take into consideration the subject's previous request history, environmental factors and security posture of both the requesting subject and resource and are governed by dynamic policies.

#### Applicability Study

In the O-RAN architecture, human users (subjects) can generate remote access requests to O-RAN architecture elements such as SMO, O-Cloud or O-CU/O-DU/O-RU:

a) from geo-locations that may or may not be under the direct control of the network operator,

b) using devices that are not managed by the operator,

c) over public or hybrid (public/private) networks.

It is therefore essential to control access to the requested resources not just based on the identity of the user, but also based on additional attributes of the end-user such as his/her location, end-user device hygiene, past history or behavioural information (risk-profile) etc. These attributes are captured as inputs to dynamic access policies that influence authentication and authorization of the user.

For a zero-trust based O-RAN architecture, every access to O-RAN resources should adapt the principle of ZT tenet 4 that defines and enforces access policies which are continuously updated based on inputs from continual monitoring (ZT tenet 5) of the network,

O-RAN Architecture currently considers OAuth based authorization decision for several of its interfaces. These are based on static policies that define the scope of access granted to the requesting subject. OAuth does not define policies that take into account the location or security posture of the requesting client. Similarly, NACM does not define dynamic policies.

Additionally, WG11 has a requirement for DDoS protection mitigation measures for the O2 interface in SMO. There are however no requirements to use these DDoS mitigation measures to continuously update the access requests decision process or dynamic block listing.

WG11 proposes to further study and define ZT tenet 4 based access controls policies for accessing the O-RAN and Non-ORAN assets.

* Define attributes for user, services, and devices that need to be continuously monitored
* Define access control policies that are dynamically updated based on inputs from continuous monitoring of the above attributes
* Study the Policy decision and enforcement points for defining and enforcing ZT tenet 4 access policies in the O-RAN architecture, as described in clause 3 of NIST SP 800-207 [i.6].

These attribute-based access control policies would effectively manage, monitor, limit, and revoke access to Device, Infrastructure, Application and Services [DIAS].

#### Conclusion

As described in clause 4.2.4.2, human users, services, and applications request access to O-RAN network components from potentially untrusted locations, using unmanaged devices and over public or hybrid networks. It is therefore essential to include these parameters while authenticating and authorizing the subjects. Dynamic policy-based infrastructure is recommended that considers these attributes for policy generation and enforcement.

This would entail defining the user, network and device attributes for defining access control policies that would apply to all interfaces in the O-RAN network, user access to all O-RAN components as described in the ZT tenet 3 study.

### ZT Tenet 5 Applicability Study

#### Introduction

**ZT tenet 5: The enterprise monitors and measures the integrity and security posture of all owned and associated assets.**

NIST 800-207 [i.6] defines Tenet 5 "The enterprise monitors and measures the integrity and security posture of all owned and associated assets". Further description in NIST SP 800-207 states, this tenet majorly covers operational security and evaluation of the asset's security posture during evaluation of resource request.

#### Applicability Study

ZT tenet 5 allows us to design continuous diagnostics of security events, logs etc. and evaluation of access requests to O-RAN and Non-O-RAN Assets based on security posture. O-RAN WG11 Security Log Management work item relates to the principle of zero trust architecture, however, gap analysis should be conducted to ensure ZT tenet 5 compliancy. The gap analysis would ensure the coverage of all the O-RAN assets that is being added as a part of the ZTA work item. The study would also ensure that the collection of data is sufficient for ZT tenet 7 to utilize it to improve the security posture.

As part of ZT tenet 5, WG11 would cover continuous monitoring and alerting of User Authorizations, Data access, Resource Authorization (Application/workload), User/Device Interactions. It is also essential to study the integration of threat Intelligence as a part of the ZT tenet 5 study. This would entail a continuous security monitoring system that measures integrity, and security posture of all assets in the areas of access management, behavioural analytics, configuration management, software integrity checks, vulnerability scans, security anomaly detection, etc.

For a zero trust O-RAN Architecture, ZT tenet 5 plays a critical role to detect and alert of Adversarial Lateral movements.

#### Conclusion

WG11 should expand on the ZT tenet 5 principles that monitors the O-RAN assets to address any gaps of security monitoring and perform "**Continuous and dynamic security monitoring**" to maintain them in their most secure states possible for comprehensive visibility. WG11 intends to come up with recommendation, industry standard security best practices to attain the advanced zero trust maturity model.

### ZT Tenet 6 Applicability Study

#### 4.2.6.1 Introduction

**ZT tenet 6: All resource authentication and authorization are dynamic and strictly enforced before access is allowed.**

According to ZT tenet 6 as stated in NIST SP 800-207 [i.6], user access to resources is continuously re-evaluated. Any changes in the security posture of either the subject or the resource trigger reauthentication and reauthorization of the access request. This tenet expands on ZT tenet 4, which pertains to access requests through dynamic policies and ZT tenet 5 of continual monitoring to re-evaluating user transactional flow and enforcing policies based on abnormal behaviour, time-based factors, and environmental considerations.

#### 4.2.6.2 Applicability Study

In the O-RAN architecture, there are multiple points of access that a user may request access to. The user undergoes authentication and authorization before granting access to the resources. Although the user was authorized for accessing the resource, the user behaviour might change on account of various factors, such as:

1. Access over a different network
2. Unknown applications on the device trying to access the resource.
3. Hidden malware on the device trying to access the resource.
4. Unusual/abnormal access patterns (e.g. location, time change compared to known user patterns)

It is essential to monitor the security posture of the subject and network resources to evaluate the trust at any given point of time and trigger reauthentication and reauthorization if needed to do so. Failure to do so may result in a compromised user account or an internal threat actor that remains undetected, and may trigger reconnaissance, continued access to the protected resource, leading to a lateral movement in the network, thus causing large outages, data theft, or sabotage of the network.

As a result, the O-RAN architecture should adapt the principle of ZT tenet 6 where every access request is continuously reevaluated to determine that the trust can be maintained and established. Continuous evaluation of all values related to the authentication, inspection, and access determinations based on the subject and destination resource should be continuously assessed.

* Utilizing ongoing security monitoring (ZT tenet 5) to identify change in the security posture of subject and resource -of user access for O-Cloud Platform, mTLS, IPsec, IEEE 802.1X for authentication, OAuth2.0 and NACM based authorization decision for different O-RAN interfaces. However, there are no requirements and controls for periodic evaluation of authentication and authorization based on continuous security monitoring related information (e.g. threat assessments, security posture etc.) as well as dynamic policies that trigger-reauthentication and reauthorization of subjects.

Therefore, WG11 proposes to further study and define ZT tenet 6 based access policies for accessing the O-RAN and Non-ORAN (defined) assets of an O-RAN deployment.

* Gap Analysis of the current authentication and authorization security mechanisms for each O-RAN network point of access.
* Define Dynamic Authentication and Authorization policies based on the continuous security monitoring related data (ZT tenet 5), user activity patterns, device hygiene, security posture of the user and the requested access resource.
* Establish Automated Identity Lifecycle Management policies that allow blacklisting, considering the ZT tenet 5 threat and security posture assessment of any user and devices.
* Identity and context-based logical access boundary for devices, infrastructure, application and data.

#### 4.2.6.3 Conclusion

WG11 has addressed DoS prevention and preventing content-based attacks through an interface as well as logging requirements on failed/malicious access request attempts related to ZT tenet 5. However, the dynamic assessment of authentication and authorization processes to continuously reassess trust during ongoing communications, as outlined in ZT tenet 6 is applicable to O-RAN and requires further study.

This entails studying the dynamic authentication and authorization mechanisms based on continuous identity and attributes verification of an ongoing communication. The dynamic access control policies will consider the security monitoring data (ZT tenet 5) and deployment related aspects to dynamically enforce reauthentication and reauthorization of User access to O-RAN assets and revoke access if needed. This tenet allows an operator to define and control the authentication and authorization decision points for the entire O-RAN deployment, that considers continual authentication and conditional authorization to prevent any lateral movement in the O-RAN network.

### ZT Tenet 7 Applicability Study

#### Introduction

**ZT tenet 7: The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.**

Further description in NIST SP 800-207 [i.6] states, this tenet covers Security posture, network traffic, and access request data analysis informs policy creation and enforcement for a robust zero-trust architecture.

#### Applicability Study

In the O-RAN architecture, security monitoring and security log and event management is crucial for maintaining a secure and robust security posture of all O-RAN components. Log analysis, including anomalous user behaviour, unusual network traffic patterns, and unauthorized access attempts, can facilitate the detection and mitigation of lateral movement as observed in [i.11].

With the **ZT tenet 5 we have a Proactive approach**. It focuses on setting up logging of security events to reduce potential damage from the beginning. With the **ZT tenet 7 we have a Reactive approach**. It involves constantly monitoring for suspicious activity after access is granted and it focuses on detecting and responding to unauthorized or unusual activity.

WG11 has specified Security Log Management requirements and controls but has not defined procedures to leverage data collection to improve asset security posture by identifying vulnerabilities, monitoring access patterns, and access request decisions based on contextual insights and behavioural analytics.

It is essential to study the logging and monitoring infrastructure to understand the type of data collected, use data analytics mechanisms to understand the security posture of O-RAN and Non-O-RAN assets. This will be an enabler to build an infrastructure to enforce dynamic security policies thus improving security posture for O-RAN assets and Non-O-RAN assets. Based on contextual insights and behavioural analytics policy enforcement can be in the area of user access to O-RAN and Non O-RAN component, service to service communication, mitigation of adversarial lateral movements, mitigation of DDOS attacks against any interface, isolation of any NF due to abnormal behaviour etc.

For a zero trust O-RAN Architecture, ZT tenet 7 plays a critical role.

#### Conclusion

WG11 should expand on the ZT tenet 7 principles that **allow us to collect as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.** This enables an operator to detect anomalous behaviour, identify potential security threats, and take timely mitigation actions as referenced in [i.10] tenet 7 evaluation**.** WG11 intends to come up with recommendation, industry standard security best practices to attain the advanced zero trust maturity model.

## NIST ZT Tenets applicability summary

All seven ZT tenets are applicable to O-RAN, with varying levels of specification in O-RAN ALLIANCE specifications. Full realization for some tenets may require integration with systems outside the scope of O-RAN, which will be left to the operator. The role of the O-RAN ALLIANCE in these cases should be to produce security requirements, controls and specifications that support these tenets. Table 4.3-1 provides a summary with justification of the NIST ZT tenet applicability study for O-RAN.

Table ‑: NIST ZT Tenet Applicability Summary

|  |  |  |
| --- | --- | --- |
| Tenet | Applicable | Justification |
| Tenet 1 | Checkbox Checked with solid fill | Recognizing all data sources and computing services as resources within O-RAN architecture is vital for holistic ZT security. |
| Tenet 2 | Checkbox Checked with solid fill | This tenet holds significant importance for O-RAN by stressing the necessity of robust security standards across all communications, regardless of their network location. With O-RAN's distinctive features like disaggregation, open interfaces, and third parties' applications, tenet 2 becomes essential for preventing security issues. |
| Tenet 3 | Checkbox Checked with solid fill | Users, services, and applications within the O-RAN system seek access to designated network components. Authenticating each entity based on its distinct identity and adhering to the principle of least privilege are crucial. Through the implementation of Access Control Policies aligned with the Principle of Least Privilege, operators can effectively prevent attackers from moving laterally within the network. |
| Tenet 4 | Checkbox Checked with solid fill | O-RAN should specify the required infrastructure and capabilities for capturing the observable state of the requesting client's (subject's) identity and the requesting device, along with any additional behavioural and environmental attributes relevant to this tenet, to facilitate creation and enforcement of dynamic policies by operators. |
| Tenet 5 | Checkbox Checked with solid fill | O-RAN should establish measures to support security monitoring, integrity assessment, and evaluation of the security posture for all O-RAN assets. These measures may include employing behavioural analytics, managing configurations, conducting software integrity checks, performing vulnerability scans, and detecting security anomalies, among other methods. Outputs from these measures are processed by the operators to decide on access requests. |
| Tenet 6 | Checkbox Checked with solid fill | It is essential to monitor the security posture of the subject and network resources to evaluate the trust at any given point of time and trigger reauthentication and reauthorization if needed to do so. Failure to do so may result in a compromised user account or an internal threat actor remaining undetected, and may trigger reconnaissance, continued access to the protected resource, or lead to a lateral movement in the network, thus causing large outages, data theft, or sabotage of the network. As a result, the O-RAN architecture should adapt the principle of ZT tenet 6 where every access request is continuously reevaluated to determine that the trust can be maintained and established. |
| Tenet 7 | Checkbox Checked with solid fill | To improve the security posture of the system, O-RAN should develop the capability to collect as much information as possible about the current state of assets, network infrastructure and communications. This will enable operators to utilize this information to improve policy creation and enforcement. |

# ZTA Assets

## Asset Categories

Traditional perimeter-based network defenses with multiple layers of disjointed security technologies have proven themselves unable to meet cybersecurity needs in the current threat environment [i.13]. Organizations require a more effective approach to securing their infrastructure and providing unified yet granular access control to data, services, applications, and infrastructure [i.13]. Zero Trust focuses on protecting critical data and resources rather than solely relying on traditional network or perimeter security. ZT implements continuous multi-factor authentication, micro-segmentation, encryption, endpoint security, automation, analytics, and robust auditing across different resources [i.14]. Zero Trust Architecture treats each asset as a micro-perimeter to protect against both internal and external threats [i.8]. To mitigate cyber risk effectively, ZT planners should define the organization's protect surface, which the NSTAC report defines as the area protected by ZT policies [i.15].

In the following, we describe five categories of assets that need to be considered for ZTA analysis. It is important to note that some categories include two types of assets: O-RAN assets and assets that are not specified by O-RAN ALLIANCE. While the later are outside the scope of O-RAN specification, we include them to highlight the importance of considering them for analysis for a holistic ZTA for O-RAN system.

1. **Data:** O-RAN data encompasses both structured and unstructured files and fragments that are currently or have previously been present in O-RAN systems, devices, networks, applications, databases, infrastructure, and backups (including both on-premises and virtual environments), along with their corresponding metadata.
2. **Interfaces:**
   1. O-RAN Interfaces: Interfaces defined and maintained by O-RAN, as specified in [i.1].
   2. Interfaces not specified by O-RAN: This includes interfaces defined and maintained by 3GPP, but seen as part of the O-RAN architecture [i.1]:
3. **Architecture Elements:** This asset category comprises the architecture elements as defined in [i.1].
4. **Infrastructure:** The infrastructure category within O-RAN assets encompasses a wide array of components, including both physical and virtual elements, as well as various platforms. It includes:
5. O-RAN infrastructure assets:
   * **Hardware:** This comprises servers, data centers, and other networking equipment that form the physical foundation of the O-RAN infrastructure. This includes FHGW (Fronthaul Gateway), FHM (Fronthaul Manager), and TNE (Transport Network Element).
   * **Operating System and Firmware:** These are essential software components that provide the foundational functionality for the hardware components, enabling them to operate efficiently and effectively. This includes OS kernel, Bootloader, O-Cloud DMS, and O-Cloud IMS.
   * **Virtualization Layer:** This refers to the software layer that enables the virtualization of hardware resources, allowing for the creation and management of virtual instances of servers, networking equipment, and other infrastructure components. This layer includes components like virtual machines (VMs), containers, and hypervisors.
6. Infrastructure assets not specified by O-RAN: These components are essential for managing and facilitating communication between various O-RAN network elements. This includes GM, which is a component within the O-RAN architecture but not defined by O-RAN ALLIANCE.
7. **Services:** A service is a software component participating in a service-oriented architecture that provides functionality or participates in realizing one or more capabilities [i.20].
   1. O-RAN services:This includes O-RAN services that operate in both on-premises and cloud environments, such as AI/ML workflow services [i.21], O-Cloud O2ims and O2dms services.
   2. Services not specified by O-RAN: It encompasses third-party services providing various functionalities for O-RAN applications, including security services like PKI, IAM, and SIEM.

## Defined Assets

The high-level scope of the assets in scope for the ZTA analysis is outlined in Table 5.2-1.

Table ‑: High Level ZTA Assets for O-RAN

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Scope | Data | Interfaces | Architecture Elements | Infrastructure | Services |
| O-RAN Assets | Keys, Credentials  RAN Analytics  UE-Id  UE-Location  AI/ML training data  Configuration data  Logs | A1, E2, O1, O2, R1, Y1  Open Fronthaul C-Plane, S-Plane, U-Plane, M-Plane  External Interfaces | SMO (including Non-RT RIC and rApps)  Near-RT RIC (including xApps)  O-CU-CP  O-CU-UP  O-DU  O-RU  O-eNB  O-Cloud\* | O-Cloud HW, OS, and virtualization infrastructure  Hardware and OS of O-RAN PNFs  FHGW, FHM, TNE | AI/ML Services |
| Assets not specified by O-RAN ALLIANCE |  | F1-c, F1-u, E1, NG-c, NG-u, X2-c, X2-u, Xn-c, Xn-u, Uu interfaces [i.1] |  | GM | Security Services (PKI, IAM, SIEM) |

NOTE: In O-RAN, O-Cloud is considered an architecture element; however for the purposes of the ZTA security analysis, it is considered as infrastructure.

The detailed list of assets in scope for the ZTA analysis is in clause 6.3 Critical Assets of [i.4] which lists the O-RAN data, interfaces and components that were used to perform security threat modelling and risk assessment and have formed the basis of the development of security requirements and controls within the various security work items.

The following clauses identify new assets in the decoupled SMO, O-Cloud and the Open Fronthaul that have not yet been incorporated into clause 6.3 of [i.4].

## New Assets

### New Assets in the SMO

Table ‑: SMO Assets

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Asset ID | Asset Description | Component | Interface | When | | Protection Level | | | | |
| **At rest** | **In transit** | **Confidentiality** | **Integrity** | **Availability** | **Replay** | **Authenticity** |
| **Components (logical, virtual, physical)** | | | | | | | | | | |
| **ASSET-C-X** | SMO Service: Service Management and Exposure (SME) |  |  | x | x | x | x | x | x | x |
| **ASSET-C-X** | SMO Service: Data Management and Exposure (DME) |  |  | x | x | x | x | x | x | x |
| **ASSET-C-X** | SMO Service: Topology Exposure and Inventory Management (TE&IM) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: rApp Management |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: Network Function Orchestrator (NFO) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: Federated O-Cloud Orchestration and Management (FOCOM) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: RAN NF Fault Management (FM) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: RAN NF Configuration Management (CM) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: RAN NF Performance Management (PM) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: A1 Enrichment Information Management |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: A1 Policy Management |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: SW Package Onboarding |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: Service Orchestration |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: Service Assurance |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: RAN Analytics |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMO Service: AI/ML Workflow |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | SMOS Communications |  |  |  | x | x | x | x | x | x |

### O-Cloud Assets

The table below lists assets associated with O-Cloud, incorporating existing assets from the Threat Model [i.4] and expanding them with new assets based on the ZTA approach.

Table ‑: O-Cloud Assets

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Asset type** | | **Asset ID** | **Asset Title** | **Asset description** | **Security properties** | | |
| **C** | **I** | **A** |
| **Data** | | Existing Assets in the Threat model: ASSET-D-12 to ASSET-D-18, ASSET-D-20, ASSET-D-29, ASSET-D-31 to ASSET-D-38 | | | | | |
| **Services** | | ZT-OCLOUD-S-X1 | O2ims services | It is responsible for infrastructure management services for O-Cloud Nodes. It offers the following services APIs [8]:   * O2ims\_InfrastuctureInventory Services * O2ims\_InfrastructureMonitoring Services * O2ims\_InfrastructureProvisioning Services * O2ims\_InfrastructureSoftwareManagement Services * O2ims\_InfrastructureLifecycleManagement Services | x | x | x |
| ZT-OCLOUD-S-X2 | O2dms services | It is responsible for the deployment management services of the NF Deployment. It offers the following services APIs [7]:   * O2dms\_DeploymentInventory Services * O2dms\_DeploymentProvisioning Services * O2dms\_DeploymentFault Services * O2dms\_DeploymentPerformance Services * O2dms\_DeploymentLifecycle Services | x | x | x |
| **Infra-structure** | **Physical** | ZT-OCLOUD-I-X1 | O-Cloud HW | It includes servers, data centers |  | x | x |
| **Logical** | Existing Assets in the Threat model: ASSET-C-08, ASSET-C-29, ASSET-C-30 | | | | | |
| ZT-OCLOUD-I-X2 | O-Cloud static SW | It includes static O-Cloud SW, e.g., Firmware and BIOS/UEFI, Bootloader, OS kernel |  | x | x |
| ZT-OCLOUD-I-X3 | O-Cloud DMS | O-Cloud DMS software responsible for automating deployment processes and managing the lifecycles of applications within the O-Cloud. |  | x | x |
| ZT-OCLOUD-I-X4 | O-Cloud IMS | O-Cloud IMS software responsible for the management of the cloud's physical and virtual resources. |  | x | x |
| **Applications** | | ZT-OCLOUD-A-X1 | O-RAN Applications workloads | The workloads of O-RAN applications deployed within the O-Cloud. | x | x | x |
| Existing Assets in the Threat model: ASSET-C-23 (O2 protocol stack) | | | | | |

### New Assets in the Open Fronthaul

Table ‑: Open Fronthaul Assets

| Asset ID | Asset Description | Component | Interface | When | | Protection Level | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| At rest | In transit | Confidentiality | Integrity | Availability | Replay | Authenticity |
| **Data & Interfaces** | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |
| **Components (logical, virtual, physical)** | | | | | | | | | | |
| **ASSET-C-X** | Transport Node Equipment (TNE) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | Fronthaul Multiplexor (FHM) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | Fronthaul Gateway (FHGW) |  |  | x |  | x | x | x |  | x |
| **ASSET-C-X** | GM (Grand Master) |  |  | x |  | x | x | x |  | x |

### New Assets in F1 (Midhaul)

Table ‑: F1 Assets

| Asset ID | Asset Description | Component | Interface | When | | Protection Level | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| At rest | In transit | Confidentiality | Integrity | Availability | Replay | Authenticity |
| **Data & Interfaces** | | | | | | | | | | |
| **ASSET-D-X** | The F1-c interface, as defined by 3GPP, is between the gNB-CU-CP and gNB-DU logical nodes. In O-RAN, it reuses the principles and protocol stack defined by 3GPP but is adopted between the O-CU-CP and the O-DU logical nodes, as well as for the definition of interoperability profile specifications. [i.1] | O-DU, O-CU-CP | F1-c |  | x | x | x | x | x | x |
| **ASSET-D-X** | The F1-u interface, as defined by 3GPP, is between the gNB-CU-UP and gNB-DU logical nodes. In O-RAN, it reuses the principles and protocol stack defined by 3GPP but is adopted between the O-CU-UP and the O-DU logical nodes, as well as for the definition of interoperability profile specifications. [i.1] | O-DU, O-CU-UP | F1-u |  | x | x | x | x | x | x |

# Reference ZTA Security Requirements

## ZTA Framework

### Introduction

There are several frameworks or roadmaps developed by US government agencies that provide organizations at the start of their ZT journey with a reference for charting their transition towards a ZTA. This clause gives an overview and comparison of the CISA Zero Trust Maturity Model and the DoD Zero Trust Strategy and Reference Architecture, and provides the selection of the ZTA framework for O-RAN evaluation.

### CISA's Zero Trust Maturity Model (ZTMM)

The US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed the Zero Trust Maturity Model (ZTMM) [i.9]. ZTMM offers a systematic approach for organizations seeking to sustain ongoing modernization initiatives in the dynamic realms of cybersecurity and technology. It serves as a guide for organizations in crafting and executing their transition plans towards Zero Trust Architectures. CISA's Maturity Model (MM) outlines a phased and incremental approach for the effective implementation of a ZTA across four stages: Traditional, Initial, Advanced, and Optimal, as illustrated in Figure 6.1‑1. Emphasizing a comprehensive perspective, the model introduces five critical pillars for Zero Trust: Identity, Devices, Networks, Applications & Workloads, and Data. Each pillar is supported by distinct Pillar-specific Functions, delineating specific requirements that should be maintained across the four stages. For instance, under the Identity pillar, functions are specified with requirements tailored to each stage. Additionally, the model incorporates Cross-cutting Functions, which traverse all pillars and can evolve throughout the four stages. These cross-cutting functions encompass Visibility and Analytics, Automation and Orchestration, and Governance. The overarching concept is for agencies to assess their current enterprise stage, establish a target stage, conduct a meticulous gap analysis, and formulate a strategic plan accordingly. This structured approach ensures a methodical progression towards optimal Zero Trust implementation, tailored to the specific needs and requirements of each organization.

Diagram

Description automatically generated with low confidence

Figure ‑: CISA Zero Trust Maturity Model

### DoD Zero Trust Strategy and Reference Architecture

The United States Department of Defense (DoD) Zero Trust Strategy [i.18] and Reference Architecture [i.14] collectively form a comprehensive framework guiding the implementation of zero trust principles. The Reference Architecture (RA) serves as a foundational element, presenting a capability-centric framework structured around architectural Pillars and Principles. This framework provides essential guidance for the strategic development of zero trust concepts, offering a systematic approach to conduct gap analyses, formulate requirements, oversee implementation, guide execution decision-making, and facilitate the procurement and deployment of necessary zero trust capabilities and activities. Simultaneously, the DoD Zero Trust Strategy serves as a crucial companion, furnishing actionable guidance that spans the entire spectrum of zero trust initiatives. The strategy encompasses a holistic approach, aligning seamlessly with the Reference Architecture to fortify the DoD's cybersecurity posture in a rapidly evolving threat landscape.

The ZT Pillars in the DoD ZT Architecture align seamlessly with industry-standard identification of ZT Pillars. As illustrated in Figure 6.1‑2, the seven Pillars within the DoD ZT Architecture include: User, Devices, Network, Applications/Workload, Data, Visibility/Analytics, and Automation/Orchestration. Each Pillar serves as a key focus area for the implementation of specific zero trust controls, ensuring a holistic and effective security approach.

Each pillar consists of multiple capabilities. Capabilities mean the ability to achieve a specific goal using different methods and resources. These capabilities use current technologies in zero trust and may change in the future. The Pillars and capabilities work together to give the best visibility and protection to data. Moreover, the DoD proposed the DoD ZT Capability roadmap that describes how the Department currently envisions achieving the capability-based outcomes and activities sequenced over time to achieve the DoD Zero Trust Target Level and Advanced Zero Trust [i.18, i.19].

The DoD framework also includes a Maturity Model that outlines the logical progression from an existing security model to an advanced zero trust architecture. This Maturity Model serves as a reference to assist information system owners in conceptualizing their transition from their current state to their desired architecture. The stages of the Maturity Model begin with As-Is state and progress through Baseline and Intermediate to Advanced stages, reflecting the evolution of zero trust capabilities and controls [i.14].

It is also important to note that the DoD Zero Trust Target Level encompasses a defined subset of DoD Zero Trust capabilities. This level includes both Baseline and Intermediate zero trust maturity stages, as outlined by the Zero Trust Reference Architecture (ZT RA). The DoD Advanced Zero Trust, on the other hand, represents the achievement of the full set of DoD-identified zero trust capabilities and aligns with the Advanced maturity stage [i.14, i.18].

Graphical user interface, table

Description automatically generated

Figure ‑: DoD ZT Capabilities

### Comparison of ZTMM models

CISA ZTMM [i.9] and DoD ZTMM [i.14] complement NIST's ZTA by offering a roadmap for organizations to assess their current maturity level and provide guidance on steps to incrementally progress to higher maturity stages. The CISA and DoD ZTMMs mostly align with some differences, as described below.

The four CISA ZTMM stages - Traditional, Initial, Advanced, and Optimal - are achieved for each of five pillars: Identity, Devices, Networks, Applications and Workloads, and Data. The CISA ZTMM also includes three cross-cutting functions across the five pillars: Visibility and Analytics, Automation and Orchestration, and Governance. These cross-cutting functions align with NIST tenets 4, 5, and 7 mentioned above.

The four DoD ZTMM stages – As-is, Baseline, Intermediate, and Advanced - are achieved for each of seven pillars: User, Device, Networks, Applications and Workloads, Data, Visibility and Analytics, and Automation and Orchestration. The last two pillars in the DoD ZTMM model are considered cross-cutting functions by CISA.

A diagram overlaying the CISA and DoD ZTMM models is shown in Figure 6.1‑3.



Figure 6.1‑3: Comparison of US CISA and DoD ZTMM

### Selection of CISA ZTMM Model

The CISA ZTMM version 2 [i.9] has been selected as the primary reference model for two reasons:

1. CISA embeds its cross-cutting functions across its five pillars, instead of making those standalone pillars as the DoD ZTMM does. The CISA approach is preferred for O-RAN since Visibility and Analytics and Automation and Orchestration are applicable to all pillars and should not be silo'd.
2. CISA does not prescribe a timeline to reach its final stage, Optimal. While the DoD provides guidelines for implementation timelines, these are applicable to DoD use cases, which are outside the scope of O-RAN ALLIANCE.

## Target ZTA Security Requirements

### Introduction

CISA's ZTMM offers four stages of zero trust journey with incremental approach to achieve ZTA for the five identified pillars - **Identity, Devices, Networks, Applications and Workloads, and Data** as well as the three cross cutting pillars - **Visibility and Analytics, Automation and Orchestration, and Governance** that encompass the five pillars. Each pillar has specific functions that progresses on the incremental journey to achieve ZTA.

In this clause, we specify the O-RAN ZTA security requirements across the five pillars to identify gaps between O-RAN's current security requirements and those outlined in the CISA-aligned O-RAN ZTA security requirements. This assessment will help evaluate O-RAN's current zero trust maturity stage and, based on the gap analysis, define new security requirements and controls if needed.

NOTE: The cross-cutting pillars **Visibility and Analytics, Automation and Orchestration, and Governance** will be included in a separate clause for specifying recommendations and requirements as needed.

Each sub-clause of this clause is dedicated to a CISA ZTMM pillar and the "Guidance for Gap Analysis" of each function of a pillar provides information that can aid in gap analysis.

The gap analysis is being performed against the INITIAL stage of CISA ZTMM security requirements.

### Identity

#### Introduction

In O-RAN identity encompasses three entities namely users, devices, and software applications. The identity plays an important role to provide a unique attribute to the entity which is used to authenticate and authorize an entity.

The Identity Pillar has the following pillar specific functions defined in CISA ZTMM:

1. **Authentication** - Verification of users, devices, and software applications identities.
2. **Access Management** - Authorization ensures what resources and data an authenticated entity (user, device, or application) can access.
3. **Identity Stores** - Identity Stores are repositories where identity information is stored, managed, and accessed.
4. **Risk Assessments** - Continuously evaluating and mitigating identity-related risks through adaptive policies and real-time monitoring.

#### Authentication

##### Introduction

Authentication function applies to the following three entities - users, devices, and software applications.

##### O-RAN ZTA Security Requirements for Authentication

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CISA ZTMM Function | Traditional | Initial | Advanced | Optimal |
| Authentication | Based on  **credentials** | **Credentials +** **Additional attributes** (policy driven) | **Phishing resistant MFA\*** (for e.g. FIDO)  \*applies to users | **Continual** Authentication |

##### Guidance for Gap Analysis:

1. Additional attributes (contextual attributes) apply only to human user and external communication, and applicable to Architecture Elements having user access such as SMO.
2. Phishing resistant MFA security control applies to human user access and not applicable to application-to-application access and device authentication.
3. If there is mutual authentication for internal communications, we consider the stage as INITIAL.
4. For internal interfaces, authentication based on credentials alone (certificate, pre-shared key, etc.) can be considered as meeting INITIAL maturity level.

#### Access Management (Authorization)

##### Introduction

Authorization ensures what resources and data an authenticated entity (user, device, or application) is allowed to access and what actions they are permitted to perform within a O-RAN network or system.

##### O-RAN ZTA Security Requirements for Access Management (Authorization)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CISA ZTMM Function | Traditional | Initial | Advanced | Optimal |
| Access management (Authorization) | **Long Lived access** with **manual revoking** for privilege and unprivileged accounts | **Short lived access** for privileged access requests, with **automated revoking** | **Need based** and **Session based access** for all accounts tailored to actions and resources | **Just-in-time** and **Just-enough** access provided through automation |

##### Guidance for Gap Analysis:

1. This function applies to APIs and user access.
2. For applications, static role assignments (e.g. role binding of a service account) with ephemeral tokens can be considered as INITIAL stage.
3. For users, tokens with expiry can be considered as INITIAL stage.

#### Identity Stores

##### Introduction

Identity Stores are repositories where identity information is stored, managed, and accessed. They are crucial for managing access, authentication, and authorization. In O-RAN, addressing Zero Trust Architecture (ZTA) requirements necessitates capturing, storing, and managing the identities of various actors—including administrators, applications, services, and devices—and their associated credentials and attributes. This is accomplished through the identity stores function within the identity pillar.

##### O-RAN ZTA Security Requirements for Identity Stores

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Identity Stores** | **Self-Managed On Prem** Identity Stores | **Self-managed** and externally **hosted identity stores** co-exist with limited connectivity (SSO) | **Consolidation** of Self-managed and hosted identity stores. | **Centralized** Identity Stores |

##### Guidance for Gap Analysis:

1. None as this is a new function.
2. WG11 to provide recommendation for Identity Stores.

#### Risk Assessment

##### Introduction

Conducting Identity Risk Assessments for users, devices, and software application entities is crucial for advancing towards a Zero Trust Architecture (ZTA). Many other CISA ZTMM functions in other pillars depend on the risk assessment function in the identity pillar. This includes Network Traffic Management in the networks pillar, application access in the applications and workloads pillar, and data access in the data pillar.

##### O-RAN ZTA Security Requirements for Risk Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CISA ZTMM Function | Traditional | Initial | Advanced | Optimal |
| Risk Assessment | **Limited** identity risk assessment | Identity risk assessment though **manual and static methods** | **Automated identity risk assessment** to enforce dynamic access decisions and response activities. | **Continuous Identity Risk Assessment** in **real time** for adapting **dynamic** ongoing protection mechanism. |

##### Guidance for Gap Analysis:

1. None as this is a new function.
2. WG11 to provide recommendation for Identity Risk Assessments.

### Devices

#### Introduction

The Devices pillar includes the O-RAN network elements that fall under the infrastructure asset category. It includes Physical devices as well as virtual and cloud hardware. The pillar specific functions are as following:

1. **Policy Enforcement & Compliance Monitoring**- Visibility of all devices and compliance and unified management and enforcement of policies.
2. **Asset & Supply Chain Risk Management**- Asset management tracks all physical, virtual, and cloud devices, using automated supply chain risk management to ensure comprehensive visibility and resilience against supply chain failures.
3. **Resource Access**- Secure and controlled access to resources based on device characteristics, risk analytics data.
4. **Device Threat Protection**- Implement security measures to detect, prevent, and respond to threats targeting devices.

The potential O-RAN relevant zero trust functions for gap analysis study are Policy Enforcement and Compliance Monitoring, Resource Access, and Device Threat Protection.

The Asset & Supply Chain Risk Management function is for further study.

#### Policy enforcement & Compliance monitoring

##### Introduction

Manage dynamic inventory of all assets including their hardware, software, firmware, etc., along with their configurations and known associated vulnerabilities. Define device compliance policies and policy enforcement for all assets.

##### O-RAN ZTA Security Requirements for Policy enforcement and compliance monitoring

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CISA ZTMM Function | Traditional | Initial | Advanced | Optimal |
| Policy Enforcement and Compliance Monitoring | **No** **device visibility** for device compliance **No policy enforcement mechanism** or managing software, configurations, or vulnerabilities. | **Basic** Device characteristics visibility. **Basic** policy enforcement mechanism for managing software, configurations, or vulnerabilities. | **Automated** methods to manage devices and virtual assets. **Automated policies** to approve software configuration and identify vulnerabilities and install patches. | **Continual verification** of devices and virtual assets compliance and **Unified management and enforcement of policies** |

##### Guidance for Gap Analysis:

1. Please refer to the table in clause 6.2.3.2.2 for different stages of this function, since there is no specific guidance.

#### Resource Access (Authorization)

##### Introduction

The access to resources is allowed only for secured devices.

##### O-RAN ZTA Security Requirements for Resource Access

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CISA ZTMM Function | Traditional | Initial | Advanced | Optimal |
| Resource Access (Authorization) | No visibility into devices or virtual assets used to access resources | **Some visibility** into devices or virtual assets' **characteristics** to **approve** resource **access**. | **Full visibility** into devices; **Initial resource access** considers **verified** device or virtual asset insights. | **All** resource access considers **real-time risk analytics** within devices and virtual assets. |

##### Guidance for Gap Analysis:

1. Use device characteristics or virtual asset characteristics (e.g. Access Control Rules (policy), environmental conditions) to approve resource access to align to the INITIAL stage.

#### Device Threat Protection

##### Introduction

The devices are deployed with threat protection solutions to detect, prevent, respond, and recover from threats.

##### O-RAN ZTA Security Requirements for Device Threat Protection

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Device Threat Protection** | **Manual deployment** of **threat protection** capabilities to some devices. | Some **automated** processes for deploying and updating threat protection capabilities to devices and to virtual assets with **limited policy enforcement and compliance monitoring integration.** | Consolidate **threat protection** capabilities to **centralized solutions** for devices and virtual assets and integrates most of these capabilities with policy enforcement and compliance monitoring. | **Centralized threat protection security solution(s)** deployed with advanced capabilities for all devices and virtual assets and **a unified approach for device threat protection, policy enforcement, and compliance monitoring.** |

##### Guidance for Gap Analysis:

1. The guidance for gap analysis of 'Device Threat Protection' function is for further study.

### Networks

#### Introduction

In O-RAN, the network pillar of CISA ZTMM encompasses internal, external interfaces of Architecture elements as well as infrastructure assets. The network pillar specific functions are as following.

1. **Network Segmentation** - Dividing the network into smaller, isolated segments to enhance security based on application profiles and risk
2. **Network Traffic Management** - Define network rules and configuration based on application profile assessment.
3. **Traffic Encryption** - All data transmitted across the network is encrypted to protect confidentiality and integrity, using robust key management and adaptive encryption strategies.
4. **Network Resilience** - Continuous availability and resilience for all workloads.

The O-RAN relevant zero trust functions for gap analysis study are **Network Segmentation**, **Traffic Encryption** and **Network Traffic Management**.

The Network Resilience function is for future study.

#### Network Segmentation

##### Introduction

The O-RAN Network functions are secured with micro-perimeters and all interfaces associated with it are secured.

##### O-RAN ZTA Security Requirements for Network Segmentation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Network Segmentation** | **Perimeter / Macro-** segmentation | **Micro segmentation** for critical workloads, and **limiting network access** to a specific function | **Application-Aware** micro-segmentation with ingress/egress micro-perimeters | **Dynamic policy driven application-Aware** Micro-segmentation; Allows for JEA/JIT setup/teardown of micro-perimeters |

##### Guidance for Gap Analysis:

1. Perimeter based security protection like VPN tunnel access is considered as Traditional.
2. Micro segmentation for critical workloads using namespaces, VLANs is considered as INITIAL .

NOTE: Definition of micro-perimeter in the scope of O-RAN ALLIANCE is yet to be specified.

#### Traffic Encryption

##### Introduction

Encryption of traffic through internal and external interfaces with secure key management.

##### O-RAN ZTA Security Requirements for Traffic Encryption

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Traffic Encryption** | **Minimal** traffic encryption with **manual or ad hoc key management** | **Encryption for all** internal (and preferably external) application traffic, with **formalized key management policies and secure encryption keys**. | Encryption for **all traffic**, with **key** and **certificate life cycle management** | Encryption of all traffic, enforces **least privilege** principles and **crypto-agility** |

##### Guidance for Gap Analysis:

1. Symmetric key based encryption methods, such as IPsec for E2, can be classified as being in the INITIAL stage.
2. Certificate lifecycle management will upgrade the maturity to Advanced.

#### Network Traffic Management

##### Introduction

Network Traffic Management involves implementing static and dynamic network rules for ingress and egress traffic, which are automatically adapted based on risk and application needs.

##### O-RAN ZTA Security Requirements for Network Traffic Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Network Traffic Management** | **Static** **network** rules/policies apply to **critical applications** | **Static Ingress** and **Egress** network rules/policies to all applications | **Dynamic** network policies based on **risk** that are automatically adapted | **Dynamic** network policies based on risk; **application** needs that are automatically adapted |

##### Guidance for Gap Analysis:

1. Support for ingress and egress policies align with the INITIAL stage.

NOTE: The support for ingress and egress policies is provided by the O-RAN Specifications. But the decision to provision the rules and policies is left to the operator.

### Applications and Workloads

#### Introduction

Applications and workloads include systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments [i.9]. In O-RAN, this pillar corresponds to the following asset categories: architecture elements, interfaces, and services. These asset categories are described in clause 5. The application and workloads pillar specific functions are as following:

1. **Application Access** - This function outlines the requirements that must be met by the access control mechanism to authorize access to various applications within the system.
2. **Application Threat Protections** – This function describes how to incorporate threat protections into the workflows of applications.
3. **Accessible Applications** – This function describes how various applications within the system should be made available and accessible.
4. **Secure Application Development and Deployment Workflow** – This function details the requirements for secure development and deployment workflows for various applications within the system.
5. **Application Security Testing** – This function specifies the requirements for testing the security of applications.

The O-RAN relevant zero trust functions for gap analysis study are **Application Access**, **Application Threat Protections**, **Accessible Applications**, **Secure Application Developments and Deployment Workflow**, and **Application Security Testing**.

#### Application Access

##### Introduction

Application Access, also known as Access Authorization, is critical for limiting access to application assets only to authorized entities and removing access when no longer needed. It evolves through four distinct stages of sophistication, reflecting the maturity in managing application access.

##### O-RAN ZTA Security Requirements for Application Access

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Application Access** | Access based on static attributes and local authorization | Begins to implement authorizing access capabilities to applications that incorporate contextual information (e.g., identity, device compliance, and/or other attributes) per request with expiration. | Automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles. | Continuously authorizes application access, incorporating real-time risk analytics and factors such as behaviour or usage patterns. |

##### Guidance for Gap Analysis

1. Access authorization capabilities utilize contextual information such as identity, device compliance, and other attributes to make decisions on various requests for accessing application assets.
2. Authorization is granted per request with expiration.

#### Application Threat Protections

##### Introduction

As reliance on applications grows, so does the risk of cyber threats targeting these critical assets. To counteract these risks effectively, O-RAN should implement Application Threat Protection capabilities.

##### O-RAN ZTA Security Requirements for Application Threat Protections

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Application Threat Protections** | Threat protections have minimal integration with application workflows, applying general-purpose protections for known threats. | Integrates threat protections into mission-critical application workflows, applying protections against known threats and addressing some application-specific threats. | Integrates threat protections into all application workflows, safeguarding against certain application-specific and targeted threats. | Integrates advanced threat protections into all application workflows, providing real-time visibility and content-aware protections against sophisticated attacks tailored to applications. |

##### Guidance for Gap Analysis

1. Threat protection is integrated into mission-critical application workflows.
2. Threat protections safeguard applications against known threats and address some application-specific threats.

#### Accessible Applications

##### Introduction

Accessibility to applications is paramount for organizational efficiency and productivity.

##### O-RAN ZTA Security Requirements for Application Accessibility

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Accessible Applications** | Some mission-critical applications are made available exclusively over private networks and protected public network connections (e.g., VPN), with monitoring. | Some of the applicable mission-critical applications are made accessible over open public networks to authorized users with specific needs via brokered connections. | Most of the applicable mission-critical applications are made available over open public network connections to authorized users as needed. | All applicable applications are made available over open public networks to authorized users and devices, where appropriate, as needed. |

##### Guidance for Gap Analysis

1. Applicable mission-critical applications are available over open public network connections to authorized users as needed.

#### Secure Application Development and Deployment Workflow

##### Introduction

The Secure Application Development and Deployment Workflow is crucial for O-RAN as it ensures the integrity and security of applications across diverse and distributed network components.

##### O-RAN ZTA Security Requirements for Secure Application Development

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Secure Application Development and Deployment Workflow** | There are ad hoc development, testing, and production environments with non-robust code deployment mechanisms. | Infrastructure is provided for development, testing, and production environments (including automation) with formal code deployment mechanisms through CI/CD pipelines and requisite access controls supporting least privilege principles. | Distinct and coordinated teams for development, security, and operations are used, while developer access to the production environment for code deployment is removed. | Immutable workloads are leveraged where feasible, only allowing changes to take effect through redeployment. Administrator access to deployment environments is removed in favor of automated processes for code deployment. |

##### Guidance for Gap Analysis

1. Infrastructure for development, testing, and production environments (including automation).
2. Formal code deployment mechanisms through CI/CD pipelines.
3. Access controls support least privilege principles.

#### Application Security Testing

##### Introduction

Application security testing is crucial for identifying and mitigating vulnerabilities early, reducing the risk of security breaches. This proactive approach ensures the consistent protection of applications, safeguarding sensitive data and maintaining the integrity of the O-RAN system.

##### O-RAN ZTA Security Requirements for Application Security Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Application Security Testing** | Application security testing is conducted prior to deployment, primarily through manual testing methods. | Static and dynamic testing methods, including manual expert analysis, are employed for security testing before application deployment. | Application security testing is seamlessly integrated into the application development and deployment process, incorporating periodic dynamic testing methods. | Application security testing is integrated across the software development lifecycle within the enterprise, with routine automated testing of deployed applications. |

##### Guidance for Gap Analysis

1. Utilization of static and dynamic testing methods for security testing.
2. Performance of security testing including manual expert analysis before application deployment.

### Data

#### Introduction

In O-RAN, data encompasses both structured and unstructured files and fragments that are currently or have previously been present in O-RAN systems, devices, networks, applications, databases, infrastructure, and backups (including both on-premises and virtual environments), along with their corresponding metadata.

1. **Data Inventory Management** – This function describes how the system inventories its data.
2. **Data Categorization** – This function outlines how data should be categorized within the system.
3. **Data Availability** – This function specifies how various data within the system should be made available.
4. **Data Access** - This function outlines the requirements that must be met by the access control mechanism to authorize access to various data within the system.
5. **Data Encryption** – This function specifies requirements for encrypting data within the system.

The potential O-RAN relevant zero trust functions for gap analysis study are **Data Inventory Management**, **Data Categorization**, **Data Availability**¸ **Data Access**, and **Data Encryption**.

#### Data Inventory Management

##### Introduction

A data inventory is a comprehensive catalogue that identifies and inventories all available data within the O-RAN system. It should detect and incorporate any changes to the data landscape. This inventory includes metadata about the data, providing a detailed reference that aids in understanding and managing the organization's data assets effectively.

##### O-RAN ZTA Security Requirements for Data Inventory Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Data Inventory Management** | Manually identifies and inventories some O-RAN data (e.g., mission critical data). | Automate data inventory processes for both on-premises and in cloud environments, covering most O-RAN data, and begins to incorporate protections against data loss. | Automate data inventory and tracking all applicable data, with data loss prevention strategies based upon static attributes and/or labels. | Continuously inventories all applicable data and employs robust data loss prevention strategies that dynamically block suspected data exfiltration. |

##### Guidance for Gap Analysis

1. Automated data inventory processes for both on-premises and in cloud environments, which covers most system data.
2. Protections against data loss are beginning to be incorporated.

#### Data Categorization

##### Introduction

Establishing granular data categorization integrated into access control systems consistently and correctly is required for machine enforceable data access controls, risk assessment, and situational awareness. As data categorization and labelling practices mature, labelling should become automated to meet scaling demands and provide better labelling accuracy.

##### O-RAN ZTA Security Requirements for Data Categorization

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Data Categorization** | Limited and ad hoc data categorization capabilities. | Implement a data categorization strategy with defined labels and manual enforcement mechanisms. | Automate some data categorization and labeling processes in a consistent, tiered, targeted manner with simple, structured formats and regular review. | Automate data categorization and labeling enterprise-wide with robust techniques; granular, structured formats; and mechanisms to address all data types. |

##### Guidance for Gap Analysis

1. A data categorization strategy with defined labels and manual enforcement mechanisms.

#### Data Availability

##### Introduction

Data Availability refers to the ability of an organization to ensure that its data is accessible when needed, both in terms of current and historical data. This function progresses through various stages of sophistication and reliability, marked by increasing redundancy, optimization, and user-centric access methods.

##### O-RAN ZTA Security Requirements for Data Availability

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Data Availability** | Data stored on-premises with some off-site backups. | Data stored in redundant mode (e.g., cloud) and maintained in off-site backups for on premises data. | Data stores in redundant mode with access to historical data. | Dynamically Optimized data availability, including historical data, as per user and entity need. |

##### Guidance for Gap Analysis

1. Data stored in redundant mode (e.g., cloud).
2. Data maintained in off-site backups for on premises data.

#### Data Access

##### Introduction

Data access control aims to restrict access to and usage of data based on properties and attributes associated with the data, the user/device, along with any other relevant information. This ensures that unauthorized entities or entities using unauthorized devices cannot access the data. Additionally, it ensures that users and devices with access to the data undergo continuous attribute inspection through various policy decisions and enforcement points within the architecture. This function progresses through several stages, evolving from static access control to dynamic, just-in-time, and just-enough data access controls.

##### O-RAN ZTA Security Requirements for Data Access

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Data Access** | Users and entities access to data is governed through static access control | Automated data access controls that incorporate elements of least privileges are deployed. | Automated data access controls are time-limited and consider contextual attributes such as identity, device risk, application, and data category. | Automated dynamic just-in-time and just-enough data access controls are implemented with continuous review of permissions. |

##### Guidance for Gap Analysis:

1. Automated data access control.
2. Elements of least privileges are incorporated with the automated data access control.

#### Data Encryption

##### Introduction

Data encryption is crucial for protecting data against unauthorized access, modification, or redistribution. Encrypting data ensures that organizations can protect their data even if it is exfiltrated or lost, as long as the decryption keys remain secure and out of the hands of malicious actors.

##### O-RAN ZTA Security Requirements for Data Encryption

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Data encryption** | Basic encryption is applied to minimal data (both at rest and in transit), utilizing manual or ad hoc processes for managing and securing encryption keys. | All data in transit and, where feasible, data at rest are encrypted. Key management policies and secure encryption keys are beginning to be formalized. | All data at rest and in transit across the O-RAN system are encrypted to the maximum extent possible, cryptographic agility is being incorporated, and encryption keys are protected. | Data in use is encrypted where appropriate, least privilege principles for secure key management system-wide are enforced, and encryption is applied using up-to-date standards and cryptographic agility to the extent possible. |

##### Guidance for Gap Analysis

1. Encrypted data in transit and, where feasible, data at rest.
2. Key management policies and secure encryption keys are beginning to be formalized.

### Cross-Cutting Capabilities

#### Introduction

The cross-cutting capabilities Visibility and Analytics, Automation and Orchestration, and Governance provide opportunities to integrate advancements across each of the five pillars. Visibility and Analytics supports comprehensive visibility that informs policy decisions and facilitates response activities. Automation and Orchestration capabilities leverage these insights to support robust and streamlined operations to handle security incidents and respond to events as they arise. Governance enables agencies to manage and monitor their regulatory, legal, environmental, federal, and operational requirements in support of risk-based decision making. Governance capabilities also ensure the right people, process, and technology are in place to support mission, risk, and compliance objectives [i.9]. CISA ZTMM recommends that these capabilities mature both in relation to each specific pillar and independently of the pillars. This clause outlines the O-RAN target security requirements for the CISA ZTMM cross-cutting capabilities. It begins by presenting the general O-RAN ZTA security requirements for visibility and analytics, and then details these requirements across the various pillars. The governance capability is considered out of scope, as it pertains to defining and enforcing policies, which falls under operational scope.

#### High level maturity evolution for Cross-Cutting Capabilities

##### Visibility and Analytics

###### O-RAN ZTA Security Requirements for Visibility and Analytics Cross-cutting Capability

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Visibility and Analytics** | Manually collecting limited logs with low fidelity and minimal analysis. | Begins the automation of the collection and analysis of logs and events for mission critical functions and regularly assesses processes for gaps in visibility. | Expands the automated collection of logs and events (including virtual environments) for centralized analysis that correlates across multiple sources. | Maintains comprehensive visibility enterprise-wide via centralized dynamic monitoring and advanced analysis of logs and events. |

###### Guidance for Gap Analysis

1. The automation of the collection and analysis of logs and events for mission-critical functions is initiated.
2. Processes are regularly assessed for gaps in visibility.

##### Automation and Orchestration

###### O-RAN ZTA Security Requirements for Automation and Orchestration Cross-cutting Capability

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Automation and Orchestration** | Relies on static and manual processes to orchestrate operations and response activities with limited automation. | Begins automating orchestration and response activities in support of critical mission functions. | Automates orchestration and response activities leveraging contextual information from multiple sources to inform decisions. | Orchestration and response activities dynamically respond to changing requirements and environmental changes. |

###### Guidance for Gap Analysis

1. The automation of orchestration and response activities in support of critical mission functions is initiated.

#### Identity Cross-Cutting Capabilities

##### Visibility and Analytics

Collecting and analyzing user and entity logs is crucial for maintaining network security and identifying potential threats. User and entity behaviour analytics (UEBA) leverages this log data to detect abnormal behaviours, which are often indicative of security incidents. By correlating information across multiple log sources, UEBA can identify unusual patterns that single or limited log sources might miss. This comprehensive analysis is essential because cyber actors frequently attempt to blend in with regular network activities, making it challenging to spot their malicious actions. Through thorough log collection and analysis, organizations can enhance their ability to detect, investigate, and respond to security threats effectively [i.22].

###### O-RAN ZTA Security Requirements for Visibility and Analytics in the Identity Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Visibility and Analytics Capability** | Collects user and entity activity logs, especially for privileged credentials, and performs some routine manual analysis. | Collects user and entity activity logs and performs routine manual analysis and some automated analysis, with limited correlation between log types. | Performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility. | Maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behaviour-based analytics. |

###### Guidance for Gap Analysis

1. Collecting user and entity activity logs.
2. Performing Routine Analysis:
   1. Conduct regular manual analysis of the logs.
   2. Implement some automated analysis, with limited correlation between different log types.

##### Automation and Orchestration

###### O-RAN ZTA Security Requirements for Automation and Orchestration in the Identity Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Automation and Orchestration Capability** | Manually orchestrates (onboards, offboards, and disables) self-managed identities (users and entities), with little integration, and performs regular review. | Manually orchestrates privileged and external identities and automates orchestration of non-privileged users and of self-managed entities. | Manually orchestrates privileged user identities and automates orchestration of all identities with integration across all environments. | Automates orchestration of all identities with full integration across all environments based on behaviours, enrollments, and deployment needs. |

###### Guidance for Gap Analysis

1. Manually orchestrates privileged and external identities.
2. Automates orchestration of non-privileged users.
3. Automates orchestration of self-managed entities.

#### Devices Cross-Cutting Capabilities

##### Visibility and Analytics

###### O-RAN ZTA Security Requirements for Visibility and Analytics in the Devices Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Visibility and Analytics Capability** | Uses a physically labeled inventory and limited software monitoring to review devices on a regular basis with some manual analysis. | Uses digital identifiers alongside a manual inventory and endpoint monitoring of devices when available. Some devices and virtual assets are under automated analysis (e.g., software-based scanning) for anomaly detection based on risk. | Automates both inventory collection and anomaly detection to detect unauthorized devices. | Automates status collection of all network-connected devices and virtual assets while correlating with identities, conducting endpoint monitoring, and performing anomaly detection to inform resource access. Tracks patterns of provisioning and/or de-provisioning of virtual assets for anomalies. |

###### Guidance for Gap Analysis

1. Digital Identifiers: Use digital identifiers alongside a manual inventory and endpoint monitoring of devices when available.
2. Automated Analysis: Ensure some devices and virtual assets are under automated analysis (e.g., software-based scanning) for anomaly detection based on risk.

##### Automation and Orchestration

###### O-RAN ZTA Security Requirements for Automation and Orchestration in the Devices Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Automation and Orchestration Capability** | Manually provisions, configures, and/or registers devices within the enterprise. | Begins to use tools and scripts to automate the process of provisioning, configuration, registration, and/or deprovisioning for devices and virtual assets. | Monitoring and enforcement mechanisms are implemented to identify and manually disconnect or isolate non-compliant devices and virtual assets. | Fully automated processes are in place for provisioning, registering, monitoring, isolating, remediating, and deprovisioning devices and virtual assets. |

###### Guidance for Gap Analysis

1. Utilization of monitoring and enforcement mechanisms to identify and manually disconnect or isolate non-compliant devices and virtual assets.

#### Networks Cross-Cutting Capabilities

##### Visibility and Analytics

###### O-RAN ZTA Security Requirements for Visibility and Analytics in the Networks Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Visibility and Analytics Capability** | Incorporates limited boundary-focused network monitoring capabilities with minimal analysis to start developing centralized situational awareness. | Employs network monitoring capabilities based on known indicators of Compromise (including network enumeration) to develop situational awareness in each environment and begins to correlate telemetry across traffic types and environments for analysis and threat hunting activities. | Deploys anomaly-based network detection capabilities to develop situational awareness across all environments, begins to correlate telemetry from multiple sources for analysis, and incorporates automated processes for robust threat hunting activities. | Maintains visibility into communication across all agency networks and environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources. |

###### Guidance for Gap Analysis

1. Utilize network monitoring capabilities based on known indicators of compromise, including network enumeration, to develop situational awareness in each environment.
2. Commence correlating telemetry across traffic types and environments to facilitate analysis and threat hunting activities.

##### Automation and Orchestration

###### O-RAN ZTA Security Requirements for Automation and Orchestration in the Networks Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Automation and Orchestration Capability** | Utilizes manual processes to manage the configuration and resource lifecycle for networks and environments with periodic integration of policy requirements and situational awareness. | Begins employing automated methods to manage the configuration and resource lifecycle for some networks or environments and ensures that all resources have a defined lifetime based on policies and telemetry. | Uses automated change management methods (e.g., CI/CD) to manage the configuration and resource lifecycle for all networks and environments, responding to and enforcing policies and protections against perceived risks. | Networks and environments are defined using infrastructure-as-code managed by automated change management methods, including automated initiation and expiration to align with changing needs. |

###### Guidance for Gap Analysis

1. Initiate the use of automated methods to manage the configuration and lifecycle of resources within specific networks or environments.
2. Ensure that all resources have a defined lifetime determined by policies and telemetry data.

#### Applications & Workloads Capabilities

##### Visibility and Analytics

###### O-RAN ZTA Security Requirements for Visibility and Analytics in the Applications & Workloads Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Visibility and Analytics Capability** | Performs some performance and security monitoring of mission critical applications with limited aggregation and analytics. | Begins to automate application profile and security monitoring for improved log collection, aggregation, and analytics. | Automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility | Performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility. |

###### Guidance for Gap Analysis

1. Initiate the automation of application profile and security monitoring processes for improved log collection, aggregation, and analytics.

##### Automation and Orchestration

###### O-RAN ZTA Security Requirements for Automation and Orchestration in the Applications & Workloads Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Automation and Orchestration Capability** | Manually establishes static application hosting location and access at provisioning with limited maintenance and review. | Periodically modifies application configurations (including location and access) to meet relevant security and performance goals. | Automates application configurations to respond to operational and environmental changes. | Automates application configurations to continuously optimize for security and performance. |

###### Guidance for Gap Analysis

1. Periodically modifies application configurations, including location and access parameters, to align with pertinent security and performance objectives.

#### Data Cross-Cutting Capabilities

##### Visibility and Analytics

###### O-RAN ZTA Security Requirements for Visibility and Analytics in the Data Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Visibility and Analytics Capability** | Limited visibility into data including location, access, and usage, with analysis consisting primarily of manual processes. | Obtains visibility based on data inventory management, categorization, encryption, and access attempts, with some automated analysis and correlation. | Maintains data visibility in a more comprehensive, enterprise-wide manner with automated analysis and correlation and begins to employ predictive analytics. | Obtains visibility across the full data lifecycle with robust analytics, including predictive analytics, that support comprehensive views of the data and continuous security posture assessment. |

###### Guidance for Gap Analysis

1. Utilizes data inventory management, data categorization, data encryption, and access attempts information with some automated analysis and correlation to obtain visibility.

##### Automation and Orchestration

###### O-RAN ZTA Security Requirements for Automation and Orchestration in the Data Pillar

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CISA ZTMM Function** | **Traditional** | **Initial** | **Advanced** | **Optimal** |
| **Automation and Orchestration Capability** | Implements data lifecycle and security policies (e.g., access, usage, storage, encryption, configurations, protections, backups, categorization, sanitization) through manual, and potentially ad hoc, processes. | Utilizes some automated processes to implement data lifecycle and security policies. | Automates orchestration and response activities that leverage contextual information from multiple sources to inform decisions. | Orchestration and response activities dynamically respond to changing requirements and environmental changes. |

###### Guidance for Gap Analysis

* + 1. Data lifecycle and security policies are automated.

# Alignment to Target ZTA Requirements

## Introduction

This clause first reviews the current status of O-RAN security specifications and then evaluates this against the reference ZTA security requirements in clause 6.2.

## Current O-RAN Security Requirements and Controls

Table 7.2‑1 is a snapshot of the interface security controls enforcing authenticity, confidentiality, integrity, authorization, data origination, and replay prevention. The protocols listed in Table 7.2‑1 are mandatory for the vendor to support and optional for the operator to use, as regional regulatory requirements may differ. The only exception is 802.1X which is optional for the vendor to support as well as optional for the operator to use. Detailed requirements can be found in [i.2] and [i.3].

Table ‑: Mandatory O-RAN interface security controls (See NOTE for 802.1X1 and PDCP2)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Security Control** | **Non-Fronthaul** | | | | | | **Open Fronthaul** | | | |
| **A1** | **O1** | **O2** | **E2** | **Y1** | **R1** | **C-plane** | **U-plane** | **S-plane** | **M-plane** |
| Authenticity | mTLS | mTLS | mTLS | IPsec | mTLS | mTLS | 802.1X1 | 802.1X1 | 802.1X1 | mTLS/SSH/802**.**1X |
| Confidentiality | TLS | TLS | TLS | IPsec | TLS | TLS |  | PDCP2 |  | TLS/SSH |
| Integrity | TLS | TLS | TLS | IPsec | TLS | TLS |  | PDCP2 |  | TLS/SSH |
| Authorization | OAuth | NACM | OAuth |  | OAuth | OAuth | 802.1X | 802.1X | 802.1X | NACM/802.1X |
| Data Origination | mTLS | mTLS | mTLS | IPsec | mTLS | mTLS |  | PDCP2 |  | TLS/SSH |
| Replay Prevention | TLS | TLS | TLS | IPsec | TLS | TLS |  | PDCP2 |  | TLS/SSH |

NOTE 1: 802.1X provides authentication of the device plugging into a network port and controls access to send/receive network traffic. 802.1X does not provide authenticity of the data flowing across the C-plane, U-plane, S-plane, and M-plane interfaces between the O-DU and O-RU.

NOTE 2: 3GPP Access Stratum (AS) Control Plane and User Plane messages that are transported via the Open Fronthaul U-Plane (LLS-UP) are confidentiality and integrity protected by the Packet Data Convergence Protocol (PDCP) [i.16]. PDCP security controls remain in place when the message traverses the Open Fronthaul U-Plane. PDCP requirements are specified by the 3GPP in TS 33.501 [i.17]. PDCP does not provide confidentiality and integrity protection for plain text messages flowing across the U-plane interface between the O-DU and O-RU.

The controls still under development are authorization for the E2 interface as well as confidentiality, integrity, data origination and replay prevention on the C-, U-, and S-plane. Authorization for the E2 interface is being developed in collaboration with the Near-Real Time RIC and E2 interface work group. Confidentiality and integrity protection on the Open Fronthaul C- and U-Planes and authenticity protection on the Open Fronthaul S-Plane are being developed in collaboration with the Open Fronthaul and Transport working groups.

Table 7.2‑2 is an overview of the mandatory O-RAN transversal requirements that support ZT tenets such as security posture, data collection, and monitoring.

Table 7.2‑2: O-RAN Cross-Platform Security Requirements

|  |  |
| --- | --- |
| **Category** | **Mandatory Requirements** |
| Application Lifecycle Management | * Application signing by vendor * Signature validation by SMO * Secure deletion of sensitive data * Secure decommissioning of applications |
| Network Protocols and Services | * Provider documentation of all required network protocols/services * Default disabling of unused network protocols/services |
| Robust Protocol Implementation | * Handle unexpected inputs without functional compromise |
| Robustness of OS and Applications | * Known vulnerabilities in the OS and applications be documented by their providers |
| Password based Authentication | * Mitigate risks from password authentication attacks where password authentication is implemented |
| Software Supply Chain Security | * Vendor signed, NTIA compliant SBOM with every O-RAN software delivery. |
| Security Log Management | * Identification of security events to log * Collection of security logs by all O-RAN elements * Least privileged access controls on security logs * Logging of anomalous events * Confidentiality and integrity protection of log data at rest and in transit * Rotation of logs to prevent data loss * Use of micro-perimeters to protect logs * Time stamping of all logged events * Inclusion of identity of O-RAN element generating event |
| Certificate Management Framework | * Support of CMPv2 |
| API Security | * Support of OWASP API Security Project * Support of certificate-based authentication using mTLS 1.2+ * Confidentiality and integrity protection of data in transit with TLS 1.2+ * Least privileged authorization using OAuth 2.0 * Input validation |
| Trust Anchor Provisioning | * Pre-provisioning of certificates that chain back to a vendor or operator CA in PNFs |

## Gap Analysis

### Gap Analysis Methodology

#### Gap Analysis Workflow

The gap analysis guidelines for addressing the Initial stage for each pillar in the CISA ZTMM within O-RAN were derived in clause 6.2. Figure 7.3‑1 outlines the high-level workflow for performing the gap analysis. The workflow is divided into two paths: one for the defined assets described in clause 5.2 [i.4] and the other for new assets identified during the ZTA WI study as described in clause 5.3.

1. **Asset Mapping:** First, list the various types of assets for each O-RAN element, and then map the assets to the corresponding CISA ZTMM Pillar.
2. **Comparison:** Compare the current security requirements and controls of the assets to the corresponding ZT pillar’s INITIAL Maturity Level security guidelines, as derived in clause 6.2.
3. **Gap Identification:** Document the gap analysis and forward the identified gaps to relevant work items (e.g., Near-RT RIC, Open Fronthaul, O-Cloud, SMO).
4. **Work Item Analysis:** Each work item performs threat analysis, determines new security requirements and controls to achieve the INITIAL ZTA Maturity Level and updates the Threat Modeling and Risk Assessment Technical Report [i.4] and Security Requirements and Controls Specifications [i.2]

Graphical user interface, diagram

Description automatically generated

Figure 7.3‑1 Gap Analysis Workflow

#### Mapping of O-RAN Assets to CISA ZTMM Pillars

In the gap analysis process, each asset is mapped to a pillar or a set of pillars in CISA ZTMM. For reference, asset categories are defined in clause 5.1. Table 7.3‑1 illustrates this mapping process.

Table ‑ Mapping of O-RAN Assets and Other Components to Different Pillars

|  |  |
| --- | --- |
| **CIZA ZTMM Pillar** | **O-RAN Asset Categories and Other O-RAN Elements** |
| Identity Pillar | Person entities: users  Non-person entities: An O-RAN asset requesting access to another O-RAN asset should be considered as a non-person entity and should be mapped to the Identity pillar |
| Devices Pillar | Hardware infrastructure  Operating system and firmware infrastructure  Virtualization layer infrastructure |
| Networks Pillar | Interfaces, including protocol stacks  APIs |
| Applications Pillar | Interfaces' functions (terminations)  Services  APIs |
| Data Pillar | Data |

NOTE: APIs, as defined by O-RAN, should be tested against both CISA’s Networks Pillar and Applications Pillar.

### Transversal Functions

This clause will be updated in a later version.

### xApp and Near-RT RIC Gap Analysis

#### xApp and Near-RT RIC Data Pillar Analysis

##### xApp Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-D-15: Application software package
* ASSET-D-23: Patches for vulnerable SW components
* ASSET-D-29: Security event log files.
* ASSET-D-31: Security telemetry from the NFV system for detecting threats and anomalies.
* Cryptographic Data:
  + ASSET-D-16: X.509 certificates
  + ASSET-D-17: Private keys
  + ASSET-D-32: Cryptographic keys used during secure boot
* AI/ML Data:
  + ASSET-D-25: Training or test data
  + ASSET-D-26: The trained ML model
  + ASSET-D-27: The ML prediction results built into the model
  + ASSET-D-28: The behavior of the ML system

##### Near-RT RIC Data Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] and the WG3 Near-RT RIC Architecture [i.23] are as follows:

* ASSET-D-39: xApp ID
* ASSET-D-10: Database holding data from xApp applications and E2 Node
* ASSET-D-16: X.509 certificates
* ASSET-D-17: Private Keys
* ASSET-D-23: Patches for vulnerable SW components.
* ASSET-D-25: Training or test data
* ASSET-D-26: The trained ML model
* ASSET-D-27: The ML prediction results built into the model
* ASSET-D-28: The behavior of the ML system
* ASSET-D-29: Security event log files.
* ASSET-D-31: Security telemetry from the NFV system for detecting threats and anomalies
* ASSET-D-32: Cryptographic keys used during secure boot
* ASSET-D-07: A1 policies that are provided to the near-RT RIC over the A1 interface
* ASSET-D-08: A1 Enrichment Information
* ASSET-D-30: O-RAN specific several UE IDs
* ASSET-D-20: Credentials (Administrators)

##### Data Pillar Transversal Functions

The following Data Pillar functions are considered transversal and are covered in 7.3.2:

* Data inventory management
* Data categorization
* Data availability

##### xApp and Near-RT RIC Data Pillar Gap Analysis

Table ‑: xApp and Near-RT RIC Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | xApp Data Assets | | | |
| Asset-D-15 | REQ-SBOM-009 REQ-SEC-ALM-PKG-11 | No gap |  |
| Asset-D-23 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| Asset-D-16 | None | Gap | No action needed. X.509 certs are publicly available |
| Asset-D-17 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-32 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-25 (included in app package) | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| Asset-D-25 (excluded from app package) | None | Gap | Authentication and authorization controls not defined |
| Asset-D-26 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap | Initial stage if we consider trained ML model as part of app package |
| Asset-D-27 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-28 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-1 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 REQ-SEC-SLM-SST-4 REQ-SEC-SLM-STR-2 | No gap |  |
| Asset-D-31 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-1 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 REQ-SEC-SLM-SST-4 REQ-SEC-SLM-STR-2 | No gap |  |
| Near-RT RIC Data Assets | | | |
| Asset-D-16 | None | Gap | No action needed. X.509 certs are publicly available |
| Asset-D-17 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-23 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| Asset-D-25 (included in app package) | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| Asset-D-25 (excluded from app package) | None | Gap | Authentication and authorization controls not defined |
| Asset-D-26 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| Asset-D-27 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-28 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESM-3 REQ-SEC-SLM-TE-5 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 | No gap |  |
| Asset-D-31 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESM-3 REQ-SEC-SLM-TE-5 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 | No gap |  |
| Asset-D-32 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-07 | REQ-SEC-NEAR-RT-5 SEC-CTL-NEAR-RT-4 | No gap |  |
| Asset-D-08 | REQ-SEC-NEAR-RT-5 SEC-CTL-NEAR-RT-5 | No gap |  |
| Asset-D-30 | None | Gap | Authentication and authorization controls not defined |
| Asset-D-39 | REQ-SEC-XAPP-3 | Partial gap | Authorization controls not defined |
| Asset-D-10 | REQ-SEC-NEAR-RT-1 REQ-SEC-NEAR-RT-2 SEC-CTL-NEAR-RT-1 SEC-CTL-NEAR-RT-3 | No gap |  |
| Asset-D-20 | None | Gap | Authentication and authorization controls not defined |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | xApp Data Assets | | | |
| Asset-D-15 | REQ-SBOM-010 REQ-SEC-ALM-PKG-10 | Partial gap | There are security requirements addressing this function, but no corresponding security controls in place. |
| Asset-D-23 | REQ-SBOM-010 REQ-SEC-ALM-PKG-10 | Partial gap | There are security requirements addressing this function, but no corresponding security controls in place. |
| Asset-D-16 | REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 SEC-CTL-ALM-PKG-2A SEC-CTL-ALM-PKG-4 | No gap |  |
| Asset-D-17 | REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 SEC-CTL-ALM-PKG-2A SEC-CTL-ALM-PKG-4 REQ-SEC-OCLOUD-PKG-3 | No gap |  |
| Asset-D-32 | REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 SEC-CTL-ALM-PKG-2A SEC-CTL-ALM-PKG-4 REQ-SEC-OCLOUD-PKG-3 | No gap |  |
| Asset-D-25 (included in app package) | REQ-SEC-ALM-PKG-10 | No gap |  |
| Asset-D-25 (excluded from app package) | None | Gap | No encryption in transit or at rest |
| Asset-D-26 | REQ-SEC-ALM-PKG-10 | No gap | If we consider trained ML model as part of app package |
| Asset-D-27 | None | Gap | No encryption in transit or at rest |
| Asset-D-28 | None | Gap | No encryption in transit or at rest |
| Asset-D-29 | REQ-SEC-SLM-TESM-2 REQ-SEC-SLM-TE-4 REQ-SEC-TESR-6 | No gap |  |
| Asset-D-31 | REQ-SEC-SLM-TESM-2 REQ-SEC-SLM-TE-4 REQ-SEC-TESR-6 | No gap |  |
| Near-RT RIC Data Assets | | | |
| Asset-D-16 | REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 SEC-CTL-ALM-PKG-2A SEC-CTL-ALM-PKG-4 | No gap |  |
| Asset-D-17 | REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 SEC-CTL-ALM-PKG-2A SEC-CTL-ALM-PKG-4 REQ-SEC-OCLOUD-PKG-3 | No gap |  |
| Asset-D-23 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| Asset-D-25 (included in app package) | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| Asset-D-25 (excluded in app package) | None | Gap | No encryption in transit or at rest |
| Asset-D-26 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| Asset-D-27 | None | Gap | No encryption in transit or at rest |
| Asset-D-28 | None | Gap | No encryption in transit or at rest |
| Asset-D-29 | REQ-SEC-SLM-TESM-2 REQ-SEC-SLM-TE-4  REQ-SEC-TESR-6 | No gap |  |
| Asset-D-31 | REQ-SEC-SLM-TESM-2 REQ-SEC-SLM-TE-4 REQ-SEC-TESR-6 | No gap |  |
| Asset-D-32 | None | Gap | No encryption in transit or at rest |
| Asset-D-07 | REQ-SEC-A1-1 SEC-CTL-A1-1 | No gap |  |
| Asset-D-08 | REQ-SEC-A1-1 SEC-CTL-A1-1 | No gap |  |
| Asset-D-30 | REQ-SEC-API-7 SEC-CTL-NEAR-RT-6 | Gap | Encryption in transit, but no encryption at rest |
| Asset-D-39 | None | Gap | No encryption in transit or at rest |
| Asset-D-10 | SEC-CTL-NEAR-RT-6 | Gap | Encryption in transit, but no encryption at rest. |
| Asset-D-20 | None | Gap | No encryption in transit or at rest |

#### xApp and Near-RT RIC Applications and Workloads Pillar Analysis

##### xApp Applications and Workloads Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] and the WG3 Near-RT RIC Architecture [i.23] are as follows:

* ASSET-C-09: xApps. This includes xApps services.

##### Near-RT RIC Applications and Workloads Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] and the WG3 Near-RT RIC Architecture [i.23] are as follows:

* ASSET-C-13: A1 termination. This includes A1 related services.
* ASSET-C-41: E2 functions. This includes E2 related services.
* ASSET-C-43: Y1 Functions. This includes Y1 related services.
* Other Services of the Near-RT RIC platform: this includes Management related services, SDL services, Enablement services, and AI/ML workflow services [i.23].

##### Application and Workloads Pillar Transversal Functions

* No transversal functions applicable

##### xApp and Near-RT RIC Application and Workloads Pillar Gap Analysis

Table ‑: xApp and Near-RT RIC Applications and Workloads Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **App/Workloads ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Application Access (Authorization) | a) Access authorization capabilities utilize contextual information such as identity, device compliance, and other attributes to make decisions on various requests for accessing application assets.  b) Authorization is granted per request with expiration. | xApp Applications and Workloads Assets | | | |
| ASSET-C-09 | REQ-SEC-NEAR-RT-3 REQ-SEC-NEAR-RT-4 SEC-CTL-NEAR-RT-2 SEC-CTL-NEAR-RT-3 | No gap |  |
| Near-RT RIC Applications and Workloads Assets | | | |
| ASSET-C-13 ASSET-C-41 ASSET-C-43 | REQ-SEC-NEAR-RT-3 REQ-SEC-NEAR-RT-4 REQ-SEC-NEAR-RT-5 SEC-CTL-NEAR-RT-1 SEC-CTL-NEAR-RT-2 SEC-CTL-NEAR-RT-3 SEC-CTL-NEAR-RT-4 SEC-CTL-NEAR-RT-5 | No gap |  |
| Other Services of the Near-RT RIC platform | REQ-SEC-NEAR-RT-3 REQ-SEC-NEAR-RT-4 SEC-CTL-NEAR-RT-1 SEC-CTL-NEAR-RT-3 | No gap |  |
| Application Threat Protections | a) Threat protections is integrated into mission-critical application workflows.  b) Threat protections safeguard applications against known threats and address some application-specific threats. | xApp Applications and Workloads Assets | | | |
| ASSET-C-09 | REQ-SEC-ALM-SU-2  REQ-SEC-ALM-SU-3 REQ-SEC-ALM-SU-4 | No gap |  |
| Near-RT RIC Applications and Workloads Assets | | | |
| ASSET-C-13 ASSET-C-41 ASSET-C-43 | REQ-SEC-ALM-SU-2  REQ-SEC-ALM-SU-3 REQ-SEC-ALM-SU-4 | No gap |  |
| Other Services of the Near-RT RIC platform | None | Gap |  |
| Accessible Applications | a) Applicable mission-critical applications are available over open public network connections to authorized users as needed. | xApp Applications and Workloads Assets | | | |
| ASSET-C-09 | None | Gap | N/A. No identified Mission critical applications |
| Near-RT RIC Applications and Workloads Assets | | | |
| ASSET-C-13 ASSET-C-41 ASSET-C-43 | None | Gap | N/A. No identified Mission critical applications |
| Other Services of the Near-RT RIC platform | None | Gap |  |
| Secure Application  Development and  Deployment Workflow  (New Function) | a) Infrastructure for development, testing, and production environments (including automation).  b) Formal code deployment mechanisms through CI/CD pipelines.  c) Access controls support least privilege principles. | xApp Applications and Workloads Assets | | | |
| ASSET-C-09 | None | Gap |  |
| Near-RT RIC Application and Workloads Assets | | | |
| ASSET-C-13 ASSET-C-41 ASSET-C-43 | None | Gap |  |
| Other Services of the Near-RT RIC platform | None | Gap |  |
| Application Security  Testing (Formerly  Application Security) | a) Utilization of static and dynamic testing methods for security testing.  b) Performance of security testing including manual expert analysis before application deployment. | xApp Applications and Workloads Assets | | | |
| ASSET-C-09 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c REQ-SEC-OCLOUD-SW-2 | No gap |  |
| Near-RT RIC Applications and Workloads Assets | | | |
| ASSET-C-13 ASSET-C-41 ASSET-C-43 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c REQ-SEC-OCLOUD-SW-2 | No gap |  |
| Other Services of the Near-RT RIC platform | None | Gap |  |

#### xApp and Near-RT RIC Identity Pillar Analysis

##### xApp Identity Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] and the WG3 Near-RT RIC Architecture [i.23] are as follows:

* ASSET-C-09: xApps.

##### Near-RT RIC Identity Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] and the WG3 Near-RT RIC Architecture [i.23] are as follows:

* ASSET-C-02: Near-RT RIC software.

##### Identity Pillar Transversal Functions

The following identity pillar functions are considered transversal and are covered in 7.3.2:

* Identity stores.
* Risk assessments.
* Access management.

##### xApp and Near-RT RIC Identity Pillar Gap Analysis

Table ‑: xApp and Near-RT RIC Identity Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Identity ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Authentication | The system authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).  a) If there is mutual authentication for internal communications, we consider the stage as INITIAL.  b) For internal interfaces, authentication based on credentials alone (certificate, pre-shared key, etc.) can be considered as meeting INITIAL maturity level. | xApp Identity Pillar Assets | | | |
| ASSET-C-09 | REQ-SEC-XAPP-3 REQ-SEC-NEAR-RT-3 SEC-CTL-NEAR-RT-1 SEC-CTL-NEAR-RT-2 | No gap |  |
| Near-RT RIC Identity Pillar Assets | | | |
| ASSET-C-02 | SEC-CTL-NEAR-RT-1 REQ-SEC-NEAR-RT-3 SEC-CTL-NEAR-RT-2 | No gap |  |
| Access Management (Authorization) | The system authorizes access, including for privileged access requests, that expires with automated review.  a) This function applies to APIs and user access.  b) For applications, static role assignments (e.g. role binding of a service account) with ephemeral tokens can be considered as INITIAL stage. | xApp Identity Pillar Assets | | | |
| ASSET-C-09 | SEC-CTL-NEAR-RT-3 | No gap |  |
| Near-RT RIC Identity Pillar Assets | | | |
| ASSET-C-09 | SEC-CTL-NEAR-RT-3 | No gap |  |

#### xApp and Near-RT RIC Networks Pillar Analysis

##### xApp Networks Pillar Assets

* No asset applicable to specific pillar

##### Near-RT RIC Networks Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] and the WG3 Near-RT RIC Architecture [i.23] are as follows:

* Near-RT RIC APIs.

##### Networks Pillar Transversal Functions

The following Network pillars functions are considered transversal and are covered in 7.3.2:

* Network Segmentation.
* Network Traffic Management.
* Network resilience.

##### Networks Pillar Gap Analysis

Table ‑: xApp and Near-RT RIC Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys. | Near-RT RIC Networks Pillar Assets | | | |
| Near-RT RIC APIs | SEC-CTL-NEAR-RT-6  SEC-CTL-NEAR-RT-7 | No gap |  |

#### xApp and Near-RT RIC Devices Pillar Analysis

##### xApp Devices Pillar Assets

* No asset applicable to specific pillar

##### Near-RT RIC Devices Pillar Assets

* No asset applicable to specific pillar

##### Devices Pillar Transversal Functions

The following devices pillar functions are considered transversal and are covered in 7.3.2:

* Policy Enforcement and Compliance Monitoring.
* Asset & Supply Chain Risk Management.

##### Devices Pillar Gap Analysis

* The Devices Pillar is out of scope for the gap analysis.

### E2 Interface Gap Analysis

#### E2 Interface Data Pillar Analysis

##### E2 Interface Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-D-09: Data transported over the E2 Interface
* ASSET-D-30: O-RAN specific several UE IDs.
* ASSET-D-16: X.509 certificates.
* ASSET-D-17: Private keys
* ASSET-D-25: Training or test data

##### E2 Interface Data Pillar Gap Analysis

Table ‑: E2 Interface Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | E2 Interface Data Assets | | | |
| Asset-D-09 | REQ-SEC-E2-1 SEC-CTL-E2-1 | Partial gap | Authorization control not defined |
| Asset-D-16 | REQ-SEC-E2-1 SEC-CTL-E2-1 | Partial gap | Authorization control not defined |
| Asset-D-17 | REQ-SEC-E2-1 SEC-CTL-E2-1 | Partial gap | Authorization control not defined |
| Asset-D-25 | REQ-SEC-E2-1 SEC-CTL-E2-1 | Partial gap | Authorization control not defined |
| Asset-D-30 | REQ-SEC-E2-1 SEC-CTL-E2-1 | Partial gap | Authorization control not defined |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | E2 Interface Data Assets | | | |
| Asset-D-09 | REQ-SEC-E2-1 SEC-CTL-E2-1 | No gap | Encryption at rest may not be needed. |
| Asset-D-16 | REQ-SEC-E2-1 SEC-CTL-E2-1 | No gap | Encryption at rest may not be needed. |
| Asset-D-17 | REQ-SEC-E2-1 SEC-CTL-E2-1 | No gap | Encryption at rest may not be needed. |
| Asset-D-25 | REQ-SEC-E2-1 SEC-CTL-E2-1 | No gap | Encryption at rest may not be needed. |
| Asset-D-30 | REQ-SEC-E2-1 SEC-CTL-E2-1 | No gap | Encryption at rest may not be needed. |

#### E2 Interface Applications and Workloads Pillar Analysis

##### E2 Interface Applications and Workloads Pillar Assets

* No asset applicable to specific pillar

##### E2 Interface Applications and Workloads Pillar Gap Analysis

* No gap analysis applies since there are no assets applicable to specific pillar

#### E2 Interface Identity Pillar Analysis

##### E2 Interface Identity Pillar Assets

* No asset applicable to specific pillar

##### E2 Interface Identity Pillar Gap Analysis

* No gap analysis applies since there are no assets applicable to specific pillar

#### E2 Interface Networks Pillar Analysis

##### E2 Interface Networks Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] and the WG3 Near-RT RIC Architecture [i.23] are as follows:

* ASSET-C-40: E2 interface, including protocol stack

##### E2 Interface Networks Pillar Gap Analysis

Table ‑: E2 Interface Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys. | E2 Networks Pillar Assets | | | |
| ASSET-C-40 | SEC-CTL-NEAR-RT-7 | No gap |  |

#### E2 Interface Devices Pillar Analysis

##### E2 Interface Devices Pillar Assets

* No asset applicable to specific pillar

##### E2 Interface Devices Pillar Transversal Functions

The following devices pillar functions are considered transversal and are covered in 7.3.2:

* Policy Enforcement and Compliance Monitoring.
* Asset & Supply Chain Risk Management.

##### E2 Interface Devices Pillar Gap Analysis

* The Devices Pillar is out of scope for the gap analysis.

### Y1 Interface Gap Analysis

#### Y1 Interface Data Pillar Analysis

##### Y1 Interface Data Pillar Assets

* Data transported over the Y1 interface

##### Y1 Interface Data Pillar Gap Analysis

Table ‑: Y1 Interface Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | Y1 Interface Data Assets | | | |
| Data Transported over Y1 Interface | REQ-SEC-Y1-2 SEC-CTL-NEAR-RT-10 | No gap |  |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | Y1 Interface Data Assets | | | |
| Data transported over Y1 Interface | REQ-SEC-Y1-3 SEC-CTL-NEAR-RT-11 | No gap | Encryption at rest may not be needed. |

#### Y1 Interface Applications and Workloads Pillar Analysis

##### Y1 Interface Applications and Workloads Pillar Assets

* No asset applicable to specific pillar

##### Y1 Interface Applications and Workloads Pillar Gap Analysis

* No gap analysis applies since there are no assets applicable to specific pillar

#### Y1 Interface Identity Pillar Analysis

##### Y1 Interface Identity Pillar Assets

* No asset applicable to specific pillar

##### Y1 Interface Identity Pillar Gap Analysis

* No gap analysis applies since there are no assets applicable to specific pillar

#### Y1 Interface Networks Pillar Analysis

##### Y1 Interface Networks Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] and the WG3 Near-RT RIC Architecture [i.23] are as follows:

* ASSET-C-42: Y1 interface, including protocol stack

##### Y1 Interface Networks Pillar Gap Analysis

Table ‑: Y1 Interface Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys. | Y1 Networks Pillar Assets | | | |
| ASSET-C-42 | REQ-SEC-Y1-3 SEC-CTL-NEAR-RT-11 | No gap |  |

#### Y1 Interface Devices Pillar Analysis

##### Y1 Interface Devices Pillar Assets

* No asset applicable to specific pillar

##### Y1 Interface Devices Pillar Transversal Functions

The following devices pillar functions are considered transversal and are covered in 7.3.2:

* Policy Enforcement and Compliance Monitoring.
* Asset & Supply Chain Risk Management.

##### Y1 Interface Devices Pillar Gap Analysis

* The Devices Pillar is out of scope for the gap analysis.

### rApp and Non-RT RIC Gap Analysis

#### rApp and Non-RT RIC Data Pillar Analysis

##### rApp Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-D-16: X.509 certificates.
* ASSET-D-17: Private keys
* ASSET-D-18: O-RAN components associated and configuration data.
* ASSET-D-20: Credentials (Administrators).
* ASSET-D-23: Patches for vulnerable SW components.
* ASSET-D-25: Training or test data
* ASSET-D-26: The trained ML model
* ASSET-D-27: The ML prediction results built into the model.
* ASSET-D-28: The behavior of the ML system
* ASSET-D-29: Security event log files.
* ASSET-D-32: Cryptographic keys used during secure boot.

##### Non-RT RIC Data Pillar Assets

This clause will be updated when Non-RT RIC/SMO architecture is finalized.

##### rApp and Non-RT RIC Data Pillar Gap Analysis

Table ‑: rApp and Non-RT RIC Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | rApp Data Assets | | | |
| ASSET-D-16 | none | Gap | No action needed. X.509 certs are publicly available |
| ASSET-D-17 | none | Gap | Authentication and authorization controls not defined |
| ASSET-D-18 | none | Gap | Authentication and authorization controls not defined |
| ASSET-D-20 | none | Gap | Authentication and authorization controls not defined |
| ASSET-D-23 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-25 (included in app package) | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-25 (excluded from app package) | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-26 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-27 | none | Gap | Authentication and authorization controls not defined |
| ASSET-D-28 | none | Gap | Authentication and authorization controls not defined |
| ASSET-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-1 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 REQ-SEC-SLM-SST-4 REQ-SEC-SLM-STR-2 | No gap |  |
| ASSET-D-32 | none | Gap | Authentication and authorization controls not defined |
| Non-RT RIC Data Assets | | | |
|  |  |  |  |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest. b) Key management policies and secure encryption keys are beginning to be formalized. | rApp Data Assets | | | |
| ASSET-D-16 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-17 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 SEC-CTL-ALM-PKG-4 | No gap |  |
| ASSET-D-18 | REQ-SEC-ALM-PKG-13 | Possible gap | Requirement is too general |
| ASSET-D-20 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-23 | REQ-SBOM-010 REQ-SEC-ALM-PKG-10 SEC-CTL-ALM-PKG-1 | No gap |  |
| ASSET-D-25 (included in app package) | REQ-SEC-ALM-PKG-10 SEC-CTL-ALM-PKG-1 | No gap |  |
| ASSET-D-25 (excluded from app package) | None | Gap | No encryption in transit or at rest |
| ASSET-D-26 | REQ-SEC-ALM-PKG-10 SEC-CTL-ALM-PKG-1 | No gap | If we consider trained ML model as part of app package |
| ASSET-D-27 | none | Gap | No encryption in transit or at rest |
| ASSET-D-28 | none | Gap | No encryption in transit or at rest |
| ASSET-D-29 | REQ-SEC-SLM-TESM-2 REQ-SEC-TESR-6 REQ-SEC-SLM-SST-2 REQ-SEC-SLM-STR-1 SEC-CTL-SLM-SST-2 | No gap |  |
| ASSET-D-32 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 SEC-CTL-ALM-PKG-4 | No gap |  |
| Non-RT RIC Data Assets | | | |
|  |  |  |  |

#### rApp and Non-RT RIC Applications and Workloads Pillar Analysis

##### rApp Applications and Workloads Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-C-10: rApps.
* ASSET-C-12: ML components deploying machine learning such as: ML training and interference hosts, ML applications (xApps, rApps).

##### Non-RT RIC Applications and Workloads Pillar Assets

This clause will be updated when Non-RT RIC/SMO architecture is finalized.

##### Applications and Workloads Pillar Gap Analysis

Table ‑: rApp and Non-RT RIC Applications and Workloads Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Application and Workloads ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Application Access (Authorization) | a) Access authorization capabilities utilize contextual information such as identity, device compliance, and other attributes to make decisions on various requests for accessing application assets.  b) Authorization is granted per request with expiration. | rApps Application and Workloads Assets | | | |
| ASSET-C-10 | None | Gap |  |
| ASSET-C-12 | None | Gap |  |
| Non-RT RIC Application and Workloads Assets | | | |
|  |  |  |  |
| Application Threat Protections | a) Threat protections is integrated into mission-critical application workflows.  b) Threat protections safeguard applications against known threats and address some application-specific threats. | rApps Application and Workloads Assets | | | |
| ASSET-C-10 | REQ-SEC-ALM-SU-2  REQ-SEC-ALM-SU-3 REQ-SEC-ALM-SU-4 | No gap |  |
| ASSET-C-12 | REQ-SEC-ALM-SU-2  REQ-SEC-ALM-SU-3 REQ-SEC-ALM-SU-4 | No gap |  |
| Non-RT RIC Application and Workloads Assets | | | |
|  |  |  |  |
| Accessible Applications | a) Applicable mission-critical applications are available over open public network connections to authorized users as needed. | rApps Application and Workloads Assets | | | |
| ASSET-C-10 | none | Gap | N/A.  No identified Mission critical applications. |
| ASSET-C-12 | none | Gap | N/A.  No identified Mission critical applications. |
| Non-RT RIC Application and Workloads Assets | | | |
|  |  |  |  |
| Secure Application  Development and  Deployment Workflow  (New Function) | a) Infrastructure for development, testing, and production environments (including automation).  b) Formal code deployment mechanisms through CI/CD pipelines.  c) Access controls support least privilege principles. | rApps Application and Workloads Assets | | | |
| ASSET-C-10 | none | Gap |  |
| ASSET-C-12 | none | Gap |  |
| Non-RT RIC Application and Workloads Assets | | | |
|  |  |  |  |
| Application Security  Testing (Formerly  Application Security) | a) Utilization of static and dynamic testing methods for security testing.  b) Performance of security testing including manual expert analysis before application deployment. | rApps Applications and Workloads Assets | | | |
| ASSET-C-10 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c | No gap |  |
| ASSET-C-12 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c | No gap |  |
| Non-RT RIC Application and Workloads Assets | | | |
|  |  |  |  |

#### rApp and Non-RT RIC Identity Pillar Analysis

##### rApp Identity Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-C-10: rApps.
* ASSET-C-12: ML components deploying machine learning such as: ML training and interference hosts, ML applications (xApps, rApps).

##### Non-RT RIC Identity Pillar Assets

This clause will be updated when Non-RT RIC/SMO architecture is finalized.

##### Identity Pillar Gap Analysis

Table ‑: rApp and Non-RT RIC Identity Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Identity ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Authentication | The system authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).  a) If there is mutual authentication for internal communications, we consider the stage as INITIAL.  b) For internal interfaces, authentication based on credentials alone (certificate, pre-shared key, etc.) can be considered as meeting INITIAL maturity level. | rApp Identity Pillar Assets | | | |
| ASSET-C-10 | REQ-SEC-NonRTRIC-7 | Partial gap | There is a security requirement addressing this function, but no corresponding security control in place.  This security requirement is defined only for Kafka streaming use case. |
| ASSET-C-12 | REQ-SEC-NonRTRIC-7 | Partial gap | There is a security requirement addressing this function, but no corresponding security control in place.  This security requirement is defined only for Kafka streaming use case. |
| Non-RT RIC Identity Pillar Assets | | | |
|  |  |  |  |
| Access Management (Authorization) | The system authorizes access, including for privileged access requests, that expires with automated review.  a) This function applies to APIs and user access.  b) For applications, static role assignments (e.g. role binding of a service account) with ephemeral tokens can be considered as INITIAL stage. | rApp Identity Pillar Assets | | | |
| ASSET-C-10 | REQ-SEC-NonRTRIC-2 REQ-SEC-NonRTRIC-3 REQ-SEC-NonRTRIC-8 SEC-CTL-NonRTRIC-4 SEC-CTL- NonRTRIC-5 SEC-CTL- NonRTRIC-6 | Partial gap | There are no requirements that govern the communication when rApp is the service producer. |
| ASSET-C-12 | REQ-SEC-NonRTRIC-2 REQ-SEC-NonRTRIC-3 REQ-SEC-NonRTRIC-8 SEC-CTL-NonRTRIC-4 SEC-CTL- NonRTRIC-5 SEC-CTL- NonRTRIC-6 | Partial gap | There are no requirements that govern the communication when rApp is the service producer. |
| Non-RT RIC Identity Pillar Assets | | | |
|  |  |  |  |

#### rApp and Non-RT RIC Networks Pillar Analysis

##### rApp Networks Pillar Assets

* No asset(s) applicable to this specific pillar.

##### Non-RT RIC Networks Pillar Assets

This clause will be updated when Non-RT RIC/SMO architecture is finalized.

#### rApp and Non-RT RIC Devices Pillar Analysis

##### rApp Devices Pillar Assets

This clause will be updated when Non-RT RIC/SMO architecture is finalized.

##### Non-RT RIC Devices Pillar Assets

This clause will be updated when Non-RT RIC/SMO architecture is finalized.

### A1 Interface Gap Analysis

#### A1 Interface Data Pillar Analysis

##### A1 Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-D-07: A1 policies that are provided to the near-RT RIC over the A1 interface.
* ASSET-D-08: A1 Enrichment Information.
* ASSET-D-16: X.509 certificates in O-RAN network such as those used for O-RAN components for authentication, encryption, and signing.
* ASSET-D-17: Security private keys in O-RAN network such as those used for O-RAN components for authentication, encryption, and signing.
* ASSET-D-25: Training or test data and associated labels: data sets collected externally or internally from the Near-RT RIC, O-CU and O-DU and passed to the ML training hosts in a ML system.
* ASSET-D-30: O-RAN specific several UE IDs.

The gap analysis for ASSET-D-16, ASSET-D-17, and ASSET-D-30 is detailed in clause 7.3.2.

##### Data Pillar Gap Analysis

Table ‑: A1 Interface Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | A1 Interface Data Assets | | | |
| ASSET-D-07 | REQ-SEC-NEAR-RT-5 REQ-SEC-NonRTRIC-1 REQ-SEC-A1-2 SEC-CTL-NEAR-RT-4 SEC-CTL-NonRTRIC-2 SEC-CTL-A1-2 SEC-CTL-A1-3 | No gap |  |
| ASSET-D-08 | REQ-SEC-NEAR-RT-5 REQ-SEC-NonRTRIC-1 REQ-SEC-A1-2 SEC-CTL-NEAR-RT-5 SEC-CTL-NonRTRIC-1 SEC-CTL-A1-2 SEC-CTL-A1-3 | No gap |  |
| ASSET-D-16 | none | Gap | Authentication and authorization controls not defined |
| ASSET-D-17 | none | Gap | Authentication and authorization controls not defined |
| ASSET-D-25 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| ASSET-D-30 | none | Gap | Authentication and authorization controls not defined |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | A1 Interface Data Assets | | | |
| ASSET-D-07 | REQ-SEC-A1-1 SEC-CTL-A1-1 | No gap |  |
| ASSET-D-08 | REQ-SEC-A1-1 SEC-CTL-A1-1 | No gap |  |
| ASSET-D-16 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-17 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 | No gap |  |
| Asset-D-25 (included in app package) | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| ASSET-D-25 (excluded from app package) | None | Gap | No encryption in transit or at rest |
| ASSET-D-30 | None | Gap | No encryption in transit or at rest |

#### A1 Interface Applications and Workloads Pillar

##### A1 Applications and Workloads Pillar Assets

* No asset(s) applicable to this specific pillar.

#### A1 Interface Identity Pillar Analysis

##### A1 Identity Pillar Assets

* No asset(s) applicable to this specific pillar.

#### A1 Interface Networks Pillar Analysis

##### A1 Networks Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-C-14: A1 interface, including protocol stack.

##### Networks Pillar Gap Analysis

Table ‑: A1 Interface Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys. | A1 Networks Pillar Assets | | | |
| ASSET-C-14 | REQ-SEC-A1-1 SEC-CTL-A1-1 | No gap |  |

#### A1 Interface Devices Pillar Analysis

##### A1 Devices Pillar Assets

* No asset(s) applicable to this specific pillar.

### R1 Interface Gap Analysis

#### R1 Interface Data Pillar Analysis

##### R1 Data Pillar Assets

* Data transported over the R1 Interface.

##### R1 Data Pillar Gap Analysis

Table ‑: R1 Interface Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | R1 Interface Data Assets | | | |
| Data transported over the R1 Interface. | REQ-SEC-NonRTRIC-2 REQ-SEC-NonRTRIC-3 REQ-SEC-R1-2 SEC-CTL-NonRTRIC-4 SEC-CTL-NonRTRIC-5 SEC-CTL-NonRTRIC-6 SEC-CTL-R1-2 SEC-CTL-R1-3 | No gap |  |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest. b) Key management policies and secure encryption keys are beginning to be formalized. | R1 Interface Data Assets | | | |
| Data transported over the R1 Interface. | REQ-SEC-R1-1 SEC-CTL-R1-1 | No gap |  |

#### R1 Interface Applications and Workloads Pillar Analysis

##### R1 Applications and Workloads Pillar Assets

* No asset(s) applicable to this specific pillar.

#### R1 Interface Identity Pillar Analysis

##### R1 Identity Pillar Assets

* No asset(s) applicable to this specific pillar.

#### R1 Interface Networks Pillar Analysis

##### R1 Interface Networks Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-C-16: R1 interface, including protocol stack.

##### Networks Pillar Gap Analysis

Table ‑: R1 Interface Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys. | R1 Networks Pillar Assets | | | |
| ASSET-C-16 | REQ-SEC-R1-1 SEC-CTL-R1-1 | No gap |  |

#### R1 Interface Devices Pillar Analysis

##### R1 Devices Pillar Assets

* No asset(s) applicable to this specific pillar.

### SMO Gap Analysis

This clause will be updated in a later version.

### O1 Interface Gap Analysis

#### O1 Interface Data Pillar Analysis

##### O1 Interface Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-D-03: Critical Management-Plane data transported over the O1 interface
* ASSET-D-16: X.509 certificates.
* ASSET-D-17: Private keys
* ASSET-D-18: O-RAN components associated and configuration data.
* ASSET-D-23: Patches for vulnerable SW components
* ASSET-D-24: NETCONF Configuration Access Control Model datastores

##### O1 Interface Data Pillar Gap Analysis

Table ‑: O1 Interface Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | O1 Interface Data Assets | | | |
| ASSET-D-3 | REQ-TLS-FUN-2 REQ-TLS-FUN-4 REQ-NAC-FUN-1 REQ-NAC-FUN-2 REQ-NAC-FUN-3 REQ-NAC-FUN-4 REQ-NAC-FUN-5 REQ-NAC-FUN-6 REQ-NAC-FUN-7 REQ-NAC-FUN-8 REQ-NAC-FUN-9 REQ-NAC-FUN-10 REQ-NAC-FUN-11 | No gap |  |
| ASSET-D-16 | REQ-TLS-FUN-2 REQ-TLS-FUN-4 REQ-NAC-FUN-1 REQ-NAC-FUN-2 REQ-NAC-FUN-3 REQ-NAC-FUN-4 REQ-NAC-FUN-5 REQ-NAC-FUN-6 REQ-NAC-FUN-7 REQ-NAC-FUN-8 REQ-NAC-FUN-9 REQ-NAC-FUN-10 REQ-NAC-FUN-11 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-17 | REQ-TLS-FUN-2 REQ-TLS-FUN-4 REQ-NAC-FUN-1 REQ-NAC-FUN-2 REQ-NAC-FUN-3 REQ-NAC-FUN-4 REQ-NAC-FUN-5 REQ-NAC-FUN-6 REQ-NAC-FUN-7 REQ-NAC-FUN-8 REQ-NAC-FUN-9 REQ-NAC-FUN-10 REQ-NAC-FUN-11 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-18 | REQ-TLS-FUN-2 REQ-TLS-FUN-4 REQ-NAC-FUN-1 REQ-NAC-FUN-2 REQ-NAC-FUN-3 REQ-NAC-FUN-4 REQ-NAC-FUN-5 REQ-NAC-FUN-6 REQ-NAC-FUN-7 REQ-NAC-FUN-8 REQ-NAC-FUN-9 REQ-NAC-FUN-10 REQ-NAC-FUN-11 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-23 | REQ-TLS-FUN-2 REQ-TLS-FUN-4 REQ-NAC-FUN-1 REQ-NAC-FUN-2 REQ-NAC-FUN-3 REQ-NAC-FUN-4 REQ-NAC-FUN-5 REQ-NAC-FUN-6 REQ-NAC-FUN-7 REQ-NAC-FUN-8 REQ-NAC-FUN-9 REQ-NAC-FUN-10 REQ-NAC-FUN-11 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | O1 Interface Data Assets | | | |
| ASSET-D-3 | REQ-TLS-FUN-1 REQ-TLS-FUN-3 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-16 | REQ-TLS-FUN-1 REQ-TLS-FUN-3 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-17 | REQ-SEC-E2-1 SEC-CTL-E2-1 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-18 | REQ-SEC-E2-1 SEC-CTL-E2-1 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-23 | REQ-SEC-E2-1 SEC-CTL-E2-1 REQ-SEC-OCLOUD-SS-1 SEC-CTL-OCLOUD-SS-1 | No gap |  |

#### O1 Interface Application and Workloads Pillar

##### O1 Interface Application and Workloads Pillar Assets

* No assets applicable to application and workloads pillar

##### O1 Interface Application and Workloads Pillar Gap Analysis

* No gap analysis applies since there are no assets applicable to specific pillar

#### O1 Interface Identity Pillar

##### O1 Interface Identity Pillar Assets

* No asset applicable to specific pillar

##### O1 Interface Identity Pillar Gap Analysis

* No gap analysis applies since there are no assets applicable to specific pillar

#### O1 Interface Networks Pillar

##### O1 Interface Networks Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4]:

* ASSET-C-22: O1, including protocol stack

##### O1 Interface Networks Pillar Gap Analysis

Table ‑: O1 Interface Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys. | O1 Networks Pillar Assets | | | |
| ASSET-C-22 | REQ-TLS-FUN-1 | No gap |  |

#### O1 Interface Devices Pillar

##### O1 Interface Devices Pillar Assets

* No assets applicable to devices pillar

##### O1 Interface Devices Pillar Transversal Requirements

The following devices pillar functions are considered transversal and are covered in 7.3.2:

* Policy Enforcement and Compliance Monitoring.
* Asset & Supply Chain Risk Management.

##### O1 Interface Devices Pillar Gap Analysis

The Devices Pillar is out of scope for the gap analysis.

### O-Cloud Gap Analysis

#### Data Pillar

##### O-Cloud Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-D-16: X.509 certificates in O-RAN network such as those used for O-RAN components for authentication, encryption, and signing.
* ASSET-D-17: Security private keys in O-RAN network such as those used for O-RAN components for authentication, encryption, and signing.
* ASSET-D-18: O-RAN components associated and configuration data
* ASSET-D-20: Credentials of O-Cloud components
* ASSET-D-29: Security event log files generated by O-RAN components
* ASSET-D-31: Security telemetry from the NFV system for detecting threats and anomalies
* ASSET-D-32: Cryptographic keys used during secure boot, for encryption/decryption
* ASSET-D-33: Data transported over AALI-C-Mgmt interface
* ASSET-D-34: Data transported over AALI-C-App & AALI-P interfaces
* ASSET-D-35: Data transported over vendor-specific interface
* ASSET-D-36: AAL profile
* ASSET-D-37: AAL LPU
* ASSET-D-38: Stored AAL data

##### Data Pillar Gap Analysis

Table ‑: O-Cloud Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | O-Cloud Data Assets | | | |
| ASSET-D-16 | REQ-SEC-OCLOUD-ISO-3 SEC-CTL-O-CLOUD-ISO-3 REQ-SEC-OCLOUD-O2dms-1 REQ-SEC-OCLOUD-O2dms-3 REQ-SEC-OCLOUD-O2ims-1 REQ-SEC-OCLOUD-O2ims-3 | No gap |  |
| ASSET-D-17 | REQ-SEC-OCLOUD-ISO-3 SEC-CTL-O-CLOUD-ISO-3 REQ-SEC-OCLOUD-O2dms-1 REQ-SEC-OCLOUD-O2dms-3 REQ-SEC-OCLOUD-O2ims-1 REQ-SEC-OCLOUD-O2ims-3 | No gap |  |
| ASSET-D-18 | REQ-SEC-OCLOUD-ISO-3 SEC-CTL-OCLOUD-ISO-3 REQ-SEC-OCLOUD-O2dms-1 REQ-SEC-OCLOUD-O2dms-3 REQ-SEC-OCLOUD-O2ims-1 REQ-SEC-OCLOUD-O2ims-3 REQ-SEC-O-CLOUD-NotifAPI-1 REQ-SEC-O-CLOUD-NotifAPI-2 SEC-CTL-O-CLOUD-INTERFACE-2 SEC-CTL-O-CLOUD-INTERFACE-3 | No gap | O-Cloud configuration is controlled by RBAC (for k8s) and OS (for VMs) |
| ASSET-D-20 | None | Gap | Credentials of O-Cloud components may not be handled by O-Cloud. This gap may require requirements on other O-RAN elements (e.g. SMO) |
| ASSET-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-1 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 REQ-SEC-SLM-SST-4 REQ-SEC-SLM-STR-2 | Partial gap | No Security controls are defined, this gap is known and intentionally gap is not closed to enable many implementations that are existing. |
| ASSET-D-31 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-1 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 REQ-SEC-SLM-SST-4 REQ-SEC-SLM-STR-2 | Partial gap | No Security controls are defined, this gap is known and intentionally gap is not closed to enable many implementations that are existing. |
| ASSET-D-32 | None | Gap |  |
| ASSET-D-33 | N/A | No gap | No access of data being transported is defined for the interface - hence this row is marked as N/A. |
| ASSET-D-34 | N/A | No gap | No access of data being transported is defined for the interface - hence this row is marked as N/A. |
| ASSET-D-35 | N/A | No gap | No access of data being transported is defined for the interface - hence this row is marked as N/A. |
| ASSET-D-36 | None | Gap | No requirements and controls are specified |
| ASSET-D-37 | None | Gap | No requirements and controls are specified |
| ASSET-D-38 | REQ-SEC-AAL-1 REQ-SEC-AAL-2 REQ-SEC-AAL-5 SEC-CTL-AAL-1 | No gap |  |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | O-Cloud Data Assets | | | |
| ASSET-D-16 | REQ-SEC-OCLOUD-SS-1 (See NOTE 1) SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-17 | REQ-SEC-OCLOUD-SS-1 (See NOTE 1) SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-18 | REQ-SEC-OCLOUD-SS-1 (See NOTE 1) SEC-CTL-OCLOUD-SS-1 REQ-SEC-OCLOUD-TS-1 | No gap |  |
| ASSET-D-20 | REQ-SEC-OCLOUD-SS-1 (See NOTE 1) SEC-CTL-OCLOUD-SS-1 | Partial gap | Credentials of O-Cloud components may not be handled by O-Cloud. This partial gap may require requirements on other O-RAN elements (e.g. SMO) |
| ASSET-D-29 | REQ-SEC-SLM-TESM-2 REQ-SEC-TESR-6 REQ-SEC-SLM-STR-1 | Partial gap | No Security controls are defined, this gap is known and intentionally gap is not closed to enable many implementations that are existing. |
| ASSET-D-31 | REQ-SEC-SLM-TESM-2 REQ-SEC-TESR-6 REQ-SEC-SLM-STR-1 | Partial gap | No Security controls are defined, this gap is known and intentionally gap is not closed to enable many implementations that are existing. |
| ASSET-D-32 | REQ-SEC-OCLOUD-SS-1 (See NOTE 1) SEC-CTL-OCLOUD-SS-1 | No gap |  |
| ASSET-D-33 | REQ-SEC-AALI-C-Mgmt-3 SEC-CTL-AALI-C-Mgmt-1 | No gap |  |
| ASSET-D-34 | None | Gap | Confidentiality and integrity requirements and controls are missing |
| ASSET-D-35 | REQ-SEC-AAL-VS-4 | Partial gap | There may not be a need to specify controls, since this is a vendor specific interface. |
| ASSET-D-36 | None | Gap | No requirements and controls are specified |
| ASSET-D-37 | None | Gap | No requirements and controls are specified |
| ASSET-D-38 | None | Gap | No requirements and controls are specified |

NOTE 1: Encryption of data in use is considered as Optimal stage according to O-RAN ZTA Security Requirements for Data Encryption.

#### Applications and Workloads Pillar

##### O-Cloud Applications and Workloads Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-C-08: O-Cloud (Covers DMS and IMS and their services)
* ASSET-C-29: AAL software including software, libraries, drivers
* ASSET-C-30: The hardware accelerator device firmware

##### Applications and Workloads Pillar Gap Analysis

Table ‑: O-Cloud Applications and Workloads Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Application and Workloads ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Application Access (Authorization) | a) Access authorization capabilities utilize contextual information such as identity, device compliance, and other attributes to make decisions on various requests for accessing application assets.  b) Authorization is granted per request with expiration. | O-Cloud Application and Workloads Assets | | | |
| ASSET-C-08 | None | Partial gap | Access to some of O-Cloud resources is based on RBAC (k8s profile) – implicit requirements are present |
| ASSET-C-29 | None | Gap | No requirements and controls are specified |
| ASSET-C-30 | None | Gap | No requirements and controls are specified |
| Application Threat Protections | a) Threat protections is integrated into mission-critical application workflows.  b) Threat protections safeguard applications against known threats and address some application-specific threats. | O-Cloud Application and Workloads Assets | | | |
| ASSET-C-08 | REQ-SEC-DOS-1 REQ-SEC-OCLOUD-SU-5 REQ-SEC-OCLOUD-SU-7 | Partial gap | No controls are specified |
| ASSET-C-29 | REQ-SEC-OCLOUD-SU-1 REQ-SEC-OCLOUD-SU-5 REQ-SEC-OCLOUD-SU-6 REQ-SEC-OCLOUD-SU-7 | Partial gap | No controls are specified |
| ASSET-C-30 | REQ-SEC-OCLOUD-SU-5 REQ-SEC-OCLOUD-SU-7 | Gap | No controls are specified |
| Accessible Applications | a) Applicable mission-critical applications are available over open public network connections to authorized users as needed. | O-Cloud Application and Workloads Assets | | | |
| ASSET-C-08 | N/A | No gap | Not available over public interface. |
| ASSET-C-29 | N/A | No gap | Not available over public interface. |
| ASSET-C-30 | N/A | No gap | Not available over public interface. |
| Secure Application  Development and  Deployment Workflow  (New Function) | a) Infrastructure for development, testing, and production environments (including automation).  b) Formal code deployment mechanisms through CI/CD pipelines.  c) Access controls support least privilege principles. | O-Cloud Application and Workloads Assets | | | |
| ASSET-C-08 | None | Gap | No requirements and controls are specified |
| ASSET-C-29 | None | Gap | No requirements and controls are specified |
| ASSET-C-30 | REQ-SEC-AAL-4 | No gap | No controls are specified |
| Application Security  Testing (Formerly  Application Security) | a) Utilization of static and dynamic testing methods for security testing.  b) Performance of security testing including manual expert analysis before application deployment. | O-Cloud Application and Workloads Assets | | | |
| ASSET-C-08 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c REQ-SEC-OCLOUD-SW-2 | Partial gap | No Security controls are defined, this gap is known and intentionally gap is not closed to enable many implementations that are existing. |
| ASSET-C-29 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c REQ-SEC-OCLOUD-SW-2 | Partial gap | No Security controls are defined, this gap is known and intentionally gap is not closed to enable many implementations that are existing. |
| ASSET-C-30 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c REQ-SEC-OCLOUD-SW-2 | Partial gap | No Security controls are defined, this gap is known and intentionally gap is not closed to enable many implementations that are existing. |

#### Identity Pillar

##### O-Cloud Identity Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-C-08: O-Cloud (Covers DMS and IMS and their services)
* ASSET-C-29: AAL software including software, libraries, drivers
* ASSET-C-30: The hardware accelerator device firmware

##### Identity Pillar Gap Analysis

Table ‑: O-Cloud Identity Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Identity ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Authentication | The system authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g., locale or activity).  a) If there is mutual authentication for internal communications, we consider the stage as INITIAL.  b) For internal interfaces, authentication based on credentials alone (certificate, pre-shared key, etc.) can be considered as meeting INITIAL maturity level. | O-Cloud Identity Pillar Assets | | | |
| ASSET-C-08 | REQ-SEC-OCLOUD-1 SEC-CTL-OCLOUD-2 REQ-SEC-OCLOUD-INST-ID-1 REQ-SEC-OCLOUD-COT-1 REQ-SEC-OCLOUD-COT-2 REQ-SEC-OCLOUD-ISO-2 REQ-SEC-OCLOUD-PKG-1 REQ-SEC-OCLOUD-PKG-2 REQ-SEC-AALI-C-Mgmt-1 REQ-SEC-AALI-C-Mgmt-2 REQ-SEC-OCLOUD-SW-1 | No gap |  |
| ASSET-C-29 | None | Gap | No requirements and controls are specified |
| ASSET-C-30 | REQ-SEC-AAL-VS-1 REQ-SEC-AAL-3 | Partial gap | No controls are specified |
| Access Management (Authorization) | The system authorizes access, including for privileged access requests, that expires with automated review.  a) This function applies to APIs and user access.  b) For applications, static role assignments (e.g. role binding of a service account) with ephemeral tokens can be considered as INITIAL stage. | O-Cloud Identity Pillar Assets | | | |
| ASSET-C-08 | REQ-SEC-OCLOUD-2 REQ-SEC-OCLOUD-3 SEC-CTL-OCLOUD-1 REQ-SEC-OCLOUD-ISO-1 REQ-SEC-OCloud-ISO-7 | No gap |  |
| ASSET-C-29 | REQ-SEC-AAL-VS-2 REQ-SEC-OCloud-ISO-7 | Partial gap | No controls are specified |
| ASSET-C-30 | REQ-SEC-OCloud-ISO-7 | Partial gap | No controls are specified |

#### Networks Pillar

##### O-Cloud Networks Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-C-08: O-Cloud (Covers DMS and IMS and their services)

NOTE: O2 interface’s networks pillar assets are covered in clause 7.3.12.4

##### Networks Pillar Gap Analysis

Table ‑: O-Cloud Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys. | O-Cloud Networks Pillar Assets | | | |
| ASSET-C-08 | REQ-SEC-OCLOUD-PKG-3 REQ-SEC-OCLOUD-ISO-5 SEC-CTL-O-CLOUD-ISO-2 REQ-SEC-OCLOUD-SS-1 (See NOTE 1) SEC-CTL-OCLOUD-SS-1 REQ-SEC-AALI-C-Mgmt-3 SEC-CTL-AALI-C-Mgmt-1 REQ-SEC-AAL-VS-3 REQ-SEC-AAL-VS-4 | Partial gap | AALI-C-App & AALI-P interface traffic encryption related requirements and controls are not present. |

NOTE 1: Encryption of data in use is considered as Optimal stage according to O-RAN ZTA Security Requirements for Data Encryption.

#### Devices Pillar

##### O-Cloud Devices Pillar Assets

The applicable assets defined in this document are as follows:

* ZT-OCLOUD-I-X1: O-Cloud hardware

##### Devices Pillar Gap Analysis

Table ‑: O-Cloud Devices Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Policy Enforcement and Compliance Monitoring | Basic Device characteristics visibility.  Basic policy enforcement mechanism for managing software, configurations, or vulnerabilities. | O-Cloud Devices Pillar Assets | | | |
| ZT-OCLOUD-I-X1 | REQ-SEC-AAL-4 SEC-CTL-AAL-2 | No gap |  |
| Resource Access | Some visibility into devices or virtual assets' characteristics to approve resource access. | O-Cloud Devices Pillar Assets | | | |
| ZT-OCLOUD-I-X1 | REQ-SEC-O-CLOUD-HW-1 SEC-CTL-O-CLOUD-HW-1 REQ-SEC-AAL-VS-1 REQ-SEC-AAL-1 REQ-SEC-AAL-5 (See NOTE 1) | No gap |  |

NOTE 1: Fine grained access to AAL applications when accessing accelerator device resources is considered as advanced stage according to O-RAN ZTA Security Requirements for Resource Access.

### O2 Interface Gap Analysis

#### Data Pillar

##### O2 interface Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are as follows:

* ASSET-D-14: O-Cloud Provisioning information, O-Cloud software management information
* ASSET-D-15: O-RAN Cloudified Network Function Software
* ASSET-D-18: O-RAN components associated and configuration data

##### Data Pillar Gap Analysis

Table ‑: O2 Interface Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | O2 interface Data Assets | | | |
| ASSET-D-14 | N/A | No gap | No access of data being transported is defined for the O2 interface - hence this row is marked as N/A. |
| ASSET-D-15 | N/A | No gap | No access of data being transported is defined for the O2 interface - hence this row is marked as N/A. |
| ASSET-D-18 | N/A | No gap | No access of data being transported is defined for the O2 interface - hence this row is marked as N/A. |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | O2 interface Data Assets | | | |
| ASSET-D-14 | REQ-SEC-OCLOUD-O2ims-2 SEC-CTL-O2-1 | No gap |  |
| ASSET-D-15 | REQ-SEC-OCLOUD-O2ims-2 SEC-CTL-O2-1 | No gap |  |
| ASSET-D-18 | REQ-SEC-OCLOUD-SS-1 (See NOTE 1) SEC-CTL-OCLOUD-SS-1 | No gap |  |

NOTE 1: Encryption of data in use is considered as Optimal stage according to O-RAN ZTA Security Requirements for Data Encryption.

#### Applications and Workloads Pillar

##### O2 interface Applications and Workloads Pillar Assets

* No asset applicable to specific pillar.

##### Applications and Workloads Pillar Gap Analysis

* No asset applicable to specific pillar.

#### Identity Pillar

##### O2 interface Identity Pillar Assets

* No asset applicable to specific pillar.

##### Identity Pillar Gap Analysis

* No asset applicable to specific pillar.

#### Networks Pillar

##### O2 interface Networks Pillar Assets

The applicable assets defined in this document are as follows:

* ZT-OCLOUD-S-X1: O2ims services
* ZT-OCLOUD-S-X2: O2dms services

##### Networks Pillar Gap Analysis

Table ‑: O2 Interface Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing** **Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys. | O2 interface Networks Pillar Assets | | | |
| ZT-OCLOUD-S-X1 | REQ-SEC-OCLOUD-O2ims-2 REQ-SEC-O2-1 SEC-CTL-O2-1 | No gap |  |
| ZT-OCLOUD-S-X2 | REQ-SEC-OCLOUD-O2dms-2 REQ-SEC-O2-1 SEC-CTL-O2-1 | No gap |  |

#### Devices Pillar

##### O2 interface Devices Pillar Assets

* No asset applicable to specific pillar.

##### Devices Pillar Gap Analysis

* No asset applicable to specific pillar.

### O-CU Gap Analysis

#### Data Pillar

##### O-CU Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modelling and Risk Assessment [i.4] are listed below. The O-CU also has O1 and E2 interfaces as well, which are discussed separately in clauses 7.3.10 and 7.3.4 respectively.

The assets associated with the O-CU are:

* ASSET-D-03: M-Plane O1 Data
* ASSET-D-11: E2 Node Data (at rest)
* ASSET-D-16: X.509 certificates
* ASSET-D-17: Private keys
* ASSET-D-18: O-RAN components associated and configuration data.
* ASSET-D-19: ETSI TS 133 501 cryptographic keys
* ASSET-D-20: Credentials (Administrators)
* ASSET-D-21: 3GPP application related data
* ASSET-D-22: Inter- and Intra- slice UE priority
* ASSET-D-23: Patches for vulnerable SW components
* ASSET-D-24: NETCONF Configuration Access Control Model datastores.
* ASSET-D-29: Security event log files.
* ASSET-D-31: Security telemetry from the NFV system for detecting threats and anomalies.
* ASSET-D-32: Cryptographic keys used during secure boot

##### Data Pillar Gap Analysis

Table ‑: O-CU Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | ASSET-D-03 | REQ-TLS-FUN-2 REQ-NAC-FUN-1 REQ-NAC-FUN-2 REQ-NAC-FUN-3 REQ-NAC-FUN-4 REQ-NAC-FUN-5 REQ-NAC-FUN-6 REQ-NAC-FUN-7 REQ-NAC-FUN-8 REQ-NAC-FUN-9  REQ-NAC-FUN-10 REQ-NAC-FUN-11 | No gap |  |
| ASSET-D-11 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-16 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-17 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-4 Clause 5.3.5 [i.17] | No gap |  |
| ASSET-D-18 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-19 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-20 | REQ-SEC-PASS-1 SEC-CTL-PASS-1 SEC-CTL-PASS-2 SEC-CTL-PASS-3 | Gap | Authentication and authorization controls not defined |
| ASSET-D-21 | None | Gap | May be outside of scope for O-RAN ALLIANCE |
| ASSET-D-22 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-23 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-24 | none | Gap | Authentication and authorization controls not defined |
| ASSET-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-1 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 REQ-SEC-SLM-SST-4 REQ-SEC-SLM-STR-2 | No gap |  |
| ASSET-D-31 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-1 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 REQ-SEC-SLM-SST-4 REQ-SEC-SLM-STR-2 | No gap |  |
| ASSET-D-32 | None | Gap | Authentication and authorization controls not defined |
| Data Encryption | | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | ASSET-D-03 | None | Gap | Requirements around authentication and authorization only. |
| ASSET-D-11 | None | No gap | Confidentiality not listed as requirement for asset. |
| ASSET-D-16 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2  Clause 5.3.5 [i.17], | No gap |  |
| ASSET-D-17 | REQ-SEC-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 SEC-CTL-OCLOUD-SS-1 SEC-CTL-ALM-PKG-2 SEC-CTL-ALM-PKG-4  Clause 5.3.5 [i.17] | No gap |  |
| ASSET-D-18 | REQ-SEC-ALM-PKG-13 | Possible gap | Requirement is too general |
| ASSET-D-19 | Clause 5.3.5 [i.17] | No gap |  |
| ASSET-D-20 | REQ-SEC-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 SEC-CTL-OCLOUD-SS-1 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-21 | Clause 5.3.8 [i.17] | No gap |  |
| ASSET-D-22 | None | No gap | Confidentiality not listed as requirement for asset. |
| ASSET-D-23 | REQ-SBOM-010 REQ-SEC-ALM-PKG-10 | No gap |  |
| ASSET-D-24 | REQ-SEC-ALM-PKG-13 | No gap | No encryption in transit or rest |
| ASSET-D-29 | REQ-SEC-SLM-TESM-2 REQ-SEC-TESR-6 REQ-SEC-SLM-STR-1 | No gap |  |
| ASSET-D-31 | REQ-SEC-SLM-TESM-2 REQ-SEC-TESR-6 REQ-SEC-SLM-STR-1 | No gap |  |
| ASSET-D-32 | Clause 5.3.5 [i.17] | No gap | Would apply to data at rest only. |

#### Application and Workloads Pillar

##### O-CU Application and Workloads Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are listed below. The O-CU also has O1 and E2 interfaces as well, which are discussed separately in clauses 7.3.10 and 7.3.4 respectively. The O-CU specific assets are as follows:

* ASSET-C-03: O-CU-UP software.
* ASSET-C-04: O-CU-CP software.
* ASSET-C-36: CU-Host (Including software)
* ASSET-C-37: CU-Tenant (Including software)

##### Application and Workloads Pillar Gap Analysis

Note that in Table 7.3‑27 below, the O-CU asset(s) are grouped together as the requirements and controls are apply at the NF level.

Table ‑: O-CU Application and Workloads Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **App/Workloads ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Application Access (Authorization) | a) Access authorization capabilities utilize contextual information such as identity, device compliance, and other attributes to make decisions on various requests for accessing application assets.  b) Authorization is granted per request with expiration. | ASSET-C-03 ASSET-C-04 ASSET-C-36 ASSET-C-37 | See [i.24] | Partial gap | Some contextual information may be operational and out of scope for specification. |
| Application Threat Protections | a) Threat protections is integrated into mission-critical application workflows.  b) Threat protections safeguard applications against known threats and address some application-specific threats. | ASSET-C-03 ASSET-C-04 ASSET-C-36 ASSET-C-37 | REQ-SEC-ALM-SU-2 REQ-SEC-ALM-SU-3 REQ-SEC-ALM-SU-4 | No gap |  |
| Accessible Applications | a) Applicable mission-critical applications are available over open public network connections to authorized users as needed. | ASSET-C-03 ASSET-C-04 ASSET-C-36 ASSET-C-37 | See [i.17] | No gap |  |
| Secure Application  Development and  Deployment Workflow | a) Infrastructure for development, testing, and production environments (including automation).  b) Formal code deployment mechanisms through CI/CD pipelines.  c) Access controls support least privilege principles. | ASSET-C-03 ASSET-C-04 ASSET-C-36 ASSET-C-37 |  | Gap | Some parts may be out of scope for O-RAN ALLIANCE Specification |
| Application Security  Testing | a) Utilization of static and dynamic testing methods for security testing.  b) Performance of security testing including manual expert analysis before application deployment. | ASSET-C-03 ASSET-C-04 ASSET-C-36 ASSET-C-37 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c REQ-SEC-OCLOUD-SW-2 | No gap |  |

#### Identity Pillar

##### O-CU Identity Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are listed below. The O-CU is considered a singular NF in terms of identity and does not have separate identities for each interface. The assets are listed as followed:

* ASSET-C-12: PNF NF equipment
* ASSET-C-36: CU-Host (Including software).
* ASSET-C-37: CU-Tenant (Including software).

##### Identity Pillar Gap Analysis

Table ‑: O-CU Identity Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Authentication | The system authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g. locale or activity).   1. if there is mutual authentication for internal communications, we consider the stage as INITIAL. 2. For internal interfaces, authentication based on credentials alone (certificate, pre-shared key, etc.) can be considered as meeting INITIAL maturity level. | ASSET-C-12 | See [i.17][i.25] | No gap |  |
| ASSET-C-36 | See [i.17][i.25] | No gap |  |
| ASSET-C-37 | See [i.17][i.25] | No gap |  |
| Access Management (Authorization) | The system authorizes access, including for privileged access requests, that expires with automated review.   1. This function applies to APIs and user accounts. 2. For applications, static role assignments (e.g. role binding of a service account) with ephemeral tokens can be considered as INITIAL stage. | ASSET-C-12 | See [i.17][i.25] | No gap |  |
| ASSET-C-36 | See [i.17][i.25] | No gap |  |
| ASSET-C-37 | See [i.17][i.25] | No gap |  |

#### Networks Pillar

##### O-CU Networks Pillar Assets

Currently there are no applicable assets or components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] for O-CU Network pillar.

##### Networks Pillar Gap Analysis

No gap analysis required.

#### Devices Pillar

##### O-CU Devices Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are listed below. The O-CU specific assets are as follows:

* ASSET-C-12: PNF NF equipment

##### Devices Pillar Gap Analysis

Table ‑: O-CU Devices Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Devices ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Policy Enforcement and Compliance Monitoring | Basic Device characteristics visibility. Basic policy enforcement mechanism for managing software configurations or vulnerabilities | ASSET-C-12 | REQ-SEC-TAP-5 REQ-SEC-SLM-NET-EVT-1 REQ-SEC-SLM-GSE-1 REQ-SEC-SLM-GSE-3 REQ-SEC-SLM-GSE-4 REQ-SEC-SLM-GSE-5 REQ-SEC-SLM-GSE-6 See [i.17] | No gap |  |
| Resource Access (Authorization) | Some visibility into devices or virtual assets’ characteristics to approve resource access | ASSET-C-12 | REQ-SEC-SLM-NET-EVT-1 REQ-SEC-SLM-GSE-6 | No gap |  |
| Device Threat Protection | Some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration. | ASSET-C-12 | REQ-SEC-SLM-NET-EVT-1 | Partial gap | REQ-SEC-ALM-PKG applies to VNF/CNF and not PNFs |

### O-DU Gap Analysis

#### Data Pillar

##### O-DU Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modelling and Risk Assessment [i.4] are listed below. The O-DU also has O1 and E2 interfaces as well, which are discussed separately in clauses 7.3.10 and 7.3.4 respectively.

The unique assets associated with the O-DU are:

* ASSET-D-01: Critical S-Plane Data
* ASSET-D-02: Critical M-Plane Data transported over Fronthaul
* ASSET-D-03: M-Plane O1 Data
* ASSET-D-04: Critical C-Plane Data
* ASSET-D-05: Critical Fronthaul U-Plane data
* ASSET-D-11: E2 Node Data (at rest)
* ASSET-D-16: X.509 certificates
* ASSET-D-17: Private keys
* ASSET-D-18: O-RAN components associated and configuration data.
* ASSET-D-20: Credentials (Administrators)
* ASSET-D-22: Inter- and Intra- slice UE priority
* ASSET-D-23: Patches for vulnerable SW components
* ASSET-D-24: NETCONF Configuration Access Control Model datastores.
* ASSET-D-29: Security event log files.
* ASSET-D-31: Security telemetry from the NFV system for detecting threats and anomalies.
* ASSET-D-32: Cryptographic keys used during secure boot

##### Data Pillar Gap Analysis

Table ‑: O-DU Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | ASSET-D-01 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-02 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-03 | REQ-TLS-FUN-2 REQ-NAC-FUN-1 REQ-NAC-FUN-2 REQ-NAC-FUN-3 REQ-NAC-FUN-4 REQ-NAC-FUN-5 REQ-NAC-FUN-6 REQ-NAC-FUN-7 REQ-NAC-FUN-8 REQ-NAC-FUN-9  REQ-NAC-FUN-10 REQ-NAC-FUN-11 | No gap |  |
| ASSET-D-04 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-05 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-11 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-16 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-17 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-4 Clause 5.3.5 [i.17] | No gap |  |
| ASSET-D-18 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-20 | REQ-SEC-PASS-1 SEC-CTL-PASS-1 SEC-CTL-PASS-2 SEC-CTL-PASS-3 | Gap | Authentication and authorization controls not defined |
| ASSET-D-22 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-23 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| ASSET-D-24 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-SLM-TESR-5 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 | No gap |  |
| ASSET-D-31 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TE-5 REQ-SEC-TESR-1 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 | No gap |  |
| ASSET-D-32 | None | Gap | There are requirements for secure storage and boot, but not access of key material. |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | ASSET-D-01 | REQ-SEC-OFSP-8 | No gap |  |
| ASSET-D-02 | See [i.26] | No gap |  |
| ASSET-D-03 | See [i.24] | No gap |  |
| ASSET-D-04 | REQ-SEC-OFCP-4 SEC-CTL-OFCP-1 | No gap |  |
| ASSET-D-05 | Clause 6.6 [i.17] | No gap |  |
| ASSET-D-11 | None | Gap | Data at rest only, see clause 7.3.4 for E2 data in transit |
| ASSET-D-16 | REQ-SEC-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13  See [i.24],[i.25] | No gap |  |
| ASSET-D-17 | REQ-SEC-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13  See [i.24],[i.25] | No gap |  |
| ASSET-D-18 | REQ-SEC-ALM-PKG-13 | Possible gap | Requirement is too general |
| ASSET-D-20 | REQ-SEC-ALM-PKG-13 | No gap |  |
| ASSET-D-22 | See [i.24],[i.25] | No gap |  |
| ASSET-D-23 | REQ-SBOM-010 REQ-SEC-ALM-PKG-10 | No gap |  |
| ASSET-D-24 | REQ-SEC-ALM-PKG-13 | No gap |  |
| ASSET-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-2 | No gap |  |
| ASSET-D-31 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-SLM-TESM-2 | No gap |  |
| ASSET-D-32 | See [i.17] | No gap | Data at rest. |

#### Applications and Workloads Pillar

##### O-DU Applications and Workloads Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are listed below. The O-DU also has O1 and E2 interfaces as well, which are discussed separately in clauses 7.3.10 and 7.3.4 respectively. The O-DU specific assets are as follows:

* ASSET-C-05: O-DU software.
* ASSET-C-34: DU-Host (Including software)
* ASSET-C-35: DU-Tenant (Including software)

##### Applications and Workloads Pillar Gap Analysis

Note that in Table 7.3‑31 below, the O-DU asset(s) are grouped together as the requirements and controls are apply at the NF level.

Table ‑: O-DU Applications and Workloads Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **App/Workloads ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Application Access (Authorization) | a) Access authorization capabilities utilize contextual information such as identity, device compliance, and other attributes to make decisions on various requests for accessing application assets.  b) Authorization is granted per request with expiration. | ASSET-C-05 ASSET-C-34 ASSET-C-35 | See [i.24] | No gap | Identity only |
| Application Threat Protections | a) Threat protections is integrated into mission-critical application workflows.  b) Threat protections safeguard applications against known threats and address some application-specific threats. | ASSET-C-05 ASSET-C-34 ASSET-C-35 | REQ-SEC-ALM-SU-2 REQ-SEC-ALM-SU-3 REQ-SEC-ALM-SU-4 | No gap |  |
| Accessible Applications | a) Applicable mission-critical applications are available over open public network connections to authorized users as needed. | ASSET-C-05 ASSET-C-34 ASSET-C-35 | See [i.17] | No gap |  |
| Secure Application  Development and  Deployment Workflow | a) Infrastructure for development, testing, and production environments (including automation).  b) Formal code deployment mechanisms through CI/CD pipelines.  c) Access controls support least privilege principles. | ASSET-C-05 ASSET-C-34 ASSET-C-35 | None | Gap | May be out of scope for O-RAN Specification. |
| Application Security  Testing | a) Utilization of static and dynamic testing methods for security testing.  b) Performance of security testing including manual expert analysis before application deployment. | ASSET-C-05 ASSET-C-34 ASSET-C-35 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c | No gap |  |

#### Identity Pillar

##### O-DU Identity Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are listed below. The O-DU is considered the NF in terms of identity and the O1 or E2 interface is not considered separate. The assets are as follows:

* ASSET-C-12: PNF NF equipment
* ASSET-C-34: DU-Host (Including software).
* ASSET-C-35: DU-Tenant (Including software).

##### Identity Pillar Gap Analysis

Table ‑: O-DU Identity Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Identity ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Authentication | The system authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g. locale or activity).   1. if there is mutual authentication for internal communications, we consider the stage as INITIAL. 2. For internal interfaces, authentication based on credentials alone (certificate, pre-shared key, etc.) can be considered as meeting INITIAL maturity level. | ASSET-C-12 | See [i.17] | No gap |  |
| ASSET-C-34 | See [i.17] | No gap |  |
| ASSET-C-35 | See [i.17] | No gap |  |
| Access Management (Authorization) | The system authorizes access, including for privileged access requests, that expires with automated review.   1. This function applies to APIs and user accounts. 2. For applications, static role assignments (e.g. role binding of a service account) with ephemeral tokens can be considered as INITIAL stage. | ASSET-C-12 | See [i.17] | No gap |  |
| ASSET-C-34 | See [i.17] | No gap |  |
| ASSET-C-35 | See [i.17] | No gap |  |

#### Networks Pillar

##### O-DU Networks Pillar Assets

Currently there are no applicable assets or components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] for O-DU Network pillar.

##### Networks Pillar Gap Analysis

No gap analysis required.

#### Devices Pillar

##### O-DU Devices Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4]. The O-DU specific assets are as follows:

* ASSET-C-12: PNF NF equipment

##### Devices Pillar Gap Analysis

Table 7.3‑33: O-DU Devices Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Devices ZT Function** | **Guidance to Reach Initial Stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Policy Enforcement and Compliance Monitoring | Basic Device characteristics visibility. Basic policy enforcement mechanism for managing software configurations or vulnerabilities | ASSET-C-12 | REQ-SEC-TAP-5 REQ-SEC-SLM-NET-EVT-1 REQ-SEC-SLM-GSE-1 REQ-SEC-SLM-GSE-3 REQ-SEC-SLM-GSE-4 REQ-SEC-SLM-GSE-5 REQ-SEC-SLM-GSE-6  See [i.17] | No gap |  |
| Resource Access (Authorization) | Some visibility into devices or virtual assets’ characteristics to approve resource access | ASSET-C-12 | REQ-SEC-SLM-NET-EVT-1 REQ-SEC-SLM-GSE-6 | No gap |  |
| Device Threat Protection | Some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration. | ASSET-C-12 | REQ-SEC-SLM-NET-EVT-1 | Partial gap | REQ-SEC-ALM-PKG applies to VNF/CNF and not PNFs |

### O-RU Gap Analysis

#### Data Pillar

##### O-RU Data Pillar Assets

The applicable assets defined in the WG11 O-RAN Security Threat Modelling and Risk Assessment [i.4] are listed below.

The unique assets associated with the O-RU are:

* ASSET-D-01: Critical S-Plane Data
* ASSET-D-02: Critical M-Plane Data transported over Fronthaul
* ASSET-D-04: Critical C-Plane Data
* ASSET-D-05: Critical Fronthaul U-Plane data
* ASSET-D-06: Reference signals, synchronization signal and channels in downlink and uplink between O-RU and UE
* ASSET-D-16: X.509 certificates
* ASSET-D-17: Private keys
* ASSET-D-18: O-RAN components associated and configuration data.
* ASSET-D-20: Credentials (Administrators)
* ASSET-D-23: Patches for vulnerable SW components
* ASSET-D-24: NETCONF Configuration Access Control Model datastores.
* ASSET-D-29: Security event log files.
* ASSET-D-32: Cryptographic keys used during secure boot

##### Data Pillar Gap Analysis

Table ‑: O-RU Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | ASSET-D-01 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-02 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-04 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-05 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-06 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-16 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-17 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-4 Clause 5.3.5 [i.17] | No gap |  |
| ASSET-D-18 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-20 | REQ-SEC-PASS-1 SEC-CTL-PASS-1 SEC-CTL-PASS-2 SEC-CTL-PASS-3 | Gap | Authorization controls not defined |
| ASSET-D-23 | REQ-SEC-ALM-PKG-11 SEC-CTL-ALM-PKG-1 | No gap |  |
| ASSET-D-24 | None | Gap | Authentication and authorization controls not defined |
| ASSET-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESM-3 REQ-SEC-TESR-1 REQ-SEC-TESR-5 REQ-SEC-TESR-7 REQ-SEC-TESR-9 REQ-SEC-TESR-11 | No gap |  |
| ASSET-D-32 | None | Gap | There are requirements for secure storage and boot, but not access of key material. |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | ASSET-D-01 | REQ-SEC-OFSP-8 | No gap |  |
| ASSET-D-02 | See [i.26] | No gap |  |
| ASSET-D-04 | REQ-SEC-OFCP-4 SEC-CTL-OFCP-1 | No gap |  |
| ASSET-D-05 | Clause 6.6 [i.17] | No gap | PDCP provides confidentiality |
| ASSET-D-06 | Clause 5.3.5 [i.17] | No gap |  |
| ASSET-D-16 | REQ-SEC-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 See [i.24],[i.25] | No gap |  |
| ASSET-D-17 | REQ-SEC-OCLOUD-SS-1 REQ-SEC-ALM-PKG-13 See [i.24],[i.25] | No gap |  |
| ASSET-D-18 | REQ-SEC-ALM-PKG-13 | Possible gap | Requirement is too general |
| ASSET-D-20 | REQ-SEC-ALM-PKG-13 | No gap |  |
| ASSET-D-23 | REQ-SBOM-010 REQ-SEC-ALM-PKG-10 | No gap |  |
| ASSET-D-24 | REQ-SEC-ALM-PKG-13 | No gap |  |
| ASSET-D-29 | REQ-SEC-SLM-TESS-6 REQ-SEC-SLM-TESS-7 REQ-SEC-TESR-1 REQ-SEC-TESR-11 REQ-SEC-SLM-TESM-2 REQ-SEC-SLM-SST-2 | No gap |  |
| ASSET-D-32 | None | Gap |  |

#### Application and Workloads Pillar

##### O-RU Application and Workloads Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are listed below. The O-RU specific assets are as follows:

* ASSET-C-06: O-RU software.
* ASSET-C-32: O-RU Host
* ASSET-C-33: O-RU Tenant (Shared Resource Operator)

##### Applications and Workloads Pillar Gap Analysis

Note that in Table 7.3‑25 below, the O-RU asset(s) are grouped together as the requirements and controls are apply at the NF level.

Table ‑: O-RU Applications and Workloads Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **App/Workloads ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Application Access (Authorization) | a) Access authorization capabilities utilize contextual information such as identity, device compliance, and other attributes to make decisions on various requests for accessing application assets.  b) Authorization is granted per request with expiration. | ASSET-C-06 ASSET-C-32 ASSET-C-33 | See [i.24]  REQ-SEC-SharedORU-1 REQ-SEC-SharedORU-2 | No gap | Identity only |
| Application Threat Protections | a) Threat protection is integrated into mission-critical application workflows.  b) Threat protections safeguard applications against known threats and address some application-specific threats. | ASSET-C-06 ASSET-C-32 ASSET-C-33 | REQ-SEC-ORU-1 REQ-SEC-ORU-2 | No gap |  |
| Accessible Applications | a) Applicable mission-critical applications are available over open public network connections to authorized users as needed. | ASSET-C-06 ASSET-C-32 ASSET-C-33 | See [i.17] | No gap |  |
| Secure Application Development and Deployment Workflow (New Function) | a) Infrastructure for development, testing, and production environments (including automation).  b) Formal code deployment mechanisms through CI/CD pipelines.  c) Access controls support least privilege principles. | ASSET-C-06 ASSET-C-32 ASSET-C-33 | None | Gap |  |
| Application Security  Testing (Formerly  Application Security) | a) Utilization of static and dynamic testing methods for security testing.  b) Performance of security testing including manual expert analysis before application deployment. | ASSET-C-06 ASSET-C-32 ASSET-C-33 | REQ-SEC-ALM-PKG-1 REQ-SEC-ALM-PKG-7a REQ-SEC-ALM-PKG-7b REQ-SEC-ALM-PKG-7c | No gap |  |

#### Identity Pillar

##### O-RU Identity Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are listed below. The O-RU is considered as a PNF in terms of identity and O-RU specific assets are as follows.

* ASSET-C-12: PNF NF equipment
* ASSET-C-32: O-RU Host
* ASSET-C-33: O-RU Tenant (Shared Resource Operator)

##### Identity Pillar Gap Analysis

Table ‑: O-RU Identity Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Authentication | The system authenticates identity using MFA, which may include passwords as one factor and requires validation of multiple entity attributes (e.g. locale or activity).  a) If there is mutual authentication for internal communications, we consider the stage as INITIAL.  b) For internal interfaces, authentication based on credentials alone (certificate, pre-shared key, etc.) can be considered as meeting INITIAL maturity level. | ASSET-C-12 | See [i.17] | No gap |  |
| ASSET-C-32 | See [i.17] | No gap |  |
| ASSET-C-33 | See [i.17] | No gap |  |
| Access Management (Authorization) | The system authorizes access, including for privileged access requests, that expires with automated review.   1. This function applies to APIs and user accounts. 2. For applications, static role assignments (e.g. role binding of a service account) with ephemeral tokens can be considered as INITIAL stage. | ASSET-C-12 | See [i.17] | No gap |  |
| ASSET-C-32 | See [i.17] | No gap |  |
| ASSET-C-33 | See [i.17] | No gap |  |

#### Networks Pillar

##### O-RU Networks Pillar Assets

Currently there are no applicable assets or components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] for O-RU Network pillar.

##### Networks Pillar Gap Analysis

No Gap Analysis required.

#### Devices Pillar

##### O-RU Devices Pillar Assets

The applicable assets and components defined in the WG11 O-RAN Security Threat Modeling and Risk Assessment [i.4] are listed below. The O-RU specific assets are as follows:

* ASSET-C-12: PNF NF equipment

##### Devices Pillar Gap Analysis

Table ‑: O-RU Devices Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Devices ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements mapped to CISA stage** | **Assessed Gap to Initial CISA Stage** | **Comments** |
| Policy Enforcement and Compliance Monitoring | Basic Device characteristics visibility. Basic policy enforcement mechanism for managing software configurations or vulnerabilities | ASSET-C-12 | REQ-SEC-TAP-5 REQ-SEC-SLM-NET-EVT-1 REQ-SEC-SLM-GSE-1 REQ-SEC-SLM-GSE-3 REQ-SEC-SLM-GSE-4 REQ-SEC-SLM-GSE-5 REQ-SEC-SLM-GSE-6 See [i.17] | No gap |  |
| Resource Access (Authorization) | Some visibility into devices or virtual assets’ characteristics to approve resource access | ASSET-C-12 | REQ-SEC-SLM-NET-EVT-1 REQ-SEC-SLM-GSE-6 | No gap |  |
| Device Threat Protection | Some automated processes for deploying and updating threat protection capabilities to devices and to virtual assets with limited policy enforcement and compliance monitoring integration. | ASSET-C-12 | REQ-SEC-SLM-NET-EVT-1 | Partial gap | REQ-SEC-ALM-PKG applies to VNF/CNF and not PNFs |

### Open Fronthaul Gap Analysis

#### Introduction

The Open Fronthaul assets considers the Open Fronthaul interface as well as the architecture elements which includes the O-DU and O-RU. The gap analysis is considered only for the Open Fronthaul interface. The Transport Network Element, Fronthaul Multiplexer, Fronthaul Gateway are considered new assets and not included in the Gap Analysis.

#### Data Pillar

##### Open Fronthaul Interface Data Pillar Assets

The applicable assets defined in the WG11 Threat Modelling and Risk Assessment document [i.4] are as following:

* ASSET-D-01: Critical S-Plane Data
* ASSET-D-02: Critical Management-Plane data transported over the Fronthaul interface such as: maintenance and monitoring signals, data collected related to O-RU operations, logs (troubleshooting, trace)
* ASSET-D-04: Critical C-Plane data
* ASSET-D-05: Critical Fronthaul U-Plane data
* ASSET-D-16: X.509 certificates in O-RAN network such as those used for O-RAN components for authentication, encryption, and signing.
* ASSET-D-17: Security private keys in O-RAN network such as those used for O-RAN components for authentication, encryption, and signing.

##### Gap Analysis for Open Fronthaul Assets

Table ‑: Open Fronthaul Data Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Data ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gap** | **Comments** |
| Data Access | a) Automated data access control  b) Elements of least privileges are incorporated with the automated data access control | Open Fronthaul Interface Data Pillar Assets | | | |
| ASSET-D-01 | REQ-SEC-OFHPLS-1-- REQ-SEC-OFHPLS-3  SEC-CTL-OFHPLS-1-- SEC-CTL-OFHPLS-5 | No gap |  |
| ASSET-D-02 | REQ-SEC-OFHPLS-1-- REQ-SEC-OFHPLS-3  SEC-CTL-OFHPLS-1-- SEC-CTL-OFHPLS-5 | No gap |  |
| ASSET-D-04 | REQ-SEC-OFHPLS-1-- REQ-SEC-OFHPLS-3  SEC-CTL-OFHPLS-1-- SEC-CTL-OFHPLS-5 | No gap |  |
| ASSET-D-05 | REQ-SEC-OFHPLS-1-- REQ-SEC-OFHPLS-3  SEC-CTL-OFHPLS-1-- SEC-CTL-OFHPLS-5 | No gap |  |
| ASSET-D-16 | None | Gap |  |
| ASSET-D-17 | None | Gap |  |
| Data Encryption | a) Encrypted data in transit and, where feasible, data at rest.  b) Key management policies and secure encryption keys are beginning to be formalized. | Open Fronthaul Interface Assets | | | |
| ASSET-D-01 | REQ-SEC-OFSP-8 SEC-CTL-OFSP-4 | No gap |  |
| Asset-D-02 | Table 5.4-1 refer [i.26] | No gap |  |
| Asset-D-04 | REQ-SEC-OFCP-4 SEC-CTL-OFCP-1 SEC-CTL-OFHMECC-1--SEC-CTL-OFHMECC-5 | No gap |  |
| Asset-D-05 | SEC-CTL-OFUP-1 Clause 5.2.5.2.2.1 | No gap |  |
| ASSET-D-16 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 | No gap |  |
| ASSET-D-17 | REQ-SEC-ALM-PKG-13 SEC-CTL-ALM-PKG-2 | No gap |  |

#### Applications and Workloads Pillar

##### Open Fronthaul Interface Applications and Workloads Pillar Assets

* No asset applicable to specific pillar

#### Identity Pillar

##### Open Fronthaul Interface Identity Pillar Assets

* No asset applicable to specific pillar

#### Networks Pillar

##### Open Fronthaul Interface Networks Pillar Assets

The applicable assets defined in the WG11 Threat Modelling and Risk Assessment document [i.4] are as following:

* ASSET-C-24: OFH M-Plane, including protocol stack
* ASSET-C-25: OFH CUS-Plane, including protocol stack

##### Gap Analysis for Open Fronthaul assets

Table ‑: Open Fronthaul Networks Pillar Gap Analysis

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Networks ZT Function** | **Guidance to reach initial stage** | **Asset(s)** | **Existing Requirements Mapped to CISA Stage** | **Assessed Gaps** | **Comments** |
| Traffic Encryption | Encryption for all internal (and preferably external) application traffic, with formalized key management policies and secure encryption keys | ASSET-C-24 | Refer [i.26] | No gap |  |
| ASSET-C-25 | SEC-CTL-OFHMECC-1-- SEC-CTL-OFHMECC-5 | No gap |  |

#### Devices Pillar

##### Open Fronthaul Devices Pillar Assets

* No asset applicable to specific pillar

## WG11 Considerations for Mapping Security Controls to CISA ZTMM

### Introduction

The following considerations were made when mapping O-RAN security controls to the CISA ZTMM, as summarized in this list below:

**List 7.4-1: Summary of CISA ZTMM Stages**

Traditional stage

* Perimeter-based security controls
* Perimeter-based monitoring
* Static network policies
* Manual processes

Initial stage

* External controls and some security controls to protect against internal threats
* Monitoring with known indicators
* Tailored policies
* Some automation
* Begin cloud migration

Advanced stage

* Security controls to protect against internal and external threats
* Centralized visibility
* Continuous monitoring of network
* Tailored policies
* Automation

Optimal stage

* Security controls to protect against internal and external threats
* Centralized visibility with situational awareness
* Continuous Monitoring of network, applications, and users
* Dynamic policies with AI
* Automation with AI

### Mapping to CISA ZTMM

The O-RAN ALLIANCE has made significant progress advancing its security specifications. Table 7.4‑1 shows how the currently specified security controls map to the CISA ZTMM stages. Some additional considerations made when mapping O-RAN specifications to the stages are as follow:

* The Devices pillar includes User Equipment and cloud infrastructure devices.
* The Networks pillar includes data-in-transit.
* The Applications pillar includes O-RAN architecture elements, such as O-RAN CNFs, SMO, and rApps/xApps.
* The Data pillar includes data-in-transit, data-at-rest, and data-in-use.

Table ‑: CISA ZTMM Mapping of O-RAN security controls

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Pillars and Functions | Traditional | Initial | Advanced | Optimal |
| Identity | Passwords | X.509 Certificates, LDAPS, mTLS, IEEE 802.1X, NACM, Principle of least privilege, **MFA** | OAuth 2.0, CMPv2 |  |
| Devices |  | Resource management | HSM, **Container hardening** |  |
| Networks | SSH, SFTP | TLS, FTPES | API security, **MACsec** | NFs secured as micro-perimeters |
| Applications and Workloads |  | Digital signatures, Volumetric DDoS Protection | **Secure On-Boarding** |  |
| Data |  | TLS for data-in-transit |  |  |
| Visibility and Analytics |  | Secure Logging |  |  |
| Automation and Orchestration |  |  |  |  |
| Governance |  |  | SBOM, **GSMA NESAS** | **AI/ML security** |

NOTE: **Bold** indicates an O-RAN specifications roadmap feature currently being addressed in a WG11 security work item.

# ZTA Threats

## Introduction

This clause reviews the O-RAN Security Threat Modeling and Risk Assessment TR [i.4] for existing threats.

## Mapping of the existing Security Principles to ZT Tenets

In the O-RAN Security Threat Modeling and Risk Assessment TR [i.4] all Threats are being mapped to Security Principles (see [i.4] clause 8.2). In order to analyse which of the Threats are related to ZT tenets and whether they are properly covered by security principles, the security principles need to be mapped to the ZT tenets. [i.4] clause 8 provides such a mapping. Table 8.2‑1 represents this mapping, which has been updated for the O-RAN Security Threat Modeling and Risk Assessment TR.

Table ‑: Mapping of security principles to ZT tenets1

| Security Principles | ZT Tenets | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| SP-AUTH - Mutual Authentication |  | X | X | X |  | X |  |
| SP-ACC - Access Control | X |  | X | X |  | X |  |
| SP-CRYPTO - Secure cryptographic, key management and PKI |  | X |  | X |  |  |  |
| SP-TCOMM - Trusted Communication |  | X |  |  |  |  |  |
| SP-SS - Secure Storage | X | X |  | X | X | X |  |
| SP-SB - Secure boot and self-configuration | X |  | X | X | X |  |  |
| SP-UPDT - Secure Update |  |  |  |  | X |  | X |
| SP-RECO - Recoverability & Backup |  |  |  |  | X | X | X |
| SP-OPNS - Security management of risks in open-source components |  |  |  | X | X | X | X |
| SP-ASSU - Security Assurance |  |  |  |  | X |  | X |
| SP-PRV - Privacy |  | X | X | X | X | X | X |
| SP-SLC - Continuous security development, testing, logging, monitoring and vulnerability handling |  |  |  | X | X | X | X |
| SP-ISO - Robust Isolation |  | X | X | X | X |  | X |
| SP-PHY - Physical security | X | X | X | X | X | X | X |
| SP-CLD - Secure cloud computing and virtualization |  | X | X | X | X | X | X |
| SP-ROB - Robustness |  | X | X |  | X | X | X |
| SP-IDM - O-Cloud ID secure management | X |  | X | X | X | X | X |

NOTE 1: **X**: mapping existing in [i.4].

NOTE 2: Access to resources is determined by dynamic policy which is mapped in the above Table 8.2-1 for SP-ACC - Access Control (Tenet 4) need to be discussed further.

## Existing defined threats

<Identify relevant existing threats from WG11 work item Technical Reports>

## New threats

<Identify new threats>

# Threat analysis

<More detailed description and analysis of new threats using STRIDE. (Existing threats already have analysis completed.)>

# Risk assessment

<Risk assessment to categorize new threats>

# Recommendations

The following preliminary recommendations from this work item will be addressed in future updates to this technical report and other specifications:

* **Complete threat and risk assessment**: Update clauses 8, 9 and 10 with identification of new threats and threat analysis and risk assessment for the newly identified threats.
* **Conduct Gap Analysis:** Perform a gap analysis for different O-RAN assets based on the guidelines in clause 6.2 and update clause 7.3 accordingly.

*Status:* Gap analysis on O-RAN architecture elements and O-RAN interfaces is complete with the exception of the SMO. The gap analysis on the SMO will be performed after the Decoupled SMO architecture is finalized.

* **Propose ZTA Security Requirements:** Based on the conducted gap analysis, propose a list of Zero Trust Architecture (ZTA) security requirements for different O-RAN assets after consultation with the relevant WG11 Work Items and update clause 11 with those recommended security requirements.
  1. ZTA WI should identify which requirements are in-scope for O-RAN ZTA but not in-scope for O-RAN specifications.
  2. ZTA WI should determine whether security specifications for human administrative access to O-RAN architecture elements are in-scope for O-RAN specifications.

*Status:* Consultation with the respective Work Items is in progress.

* **Define relevant terms:** ZTA WI should define the terms 'micro-perimeter' and 'micro-segmentation' in the context of O-RAN, while considering exiting definitions from authoritative sources.

*Outcome:* Micro-segmentation term is defined in this document.

* **Identify Continuous Monitoring Needs:** Based on the study of NIST ZT tenets applicability in clause 4.2 and the target ZTA security requirements in clause 6.2, continuous monitoring is identified as a critical aspect of ZTA for the following reasons:
  1. It is critical to fully address tenet 4, 5 and 7.
  2. It is critical to fully address the following CISA ZTMM functions:
     + Risk assessment function and visibility and analytics capability in the Identity pillar.
     + Asset & supply chain risk management function, resource access function, and visibility and analytics capability in the Devices pillar.
     + Network traffic management and visibility and analytics capability in the Networks pillar.
     + Application access and visibility and analytics capability in the Applications and Workloads pillar.
     + Visibility and analytics capability in the Data pillar.

Therefore, we recommend conducting a comprehensive study on continuous monitoring in O-RAN as a separate supporting work item or work items. This WI or WIs should define the critical characteristics and attributes that need to be continuously captured in different O-RAN components to address tenets 4, 5, and 7, as well as the CISA ZTMM functions and capabilities listed above.

*Outcome:* WG11 Continuous Security Monitoring Work Item was initiated in August 2024.

# Annex: Change history/Change request (history)

|  |  |  |
| --- | --- | --- |
| Date | Revision | Description |
| 2024.07.24 | 01.00 | Final Version 1 of the Technical Report |
| 2024.11.26 | 02.00 | Final Version 2 of the Technical Report |
|  |  |  |
|  |  |  |