Module by Module - Self Study Note Guide

Nokia Bell Labs 5G Certification Program

Nokia Bell Labs 5G Secured Networks Course

Instructions

Research has shown that learning is most effective when understood from one's own personal perspective. As such, we have created this learning guide for you to use as a personal reference and study guide.

For each module, the guide starts with the objectives, potential exam topics, course topics, and then concludes with key takeaways. For each topic, space is provided for you to take notes, capture observations and insights, or simply create a study guide for reference in preparation for your certification exam.

Table of Contents....

Exam Table

Exam Breakdown – The following table identifies the proportion of questions from each topic area that will appear on the certification examination.

Number of Questions: 60 Questions

Exam Time Limit: 90 Minutes

Approximate Exam Breakdown	% of Total Questions
Security Overview and 5G Security Landscape	
Security Overview	10%
5G Security Landscape	7%
5G Security Features	
5G Security features introduction	7%
Subscriber Identification and Network Access Security	8%
Network Domain Security	8%
RAN and O-RAN security	7%
5G Security compared to other technologies	7%
5G Software, Network Design, Cloud and Operation Security	
5G Software, Cloud and Operation Security Overview	7%
Software (Development) Security	8%
System Architecture and Cloud Security	8%
System Operation Security	8%
5G Security Orchestration and Analytics	
Security Orchestration and Analytics Overview	7%
Security Orchestration Automation and Response	8%

Overall Course Learning Objectives

- Understand foundational security concepts and requirements, including the principles of a security solution.
- Articulate the role of security in a 5G system, and the challenges for network security in the 5G world.
- Picture the 5G Security landscape, from threats actors to standardization bodies.
- Explore standards and practices supporting layered security in 5G networks, including Security Assurance.
- Apply our understanding of security threats, protections and potential responses through a series of real-world case study exercises.
- Consider how Security Orchestration Automation and Response provides a dynamic security approach for the move to 5G.

Module by Module

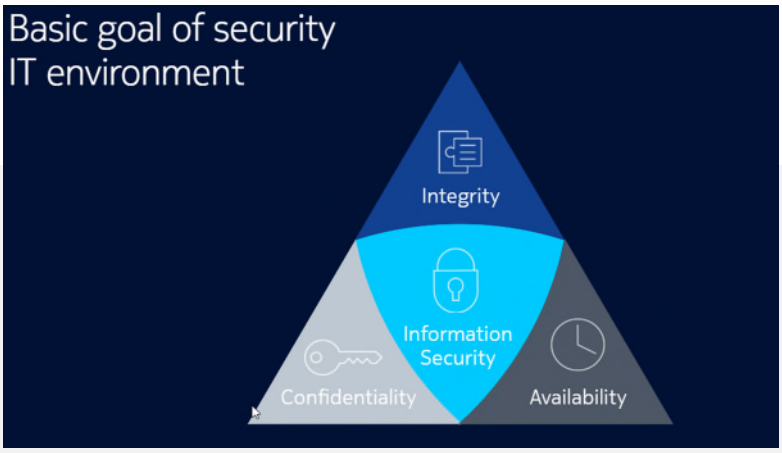
Unit 1 – Introduction

- This module provides an orientation and introduction to the course.

Notes

	Your Notes
Introduction	Instructions. Type your notes in here. Box will expand to accommodate your text. Note: Select and Delete this comment.
Notes	

Unit 2 Module 1 – Security Overview



Key Objectives

Here are our learning objectives for this module.

- Describe foundational security concepts and requirements for IT, Telco and Industrial security environments.
- Understand the CIA triad of cybersecurity which consists of confidentiality, integrity, availability, and how it can be complimented with other goals such as authentication or access control.
- Articulate the concepts of threats and mitigation, risk assessment, damage and compromised assets.
- Recall the 3 pillars of threat mitigation: people, technology, processes
- Identify and understand basic security features such as encryption, digital signature, and Public Key Infrastructure and define the 5 principles for designing a Security solution.
- Define Security Assurance, show how it supports the assessment of a Security Solution, and highlight how security is not an exact science, but rather a continuous process.

Potential Exam Topics

- 3 basic goals for IT Security
- 3 pillars that effective security is built on.
- Integrity, Authentication and Non-Repudiation – ways to ensure these
- What is cryptanalyst
- Know about PKI, MAC, Standards, Access Control
- 5 design principles for a Security Solution

Notes Section

Topic Names	Your Notes
1: Security concepts & requirements	
CIA Triad	
Basic goals of security	

6 security goal
Communication Service Providers specific strong requirements
Common threats
3 pillars: people, technology, and processes.
2. Risk Management basics
Risk assessment
Risk Analysis
Prioritization
Standards
Characterizing a Risk
Risk mitigation & accepted residual risks
3. Basic security features
Encryption
Encryption algorithms
Secured channel data establishment
Hash functions
MAC
Digital Signatures
PKI
Access Control Techniques
4. Design for Security Solution

Five design principles for Security Solutions	
Concept of Security Assurance	
5. Security as a continuous process	
Attacker Side	
Defender Side	
Other Notes	

Key Takeaways:

Here are the key points to remember from this module.

- The main security services are confidentiality, integrity, and availability and are complemented by other goals such as authentication and non-repudiation. The purpose of security is to protect our assets with regards to these goals.
- People, process, and technology often need to go hand in hand to mitigate threats and achieve the security goals, even for services like authentication that may appear mainly a technical issue.
- Core security features and mechanism such as encryption, digital signature, certificates and public key infrastructure form the foundation of security services.
- Risk assessment methodology helps define requirements and recommendations for designing security solutions
- Security principles includes Security by Design, Layered security, Defense-in-depth, Zero-trust, Orchestration and Automation.
- The process of Security Assurance provides confidence that a Security Solution meets its intended requirements
- A Security Solution can't provide 100% protection. Security is not a static process but needs to dynamically improve over time through a continuous process.

Unit 2 Module 2 – Security Landscape

Key Objectives

- Explain the evolution of Security features and requirements for each wireless network generation.
- List the various industry bodies influencing 5G Security, including local regulatory authorities.
- Illustrate the process of threat modelling and risk assessment for 5G Networks.
- Articulate the concepts of threats, threat agents, assets—both tangible and intangible—and risks in 5G security
- Explain the principle of risk matrix and treatment in Risk Management, and how to reduce risk through an iterative process.

Potential Exam Topics

- Know the main players and governing bodies in 5G security
- Threat modelling belongs in what standard series.
- Know different risk treatments
- Know how we can reduce or mitigate risks

Notes Section

Topic Names	Your Notes
Evolution in Cellular security	
1. Main players in the 5G Security landscape	
5G networks and the role for regulators	
OT for Industrial Automation	
2. Threats and Risk Assessment	
Requirements: Future-proof 5G security	

Threat and risk assessment	
Domains to be protected	
Assets to be protected	
Threats classification with impacts and assets	
Risk Management Toolbox – Risk Analysis	
3. 5G Security Landscape	
5G Security split by activities and domain	
Additional Notes	

Key Takeaways:

Let's sum up the key points to remember about this module.

- New use cases and the advent of cloud native applications are driving the need for advanced 5G security.
- Multiple industry players are shaping 5G Security, including regulatory authorities who leverage strong regulation and enforcement.
- Threat modeling and risk assessment are crucial for defining security requirements and protecting the different domains and assets of a 5G Network.
- Tools and reference documents help in Risk Management, however good risk analysis should be performed on real, specific use cases.
- The Risk Matrix is the heart of the iterative Risk Management process, helping reduce the risks while building security measures.
- 5G Security Risk Management includes security features for physical and logical assets, as well as an orchestration and automation approach for the ever-evolving security landscape.

Unit 3 Module 1- 5G Security Use Cases

Key Objectives

- Module introduces the case studies that will be covered in the course.

Notes Section

	Your Notes
Notes	

Unit 4 Module 1 – 5G Security features introduction

Key Objectives

Here are our learning objectives for these modules.

- Recall the 5G system architecture and reference points between functions.
- Identify the 3GPP 5G security specification and describe the different security domains covered.
- Explain 5G Security Assurance and how it benefits operators and equipment vendors.
- Recognize GSMA NESAS as the emerging 5G Security Assurance standard scheme.

Potential Exam Topics

- Difference between the User Plane and Control Plane in a 5G system?
- Security standards provided by 3GPP, GSMA, and the O-RAN Alliance.
- Radio Interface Security belongs where in 3GPP Technical Specification 33.501
- Know what is Network Equipment Security Assurance Scheme (NESAS)

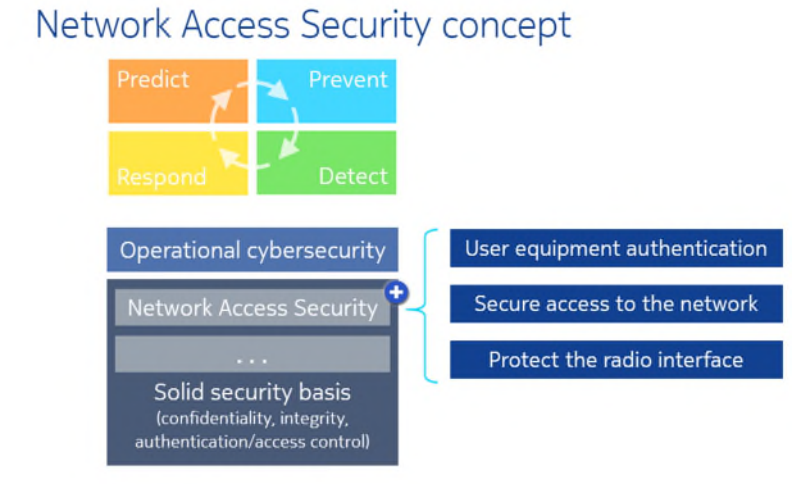
Notes Section

Topic Names	Your Notes
1.5G System Recall	
System Architecture	
2. 5G Overall Security Architecture and Standards	
From 4G to 5G , 2.5 5G System architecture – CP vs UP, SBA	
User Plane and the Control Plan	
Crucial security functions	
3. 5G Security Assurance	
Product Security Assurance Standardization	
3. 5G Security Features Map of rest of unit	
Additional notes	

Key Takeaways:

- The 5G security architecture and procedures are specified in 3GPP TS33.501, which defines 6 different security domains.
- The crucial 5G system functions related to security include the gNB, AMF, NRF, SEPP, AUSF and UDM, which play different roles in the different security domains.
- 5G security assurance is needed to ensure robust and reliable networks and ensure all components are trustworthy and will work with a common, agreed set of security requirements.
- GSMA NESAS is the emerging standard for the 5G Security Assurance Scheme.

Unit 4 Module 2 – Subscriber Identification and Network Access Security



Key Objectives

- Explain the main elements of 5G user identity protection and security.
- Articulate the 5G Authentication and Key Agreement approach.
- Understand how Access Stratum and Non-Access Stratum Security work together to enhance security and describe both set up procedures in details.
- Describe the principles of security key hierarchy for 5G
- Understand network access encryption, integrity protection and authentication

Potential Exam Topics

- Know about access stratum
- Know about different identifiers
- Know about different Authentication mechanisms, and what are in 3GPP release 15
- Know about different parts of Network access security.

Notes Section

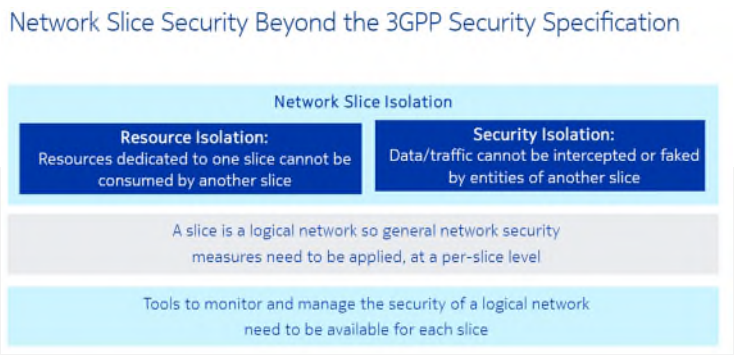
Topic Names	Your Notes
1 Introduction to Network Access Security	
Network Access Security concept	
Entities Involved in Network Access Security	
2. Protecting the Subscriber Identity	
Protecting the Subscriber Identity	

Identifying Mobile Subscribers
Subscriber Privacy, Identifiers, etc
3.Authentication and key agreement
Network Access
New Authentication Framework
4. Access Stratum and Non-Access Stratum Security set up
Non-Access Stratum Security Mode Command Procedure
AKA and Non-Access Stratum Security
5. Key hierarchy, Encryption and Integrity protection
Encryption Mechanism
Attacks
Exercise

Key Takeaways:

- 5G Network security consists of both Access Stratum and Non Access Stratum.
- Frequently changing temporary identifiers such as GUTI and SUCI are used between User Equipment and the network in messages that cannot be cryptographically protected in order to keep user identity secure.
- The UE and the Core Network performs mutual authentication using protocols such as 5G-AKA or EAP- AKA prime as part of a successful authentication procedure using parameters and functions that are present in both the UE and the Core Network.
- Cryptographic functions are used in encryption for security and for integrity protection to check the integrity of the transmitted messages
- The key hierarchy provides for layered security and defense-in-depth.

Unit 4 Module 3 - Network Domain Security



Key Objectives

- Review the role of Service Based Architecture and non-Service Based Architecture in 5G networks.
- Articulate the security mechanisms available to protect both non-SBA and SBA interfaces and their related applications
- Explain how signaling plane and user plane inter-network traffic is secured
- Identify the approaches to securing network slicing

Potential Exam Topics

- Access Stratum and Non-Access Stratum
- Parts of a Certificate
- Asymmetric cryptography.
- Different Authorization Concepts
- Token format used on service based interfaces?

Notes Section

Topic Names	Your Notes
1 Introduction to Network Domain Security	
Security for IP-Based Interfaces	
2. Non-Service Based interface	
Security for Non-Service-Based Network Interfaces	
Security for other Interfaces	
3. Service Based interfaces security.	

Token Request and Service Request (Simplified)	
Security Aspects of the Network Exposure Function (NEF)	
4. Interconnection security	
SBA- Interworking Between PLMNs	
Interconnection Security Enhancement	
5. Network Slicing Security	
3GPP Release 15 & 16 Details	
Network Slice Security Beyond the 3GPP Security Specification	
6. Exercises	

Key Takeaways:

- The Network domain security involves security for 3 areas: the service-based interfaces between control plane functions, the non-service based interfaces between the user plane functions, and the interconnection between the home network and the roaming networks.
- The security for IP based interfaces in 5G is enabled with the use of IPSec for encryption and integrity protection and IKEv2 for negotiation of IPSec keys.
- Network domain security for service-based interfaces uses new protocols like http/2 and security mechanisms based on TLS and OAuth authentication framework.
- Interconnection security for service based interfaces is enabled via SEPP that uses TLS and a new PRotocol for N32 INterconnect Security (PRINS) to secure network function traffic over public networks.

Unit 4 Module 4 - RAN and O-RAN security

Key Objectives

- Contrast RAN and O-RAN architectures and their impact on Security requirements
- Understand the need for O-RAN security standardization
- Describe the security threats and solutions for Transport, Fronthaul, Platform and RAN Intelligent Controller (RIC) in O-RAN deployment

Potential Exam Topics

- Security benefits of O-RAN
- Standardized body working on security challenges for O-RAN interfaces and components
- RIC and x/rApps security
- O-RAN ALLIANCE Security Focus Group

Notes Section

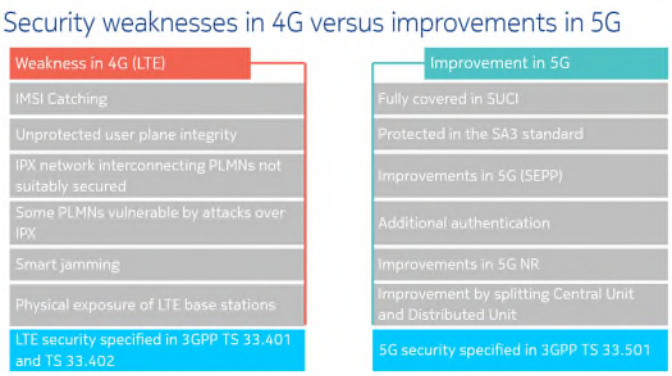
Topic Names	Your Notes
1. RAN and O-RAN Architecture and security	
Contrast traditional RAN with Cloud RAN and Open RAN.	
2.Open RAN security features and threats	
Threat landscape	
Features	

3.Case Study Exercises	
Other notes	

Key Takeaways:

- Traditional RAN architecture is evolving to include Cloud RAN and O-RAN, which deliver openness and intelligence benefits
- The decoupling of RAN hardware and software, along with the increasing number of network elements and interfaces, can lead to a broader surface of attack
- The Security Focus Group of the O-RAN ALLIANCE has specified discreet security measures for the entire O-RAN architecture.

Unit 4 Module 5 - Security in 5G versus other technologies



Key Objectives

- Articulate the security improvements in 5G vs 4G.
- Describe the security principles in Wi-Fi systems and identify the differences between 5G and Wi-Fi security
- Contrast trusted vs. untrusted Non-3GPP access for 5G networks
- Explain how authentication and confidentiality mechanisms allow secure non-3GPP access to 5G networks

Potential Exam Topics

- 5G Security Improvements
- Trusted or Non-Trusted access in a 5G Network
- Non-3GPP access
- Authentication methods supported by the 5G core network functions

Notes Section

Topic Names	Your Notes
1.Security in 5G versus 4G and WiFi networks	
5G and/or WiFi 6	
Other notes	
2.Security for non-3GPP accesses in 5G Network	
Untrusted, Trusted, Authentication, Transport Security	
3. Case Study Exercise	
Other notes	

Key Takeaways:

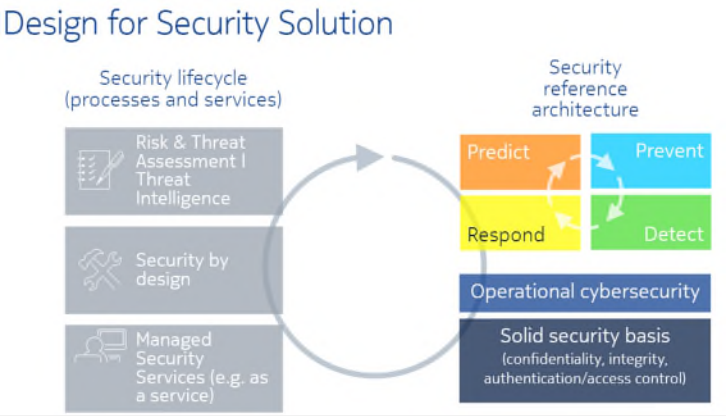
- 5G standards provide improved security compared to 4G, addressing most 4G weaknesses
- 5G and Wifi6 are more complementary than competitive, with Wi-Fi offering simple, low-cost stationary coverage, and 5G providing greater mobility and flexibility.
- Wifi security has also evolved with each generation, leveraging both authentication and encryption.
- 5G systems can host non-3GPP wireline as well as wireless access, including Wi-Fi.
- Standards-based authentication and encrypted transport allow trusted and untrusted non-3GPP secure access to 5G networks

Unit 4 Module 6 – Case Study

Notes Section

Topic Names	Your Notes
Case Study Notes	

Unit 5 Module 1 - 5G System Security Overview



Key Objectives

- Articulate the evolution of how applications have become Cloud Native
- Highlight the flexibility of Cloud Native in network implementations
- Summarize modern software development approaches, including SDLC, DevOps and CI/CD
- Describe the Software Development Security concept, including both proactive and reactive security
- Define the core challenges of Cloud Security

Potential Exam Topics

- Steps of the Software Development Lifecycle (SDLC)
- Security by Design
- Proactive and Reactive security activities

Notes Section

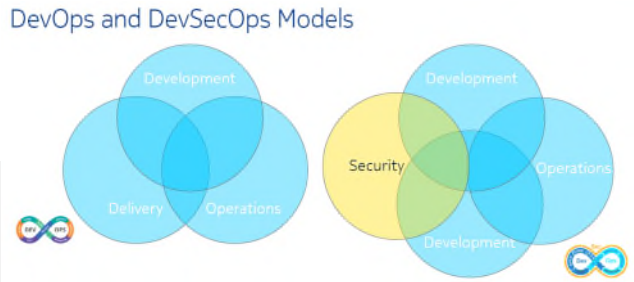
Topic Names	Your Notes
1.5G Cloud Native Principles and Modern Software Development Approach	

Design for Security Solution, Cloud Native	
Software Development Lifecycle (SDLC), DevOPS. CI/CD	
Modern Software Development approach, MoO	
2.Software, Cloud, and System Security Introduction.	
Software development security concept basics	
Proactive and reactive security activities	
Challenges	
Other Notes	

Key Takeaways:

- 5G Security is driven by the specific solution implementation, especially in Cloud Native environments.
- Cloud Native is a highly flexible Cloud implementation but comes with various Security Challenges.
- Software Development Security practices aim to put Security at the heart of the lifecycle in all phases of development and operation.
- A Microservice with Containers provides an architecture a variable border—and variable Mode of Operation—between the vendor and the operator.
- Proactive and reactive activities, as well as Cloud and Network Operation security features, support the overall system security.

Unit 5 Module 2 - Software (Development) Security



Key Objectives

- Explain both proactive and reactive approaches for software security
- Articulate how the main software development models can be secured
- Convey how integrity and hardening protect software in open environments
- Describe how vulnerability management and scoring are strong reactive approaches to software security

Potential Exam Topics

- Proactive and reactive security (continued)
- SDLC
- DevOps
- DevSecOps
- CICD
- Common Vulnerability Scoring System (CVSS)
- Hardening

Notes Section

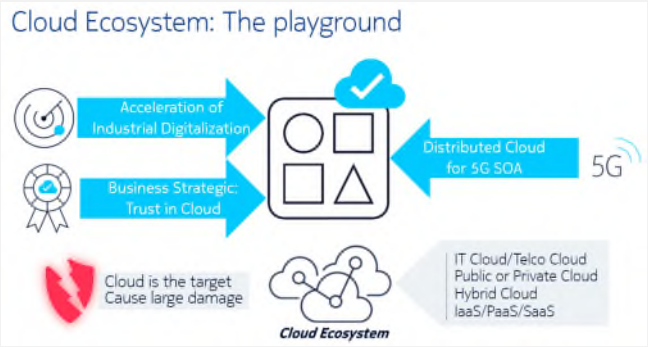
Topic Names	Your Notes
1.Proactive Secure Software : Development Life Cycle	
SDLC, S-SDLC	
Security responsibilities in DevSecOps, CI/CD	
2.Proactive Secure software: Integrity and Hardening	
Open source as a CSP Industry Accelerator	

Hardening	
Software Integrity Protection	
3.Reactive Secure software: Vulnerability management	
Security Vulnerability Management	
4. Exercise	
Additional Notes	

Key Takeaways:

- S-SDLC and DevSecOps are two important software development models that have security built into all of their phases
- Continuous integration and delivery enables software changes in production or directly to users, safely, quickly and in a continuous, sustainable way.
- Hardening is a process used to secure 3rd party vendor integration, especially in open environments
- SVM is a reactive process that keeps software secure during their whole lifecycle

Unit 5 Module 3 - Cloud Ecosystem Security (Cloud and Network Design Security)



Key Objectives

- Be able to identify the main Cloud domains to be secured, and the associated user's role and responsibility in managing security.

- Articulate how to secure a Cloud Software Platform.
- Describe how to secure the main components of each Cloud Infrastructure hardware type
- Plan how to secure Cloud resources for applications and services.
- Explain how to achieve network hardening through a Cloud network security design.

Potential Exam Topics:

- Challenges of Cloud Security
- Security issues applicable to a Distributed Cloud environment
- Important targets for physical compute node security hardening
- Operational isolation for multi-tenancy focus on in a Cloud Environment
- Security tasks applied to secure containers over servers in a Cloud system

Notes Section

Topic Names	Your Notes
1. Big Picture of Cloud Security	
Cloud Ecosystem	
The decision framework stages, Cloud domains, Main threats	
2.Cloud Software Platform Security	
Functional view of cloud software platform, DOS, Hardening	
3.Cloud Infrastructure Security	
Hardening	
HSM	
4.Cloud Resources Security	
Multi-tenancy, Isolation	
VM, Container securing	
5.Cloud Network Security	

Trusted/untrusted zones, access	
6.Exercise	
Additional Notes	

Key Takeaways:

- Securing all domains of a Cloud will secure the entire cloud environment.
- All parts of the Cloud software platform can be secured through targeted techniques.
- Successfully securing the Cloud infrastructure starts at the hardware level of the datacenter
- Securing Cloud resources is critical, as they provide essential links between Cloud services, infrastructure and the management
- Network security design is the key to secure networks and brings Cloud success

Unit 5 Module 4 - Network Design & Operation Security (Transport and Network Operation Security)

Key Objectives

- Describe the main cloud operational domains to identify what to secure
- Detail security of Cloud access and interfaces
- Describe operational security between regular cloud users and the cloud administrator
- Explain security issues of cloud automation and orchestration

Potential Exam Topics

- Functional blocks in a Cloud system
- Security Controls
- Benefits of collecting activity monitoring data
- Different Certificate types
- Applications of continuous security

Notes Section

Topic Names	Your Notes
1. Cloud operational domain	
Cloud operational security, risks, monitoring	
2.Securing Operational Access	
Cloud users access and management	
Certificate management, encryption/isolation	
3.Securing Administration	
Split the system between administrator and operator	
5. Automation & Orchestration for Operational Cloud Security	
orchestration/automation securing	
Exercise	
Additional Notes	

Key Takeaways:

- Operational security is directly linked to the user profile and role
- Access is the gate or door to the system to operate the service and cloud
- Administration tasks require higher security because they are more sensitive operations than regular operations
- Automation and orchestration are key to the operational success of cloud and therefor can be the target of attacks because of its strategic operational importance.

Unit 5 Module 5 – Case Study

Notes Section

Topic Names	Your Notes
Notes on Case Study	

Unit 6 Module 1 - 5G Risk Management applied to Use Cases

Notes Section

Topic Names	Your Notes
5G Risk Management applied to Use Cases	
Notes on Case Study	

Unit 7 Module 1 - Security Orchestration and Analytics (SOAR) Overview

Key Objectives

- Describe the need for Security Orchestration
- Identify the major stages of an Advanced Persistent Threat
- Articulate the role Artificial Intelligence and Machine Learning play in security
- Explain the general concept of security orchestration and analytics
- Define the basics of SOAR technologies

Potential Exam Topics

- APT
- Artificial Intelligence and Machine Learning in security
- SOAR

Notes Section

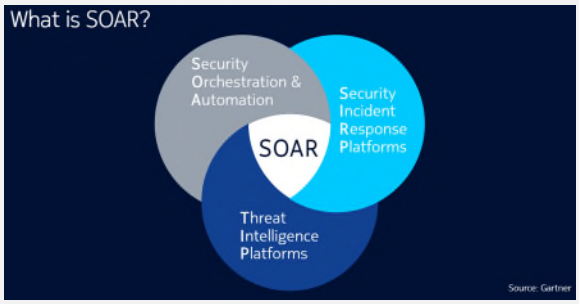
Topic Names	Your Notes
1.Need for Security Orchestration	
Introduction to the Decision Framework	
New security risks, Challenges, Framework	
2.What is an APT	
APT details	

3.AI and ML in Security orchestration and automation	
How will AI and ML be Utilized	
4.Introduction to SOAR	
Role of SOAR in Cyber Defense Center	
Additional Notes	

Key Takeaways:

- The main drivers of SOAR adoption are staff shortages, alert overload, and the complexity of cyber threats
- Advanced Persistent Threat (APTs) attacks complex versions of Multi-Stage Attacks (MSAs) and include 3 major stages: Infiltration, Expansion, Extraction
- A range of bad actors including financial criminals or state actors can execute Advanced Persistent Threat attacks
- SOAR is an emerging security approach that combines Threat Intelligence with Orchestration and Automatic incident response

Unit 7 Module 2 - Security Orchestration Automation and Response



Key Objectives

- Explain how multi-dimension security analytics is the basis of SOAR
- Articulate how SOAR improves security operations in the field
- Map the Architecture and Core Components of SOAR
- Describe the use and functionality of SOAR in different technology situations ….and finally,
- You should be able to explain the practical application of SOAR through several use case examples

Potential Exam Topics

- SOAR (continued)
- Threat Intelligence Platform
- Playbooks
- Different types of Threats

Notes Section

Topic Names	Your Notes
Security Orchestration Automation and Response	
1.Drivers and Enablers	
What is SOAR?	
2.Core components of SOAR.	
Workflow and collaboration engine, Case and ticket management, Orchestration and automation	
3. Architecture	
SOAR deployment architecture	
4.SOAR use cases	
Use Case Examples	
Exercises	

Key Takeaways:

- SOAR drivers include the increased volume of threats, the need to reduce the time to respond, contain and remediate those threats, and the need to improve triage quality and speed.

- SOAR helps a Security Operation Center (SOC) qualify, investigate and remediate threats by utilizing standardized workflows and automation
- Benefits of using SOAR include enhanced intelligence quality, improved efficiency of operations and more rapid incident response times.
- The key components of SOAR are:
- Workflow and collaboration engine
- Care and ticket management system
- Orchestration and automation
- Threat intelligence management.

Unit 8 Module 2 - 5G Secured Networks wrap-up

Topic Names	Your Notes
Industrial Automation Networks: The Decision Framework	Instructions. Type your notes in here. Box will expand to accommodate your text. Note: Select and Delete this comment.
Introduction to the Decision Framework	
The decision framework stages	

Industry Acronyms

The following Industry relevant acronyms may be referenced during the course and on the certification exam. You should become familiar with these terms as the acronym may be used on the certification exam.

Acronym	Meaning
(5G) CN	(5G) Core Network
(5G) RAN	(5G) Radio Access Network
3GPP	3rd Generation Partnership Project - a Standards organization
5G	Fifth Generation (of Wireless Networks)
5G -AKA	5G Authentication and Key Agreement
5GLAN	5th Generation Local Area Network
AAA	Authentication, Authorization and Accounting
ABAC	Attribute Based Access Control
ACL	Access Control List
ACM	Audit and Compliance Management
AES	Advanced Encryption Standard (AES)
AF	Application Function
AI/ML	Artifical Intelligence/Machine Learning
AK	Anonymity Key

AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
ANSSI	Agence nationale de la sécurité des systèmes d'information (France IT Security Agency)
ANT	Antenna
AP	Access Point
APAC	Asia-Pacific
API	Application Programmable Interface
APT	Advanced Persistent Threat
APT	Advanced Persistent Threat
ARPF	Authentication Credential Repository and Processing Function
AS	Access Stratum
AUSF	Authentication Server Function
AUTN	Authentication Token
BIST	Built In Self Test
BTS	Base Transceiver Station
CA	Certification Authority
CaaS	Container as a Service
CAPIF	Common Application Programming Interface Framework
CBC	Cipher Block Chaining
CC	Common Criteria (for Information Technology Security Evaluation (ISO 15408))
CDC	Cyber Defense Center
CDMA	Code Division Multiple Access
CI/CD	Continuous Integration & Continuous Delivery
CI/CD2	Continuous Integration & Continuous Delivery & Continuous deployment
CIA	Confidentiality, Integrity, Availability
Ck	Ciphering Key
CLI	Command Line Interface
CN	Core Network
cNF	Consumer Network Function
CP	Control Plane
CPE	customer-premise equipment
CPU	Central Processing Unit
C-RNTI	Cell Radio Network Temporary Identifier
cSEPP	Consumer Security Edge Protection Proxy
CSP	Communication Service Provider
CU	Centralized Unit
CU-CP	Centralized Unit Control Plane
CUS Plane	Control, User , Synchronization Plane
CU-UP	Centralized Unit User Plane
CVSS	Common Vulnerability Scoring System
DAC	Discretionary Access Control
DB	DataBase
DC	Datacenter
DDos	Distributed Denial of Services
DevOps	Development and Operations
DevSecOps	Development, Security and Operations
DH	Diffie-Hellman

DHCP	Dynamic Host Configuration Protocol
DN	Data Networks
DNS	Domain Name System
DoS	Denial of Service
DPD	Dead Peer Detection
DRB	Dedicated Radio Bearer
DSP	Digital Service provider
DTLS	Datagram Transport Layer Security
DU	Distributed Unit
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol - Authentication and Key Agreement
ECC	Elliptic Curve Cryptography
ECIES	Elliptic Curve Integrated Encryption Scheme
eCPRI	Enhanced Common Public Radio Interface
ECU	Electronic Control Unit
EDR	Endpoint Detection and Response
eHRPD	Enhanced High Rate Packet Data
eMBB	Enhanced Mobile Broadband
EMEA	Europe Middle East and Africa
ENISA	European Network and Information Security Agency
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
ETSI	European Telecommunications Standards Institute
ETSI NFV-SEC	ETSI Network Functions Virtualisation - Security
FCC	Federal Communications Commission (US Agency)
FH-M Plane	Front Haul Management Plane
FTTH	Fiber to the Home
gNB	g-NodeB - the name of the New Radio 5G Base Station Transceiver
GSM	Global System for Mobile Communications, originally "Groupe Spécial Mobile"
GSMA	GSM Association - an industry organisation that represents the interests of mobile network operators worldwide
GUI	Graphical User Interface
GUTI	Global Unique Temporary Identifier
HCI	Hyperconverged infrastructure
HE	Home Environment
HN Priv Key	Home Network Private Key
HN Pub Key	Home Network Public Key
HPLMN	Home Public Land Mobile Network
HRES	Hashed Response
hSEPP	Home Network Security Edge Protection Proxy
HSM	Harware Security Module
HSM	hardware security module
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
HXRES	Hashed Expected Reponse
IAB	Integrated Access Backhaul
IAM	Identity Access Management
IAM	identity and access management

ICE	In-Car Entertainment
ICMP	Internet Control Message Protocol
ICT	Information and Computer Technology
ID Card	Identity Card
IEC	International Electrotechnical Commission
IETF RFCs	Internet Engineering Task Force Request for Comments
Ik	Integrity Key
IKE	Internet Key Exchange
IM	identity management
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IOC	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IPUPS	Inter-PLMN User Plane Security
IPX	IP based Exchange Network
IR	Incident response
ISO	International Organization for Standardization
IT	Information Technology
IT	intelligent Technology
ITU	International Telecommunication Union
JBOD	Just a Bunch Of Disks
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group (IEEE 1149.1)
KASUMI	Block cipher designed for 3GPP. Named after the original algorith MISTY1 - Kasumi is Japanese word for "mist"
KPI	Key Performance Indicator
LLS	Lower Layer Split
LTE	Long Term Evolution (name of the 4G System)
MAC	Message Authentication Code
MAC	Mandatory Access Control
MACSec	Medium Access Control Security (IEEE 802.1AE)
MANO	MANagement and Orchestration
ME	Mobile Equipment
MH	Mid-haul
MITRE ATT@CK	Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, from MITRE, an American not-for-profit organization
mMTC	Massive Machine-Type Communications
M-Plane	Management Plane
MRTI	Machine-Readable Threat Intelligence
MSA	Multi-Stage Attack
MTTD	Mean Time To Detect
MTTR	Mean Time To Respond
N3IWF	Non-3GPP Interworking Function
NAS	Non Access Stratum
NAT	Network Address Translation
NDS	Network Domain Security
NEA	NR Encryption Algorithm

Near-RT	Near Real Time
NEF	Network Exposure Function
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
NFV	Network Functions Virtualisation
NFV	Network Function Virtualization
NFVO	Network Function Virtualization Orchestration
NG-RAN	Next Generation Radio Access Network
NIA	NR Integrity Algorithm
NIST	National Institute of Standards and Technology (US agency)
NOC	Network Operations Center
Non-RT	Non Real-Time
NR	New Radio (the 5G new RAT)
NRF	Network Repository Function
NSSF	Network Slice Selection Function
NVD	National Vulnerability Database
Oauth	Open Authentication
O-DU	Open Distributed Unit
OEM	Original Equipment Manufacturer
ONAP	Open Network Automation Platform
O-RAN	Open Radio Access Network
O-RU	Open Radio Unit
OS	Operating System
OSI model	Open Systems Interconnection model
OT	Operational technology
PCF	Policy Control Function
PDCP	Packet Data Convergence Protocol
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PLMN	Public Land Mobile Network
pNF	Producer Network Function
PRINS	Protocol for N32 Interconnect Security
pSEPP	Producer Security Edge Protection Proxy
QoE	Quality of Experience
R&D	Reseach and Development
RA	Registration Authority
RAM	Random Access Memory
RAN	Radio Access Network
RAND	Random Challenge
RAT	Radio Access Technology
RBAC	Role-Based Access Control
RBAC	Role Based Access Control
RES	Response
RIC	Radio Access Network Intelligent Controller
ROI	Return On Investment
RRC	Radio Resource Control

RSA	Rivest–Shamir–Adleman - a public-key cryptosystem
RSS	Rich Site Summary or Really Simple Syndication
RU	Radio Unit
SA	Security Assurance
SA3 standard	3GPP Technical Specification Group Service and System Aspect Work Group 3
SAN	Storage Area Network
SANS	SysAdmin, Audit, Network, and Security
SBA	Service Based Architecture
SBI	Service Based Interface
SCAS	Security Assurance Specification
SDLC	Software Development Lifecycle
SDN	Software Defined Networking
SDN	Software-Defined Network
SEAF	Security Anchor Function
SECAG	GSMA Security Assurance Group
SEPM	Symantec Endpoint Protection Manager
SEPP	Security Edge Protection Proxy
SFTP	Secured File Transfer Protocol
SHA-1	Secure Hash Algorithm 1 - a cryptographic hash function
SIDF	Subscription Identity De-concealing Function
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIRP	Security Incident Response Platforms
SLA	Service Level Agreement
SMC	Security Management Center
SMF	Session Management Function
SMO	Service Management and Orchestration
SOA	Security Orchestration and Automation
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
SQN	Sequence Number
SRB	Signaling Radio Bearer
SRVCC	Single Radio Voice Call Continuity
SS7	Signaling System # 7
S-SDLC	Secure-Software Development LifeCycle
SSHv2	Secure Shell 2.0
SSO	Single Sign-On
S-TMSI	Short temporary Mobile Subscriber Identity
SUCI	Subscriber Concealed Identifier
SUPI	Subscriber Permanent Identifier
SVM	Security Vulnerability Management
SW	Software
TI	Threat Intelligence
TIP	Threat Intelligence Platform
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TNGF	Trusted non 3GPP Gateway Function

TPM	Trusted Platform Module
TPS	Time Packet Sensitive Switch
TR	Technical Report
TS	Technical Specification
TSG	Technical Specification Group
TSG SA	Technical Specification Group Service and System Aspects
UDM	Unified Data Management
UE	User Equipment
UEBA	User and Entity Behavior Analytics
UP	User Plane
UPF	User Plane Function
URL	Uniform Resource Locator
URLLC	Ultra-Reliable Low-Latency Communications
USIM	Universal Subscriber Identity Module
V2X	Vehicle to Everything
VA	Validation Authority
VIM	Virtualized Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
VPLMN	Visitor Public Land Mobile Network
VPN	Virtual Private Network
v-RAN	Virtualized Radio Access Network
vSEPP	Visitor Security Edge Protection Proxy
VXLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WEP	Wired Equivalent Privacy
WG	Working Group
WiFi	Wireless Fidelity
WPA	Wifi Protected Access
XMAC	Expected Message Authentication Code
XOR	Exclusive OR
XRES	Expected Response
ZTNA	Zero-trust network access
ZTS	Zero Touch Service

Document Control

JUL 28 2020 Version 1.0 – JRS