ENG-516 - Network Security Auditing

Description

This 5-day course is designed to provide a detailed understanding of the telecommunication network security audit processes and parameters, change management processes and how to minimize the risk of network breach. Candidates who attend this course should have a good understanding of general telecom fundamentals, knowledge of nodes in telecommunications, telecommunications connectivity and basics of operation.

Learning Outcomes

At the end of the course, participants will be able to:

- Understand and discuss network security compliance
- Explain the need for network security checks
- Identify security check parameters
- Characterize the processes needed to minimize the risk of network vulnerability
- Identify network change management processes
- Outline the requirements for end to end network security
- Discuss and design policy and permission methods
- Specify template reports, tests and KPIs for network security audits

Topics

The training course covers the following topics:**DAY 1**

Introduction

- Why security is particularly important for telecom operators
- Proper security starts with internal accountability
- Internal fraud
- Internal mistakes that can cost millions
- Objective of audit
- Scope of audit
- Different frameworks for auditing schemes – continuous monitoring vs point-in-time monitoring, incident reporting, preventive auditing vs post-incident investigations
- Mobile industry safety, privacy and security principles
    - Protecting consumers
    - Protecting consumer privacy
    - Protecting public safety
    - Protecting network security and device integrity
- *Case study: Ofcom guidance on security requirements*

Day 2

Technical background- Interconnection in mobile networks

- Network overview

    - Network architecture diagram
    - Internal & external connectivity
    - Server physical accessibility security
    - Terminal password and security management
    - User account management
    - Logout on timeout session
    - Prevention of unauthorized access
    - Remote login access and log capture
  - Interconnection security risks
    - 2G, 3G and SS7
    - External toll fraud in fixed networks, including with wholesale voice transit operations
    - External fraud in mobile networks
    - Roaming fraud
    - SS7 vulnerability risks and challenges
    - Famous SS7 exploitations and impacts
    - 4G and evolution to Diameter

Protection of critical service provider infrastructure

  - Security controls for core equipment
  - Security testing
- *Case study: Security best practices for Canadian telecommunications service providers*

DAY 3

Interconnect security implications for mobile services

- Security
  - Location and tracking of mobile users
  - Eavesdropping via ‘man in the middle' attack - 2G and 3G
  - Traffic diversion
  - De-anonymization (disclosure of IMSI)
  - Spam
- Denial of service
  - Overloading a network node
  - Disconnect customers
  - Send malformed messages
-

Fraud

  - Avoid service charges
  - Resell service (e.g. SMS termination)
  - Impersonate a customer

- Protecting consumers
  - Children and vulnerable individuals
  - Stolen and counterfeit devices
  - Fraud on mobile devices

- Protecting consumer privacy
  - Data collection and usage
  - Consumer choice
  - Cross border transfer of personal data

- Protecting public safety
  - Law enforcement assistance requests
  -

- Service restriction orders and signal inhibitors
- Mandatory prepaid sim card registration

- Protecting network security and device integrity
  - Network security
  - Mobile device integrity
  - Futuristic networks: IOT/Blockchain/5G
- *Workshop: Specifying tests for auditing security measures*

DAY 4

Network security monitoring and detection capabilities

- Requirements for Telecommunications Service Providers' (TSPs) to monitor Network infrastructure
- Types of traffic to monitor
- Subscriber management
  - System data backup management
  - CDR backup management
  - Network authentication & encryption
  - Data integrity and subscriber data security

    - Parameters & configuration backup
    - NTP synchronization monitoring

- Privacy

Security incident response capabilities

- Telecommunications Service Providers' (TSPs) incident response capabilities
- Response procedures for issues affecting customers
- Remediation and mitigation of malicious or inappropriate traffic

Information sharing and reporting

- Sharing of information for telecommunications critical infrastructure protection
- Establishment of mechanisms for information-sharing

Change management

- Change management processes
- Change request execution and method of procedures validation
- Network daily activity monitoring
- Activity and command logs storage

- *Workshops: Specifying test result standards and KPIs – best practices*

- *Workshop: Specifying response and report processes for security incidents*

Day 5

Vendor management

- Equipment supply chain
- Vendor security management
    - Software & patches with release version
    - Antivirus security updates
    - End points security checks
    - System log monitoring
    - Third party software
    - Firewall and IP security audit

Validation

- Unsecured website
- Connected lost device
- Unused configuration & clean up audit
- Audit report validation
- *Examples of schemes and certifications for auditing security measures*

- *Workshops: Developing template reports to be submitted to the Regulator on security measures and statistics*

Target Audience

- Regulatory Authority Technical Staff, Network Engineers, Network Operation Experts

Methodology

A combination of engaging activities and dynamic presentations to stimulate and maximize participants' learning.

- Dynamic and interactive presentations
- Covering key concepts in a concise manner

- Presentation of a given situation
- Analysis
- Recommendations & course of action

- Real-life examples illustrating key concepts
- Focusing on recent events

- Individual and group work to practice using the tools acquired during the course

- Discussions about on-the-job situations faced by participants
- Sharing of experiences

Location

A selection of Neotelis' training courses is held in various cities around the world. Please contact us at training@neotelis.com for the complete Yearly Training Calendar.

Neotelis can also deliver in-house sessions of this course specifically for your organization. Please contact us at training@neotelis.com for more information and a Proposal.

About Neotelis

Neotelis provides training, consulting, conferences and publications to the telecommunications industry worldwide. Its team of senior experts has trained thousands of executives and managers working for operators, regulators, policy-makers and governments in over 120 countries around the world.

... Telecom Leaders Use Neotelis. Don’t Get Left Behind! ...

URCA
airtel
MTN
everywhere you go
TM
zain
ICASA
ooredoo
ARTP
Spectrum Management Authority
Digicel
هيئة الاتصالات وتقنية المعلومات
Communication and Information Technology Commission
STC
LIME
هيئة تنظيم الاتصالات
Telecommunications Regulatory Authority
tigo
vodacom
vodafone
ANRT
Telecommunications Authority of Trinidad and Tobago
اتصالات
etisalat
orange
Bell

4802 de Verdun St, Office #1, Montreal, QC, H4G 1N1 Canada
Tel: +1 514 281 1211 Fax: +1 514 281 2005
info@neotelis.com