Network Security Specialist to CloudOps Security Architect

SKILLSOFT ASPIRE JOURNEY

skillsoft

Głównym wyzwaniem przed którym stają dziś organizacje na całym świecie jest konieczność ciągłego podnoszenia umiejętności i poziomu wiedzy w ślad za gwałtownym rozwojem nowych technologii i zmian na globalnym rynku.

Stały rozwój i podnoszenie kwalifikacji w IT od dawna jest już rzeczą oczywistą, a możliwość zapewnienia wsparcia specjalistom chcącym stale się rozwijać jest jedną z głównych kart przetargowych w walce o pracownika.

Na rynku liczą się dziś ludzie, którzy posiadają konkretne kompetencje i zestaw umiejętności pozwalający im wykonywać zadania efektywnie, a nie Ci z najdłuższym stażem pracy.

Dziś, bardziej niż kiedykolwiek w cenie jest umiejętność budowania ścieżki kariery dla profesjonalistów IT, którzy wciąż chcą się liczyć na rynku pracy.

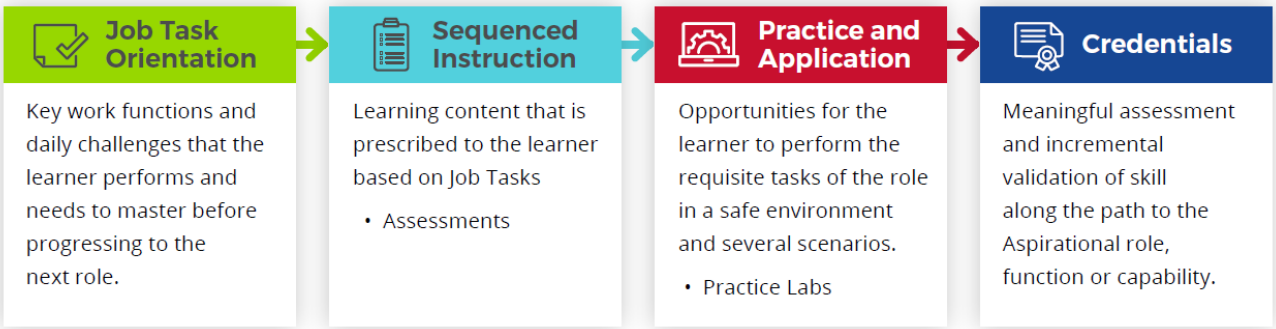
Skillsoft Aspire Journey stanowi odpowiedź na pytanie, jakie szkolenia muszę ukończyć, aby być przygotowanym do mojej wymarzonej pracy. Spośród kilkuset kanałów tematycznych dostępnych na naszej platformie szkoleniowej nasi specjaliści wybrali te, które naszym zdaniem najlepiej wyposażą uczących się w narzędzia potrzebne do realizacji zadań w nowej roli.

Skillsoft Aspire Journey to zestawy szkoleń i ćwiczeń w języku angielskim, które metodycznie, krok po kroku pozwalają specjalistom przejść od poziomu podstawowego do zaawansowanego.

Każda ścieżka zawiera szkolenia, laboratoria wirtualne, video i książki, które pomogą uczącym się osiągnąć pożądane kompetencje poświadczone certyfikatem.

Aspire Journey Model

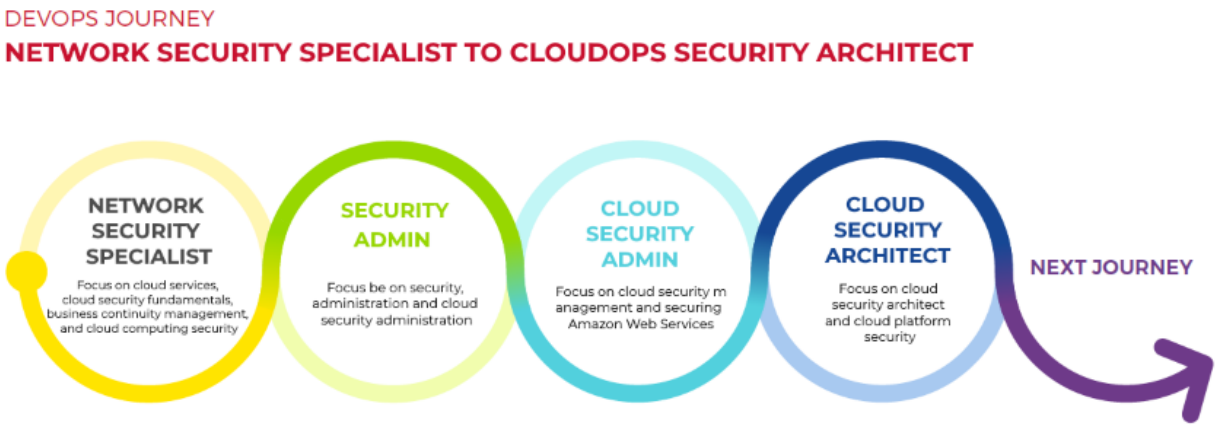
Cała ścieżka opiera się na 4-elementowym cyklu powtarzanym na kolejnych etapach nauki.



1. Określenie kluczowych funkcji i wyzwań, z którymi musi poradzić sobie uczący się w chwili obecnej, jak i tymi, z którymi przyjdzie mu się zmierzyć w nowej pracy.
2. Przejście zaprojektowanych ścieżek w proponowanej kolejności, wykonanie ćwiczeń i zaliczenie testów.
3. Przećwiczenie nowych umiejętności w kontrolowanym środowisku w oparciu o gotowe scenariusze działań. Laboratoria wirtualne Skillsoft
4. Certyfikat – zaliczenie testu końcowego na poziomie co najmniej 70% i uzyskanie certyfikatu potwierdzającego ukończenie danego etapu nauki.

Aspire Journey – Network Security Specialist to CloudOps Security Architect

Analizując trendy opisujące zachowanie użytkowników na naszych platformach szkoleniowych i współpracując ściśle z naszymi klientami na całym świecie Skillsoft wyselekcjonował najlepsze materiały szkoleniowe i ułożył je w ustrukturalizowaną ścieżkę rozwoju. Ścieżka zawiera niemal 23 godziny szkoleniowe materiałów.



11 courses
8h 34m 43s

- Cloud services
- Cloud security fundamentals
- Business continuity management,
- Cloud computing security

6 courses
5h 52m 10s

- Security administration
- Cloud security administration.

7 courses
5h 15m 22s

- Cloud security management
- Securing Amazon Web Services

3 courses
2h 24m 37s

- Cloud security architect
- Cloud platform security

DEVOPS JOURNEY

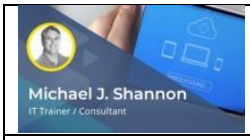
NETWORK SECURITY SPECIALIST TO CLOUDOPS SECURITY ARCHITECT

Track 1: Network Security Specialist (duration: 8h 34m 43s)

 Cloud Services: Cloud Computing Concepts	 Cloud Security Fundamentals: Basics of Cloud Operations
Objectives: ▪ specify cloud benefits, components, and service models ▪ differentiate between cloud computing roles such as cloud service customer, cloud service architect, and cloud auditor ▪ differentiate between on-premise and cloud implementations ▪ provide an overview of the IaaS cloud service model ▪ describe the SaaS cloud service model ▪ describe considerations when using the PaaS cloud service model ▪ list benefits and potential pitfalls for private cloud implementation ▪ recognize advantages and disadvantages of using a public cloud ▪ describe the benefits of using a hybrid cloud solution ▪ list the benefits and potential pitfalls of using a community cloud ▪ list potential risks and benefits of migrating to the cloud ▪ describe common cloud vulnerabilities such as negligence, cyber threats, and system vulnerabilities	Objectives: ▪ describe cloud computing definitions and roles ▪ describe key cloud characteristics ▪ describe virtualization technologies ▪ describe compute technologies ▪ describe storage technologies ▪ describe networking technologies ▪ describe database technologies ▪ compare public CSP product offerings ▪ describe cloud computing technologies and concepts

 Cloud Security Fundamentals: Architectural & Design	 Cloud Security Fundamentals: Cloud Infrastructure Security
Objectives: ▪ describe the three-tier design model ▪ define shared responsibility ▪ perform cost-benefit analysis for the cloud service provider (CSP) ▪ describe common development lifecycles ▪ define the basics of risk management ▪ describe common deployment and migration strategies ▪ describe the CSA cloud data lifecycle ▪ define the basics of storage management lifecycles ▪ describe cloud architecture concepts	Objectives: ▪ design and plan security controls ▪ secure the root account ▪ configure IAM groups and users ▪ describe IAM policies and permissions ▪ define IAM roles ▪ secure management access ▪ define network access control lists ▪ configure stateful firewalls in the cloud ▪ describe web application firewalls ▪ describe best practices for hardening VMs ▪ describe cloud infrastructure security

 Cloud Security Fundamentals: Cloud Data Security	 Cloud Security Fundamentals: Cloud Application Security
Objectives: ▪ describe cryptographic mechanisms ▪ describe common cryptographic protocols ▪ compare client and server-side encryption ▪ define file and database security ▪ define object storage security ▪ classify key management services ▪ define public key infrastructure ▪ describe hardware security modules ▪ describe cloud data security	Objectives: ▪ define training and awareness security ▪ describe software assurance and validation ▪ use verified secure software ▪ apply the secure software development lifecycle ▪ compare cloud application architectures ▪ describe federation and SSO solutions ▪ compare advanced cloud security products ▪ list methods of creating security awareness, methods for enhancing application security in the cloud, and the steps of successful software validation



Cloud Security Fundamentals: Legal & Compliance

Objectives:

- manage compliance with regulations and controls
- describe legal requirements and risks
- define privacy issues and jurisdiction
- use audit processes and methodologies in the cloud
- describe outsourcing issues and contract design
- survey common regulations and mandates
- describe legal and compliance issues in the cloud

Business Continuity: Cloud Integration

Objectives:

- describe the six key stages in the data lifecycle - Create, Store, Use, Share, Archive, and Destroy
- recognize key access control considerations
- list network security concepts such data and media sanitization
- list virtualization security concepts such as hypervisor and container security
- list potential threats against cloud computing infrastructure
- describe considerations when evaluating cloud service providers
- list common cloud infrastructure components such as network, virtualization, and computer
- recognize how to analyze cloud risks
- list data security strategies such as encryption and key management
- list data discovery techniques
- describe data rights management
- describe information rights management

Business Continuity: Secure Cloud Computing

Objectives:

- list requirements for business continuity strategy
- recognize requirements for disaster recovery strategy
- recognize considerations when moving applications to the cloud
- differentiate between data ownership and data custody
- describe key legal considerations when moving to the cloud
- list the importance of performing a cost-benefit analysis
- recognize factors that can impact confidentiality, integrity, and availability of cloud data
- describe the benefits of cloud offerings such as AWS and Azure
- list functional security requirements such as portability, interoperability, and vendor lock-in
- design and plan security controls including on-premise physical controls, virtualization protection, and authorization
- describe the importance of retention policies and archiving procedures
- list considerations that relate to traceability and accountability such as logging, event sources, and chain of custody

Cloud Management

Objectives:

- recognize challenges of cloud service such as IaaS, PaaS, SaaS
- describe challenges introduced by different types of cloud platforms such as public, private, hybrid, and community
- recognize considerations related to cloud management
- list specifics about cloud application architecture such as supplementary security components, cryptography, and sandboxing
- list IAM solutions such as Federated Identity, single sign-on, and multifactor authentication
- differentiate between physical and logical infrastructure for cloud operations
- recognize how to implement operational controls and standards
- ensure compliance with regulations and controls, like ITIL and ISO/IEC 20000-1
- recognize different privacy concerns such as private data and jurisdictional concerns
- describe audit processes and methodologies
- recognize the importance of SLAs
- describe vendor management considerations such as supply chain risk

Final Exam: Network Security Specialist

Objectives:

- apply the secure software development lifecycle
- classify key management services
- compare client and server-side encryption
- configure stateful firewalls in the cloud
- define file and database security
- define IAM roles
- define object storage security
- define privacy issues and jurisdiction
- define shared responsibility
- define the basics of risk management
- define training and awareness security
- describe challenges introduced by different types of cloud platforms such as public, private, hybrid, and community
- describe cloud computing definitions and roles
- describe common cloud vulnerabilities such as negligence, cyber threats, and system vulnerabilities
- describe common cryptographic protocols
- describe common development lifecycles
- describe compute technologies
- describe considerations when evaluating cloud service providers
- describe considerations when using the PaaS cloud service model
- describe key cloud characteristics
- describe key legal considerations when moving to the cloud
- describe legal requirements and risks
- describe software assurance and validation
- describe storage technologies
- describe the benefits of cloud offerings such as AWS and Azure
- describe the common deployment and migration strategies
- describe the SaaS cloud service model
- describe the six key stages in the data lifecycle - Create, Store, Use, Share, Archive, and Destroy
- describe the three-tier design model
- describe virtualization technologies
- describe web application firewalls
- design and plan security controls
- differentiate between cloud computing roles such as cloud service customer, cloud service architect, and cloud auditor
- differentiate between data ownership and data custody
- differentiate between on-premise and cloud implementations
- differentiate between physical and logical infrastructure for cloud operations
- ensure compliance with regulations and controls, like ITIL and ISO/IEC 20000-1
- list common clouds infrastructure components such as network, virtualization, and computer
- list data security strategies such as encryption and key management
- list network security concepts such data and media sanitization
- list potential threats against cloud computing infrastructure
- list requirements for business continuity strategy
- list specifics about cloud application architecture such as supplementary security components, cryptography, and sandboxing
- list the importance of performing a cost-benefit analysis
- list virtualization security concepts such as hypervisor and container security
- manage compliance with regulations and controls
- provide an overview of the IaaS cloud service model
- recognize challenges of cloud service such as IaaS, PaaS, SaaS
- recognize considerations related to cloud management
- recognize considerations when moving applications to the cloud
- recognize different privacy concerns such as private data and jurisdictional concerns
- recognize factors that can impact confidentiality, integrity, and availability of cloud data
- recognize how to implement operational controls and standards
- recognize key access control considerations
- recognize requirements for disaster recovery strategy
- secure management access
- secure the root account
- specify cloud benefits, components, and service models
- use audit processes and methodologies in the cloud
- use verified secure software

DEVOPS JOURNEY

NETWORK SECURITY SPECIALIST TO CLOUDOPS SECURITY ARCHITECT

Track 2: Security Admin (duration: 5h 52m 10s)

 Cloud Security Administration: Introduction	 Cloud Security Administration: Cloud Data & Application Security
Objectives: ▪ describe cloud administration and management ▪ describe security base parameters and recall what creates baselines ▪ describe the service stack of cloud operation as it maps to customer business requirements ▪ recognize the core architecture of cloud and its importance for data security ▪ describe cloud under compliance and the need to comply with the attesting bodies ▪ recognize the concepts of data handling, hardware, software and breach planning, and secure environment ▪ describe audit and compliance keeping services stacks in mind ▪ define integration of security services as a service or offering ▪ identify the building blocks of designing security plans and infrastructure development	Objectives: ▪ work with shared services and data protection ▪ perform fine-grained queries to get selective access control ▪ use secure deployment practices to develop and secure cloud applications ▪ describe identity access control including details on authentication and authorization ▪ identify actions of IAM in AWS and Azure ▪ describe the software development life cycle and issues ▪ recognize the importance of encryption and key management ▪ describe how to secure SAAS cloud by focusing on SAAS applications ▪ create a business continuity plan and work on its implementation ▪ identify various techniques including crypto, tokenization, data masking, and dip ▪ describe DRM, different data protection policies, event handing, and SIEM

 Cloud Security Administration: Hardened Cloud Security	 Cloud Security Administration: Continuous Operational Improvement
Objectives: ▪ describe how to harden physical hosts and help reduce the attack surface by using a virtual guest ▪ identify the importance of control over physical security and assets ▪ define data outsourcing and how to prevent loss of control on data ▪ specify how to provide cloud security while keeping track of limitations including vulnerability of infrastructure, platform, and service ▪ define deceptive information and how to protect data ▪ recognize the importance of encrypted queries and protecting personal data ▪ differentiate between privacy and information systems ▪ describe the life cycle of securing data in cloud	Objectives: ▪ identify various design concepts including logical and physical design ▪ recognize best practices for servers, storage networks, and virtual switches ▪ describe how to secure network operations including network isolation, VLANs, TLS, DNS, and IPsec ▪ list the key features of dynamic clusters, storage maintenance, and HA on cloud ▪ define patch management, performance monitoring, and backup ▪ describe the need for patch management and the process involved ▪ describe information security and how to manage operations ▪ describe the risk management process in logical and physical infrastructures ▪ list best practices for communicating with vendors, partners, and customers

Cloud Security Administration: Regulatory Conformance

Objectives:

- list common legislation conflicts and compliance issues
- describe data protection guidelines including ISO/IEC 27015:2015, 27002, and EU data protection
- recognize the e-Discovery process
- describe internal and external audits and identify various types of audits and audit scope
- describe standards, such as internal ISMS and ISO 27001:2013
- identify the purpose, types, and common components of service level agreements
- define risk profile, appetite, and risk management
- recognize concepts relating to contract management and its key components
- describe supply chain risk, CSA CCM, and ISO 28000:2007

Final Exam: Security Admin

Objectives:

- apply BCDR planning in various scenarios
- categorize different types of web services including CAAS, IAAS, MAAS, PAAS, and SAAS
- classify different types of web services including CAAS, IAAS, MAAS, PAAS, and SAAS
- compare the privacy and information systems
- create a maintenance plan using orchestration units
- create business continuity plan and work on its implementation
- define data outsourcing and how to prevent loss of control on data
- define deceptive information and how to protect data
- define internal and external audit and identify various types of audits and audit scope
- define patch management, performance monitoring, and backup
- define risk profile, appetite, and risk management
- define the integration of security services as a service or offering
- describe audit and compliance keeping services stacks in mind
- describe cloud administration and management
- describe cloud under compliance and the need to comply with the attesting bodies
- describe deceptive information and how to protect data
- describe DRM, different data protection policies, and event handing including SIEM
- describe how security policy implementation mitigates cloud security challenges
- describe how to secure network operations including network isolation, clans, TLS, DNS, and IPSec
- describe how to secure SAAS cloud by focusing on SAAS applications
- describe identity access control including details on authentication and authorization
- Describe information security and how to manage operations
- describe security base parameters and recall what creates baselines
- describe supply chain risk, CSA CCM, ISO 28000:2007
- describe the business high availability and continuity techniques
- describe the data protection guidelines including ISO/IEC 27015:2015, 27002, and EU data protection
- describe the evolution of cloud including hardware, software, and server virtualization
- describe the importance of encryption in and out of cloud
- describe the life cycle of securing data in the cloud
- describe the risk management process in logical and physical infrastructures
- describe the software development life cycle and issues
- describe the standards, such as Internal ISMS, ISO 27001:2013
- develop a maintenance plan using orchestration units
- Identify cloud model types and their approach towards adopting the model

- identify cloud software security measures including security principles and testing
- identify common stake holders and governance challenges and how to coordinate communication with them
- identify the building blocks of security planning designing and Infrastructure development
- identify the different service provider risks including back door spoofing
- identify the importance if open-source in cloud infrastructure
- identify the importance of control over physical security and assets
- identify the software development life cycle and issues
- identify various design concepts including logical and physical design
- identify various techniques including Crypto, tokenization, data masking, and dip
- issue excellent grain queries to get selective access control
- list the best practices for servers, storage network, and virtual switches
- list the best practices to communicate with vendors, partners, and customers
- list the common legislation conflicts and compliance issues
- list the importance of encryption and key management
- list the key features of dynamic clusters, storage maintenance, and HA on cloud
- perform excellent grain queries to get selective access control
- recall the importance of control over physical security and assets
- recognize the concepts of data handling, hardware, software and breach planning, and secure environment
- recognize the concepts relates to contract management and its key components
- recognize the core architecture of cloud and importance to data security
- recognize the e-discovery process
- recognize the importance of control over physical security and assets
- recognize the risks and threats involved in cloud computing and their analysis
- specify how to provide security on cloud keeping track of limitations including vulnerability of infrastructure, platform, and service
- specify the need for cloud datacenter
- use secure deployment practices to develop and secure cloud application

DEVOPS JOURNEY

NETWORK SECURITY SPECIALIST TO CLOUDOPS SECURITY ARCHITECT

Track 3: Cloud Security Admin (duration: 5h 15m 22s)

 Cloud Security Management: Architecture Security	 Cloud Security Management: Operations Security
Objectives: ▪ recall the steps to plan cloud security management ▪ recognize cloud computing definitions ▪ classify various cloud deployment models ▪ describe the different cloud transition scenarios and functions ▪ recognize how to secure the perimeter using key technologies ▪ define IAM and identify the importance of access control ▪ identify common threats in cloud ▪ match different models with security considerations ▪ describe the security data life cycle ▪ define business continuity and DR planning including high availability and disaster recovery	Objectives: ▪ describe the importance of design in security operations ▪ list enterprise operation best practices ▪ configure security networks in the workplace ▪ describe how dynamic operations in the cloud work ▪ identify the importance of patch management operations ▪ define performance monitoring ▪ define operations management ▪ specify how business continuity management is planned ▪ describe how digital evidence operations function ▪ identify how to communicate with stakeholders

Cloud Security Management: Data Security

Objectives:

- describe the fundamentals of data security
- recognize the dynamics of data and data controls
- recognize technologies used in secure data management
- recognize how data is classified and mechanisms for managing data classification
- recognize the importance of privacy and various data privacy acts
- recognize DRM and its importance in corporate scenarios
- use AWS key management services
- recognize the importance of events and their relationship with data

Cloud Security Management: Risk Management

Objectives:

- identify potential cloud risks
- describe risk from the perspective of the physical site and environment
- list the risks involved in software-defined datacenters
- describe risk audit mechanisms
- describe business continuity and disaster recovery
- identify the potential risks undertaken in BCDR
- create a BCDR plan

Cloud Security Management: Platform & Infrastructure Security

Objectives:

- describe network functionality and technologies
- list the key regulations used to protect datacenter facilities
- define identification, authentication, and authorization for resources
- recognize the different types of storage in AWS
- describe countermeasure strategies including uptime automation of controls and access controls
- define configuration and data life cycle automation

Cloud Security Management: Legal & Compliance

Objectives:

- define the ISO/IEC 27017:2015 security techniques and code of practice
- specify how e-Discovery provides legal controls to cloud service providers
- list different types of audits and impact of requirement programs
- describe the ISO/IEC 27018 standard
- identify the impact of clear communication and governance on process and activities
- describe the implications of risk profile and the difference between data owner and controller, keeping in mind the cloud paradigm
- identify common criteria assurance frameworks, CSA STAR, and contract management

Securing AWS: Fundamentals

Objectives:

- describe the AWS Shared Responsibility Model
- recognize the CIA triad
- describe control types and categories
- identify core AWS services
- specify common threats to AWS
- describe AWS compliance services
- describe the Shared Responsibility Model, security services and controls, core AWS services and threats, and AWS compliance

Securing AWS: Identity & Access Management

Objectives:

- describe root account security
- compare credentials, passwords, and access keys
- configure the AWS CLI
- describe how a bastion host is used
- configure the AWS Identity and Access Management (IAM) service
- define IAM managed policies
- describe root account security, credentials, AWS CLI, bastions, and AWS Identity and Access Management (IAM)

Securing AWS: Infrastructure Security

Objectives:

- design a secure virtual private cloud
- configure network ACLs
- configure security groups for Linux instances
- configure security groups for Windows instances
- describe AWS WAF
- describe AWS Shield and AWS Inspector
- define AWS GuardDuty
- configure a managed site-to-site VPN
- define AWS SSO and AWS Cognito
- describe secure VPC design, NACLs, security groups, AWS WAF, AWS Shield and Inspector, Site-to-Site VPN, AWS SSO, and AWS Cognito

Securing AWS: Data Protection

Objectives:

- describe AWS cryptography basics
- configure access keys and key pairs
- compare client-side and server-side encryption
- describe AWS KMS
- describe AWS Certificate Manager
- define CloudHSM
- list attributes of cryptographic hashing, options for encrypting an S3 bucket object, and security services provided by digital signatures

Final Exam: Cloud Security Admin

Objectives:

classify various cloud deployment models
compare client-side and server-side encryption
compare credentials, passwords, and access keys
configure access keys and key pairs
configure network ACLs
configure security groups for Linux instances
configure the AWS CLI
configure the AWS Identity and Access Management (IAM) service
create a BCDR plan
define AWS GuardDuty
define AWS SSO and AWS Cognito
define IAM and identify the importance of access control
define identification, authentication, and authorization for resources
define international standards like ISO/IEC 17788
define operations management
define performance monitoring
define the ISO/IEC 27017:2015 security techniques and code of practice
describe AWS Certificate Manager
describe AWS cryptography basics
describe AWS KMS
describe AWS Shield and AWS Inspector
describe AWS WAF
describe business continuity and disaster recovery
describe control types and categories
describe countermeasure strategies including uptime automation of controls and access controls
describe different cloud transition scenarios of functions
describe how a bastion host is used
describe how digital evidence operations functions
describe how dynamic operations in cloud work
describe ISO/IEC 27018 standard
describe root account security
describe the AWS Shared Responsibility Model
describe the importance of design in security operations
describe the risk in the perspective of the physical site and environment
describe the security data life cycle
design a secure virtual private cloud
Different technologies to secure data management
identify core AWS services
identify network functionality and technologies including SDN
identify the common threats in the cloud
identify the impact of clear communication and governance on process and activities
identify the importance of patch management operations
identify the potential risks in cloud
Importance of Privacy and different acts
Introduction to Data Security
list different types of audits and impact of requirement programs
list the best practices of enterprise operations
list the key regulations required to protect data center facilities
list the risks involved in a software-defined datacenter
match different models with security considerations
name different risk audit mechanisms
recognize how to secure the perimeter using key technologies
recognize the CIA triad
recognize the different concepts related to object storage and management plane
specify common threats to AWS
specify how business continuity management is planned
specify how e-discovery provided legal controls to the cloud service provider
Understand different Data policies and managing those policies
Understand DRM and its importance in the corporate scenario
Understand the classification of data and mechanisms to manage those

DEVOPS JOURNEY

NETWORK SECURITY SPECIALIST TO CLOUDOPS SECURITY ARCHITECT

Track 4: Cloud Security Architect (duration: 2h 24m 37s)

 Cloud Platform Security: Designing Secure Access	 Cloud Platform Security: Infrastructure Protection
Objectives: ▪ define IAM methodologies for the cloud ▪ list the groups and permissions in GCP/Azure ▪ describe access and segregation of access using roles ▪ describe how IAM works on Azure ▪ use Azure Active Directory to perform configurations ▪ describe the process of configuring IAM in Azure ▪ identify the zones and regions specific to AWS and GCP ▪ describe functions of VPC ▪ recognize the services used by VPCs including PrivateLink, secure endpoints, and Direct Connect ▪ configure VPC on AWS ▪ identify the service controls in GCP ▪ configure secure VPC in GCP ▪ describe security groups and subnet concepts in Azure ▪ apply and configure NSGs in VNets	Objectives: ▪ identify how to secure your cloud deployments ▪ describe functions of Azure Advisor ▪ specify the security levels of cloud infrastructure ▪ identify ways how to secure content using cloud infrastructure ▪ describe the process that Google uses to setup their security using cloud infrastructure ▪ list methods for implementing ACLs in GCP and AWS ▪ use ACLs to provide custom access ▪ identify how to secure cloud storage using ACL in GCP ▪ describe the applications of ACL in Azure ▪ list the ways to control the access on cloud infrastructure network ▪ use hardware encryption to secure hardware data ▪ configure the Hardware Security Module in Azure ▪ apply the cloud Hardware Security Module in GCP ▪ distinguish between KMS and cryptographic keys ▪ describe Azure Key Vault ▪ identify the features of Cloud KMS and describe how the cloud-hosted key management service lets you manage cryptographic keys for your cloud services

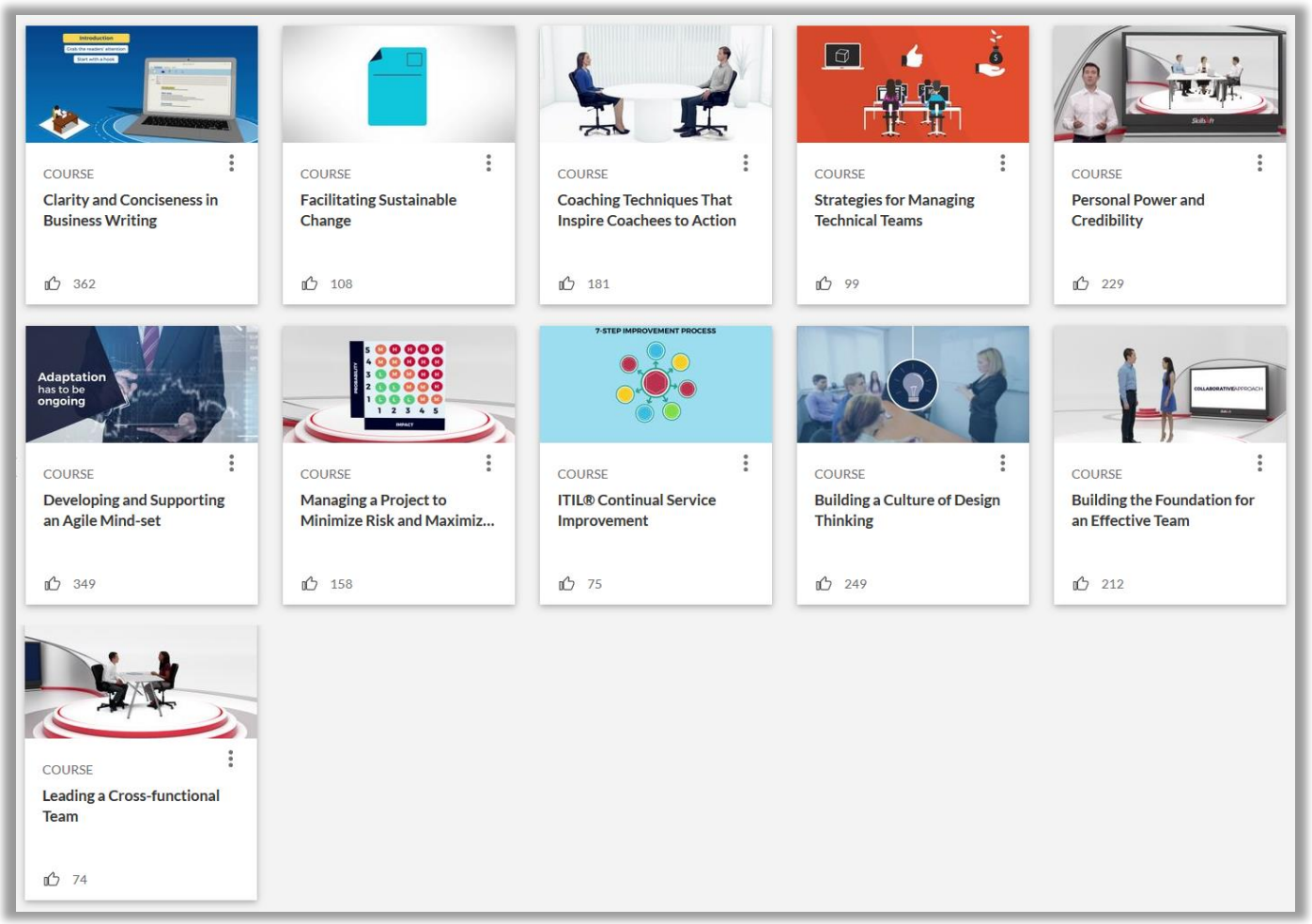
 Cloud Platform Security: System Monitoring & Protection	 Cloud Platform Security: Platform & Infrastructure
Objectives: ▪ describe how monitoring works in a cloud infrastructure ▪ identify how to protect data, apps, and infrastructure quickly with built-in security services in Azure ▪ recognize ways to perform monitoring in GCP ▪ recognize cloud infrastructure security flaws ▪ identify the common risks in security infrastructure ▪ list common techniques for tackling threats ▪ list Azure cloud tools ▪ describe how to protect your services against denial of service and web attacks ▪ use Google Cloud Security Scanner you automatically scan App Engine, Compute Engine, and Google Kubernetes Engine apps for common vulnerabilities ▪ describe how the VM placement algorithm works ▪ describe how to implement threat prevention mechanisms using VM placement algorithm	Objectives: ▪ describe network functionality and technologies including SDN ▪ list the key regulations used to protect datacenter facilities ▪ define identification, authentication, and authorization for resources ▪ recognize different concepts related to object storage and management plans ▪ describe countermeasure strategies including uptime automation of controls and access controls ▪ define configuration and data life cycle automation

Final Exam: Cloud Security Architect

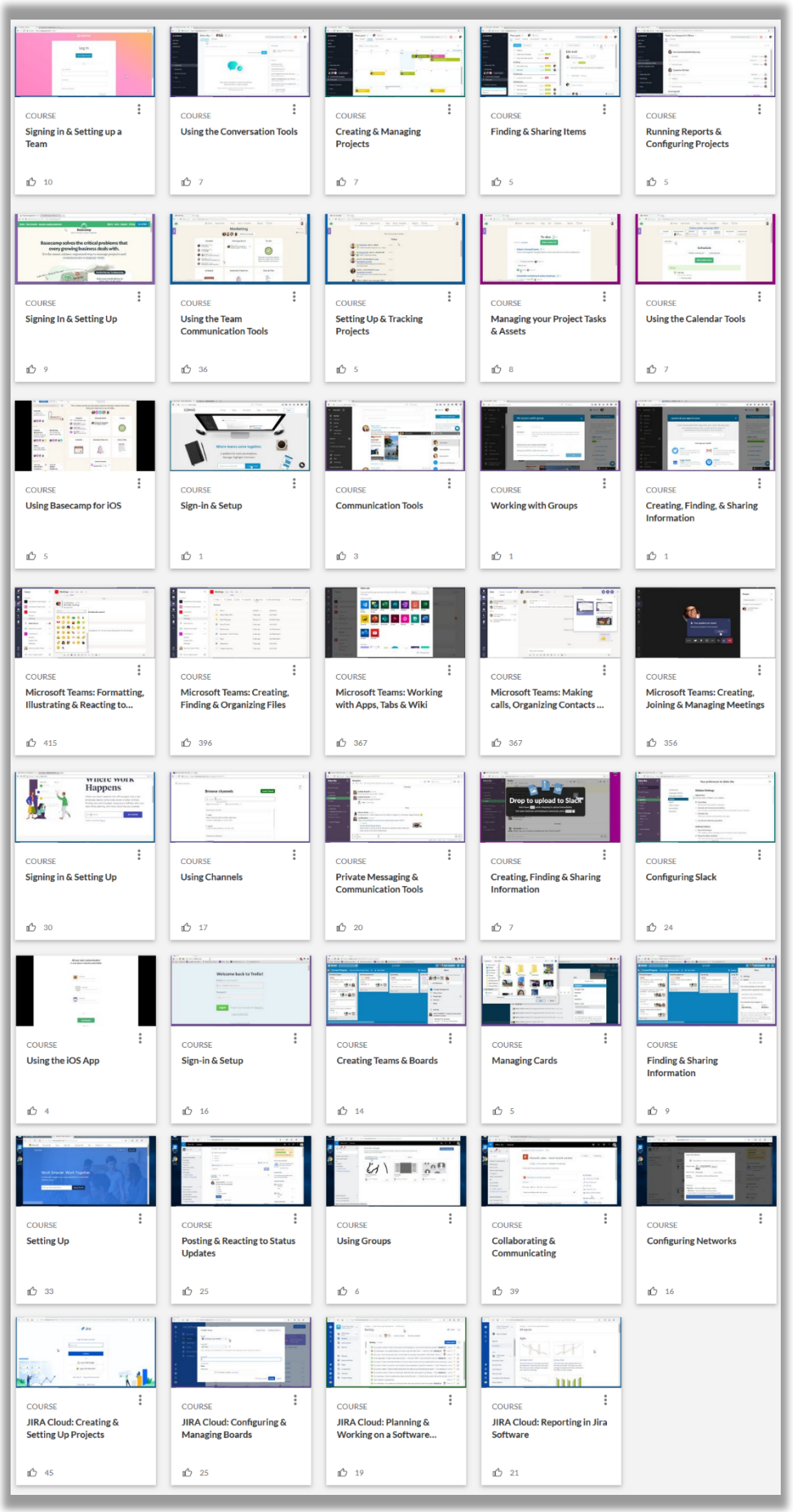
Objectives:

apply and configure NSGs in VNets
apply cloud hardware security module in GCP
configure hardware security module in Azure
configure secure VPC in GCP
configure VPC on AWS
define IAM methodologies in cloud
define security groups and subnet concepts in Azure
define the rules and standards with respect to the cloud security provider
describe Azure Key Vaults
describe functions of VPC
describe how does monitoring work in a cloud infrastructure
describe how IAM works on Azure
describe how to recover data using ASR
describe how to recover data using CDM
describe how VM Placement Algorithm works
describe responsibility model to achieve the compliance
describe the applications of ACL in Azure
describe the functions of the advisor tool
describe the methodology to implement preventing mechanism using VM replacement algorithm
describe the policies and ways to meet compliance
describe the process of configuring IAM in Azure
describe the process that Google uses to setup their security using cloud infrastructure
describe the ways to react to vulnerabilities in Azure
describe the ways to react to vulnerabilities in GCP
describe why due diligence is required to complete the audits successfully
distinguish between KMS and Cryptographic Key
identify how to secure cloud storage using ACL in GCP
identify how to secure your cloud deployments
identify responsibility model to achieve the compliance
identify the common risks in security infrastructure
identify the features of GCP cloud in GCP
identify the service controls in GCP
identify the specific tools within Google cloud
identify the ways on how to prevent vulnerabilities in Azure proactively
identify the ways on how to prevent vulnerabilities in GCP proactively
identify the ways to react to vulnerabilities in GCP
Identify the zones and regions specific to AWS and GCP
identify ways how to secure content using cloud infrastructure
identify ways to perform monitoring in GCP
list the common techniques around tackling threats
list the groups and permissions in GCP/Azure
list the methods to implement ACLs in GCP and AWS
list the specific tools within Azure cloud
list the specific tools within Google cloud
list the various methods to detect vulnerabilities in Azure
list the ways to control the access on cloud infrastructure network
recall how to recover data using CDM
recall the service used by VPCs including Private Link, secure endpoints, and Direct Connect
recall understanding the built SIEM system in Azure
recognize how to recover data using CDM
recognize the features of responsibility model in Azure
recognize the methodology to implement preventing mechanism using VM replacement algorithm
recognize the security flaws within a cloud infrastructure
recognize the ways to react to vulnerabilities in GCP
recognize why due diligence is required to complete the audits successfully
specify access and segregation of the access by roles
specify the security levels of cloud infrastructure
use ACLs to provide custom access
use Azure active directory to perform configurations
use hardware encryption to secure hardware data

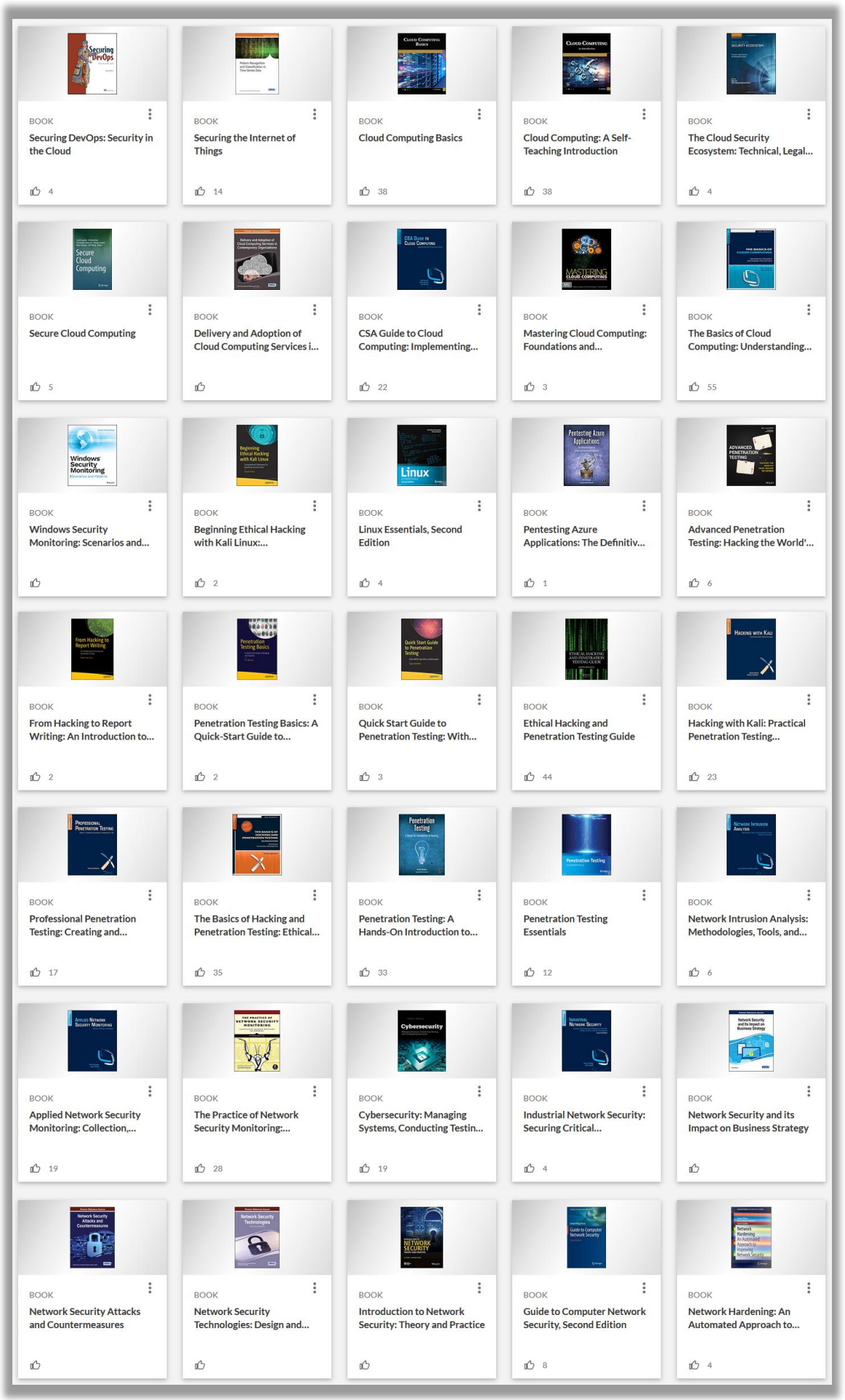
Business & Leadership for CloudOps Security Architect



Productivity Tools for CloudOps Security Architect



Bookshelf



BOOK
Securing DevOps: Security in the Cloud
4

BOOK
Securing the Internet of Things
14

BOOK
Cloud Computing Basics
38

BOOK
Cloud Computing: A Self-Teaching Introduction
38

BOOK
The Cloud Security Ecosystem: Technical, Legal...
4

BOOK
Secure Cloud Computing
5

BOOK
Delivery and Adoption of Cloud Computing Services i...

BOOK
CSA Guide to Cloud Computing: Implementing...
22

BOOK
Mastering Cloud Computing: Foundations and...
3

BOOK
The Basics of Cloud Computing: Understanding...
55

BOOK
Windows Security Monitoring: Scenarios and...

BOOK
Beginning Ethical Hacking with Kali Linux:...
2

BOOK
Linux Essentials, Second Edition
4

BOOK
Pentesting Azure Applications: The Definitiv...
1

BOOK
Advanced Penetration Testing: Hacking the World'...
6

BOOK
From Hacking to Report Writing: An Introduction to...
2

BOOK
Penetration Testing Basics: A Quick-Start Guide to...
2

BOOK
Quick Start Guide to Penetration Testing: With...
3

BOOK
Ethical Hacking and Penetration Testing Guide
44

BOOK
Hacking with Kali: Practical Penetration Testing...
23

BOOK
Professional Penetration Testing: Creating and...
17

BOOK
The Basics of Hacking and Penetration Testing: Ethical...
35

BOOK
Penetration Testing: A Hands-On Introduction to...
33

BOOK
Penetration Testing Essentials
12

BOOK
Network Intrusion Analysis: Methodologies, Tools, and...
6

BOOK
Applied Network Security Monitoring: Collection,...
19

BOOK
The Practice of Network Security Monitoring:...
28

BOOK
Cybersecurity: Managing Systems, Conducting Testin...
19

BOOK
Industrial Network Security: Securing Critical...
4

BOOK
Network Security and its Impact on Business Strategy

BOOK
Network Security Attacks and Countermeasures

BOOK
Network Security Technologies: Design and...

BOOK
Introduction to Network Security: Theory and Practice

BOOK
Guide to Computer Network Security, Second Edition
8

BOOK
Network Hardening: An Automated Approach to...
4

BOOK

Amazon Web Services in Action, Second Edition

8

BOOK

Securing the Perimeter: Deploying Identity and...

5

BOOK

Contemporary Identity and Access Management...

4

BOOK

Securing Office 365: Masterminding MDM and...

2

BOOK

Cyber Security on Azure: An IT Professional's Guide to...

1

BOOK

Implementing Operations Management Suite: A...

5

BOOK

Practical Microsoft Azure IaaS: Migrating and Buildin...

6

BOOK

Pro Azure Governance and Security: A Comprehensive...

2

BOOK

Google Cloud Platform in Action

7

BOOK

Pro DevOps with Google Cloud Platform: With...

7

BOOK

Beginning Serverless Computing: Developing wit...

2

BOOK

COBIT 5 Assessor Guide: Using COBIT 5

2

BOOK

COBIT 5 for Risk

1

BOOK

COBIT 5: Enabling Information

4

BOOK

Configuration Management: Using COBIT 5

4

BOOK

Controls and Assurance in the Cloud: Using COBIT 5

5

BOOK

Transforming Cybersecurity: Using COBIT 5

7

BOOK

Risk Scenarios: Using COBIT 5 for Risk

1

BOOK

Governance of Enterprise IT Based on COBIT® 5: A...

4

BOOK

IT Auditing: Using Controls to Protect Information...

2

BOOK

Security, Privacy, and Digital Forensics in the Cloud

2

BOOK

Networked Control Systems: Cloud Control and Secure...

BOOK

Securing an IT Organization through Governance, Risk...

6

BOOK

Cyber Security Management: A Governance, Risk and...

8

BOOK

Data Protection and the Cloud: Are You Really...

8

BOOK

EU GDPR: A Pocket Guide, Second Edition

1

BOOK

EU GDPR & EU-US Privacy Shield: A Pocket Guide,...

1

BOOK

EU General Data Protection Regulation (GDPR): An...

2

BOOK

Federal Cloud Computing: The Definitive Guide for...

BOOK

Oracle High Availability, Disaster Recovery, and Clo...

1

BOOK

Disaster Recovery and Business Continuity: A Quic...

3

FOLLOW US ON:

www.skilltech.pl

email: biuro@skilltech.pl

tel. +48 22 44 88 827

SkillTech

Technology hired for excellence