1.

Record Nr.	UNINA9910860868003321
Autore	Mishra Ashish
Titolo	Cloud Security Handbook for Architects
Pubbl/distr/stampa	Delhi : , : Orange Education PVT Ltd, , 2023 ©2023
ISBN	9789395968997
Edizione	[1st ed.]
Descrizione fisica	1 online resource (291 pages)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Cover Page -- Title Page -- Copyright Page -- Foreword -- Dedication Page -- About the Author -- Technical Reviewers -- Acknowledgements -- Preface -- Errata -- Table of Contents -- SECTION I: Overview and Need to Transform to Cloud Landscape -- 1. Evolution of Cloud Computing and its Impact on Security -- Introduction -- Structure -- Evolution of cloud -- Cloud computing journey -- Cloud computing overview -- Characteristics of cloud computing -- Cloud types -- Cloud computing service model -- Cloud computing trends -- Recognizing the development of cloud -- Justifications for using the cloud -- Analyzing the risk of cloud services -- Inherent risk -- Techniques to reduce the inherent risk -- Cloud computing privacy concerns -- Assessing your organization's cloud maturity -- Analyzing the development of cloud risk -- Shadow IT and its rise -- Understanding the shared responsibility paradigm -- Key considerations for the upliftment of cloud security -- Risk analysis -- Controls on user access -- Automation -- Continual monitoring -- Conclusion -- Reference -- 2. Understanding the Core Principles of Cloud Security and its Importance -- Introduction -- Structure -- Principles and concept understanding -- Most restrictive -- Defense in Depth -- Threat actors as well as trust limits -- Segregation of duties -- Fail-safe -- Economy of mechanism -- Complete mediation -- Open design -- Least common mechanism -- Weakest chain -- Making use of the current landscape -- Architectural considerations -- Basic concerns -- Compliance -- Security control -- Controls -- Additional

controls -- Information classification -- Objectives for information classification -- Benefits of information classification -- Concepts behind information classification -- Classification criteria -- Procedures for classifying information.

Security awareness, training, and education -- Security awareness -- Instruction and learning -- PKI and encryption key management -- Digital certificate -- Identity and access management -- Identity management -- Passwords -- Implementing identity management solution -- Access controls -- Controls -- Controlling access types -- Mandatory access control -- Discretionary access control -- Non-discretionary access control -- Single Sign-On (SSO) -- Strategy to adopt cloud security -- Enabling secure cloud migrations with a cross-platform, integrated segmentation strategy -- Avoiding problems associated with complex, segregated, and bloated legacy data -- Examining the danger posed by the extended attack surface of the cloud -- Best practices on cloud security -- Recognizing the shared responsibility model -- Asking detailed security questions to your cloud provider -- Installing Identity and Access Management (IAM) software -- Your staff should receive training -- Creating and enforcing cloud security guidelines -- Protecting your endpoints -- Securing data while it is moving and at rest -- Utilizing technology for intrusion detection and prevention -- Audits and penetration testing should be performed -- Conclusion -- References -- 3. Cloud Landscape Assessment and Choosing a Solution for Your Enterprise -- Introduction -- Structure -- Defining organization cloud security roles and responsibilities -- Deep-dive into the Shared Responsibility Model -- Cloud Service Provider (CSP) responsibilities -- Customer responsibilities -- Core cloud team roles and responsibilities -- Understanding team structures -- Managing risk in the cloud -- Risk Management Framework (RMF) -- Cloud Service Provider (CSP) risk management process -- Customer's risk management process for cloud landscape -- Monitoring and managing cloud risk.

An approach towards cloud security assessment -- Basic principles for cloud security assessment -- Need to adopt cloud security assessment -- Benefits of adopting cloud security assessment -- Ideas to keep in mind before beginning your assessment -- Executing cloud security assessment -- Architecture overview -- Internal versus internet-based enterprise assessments -- Guidelines -- Account management and user authentication -- Vulnerability assessments for network and systems -- External alone, internal only, or both -- Server and workstation compliance assessment -- Network and security system compliance assessment -- Testing the security of web applications -- Hypervisor layer assessment -- Reporting and sharing the data that follows -- Selecting the right cloud service provider (CSP) -- Time to choose the right cloud service provider -- Cloud security -- Standards and accreditations -- Roadmap for technologies and services -- Security and data governance -- Dependencies and partnerships for services -- SLAs, commercials, and contracts -- Performance and dependability -- Provider lock-in, exit strategy, and migration support -- Conclusion -- References and useful information -- SECTION II: Building Blocks of Cloud Security Framework and Adoption Path -- 4. Cloud Security Architecture and Implementation Framework -- Introduction -- Structure -- Cloud security architecture overview -- Key elements and responsibilities of cloud architecture -- Shared responsibilities in cloud security architecture -- Infrastructure as a Service (IaaS) -- Software as a Service (SaaS) -- Platform as a Service (PaaS) -- Architectural type for cloud security -- Cloud security architecture building blocks -- Evolution of cloud security architecture

communications -- Web Application Firewall (WAF) -- DDoS protection. Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).

Sommario/riassunto

Cloud platforms face unique security issues and opportunities because of their evolving designs and API-driven automation. We will learn cloud-specific strategies for securing platforms such as AWS, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure, and others. The book will help you implement data asset management, identity and access management, network security, vulnerability management, incident response, and compliance in your cloud environment. This book helps cybersecurity teams strengthen their security posture by mitigating cyber risk when "targets" shift to the cloud. The book will assist you in identifying security issues and show you how to achieve best-in-class cloud security. It also includes new cybersecurity best practices for daily, weekly, and monthly processes that you can combine with your other daily IT and security operations to meet NIST criteria. This book teaches how to leverage cloud computing by addressing the shared responsibility paradigm required to meet PCI-DSS, ISO 27001/2, and other standards. It will help you choose the right cloud security stack for your ecosystem. Moving forward, we will discuss the architecture and framework, building blocks of native cloud security controls, adoption of required security compliance, and the right culture to adopt this new paradigm shift in the ecosystem. Towards the end, we will talk about the maturity path of cloud security, along with recommendations and best practices relating to some real-life experiences.