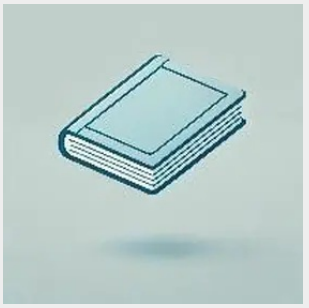
Walshe

The Identity Attack Life Cycle

A Defender's Guide to Modern Identity Security in Cloud and Enterprise Systems



64,19 €
64,19 € (zzgl. MwSt.)

vorbestellbar, Erscheinungstermin ca. Februar 2027

Artikelnummer: 9798868834455
Medium: Buch
ISBN: 979-8-8688-3445-5
Verlag: APRESS L.P.
Erscheinungstermin: 15.02.2027
Sprache(n): Englisch
Auflage: 1. Auflage 2027
Produktform: Kartoniert
Format (B x H): 155 x 235 mm

Identity is no longer just an access control mechanism—it is the attack surface. As cloud platforms, SaaS ecosystems, APIs, and automation become governed by identity-driven trust, the most damaging breaches no longer resemble traditional compromises. Attackers don’t break in; they log in, assume roles, chain tokens, and quietly assemble authority using permissions that already exist. These incidents often unfold within policy boundaries and routinely evade account-centric detection. This book reframes how defenders understand and detect these threats. Rather than treating identity incidents as isolated credential failures, the book introduces a life cycle-based model of attack progression. You will see how modern identity attacks advance through recognizable behavioral stages (accumulating capability, establishing trust relationships, activating latent access paths, coordinating actions across multiple identities and services) and reveal attacker intent even when individual events appear legitimate. Written for practitioners, the book delivers a practical, real-world detection methodology. You’ll learn to model identity environments as interconnected graphs of permissions, tokens, workflows, and trust, enabling detection based on structure and behavior rather than alerts alone. Through concrete attack patterns—such as the Quiet Privilege Ladder, Token Ghosts, Session Chaining, and the Invisible Hand—the book shows how identity attacks actually operate, and how to introduce precise friction that disrupts attackers without disrupting business. Concise, vendor-agnostic, and immediately applicable, this book offers a unifying framework for IAM practitioners, cloud security engineers, detection engineers, and security architects navigating a fragmented identity security landscape. By the final chapter, you will be equipped to spot identity-driven attacks early, design identity-aware detection systems, and respond decisively—long before traditional security tools raise an alarm. What You Will Learn: - Recognize how modern identity attacks progress through life cycle stages rather than isolated credential events - Understand how workload identity, tokens, and delegated trust relationships create hidden attack paths in cloud systems - Design detection approaches that identify behavioral patterns across identities instead of focusing only on compromised accounts - Apply identity graph modelling to reconstruct attacks and identify attack progression - Introduce friction-based controls that slow attackers without disrupting legitimate system operation Who This Book Is For Security professionals responsible for protecting modern cloud and enterprise environments where identity systems control access across infrastructure and applications, including identity and access management (IAM) architects, cloud security engineers, security operations and detection engineers, and security architects and technical security leaders. Readers should have a working understanding of identity systems, authentication concepts, and cloud platforms. Familiarity with technologies such as OAuth, federation, privileged access management, and API security will help readers understand the examples in the book. The book does not require expertise in graph databases or data science; the focus is on conceptual modelling and practical detection approaches rather than specific implementation technologies.

Identity is no longer just an access control mechanism—it is the attack surface. As cloud platforms, SaaS ecosystems, APIs, and automation become governed by identity-driven trust, the most damaging breaches no longer resemble traditional compromises. Attackers don’t break in; they log in, assume roles, chain tokens, and quietly assemble authority using permissions that already exist. These incidents often unfold within policy boundaries and routinely evade account-centric detection. This book reframes how defenders understand and detect these threats. Rather than treating identity incidents as isolated credential failures, the book introduces a life cycle-based model of attack progression. You will see how modern identity attacks advance through recognizable behavioral stages (accumulating capability, establishing trust relationships, activating latent access paths, coordinating actions across multiple identities and services) and

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)