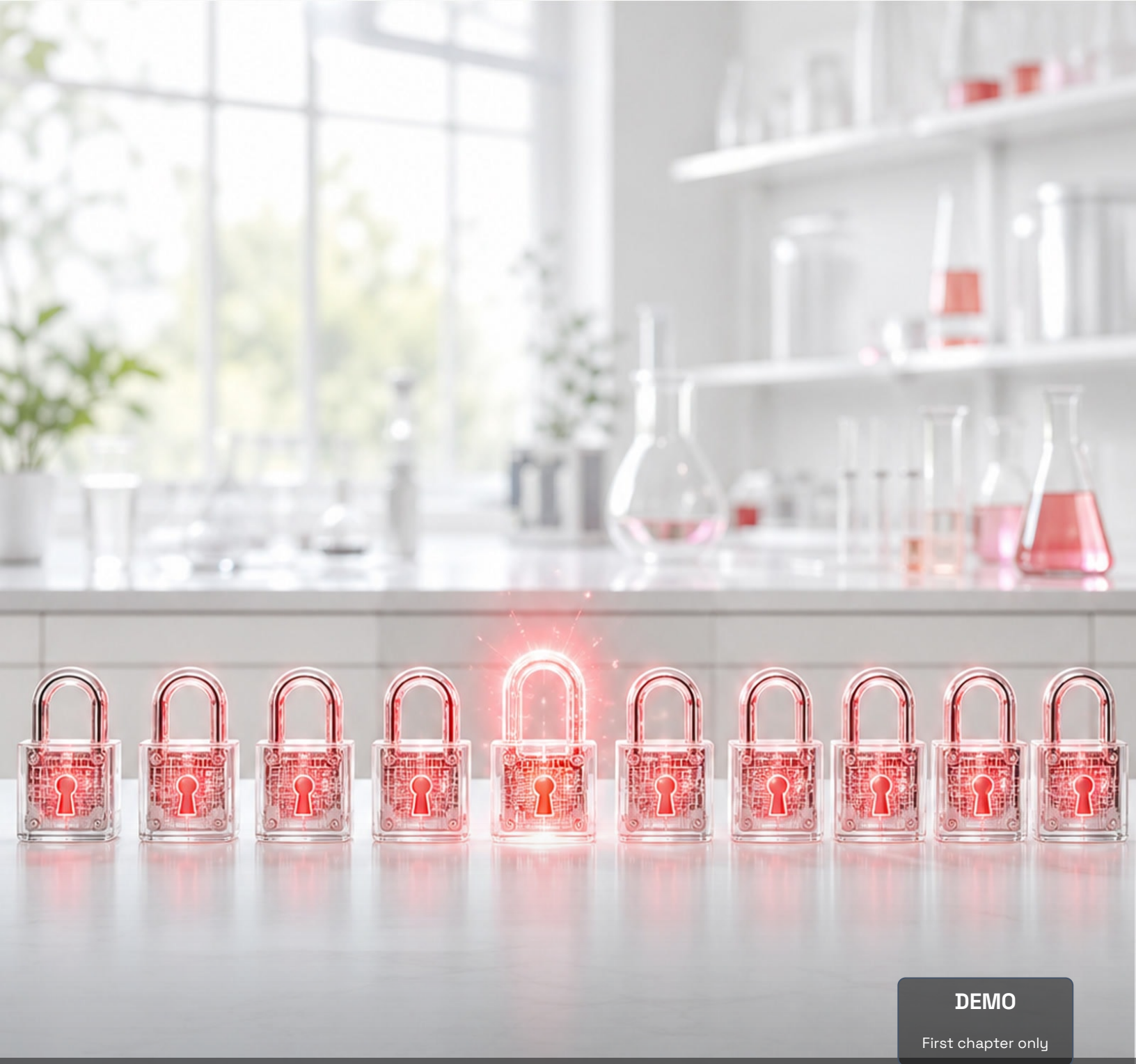

DEMO

First chapter only

OWASP NHI Top 10 Remediation Playbook

Detection, Fix, and Verification for Every Non-Human Identity Risk

pragma.vision

TRUSTAUTHORITY.AI

OWASP NHI Top 10 Remediation Playbook

Trademark Notice

No Affiliation

This book is an independent publication. It is not authorized, sponsored, or endorsed by any of the companies or organizations whose products or services are mentioned herein.

No Professional Advice

The information in this book is provided for educational purposes only. It does not constitute legal, financial, investment, tax, or other professional advice. Readers should consult qualified professionals for guidance specific to their situation.

Code Examples

Code examples in this book are provided for illustration only. They may not be suitable for production use without additional validation, error handling, and security review.

Published by Pragma Vision LLC

First edition, 2026.

Contents

1

The Non-Human Identity Crisis

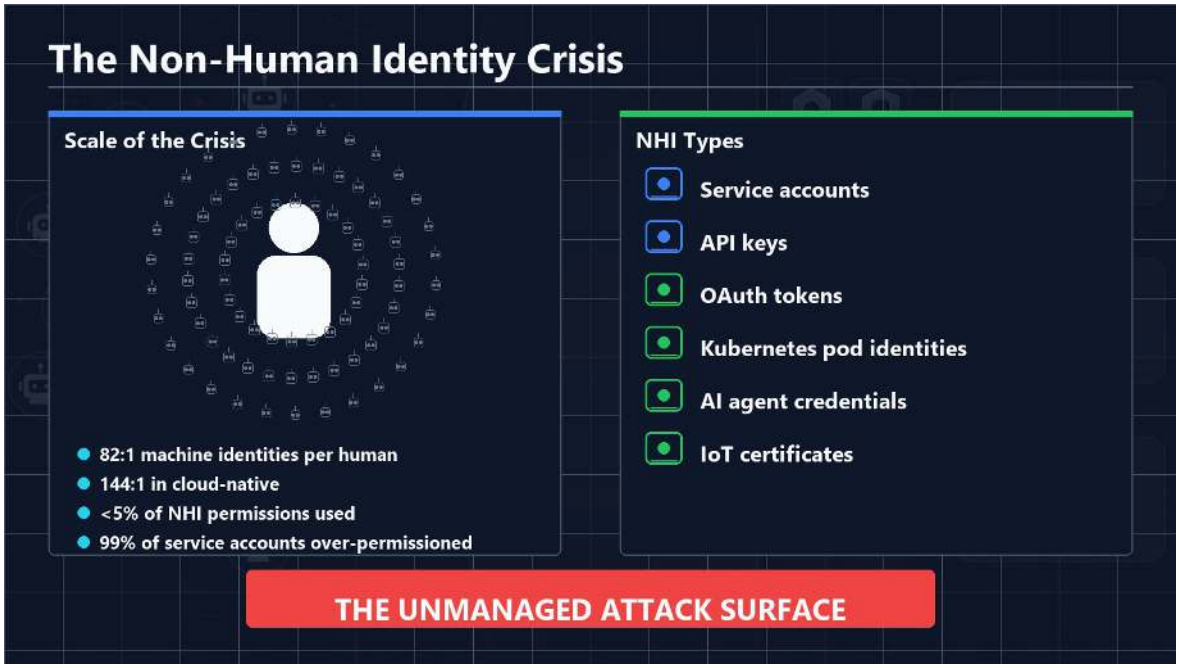

Figure 1. The scale of the non-human identity crisis: 82 machine identities per human (144:1 in cloud-native), with under 5% of NHI permissions ever used and 99% of service accounts over-permissioned across service accounts, API keys, OAuth tokens, and AI agent credentials

1.1 Machines Outnumber People—And Nobody Is Watching

Every enterprise today runs on a hidden workforce. Service accounts push code to production. API keys authorize million-dollar transactions. OAuth tokens link SaaS applications into sprawling dependency chains. Kubernetes pods spin up with credentials provisioned months ago by engineers who have since left. This invisible workforce of non-human identities (NHIs) now outnumbers human users by ratios that defy intuition.

In cloud-native environments, that ratio reaches tens of thousands of machine identities for every human employee. The average enterprise maintains 82 machine identities per human user across its infrastructure. Yet fewer than 5% of the permissions granted to these identities are actually used, and over half are classified as high-risk. Ninety-nine percent of service accounts in cloud environments carry permissions far beyond what their function requires.

80%

of identity-related breaches now involve compromised non-human identities[1]

The OWASP Non-Human Identities Top 10, published in 2025, is the first industry-standard framework for classifying and remediating NHI-specific security risks. It was developed by a coalition of security practitioners, cloud providers, and identity vendors who recognized that the existing OWASP Top 10 for web applications does not address the unique attack surface of machine credentials, service accounts, and automated workload identities.

This book provides a practitioner-level remediation playbook for each of the ten risks. Every chapter follows the same structure: what the risk is, how to detect it in your environment, how to fix it, how to verify the fix is working, and how trustauthority.ai addresses that risk natively through its credential infrastructure.

[1] Cloud Security Alliance and Astrix Security, "State of Non-Human Identity Security," 2025.

Key Insight

Non-human identities are the largest unmanaged attack surface in modern enterprises. Credential abuse remains the top initial attack vector in data breaches, frequently involving compromised API keys, service accounts, or automation credentials. The cost per breach now averages $4.88 million.

1.2 About Pragma.Vision

Pragma.Vision is an AI-native commerce ecosystem where multiple platforms work together to fulfill human needs through intelligent orchestration. The ecosystem includes a growing family of interconnected platforms—from wish fulfillment to logistics to professional services—all connected by three protocol layers: identity verification (Visa TAP), user authorization (Google AP2), and payment execution (Stripe ACP), secured with quantum-safe hybrid cryptography.

trustauthority.ai is the Trust Authority layer of this ecosystem—a Certificate Authority purpose-built for AI agents and machine identities. It issues W3C Decentralized Identifiers and Verifiable Credentials with ML-DSA-65 quantum-safe signatures, providing the identity infrastructure that this book's recommendations build upon. This book draws from the real architecture and security decisions made while building that infrastructure.

1.3 How to Use This Book

Each of the ten risk chapters follows an identical structure for rapid reference:

1. **Risk Description**: What the vulnerability is, why it matters, and real-world attack scenarios.

2. **Detection Checklist**: Specific, actionable items to identify whether this risk exists in your environment.
3. **Fix Steps**: Ordered remediation procedures with code examples and configuration patterns.
4. **Verification Procedure**: How to confirm the fix is working and establish ongoing monitoring.
5. **trustauthority.ai Coverage**: How the Trust Authority platform addresses this risk natively through its credential and identity infrastructure.

The final chapter synthesizes all ten risks into a comprehensive remediation roadmap with prioritization guidance, timeline estimates, and integration points for automated NHI governance.

1.4 The Ten Risks at a Glance

Risk	Description
NHI1	Improper Offboarding — orphaned credentials persist after decommissioning
NHI2	Secret Leakage — credentials exposed in code, logs, and collaboration tools
NHI3	Vulnerable Third-Party NHIs — supply chain risk from integrated services
NHI4	Insecure Authentication — deprecated or weak authentication mechanisms
NHI5	Overprivileged NHIs — excessive permissions beyond functional requirements
NHI6	Insecure Cloud Deployment — static credentials in CI/CD and IaC pipelines
NHI7	Long-Lived Secrets — credentials that never expire or rotate
NHI8	Environment Isolation Failure — shared credentials across dev/staging/prod
NHI9	NHI Reuse — same credential shared across multiple applications
NHI10	Human Use of NHIs — developers using service accounts for manual tasks

DEMO

This is a free preview of the full edition.

Get the complete book at:

https://shop.pragma.vision