



DEMO
First chapter only

OWASP NHI Top 10 Remediation Playbook

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

OWASP NHI Top 10 Remediation Playbook

© 2026 Pragma Vision LLC. All rights reserved.

Trademark Notice

Google, Google Pay, Google Cloud, and Android are trademarks of Google LLC. Stripe is a trademark of Stripe, Inc. Cloudflare and Cloudflare Workers are trademarks of Cloudflare, Inc. Supabase is a trademark of Supabase, Inc. OpenAI and ChatGPT are trademarks of OpenAI, Inc. Claude is a trademark of Anthropic, PBC. W3C is a trademark of the World Wide Web Consortium. Visa is a trademark of Visa International Service Association. OWASP is a trademark of the OWASP Foundation. Midjourney is a trademark of Midjourney, Inc. Canva is a trademark of Canva Pty Ltd. Etsy is a trademark of Etsy, Inc. Amazon is a trademark of Amazon.com, Inc. All other trademarks are the property of their respective owners.

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	8
1.1	Machines Outnumber People—And Nobody Is Watching	9
1.2	About Pragma.Vision	10
1.3	How to Use This Book	10
1.4	The Ten Risks at a Glance	12
2	NHI1: Improper Offboarding	13
2.1	Risk Description	14
2.2	Detection Checklist	15
2.3	Fix Steps	16
2.3.1	Step 1: Establish an NHI Ownership Registry	16
2.3.2	Step 2: Implement Automated Lifecycle Triggers	17
2.3.3	Step 3: Enforce Mandatory Quarterly Reviews	18
2.3.4	Step 4: Implement Last-Used Monitoring	18
2.4	Verification Procedure	18
2.5	trustauthority.ai Coverage	19
3	NHI2: Secret Leakage	20
3.1	Risk Description	20
3.2	Detection Checklist	21
3.3	Fix Steps	22
3.3.1	Step 1: Deploy Pre-Commit Secret Scanning	22
3.3.2	Step 2: Centralize Secrets in a Vault	22
3.3.3	Step 3: Rotate All Previously Exposed Secrets	22

3.3.4	Step 4: Implement Secret-Free Authentication Where Possible . . .	23
3.4	Verification Procedure	23
3.5	trustauthority.ai Coverage	23
4	NHI3: Vulnerable Third-Party NHIs	25
4.1	Risk Description	25
4.2	Detection Checklist	26
4.3	Fix Steps	27
4.3.1	Step 1: Enforce Least-Privilege for All Third-Party Grants	27
4.3.2	Step 2: Implement Third-Party NHI Approval Workflow	27
4.3.3	Step 3: Deploy Behavioral Monitoring for Third-Party Access . . .	27
4.3.4	Step 4: Implement Token Scoping and Expiration	27
4.4	Verification Procedure	28
4.5	trustauthority.ai Coverage	28
5	NHI4: Insecure Authentication	29
5.1	Risk Description	29
5.2	Detection Checklist	30
5.3	Fix Steps	30
5.3.1	Step 1: Replace Static Credentials with Identity Federation	31
5.3.2	Step 2: Enforce Mutual TLS for Service Communication	31
5.3.3	Step 3: Migrate from API Keys to Short-Lived Tokens	31
5.3.4	Step 4: Implement Protocol Minimums	32
5.4	Verification Procedure	32
5.5	trustauthority.ai Coverage	32
6	NHI5: Overprivileged NHIs	34
6.1	Risk Description	34
6.2	Detection Checklist	35
6.3	Fix Steps	36
6.3.1	Step 1: Implement Permission Right-Sizing	36
6.3.2	Step 2: Adopt Policy-as-Code	36

6.3.3	Step 3: Enforce Separation of Duties	37
6.3.4	Step 4: Implement Just-in-Time Privilege Elevation	37
6.4	Verification Procedure	37
6.5	trustauthority.ai Coverage	38
7	NHI6: Insecure Cloud Deployment Configurations	39
7.1	Risk Description	39
7.2	Detection Checklist	40
7.3	Fix Steps	41
7.3.1	Step 1: Migrate to OIDC-Based Pipeline Authentication	41
7.3.2	Step 2: Implement Pipeline-Specific Deployment Roles	41
7.3.3	Step 3: Enforce Deployment Approval Gates	41
7.3.4	Step 4: Scan IaC Templates for Security Misconfigurations	42
7.4	Verification Procedure	42
7.5	trustauthority.ai Coverage	42
8	NHI7: Long-Lived Secrets	44
8.1	Risk Description	44
8.2	Detection Checklist	45
8.3	Fix Steps	46
8.3.1	Step 1: Implement Automated Credential Rotation	46
8.3.2	Step 2: Prefer Ephemeral Credentials Over Rotated Ones	47
8.3.3	Step 3: Implement Hard Expiration Enforcement	47
8.3.4	Step 4: Monitor Rotation Compliance	47
8.4	Verification Procedure	47
8.5	trustauthority.ai Coverage	48
9	NHI8: Environment Isolation Failure	49
9.1	Risk Description	49
9.2	Detection Checklist	50
9.3	Fix Steps	51
9.3.1	Step 1: Issue Separate Credentials Per Environment	51

9.3.2	Step 2: Implement Network-Level Isolation	52
9.3.3	Step 3: Use Ephemeral Development Environments	52
9.3.4	Step 4: Enforce Environment Tags on All Resources	52
9.4	Verification Procedure	52
9.5	trustauthority.ai Coverage	53
10	NHI9: NHI Reuse	54
10.1	Risk Description	54
10.2	Detection Checklist	55
10.3	Fix Steps	56
10.3.1	Step 1: Provision Per-Workload Credentials	56
10.3.2	Step 2: Implement Automated NHI Provisioning	56
10.3.3	Step 3: Decompose Shared Credentials	57
10.3.4	Step 4: Enforce Uniqueness Policies	57
10.4	Verification Procedure	57
10.5	trustauthority.ai Coverage	58
11	NHI10: Human Use of NHIs	59
11.1	Risk Description	59
11.2	Detection Checklist	60
11.3	Fix Steps	61
11.3.1	Step 1: Provide Equivalent Human-Identity Access Paths	61
11.3.2	Step 2: Block Interactive Authentication for NHIs	62
11.3.3	Step 3: Deploy Behavioral Analytics	62
11.3.4	Step 4: Establish a Clear Break-Glass Protocol	62
11.4	Verification Procedure	62
11.5	trustauthority.ai Coverage	63
12	Comprehensive Remediation Roadmap	64
12.1	Prioritization Framework	65
12.1.1	Tier 1: Immediate Action (Weeks 1–4)	65
12.1.2	Tier 2: Structural Remediation (Months 2–3)	66

12.1.3 Tier 3: Governance Maturity (Months 3–6)	66
12.2 The 90-Day Quick-Start Plan	67
12.3 Metrics That Matter	67
12.4 trustauthority.ai Integration Map	68
12.5 Building an NHI Governance Program	70
What’s Next	72
About Pragma.Vision	74

1

The Non-Human Identity Crisis

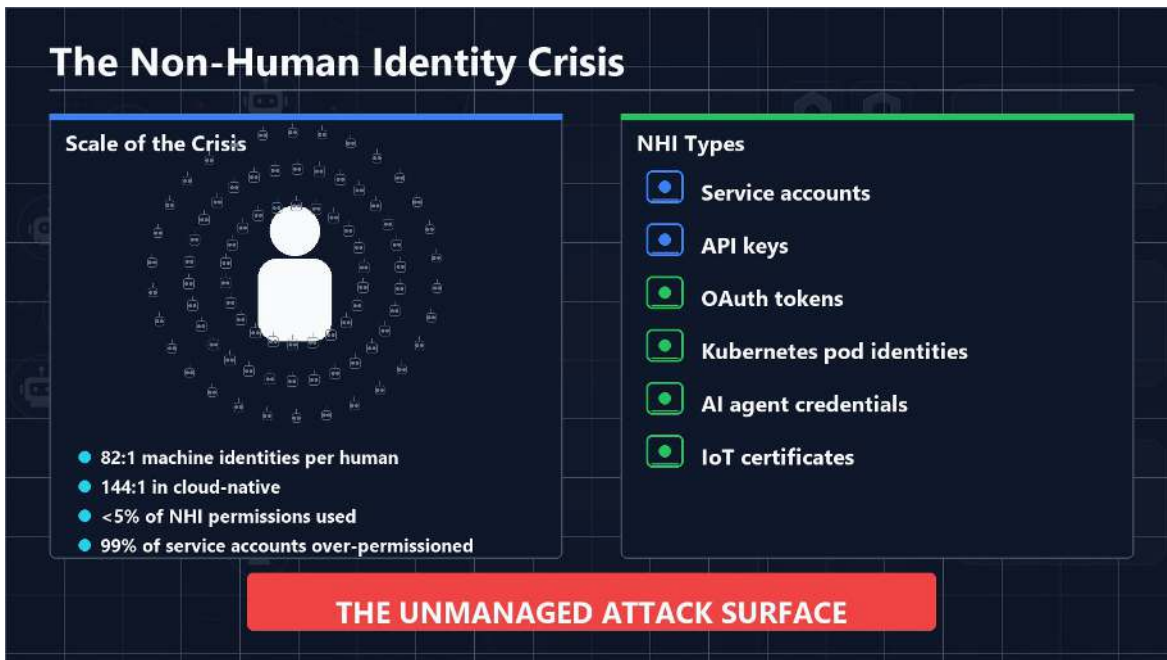


Figure 1. The scale of the non-human identity crisis: 82 machine identities per human (144:1 in cloud-native), with under 5% of NHI permissions ever used and 99% of service accounts over-permissioned across service accounts, API keys, OAuth tokens, and AI agent credentials

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 identities¹

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.

¹Cloud 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

Get the complete book — <https://shop.pragma.vision>

DEMO

This is a free preview of the full edition.

Get the complete book at:

<https://shop.pragma.vision>