SANDBOXAQ™
Public Sector

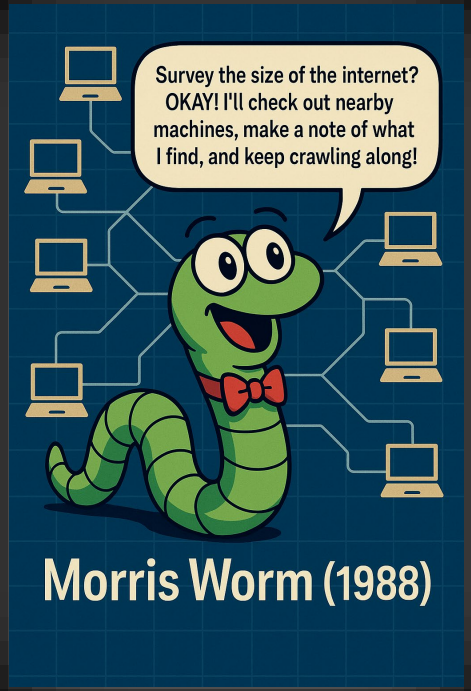
Cryptographic Blind Spots:
AI's FASTEST WAY IN

Kathryn Wang / Principal, Public Sector / kathryn.wang@sandboxaq.com (Primary)
Michael Toney / Solution Architect / michael.toney@sandboxaq.com

SandboxAQ is a **US-Based Company** with **cleared personnel** and **past performance** supporting US Government, Federal Civilian, and the Department of Defense.

April 2025

Historical Lessons from Autonomous Disasters



The AI Cryptography Collision

AI adoption is accelerating across all sectors.

Cryptography underpins all AI functions.

Our cryptographic problems are about to get a lot **more complicated**.

You can't protect what you can't see.

Cryptographic controls were built for a human world. **AI broke that.**

The Non-Human Identity Cryptography Collision

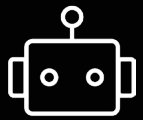
Types of Non-Human Identities

APIs

Service Accounts

IoT Devices

Container and Workloads



RPAs or Bots

AI Agents

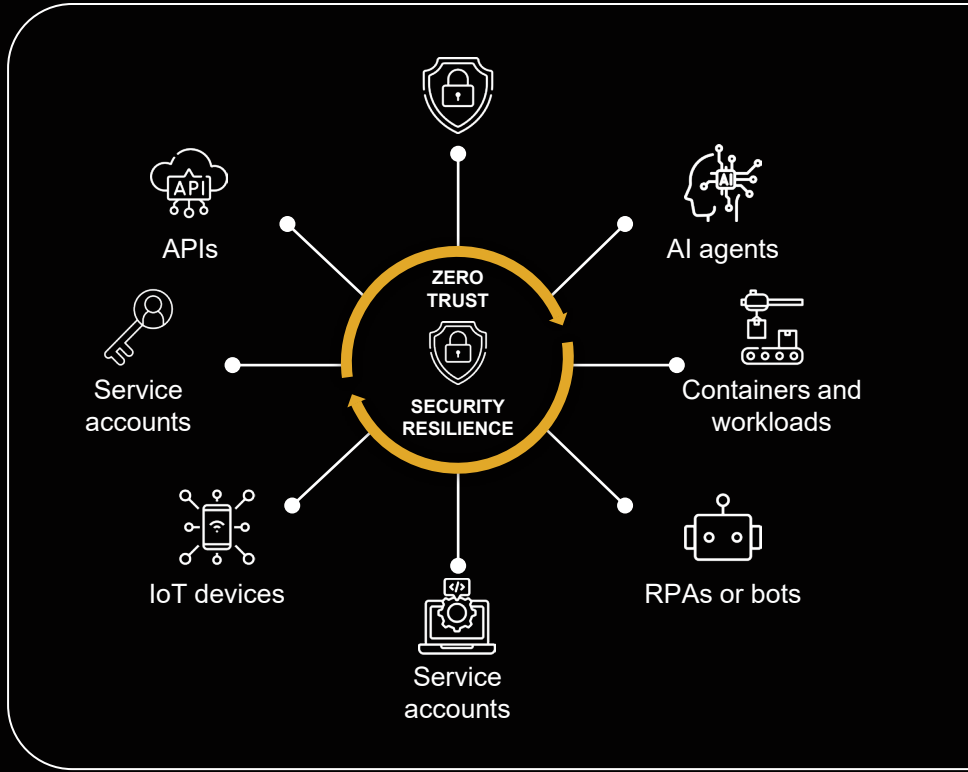
A **non-human identity** is **any entity that isn't a person** but still needs authenticated **access to digital resources** using cryptographic credentials.

It's the "machine equivalent" of a user account.

AI is a subset of NHI.

Where Zero Trust Stops Short

- **Zero Trust Architecture (ZTA)** improves authentication and microsegmentation
- **Cryptographic assets are assumed secure,** not continuously validated
- Expired, hardcoded, or even unknown certificates in lead to **silent access by NHIDs and AI Agents**
- ZTA is only as good as your ability to **enforce it on every identity**
- **Cryptographic management is the missing link of Zero Trust** in today's digital ecosystem



How Attackers Exploit Crypto Gaps in AI Workflows

Non-Human Identity Explosion

proliferation of API, RPA, IoT, service accounts & AI identities

Cryptographic Blind Spots

unknown keys, expired certs, & weak protocols

Misuse & Exfiltration

overprivileged AI, data access bypass, & credential theft

Compromise

cryptojacking AI model poisoning & supply chain attacks

Poor Cryptographic Resilience has a Big Blast Radius

Supply Chain Attacks
Insecure CI/CD secrets or signing certs

Malware injection, build manipulation

Data Exfiltration
Poor key management or weak encryption

Silent data theft, unrevoked decryption

Credential Compromise & Impersonation
Weak, expired, or hardcoded keys

API token leaks, service account key theft

Denial of Service (DoS)
Abusing expensive crypto operations

TLS renegotiation, expired cert floods

Cryptographic Vulnerabilities

AI/ML Manipulation
Cryptographic gaps in AI workflows

Prompt history access, model poisoning

Quantum Threats
Adversaries collect encrypted data now

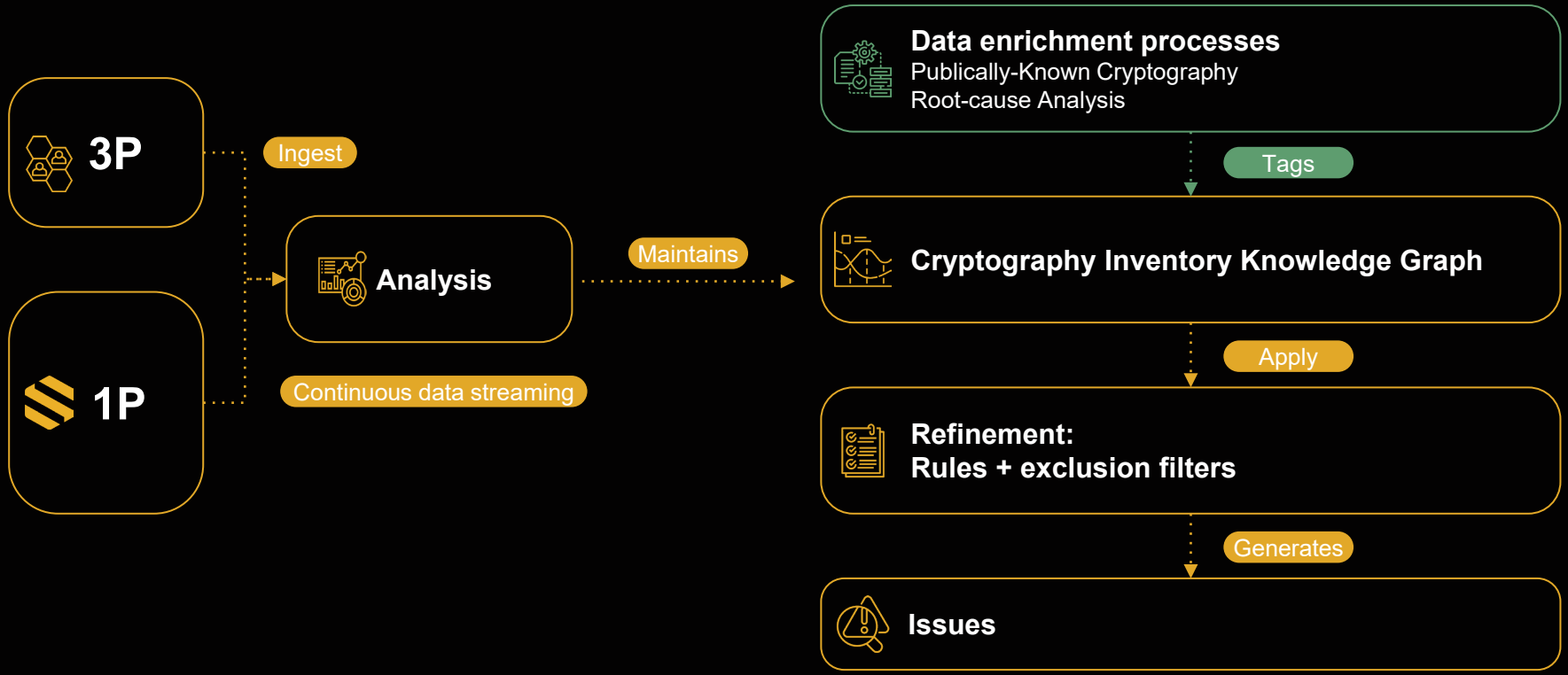
Decrypt later with quantum advantage

Insider Abuse
Stale credentials, shared secrets

Unmonitored lateral access

SANDBOXAQ™

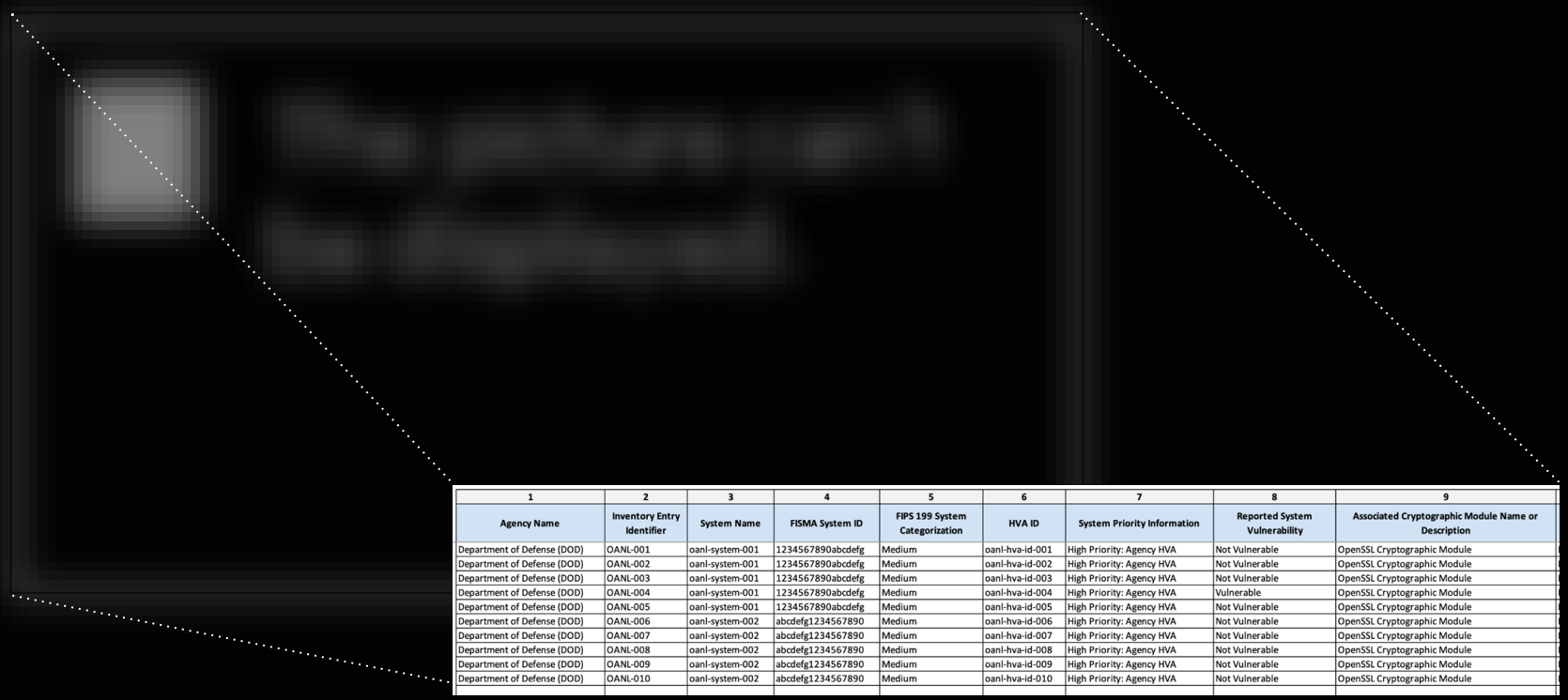
Inventory + Identity = Cryptographic Defense



DEMO

Modernization | Automation | Efficiency

Satisfying Compliance requirements with continuous inventory



1	2	3	4	5	6	7	8	9
Agency Name	Inventory Entry Identifier	System Name	FISMA System ID	FIPS 199 System Categorization	HVA ID	System Priority Information	Reported System Vulnerability	Associated Cryptographic Module Name or Description
Department of Defense (DOD)	OANL-001	oanl-system-001	1234567890abcdefg	Medium	oanl-hva-id-001	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-002	oanl-system-001	1234567890abcdefg	Medium	oanl-hva-id-002	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-003	oanl-system-001	1234567890abcdefg	Medium	oanl-hva-id-003	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-004	oanl-system-001	1234567890abcdefg	Medium	oanl-hva-id-004	High Priority: Agency HVA	Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-005	oanl-system-001	1234567890abcdefg	Medium	oanl-hva-id-005	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-006	oanl-system-002	abcdefg1234567890	Medium	oanl-hva-id-006	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-007	oanl-system-002	abcdefg1234567890	Medium	oanl-hva-id-007	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-008	oanl-system-002	abcdefg1234567890	Medium	oanl-hva-id-008	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-009	oanl-system-002	abcdefg1234567890	Medium	oanl-hva-id-009	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module
Department of Defense (DOD)	OANL-010	oanl-system-002	abcdefg1234567890	Medium	oanl-hva-id-010	High Priority: Agency HVA	Not Vulnerable	OpenSSL Cryptographic Module

Cryptographic Resilience is the tide that lifts all boats

Capability	Benefit
Discovery & Classification	Real-time scanning of keys, certs, and protocols across environments
Identity-Aware Access Control	Enforce fine-grained policy per identity—human, AI, API, or workload
Crypto Hygiene Automation	Automatically rotate, expire, and retire secrets without breaking applications
Vendor & Supply Chain Enforcement	Extend cryptographic policy to third-party integrations and CI/CD pipelines
Quantum-Resilient Migration	Build agility now to adopt quantum-safe algorithms before it's too late
Bonus: Regulatory Alignment	NSM 10 • OMB M 23-02 • EO 14028 • NIST CSWP • FIPS • — readiness out of the box

SANDBOXAQ™
Public Sector

Questions?

THANK YOU

Kathryn Wang / Principal, Public Sector / kathryn.wang@sandboxaq.com (Primary)
Michael Toney / Solution Architect / michael.toney@sandboxaq.com

SandboxAQ is a **US-Based Company** with **cleared personnel** and **past performance** supporting US Government, Federal Civilian, and the Department of Defense.

April 2025