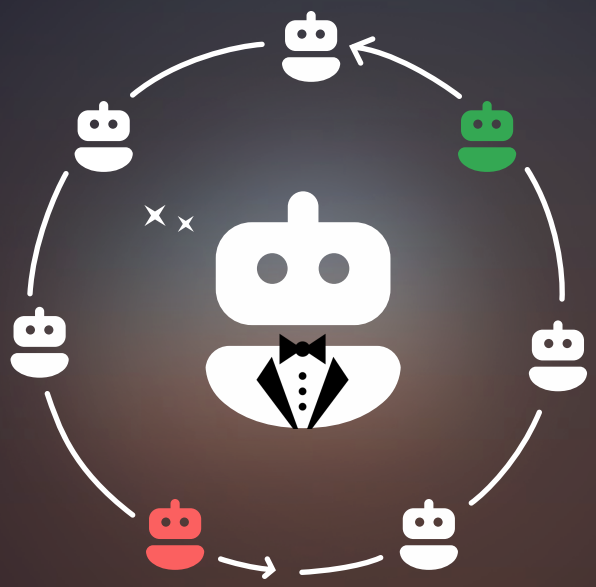
OASIS

White Paper

NHI ILM Best Practices



Best Practices for Non-Human Identity Lifecycle Management

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks.

In this article, we apply the CSF 2.0 framework to Non-Human Identity (NHI) security. Adopting these best practices can help you establish an effective NHI ILM (Identity Lifecycle Management) strategy. We'll describe how you can use Oasis to support and operationalize this strategy.

The CSF 2.0 framework includes six major principles:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

Source: NIST

NIST principles applied to NHI security

Principal	Challenge	Recommendation
Govern (GV) The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	• Understanding ownership of NHIs - critical for effective incident response & ILM. • Documenting the business justification of identities & performing identity certification in accordance with the principle of least privilege. • Achieving full visibility of NHIs across Cloud platforms and SaaS applications. Asset management is a challenge for NHIs, as they are typically shared, privileged accounts, with no central authoritative source of ownership. This means NHIs are often 'invisible' to security & identity teams.	• Add NHIs to your governance frameworks, policies, procedures and SLAs. • Adhere to modern IAM Zero Trust security architecture, the principle of least privilege, & RBAC (Role Based Access Controls). • Establish NHI risk policies and rotation cadences. • Perform recertification campaigns to reassess the business justification of each identity & the scope of permissions.
Identify (ID) The organization's current cybersecurity risks are understood	• Organizations lack established frameworks for identifying risks related to NHIs. • Due to their nature, NHIs tend to be neglected and are more vulnerable to unauthorized access if compromised. • NHIs are prone to poor security practices such as being left stale, unrotated, over-consumed, over-privileged & exposed to external access. • Unrotated NHIs exposed to offboarded employees present a clear security risk. Removing Active Directory/OU access prevents human access to a tenant or workload, yet users are still able to log in to that tenant using an NHI. These factors raise the risk of compromise & increase the blast radius once compromise occurs.	• Identify NHIs that pose security risks, such as unrotated, overprivileged, or external-facing NHIs, or those exposed to offboarded employees. • Categorize risks and prioritize them according to severity.

Principal	Challenge	Recommendation
Protect (PR) Safeguards to manage the organization's cybersecurity risks are used.	NHIs present several unique risk factors: • NHIs often lack tools for efficient lifecycle management processes, e.g. automatic rotation of secrets. • It's necessary to interact with different personas within the organization to safely disable or rotate secrets. • Lack of consumer visibility can cause operational continuity issues, as unknown services can break during rotation. • Current HR policies neglect the potential exposure of valid secrets to offboarded employees, which raises the risk of compromise.	• Include NHI ownership assignments and definitions in user ILM schemas. Enable rotation of NHIs triggered by user-based offboarding workflows already in place. • Establish a 1-to-1 ratio of NHI to Resource instead of a shared schema. • Enforce that NHIs be recertified and attested to on a regular cadence, to identify identities with no business justification. • Establish auto-rotation policies for NHIs.
Detect (DE) Possible cybersecurity attacks & compromises are found and analyzed.	Complex interactions between human users, resources, consumers and NHIs are often difficult to monitor effectively without clear definitions of ownership. In the event of a suspected compromise, it's difficult to assess if a compromise has occurred or if the alert is a false positive, and who needs to be contacted to quickly assess the incident.	• Gain understanding of NHI relationships and privileges. This information is critical in the event of a suspected attack, to reduce investigation times. • Establish methods of assigning and determining ownership for NHIs. • Set geolocation restrictions to identify identity consumers that are in forbidden geolocations. • Detect abnormal activities related to identities, such as an identity which is used by a third-party consumer outside of the Cloud perimeter.

Principal	Challenge	Recommendation
Respond (RS) Actions regarding a detected cybersecurity incident are taken.	Create a response and mitigation strategy for NHIs.	• Create a response framework that includes NHIs such as workload identities (Application's using OAuth tokens, SAS tokens, etc.) which can be used by human users or attackers to bypass security controls such as MFA/ SSO/PAM/firewalls, etc. • Create an escalation process for NHI-related incidents, such as automated workflows that notify relevant stakeholders. • Collect evidence related to the incident, including logs, events and context details.
Recover (RC) Assets and operations affected by a cybersecurity incident are restored.	Since NHIs can be created by anyone with permissions to do so, manually managing the provisioning lifecycle is labor-intensive and can slow down development timelines. In the event of a cybersecurity incident, restoring operations for NHIs is an operational challenge, as they often lack a streamlined and secure provisioning process.	• Establish documented provisioning processes for NHIs. • While testing workflow functionality and SLAs for automated Joiner-Mover-Leaver processes, include NHIs early in the process. • Ensure that each new identity is assigned an owner and has a business justification. • Ensure the rotation policies meet the organization's requirements per project/ team.

Implementing NIST Security Principles for Non-Human Identities with Oasis

Oasis NHI Security Cloud is the first integrated solution purpose-built to address the unique challenges of visibility, cybersecurity, and governance of non-human identities across hybrid-cloud environments. It combines advanced capabilities in NHI discovery, risk assessment, rapid remediation, policy-based lifecycle orchestration, and compliance management within a single integrated platform.

Govern (GV)

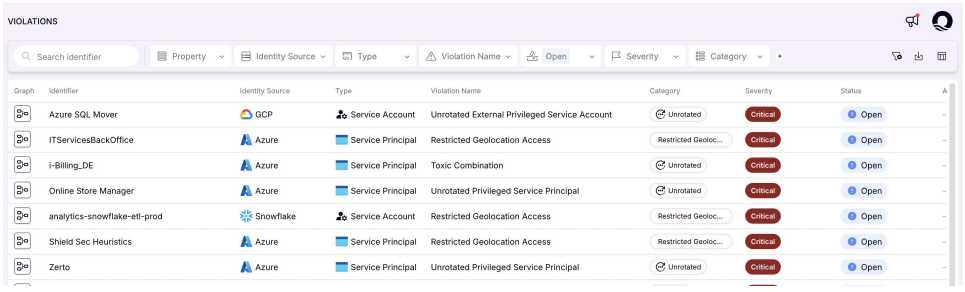
- Oasis helps you understand your NHI landscape, providing a centralized view into all types of identities and authentication mechanisms found within your organization.
- Oasis maps the relationships between NHIs, showing an identity's consumers (e.g. applications and workflows) and the resources to which it provides access.
- Oasis provides visibility into NHI ownership, helping you establish a governance framework for managing non-human identities.
- Use policies to set baseline targets for the management and security of NHIs.

Outcome: The establishment of policies and procedures for the governance of NHIs.

Identify (ID)

- Oasis enables you to review NHI-related risks according to security category.
- Oasis enables you to prioritize these risks according to their severity.

Outcome: A clear record of your NHI-related risks according to priority.



Inventory of your NHI

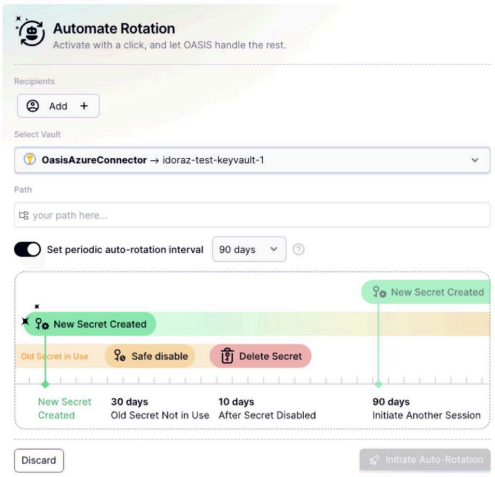
Protect (PR)

Oasis provides step-by-step guides to resolve violations, including quick, automated remediation actions:

- Remediate 'Unrotated' violations with visibility into secret usage, enabling safe rotation.
- Remediate 'Exposed to offboarded employee' violations by rotating secrets that are still exposed to offboarded employees.
- Remediate 'Overconsumed' violations, limiting NHIs to a minimum number of consumers.
- Establish automated rotation workflows for NHIs.
- Disable multiple identities that are not in use quickly and in bulk.
- Create tickets in your ITSM to track & monitor security-related tasks for the resolution of issues.

Outcome:

1. Rotating NHIs that have been viewed by offboarded employees will help prevent unauthorized use of privileged identities.
2. Having a 1-to-1 ratio between NHI & resource will streamline potential audits/reviews, enabling you to certify which NHIs have access to what type of sensitive data.
3. Auto-rotation workflows will ensure NHIs are rotated on a periodic basis, reducing the risk of compromise.



Automatic Safe Secret Rotation

Detect (DE)

- Oasis can detect abnormal activities related to identities, including consumers authenticating from forbidden geolocations.
- Oasis can help you investigate potential attacks by giving you comprehensive context on NHI relationships and owners.
- Oasis provides ownership suggestions using Machine Learning models, for efficient response in case of suspected compromise.

Outcome: Understanding NHI ownership and relationships can reduce MTTR (Mean Time To Remediation) in the event of an attack.

Respond (RS)

- Use the inventory to gain visibility into your NHIs from multiple business systems.
- Use violations' details to investigate the attack chain of an incident and collect the relevant evidence.
- Gain deep context to understand the relationships and access privileges of each NHI.
- Build workflows that will be triggered by suspicious and high severity issues and will generate notification actions.

Outcome: With a comprehensive response and mitigation strategy, you'll be in a better position to prevent attacks and respond to risks.

Recover (RC)

- Provisioning NHIs is on our roadmap, and our vision includes end-to-end management of NHIs.

Outcome:

1. Establish benchmarks for Mean-Time-to-Remediation and Mean-Time-to-Provisioning for NHIs, similar to how human identities are managed today.
2. Establish effective workflows to stress test/streamline security events for business continuity plans and streamline developer provisioning requests, in addition to adding another layer of security against supply chain attacks.

OASIS

Simple. Smart. Effective.

Our mission is to fortify cybersecurity defenses by enabling enterprises to efficiently secure non-human identities throughout their lifecycle.

Get a Demo

Get a Free Assessment

Learn more

Contact us at sales@oasis.security or visit our website at oasis.security