Astrix

NHI Security POC: Key Requirements for Success

When evaluating a Proof of Concept (POC) for a Non-Human Identity security solution, it's crucial to assess specific capabilities that ensure proper protection. This guide outlines the essential requirements, significance, and success metrics.

1. Discovery

Comprehensive visibility into all NHIs across various environments is foundational for effective security.

Key aspects to evaluate:

Platform coverage:

- [ ] IaaS monitoring: Monitor NHIs within Infrastructure as a Service platforms like AWS, Azure, and GCP.
- [ ] SaaS applications: Monitor NHIs across Software as a Service applications such as GitHub, NetSuite, Salesforce, Google Workspace, and Office 365.
- [ ] On-premises and self-hosted platforms: Monitor NHIs in environments like Active Directory, self-hosted GitLab, and GitHub Enterprise.
- [ ] PaaS monitoring: Support for monitoring NHIs across Platform as a Service offerings like Workato and Snowflake.
- [ ] Identity providers: Ability to monitor NHIs within identity providers such as Active Directory, EntraID, and Okta.

Comprehensive inventory:

- [ ] Maintain an inventory of NHIs, including OAuth apps, API keys, tokens, webhooks, service accounts, IAM roles, service principals, secrets, managed service accounts, managed identities, and storage accounts.
- [ ] Identify unique NHIs using static and dynamic analysis, distinguishing user accounts acting as service accounts.
- [ ] Inventory NHIs stored in cloud-native vaults like AWS Secrets Manager and Azure Key Vault.

Contextual association:

- [ ] Associate NHIs with related employees and potential owners, including metadata such as email, department, and position.
- [ ] Identify the authentication mechanisms associated with each NHI.

Usage metrics and historical data:

- [ ] Provide usage metrics for each identity based on its type.
- [ ] Identify used IPs and associate geolocation information.
- [ ] Maintain historical and contextual information of all identities created and offboarded.

Example:

An organization discovers that an API key associated with a deprecated service still has access to critical production data, posing a significant security risk.

Success metrics:

Continuous, comprehensive visibility into all NHIs across environments, with detailed context and usage metrics to prioritize and remediate risks effectively.

2. Posture Management

Understanding and managing the risk associated with NHIs is vital for maintaining a solid security posture.

Key aspects to evaluate:

Risk analysis:

- [ ] List and describe all permissions and entitlements of every discovered NHI.
- [ ] Provide a risk prioritization mechanism to surface the top 1-10% of risky NHIs within monitored environments.
- [ ] Identify NHIs with administrative access levels.
- [ ] Analyze used permissions compared to granted permissions in log-supported platforms.
- [ ] Identify NHIs used by internal entities versus those used by external entities.
- [ ] Detect non-expiring NHIs.
- [ ] Identify individual and organization-wide NHIs.
- [ ] Provide best practice recommendations for privileged identities and credentials.
- [ ] Identify redundant NHIs and permissions (e.g., unused, overly permissive).
- [ ] Offer native language search of NHIs and related information.

Risk analysis:

- [ ] Associate third-party vendors with connected NHIs to provide complete vendors identification.
- [ ] Identify and catalog trusted/untrusted vendors to pinpoint untrustworthy vendors and individual developers connected to sensitive resources.
- [ ] Inventory third-party access to environments, exposure to sensitive platforms, and total NHI connections to identify and respond to third-party incidents.
- [ ] Detect unmaintained third-party integrations.
- [ ] Detect compromised third parties and the associated NHIs.

Example:

A third-party vendor's integration is found to have excessive permissions, granting unnecessary access to sensitive data.

Success metrics:

A clear understanding of NHI risk posture, with prioritized risk metrics and actionable insights to minimize internal and third-party exposures.

3. Non-Human ITDR

Proactive monitoring and response are essential to detect and mitigate potential threats involving NHIs.

Key aspects to evaluate:

Anomaly detection:

- [ ] Detect behavioral-based anomalies in access to resources based on IP, geolocation, resources accessed, client IDs, and user agents.
- [ ] Detect behavioral-based anomalies in access to credentials in secret managers based on similar parameters.
- [ ] Detect unsuccessful authentication attempts.
- [ ] Detect policy violations, such as access from a forbidden country.
- [ ] Detect access attempts by former employees.

Behavioral baselining:

- [ ] Utilize AI/ML to establish normal patterns for NHIs and detect deviations.

Proactive threat detection:

- [ ] Continuously monitor NHIs for signs of lateral movement, privilege escalation, and misuse.

Example:

An NHI exhibits unusual access patterns from an unexpected geolocation, triggering an alert for potential compromise.

Success metrics:

Early detection and mitigation of NHI-related threats with minimal impact on business operations.

4. Secret Scanning and Vault Monitoring

Secrets such as API keys, tokens, and passwords are prime attack vectors in the NHI landscape. Effective secret scanning and vault monitoring capabilities are critical.

Key aspects to evaluate:

Secret scanning :

- [ ] Detect & alert on secrets that have been leaked within the CI/CD tool stack (GitHub, GitLab, etc.)
- [ ] Detect & alert on secrets that have been leaked within collaboration tool stack (Slack, etc.)
- [ ] Detect & alert on secrets that have been leaked within support tools stack (Atlassian Jira, etc.)

Secret rotation and revocation:

- [ ] Enable automated detection and rotation of exposed secrets.
- [ ] Provide workflows to revoke or rotate secrets without operational disruption.

Vault protection:

- [ ] Monitor access and enforce compliance policies across secret managers.
- [ ] Ensure timely rotation of secrets and enforce retrieval policies.

Secretless authentication transition:

- [ ] Provide step-by-step guidance for transitioning from long-lived credentials to secure alternatives like IAM roles or managed identities.

Example:

A leaked secret that allows access to a sensitive GitHub repo is found in a public Slack channel, triggering an alert and rotation workflow.

Success metrics:

A fully mapped and secured secret landscape with automated rotation for leaked secrets, vault compliance, and reduced reliance on long-lived credentials.

5. Lifecycle Management

NHIs must be effectively managed throughout their lifecycle to minimize risks, streamline processes, and ensure compliance. This includes capabilities for provisioning, monitoring, and decommissioning NHIs and associated entities.

Key aspects to evaluate:

Provisioning:

- [ ] Ensure NHIs are created with least-privilege access and tied to specific roles or operations.
- [ ] Assign owners to NHIs to maintain accountability and track ownership over time.

Offboarding:

- [ ] Streamline offboarding processes:
  - Automate the removal of NHIs associated with employee offboarding.
  - Offboard third-party vendors and associated NHIs promptly to eliminate residual access risks.
- [ ] Remove unused or orphaned NHIs efficiently to reduce the attack surface.

Compliance and documentation:

- [ ] Document changes to identities, such as ownership transfers, access activity, and approval processes.
- [ ] Track business justifications for NHIs, ensuring their creation and access align with organizational policies.

Policy enforcement:

- [ ] Identify NHIs outside of rotation policies or those in violation of defined security standards.
- [ ] Enforce approval actions for NHIs, including time limitations to reduce over-privileged, long-lived credentials.

Example:

When an employee is offboarded, all associated NHIs, including service accounts and API tokens, are identified and decommissioned, and any lingering third-party vendor NHIs are automatically revoked to prevent unauthorized access.

Success metrics:

Efficient and automated lifecycle processes that streamline provisioning and offboarding, enforce compliance policies, and document all changes for accountability and governance.

6. Enterprise Integrations & Operations

A good NHI security solution should integrate seamlessly with your existing tech stack and support operational efficiency.

Key aspects to evaluate:

Enterprise integrations:

- [ ] Support for CI/CD pipelines, ITSM tools, SIEM platforms, and other critical enterprise systems.
- [ ] Automate ticket creation and remediation workflows.

In-platform operations:

- [ ] Provide built-in capabilities to define workflows and automation rules.
- [ ] Ensure comprehensive reporting and visibility into operational metrics.
- [ ] Allow for custom policy creation and enforcement directly within the platform.

Example:

An NHI-related alert triggers an automatic ticket in an ITSM platform, initiating a remediation workflow without requiring manual intervention.

Success metrics:

Streamlined workflows, reduced manual effort, and full compatibility with enterprise tools and operations.