Astrix

Securing Non-Human Identities

RSAC Innovation Sandbox 2023 FINALIST

Gartner COOL VENDOR 2023

whoami

- Background in networking, distributed data fabrics, cloud computing and of course security.
- Passionate about learning, teaching and collaborating.
- US Marine Corps veteran

Director, Solutions Engineering

Astrix

Agenda

- What are Non-human Identities?
- CSA Report on NHI
- Walkthrough of an Attack Leveraging NHIs
- Astrix Solution

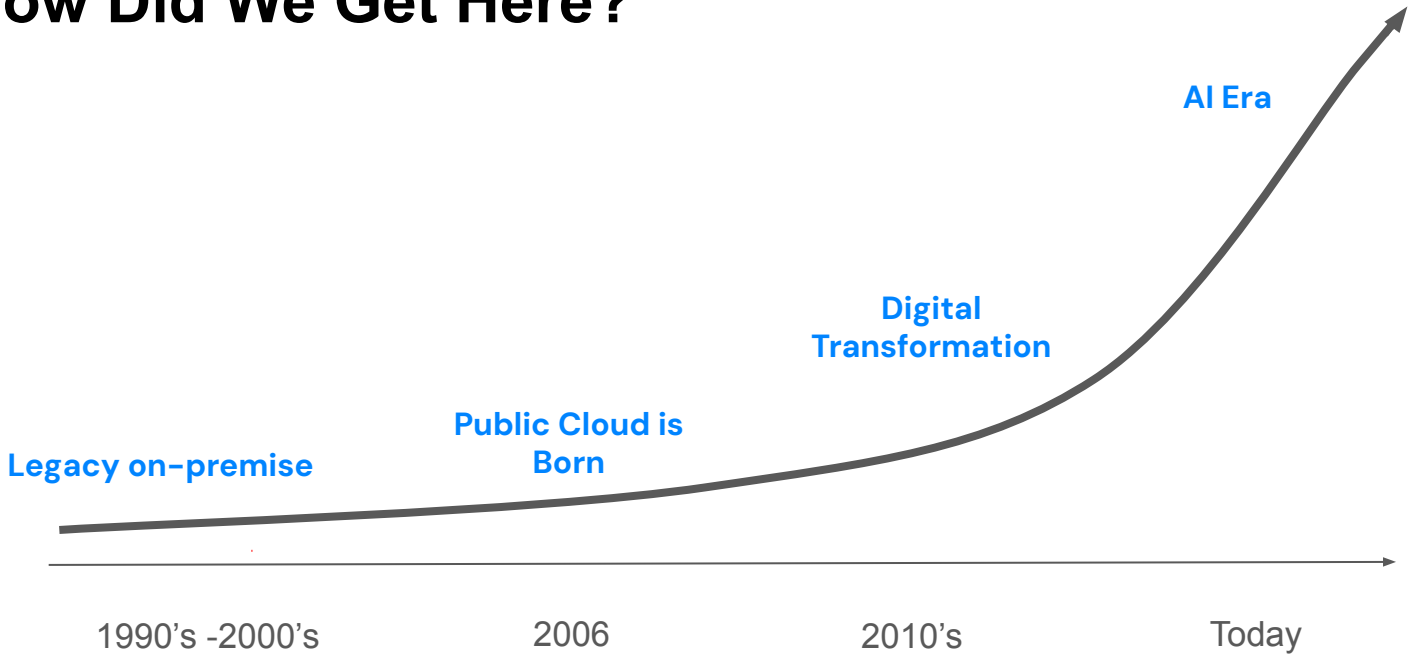
What are Non-human Identities?

What Are Non-Human Identities?

"Programmatic access to a process or data where a human is not required to be involved."

- API Keys
- Service Accounts
- SaaS Marketplace Apps
- Service Principals
- Cloud Roles
- Application Extensions
- Webhooks
- OAuth Apps
- SSH Keys
- Machine Identities
- *and more…*

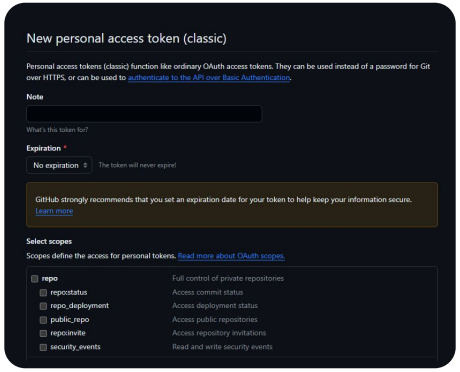
How Did We Get Here?



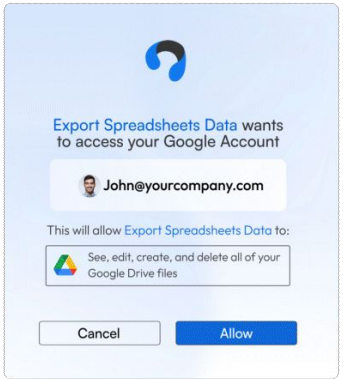
1 employee	=	20+ NHIs

Evolution of NHI Creation

Humans creating NHIs



Humans authorizing NHIs



NHIs creating NHIs

```
aws iam create-user \
    --user-name Bob \
    --path /division_abc/subdivision_xyz/
```

```
{
    "User": {
        "Path": "/division_abc/subdivision_xyz/",
        "UserName": "Bob",
        "UserId": "AIDAIO5FODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:user/division_abc/subdivision_xyz/Bob",
        "CreateDate": "2023-05-24T18:20:17+00:00"
    }
}
```

CSA Report

Astrix | CSA cloud security alliance®

NHI SECURITY TODAY:

Data-Driven Insights

John Yeoh

Global VP of Research, CSA

Key Finding: Struggling with the basics of NHI security

Top challenges for NHI security

- 32% - Service accounts
- 25% - Auditing and monitoring
- 25% - Access and privileges
- 24% - Discovering NHIs

Visibility into third party OAuth apps

- 38% have no or low visibility
- Only 16% have full visibility

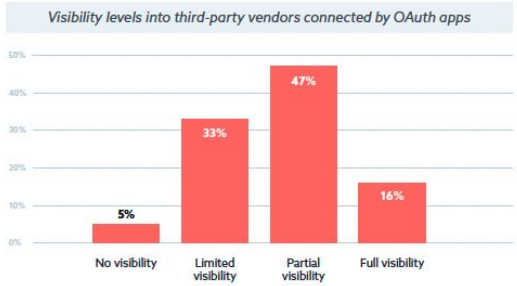
Reactive security leading to security gaps

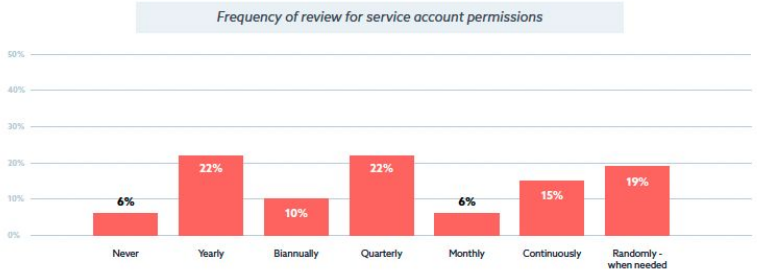
- Only 15% continuously review permissions for service accounts

Conclusion: Foundational NHI security and automation for discovery and permissions – NHIs are deterministic

Most challenging aspects of NHI management

32%	Service accounts	20%	IAM roles	9%	Procuring, tracking, terminating
25%	Auditing and Monitoring	19%	Vendor-owned APIs	7%	AuthN (Authentication)
25%	Access and privileges	18%	Managing requests for third-party tools and services	7%	AuthZ (Authorization)
24%	Discovering NHIs	16%	Managing credentials	6%	Scalability
21%	Policy enforcement	16%	Integration and interoperability		
21%	Managing the secrets lifecycle	11%	Categorizing NHIs		





Key Finding: Challenges w/ Managing Permissions and API Keys

Difficulties with service accounts and tech debt

- Only 9% of orgs find highly difficult to manage permissions on new accounts vs 22% of existing accounts

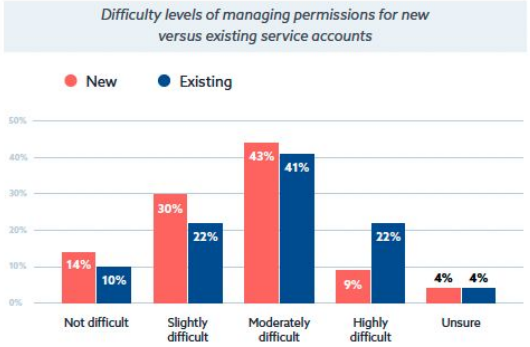
Managing and offboarding API keys

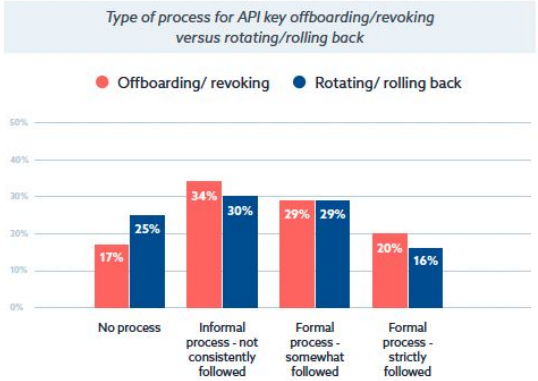
- **Only 20% have a formal process for offboarding and revoking API keys**, and even fewer (16%) have a process for rotating or rolling back API keys

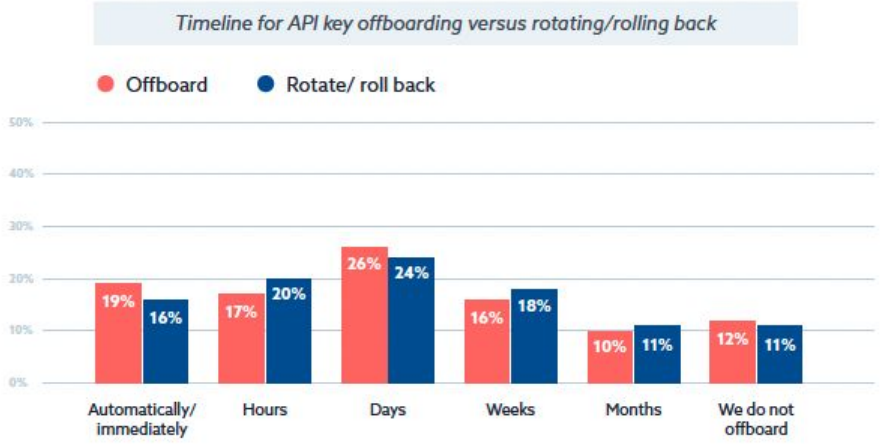
Manual offboarding API keys leading to long timelines

- Only 19% of organizations have automated processes for offboarding, and 16% for rotating/rolling back API keys.

Conclusion: Orgs need to formalize and automate API management - Response time







Key Finding: Fragmented Approaches Lead to Security Incidents

Utilizing a variety of non NHI security specific tools

- 58% - IAM
- 54% - PAM
- 40% - API security, etc.

Causes of the incidents

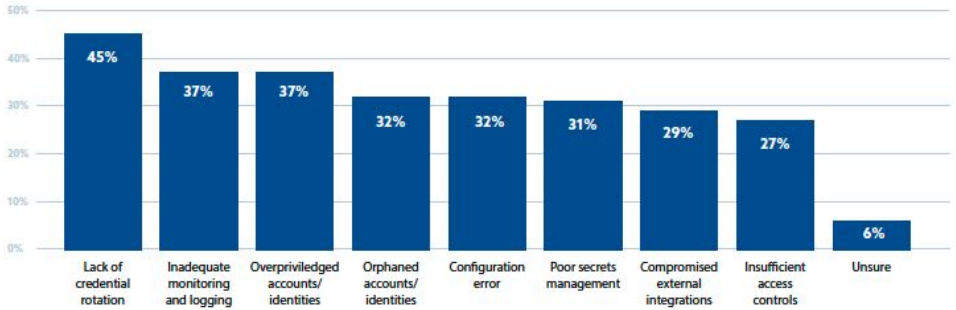
- 45% - lack of credential rotation
- 37% - inadequate monitoring and logging
- 37% - over privileged accounts/identities

Conclusion: Organizations need to unify their NHI security strategies and invest in tools specifically designed for managing NHIs – Unified Platform, Mirrored Privileges

Solutions and strategies currently used to manage NHIs

58%	Identity and Access Management (IAM)	35%	Behavioral Analytics and Anomaly detection	20%	Custom Scripts/Tools
54%	Privileged Access Management (PAM)	35%	Auditing and monitoring	18%	Machine identity protection
40%	API security	34%	Cloud Access Security Broker (CASB)	14%	Robotic process automation(RPA)
38%	Zero trust/least privilege	23%	Workload identity management	2%	We do not use any specific technology
36%	Secrets Management tools	22%	Automated Discovery and Management tools		

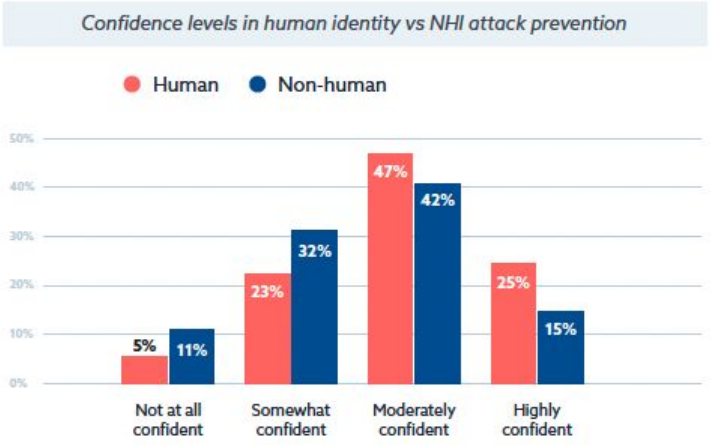
Causes of NHI security incidents

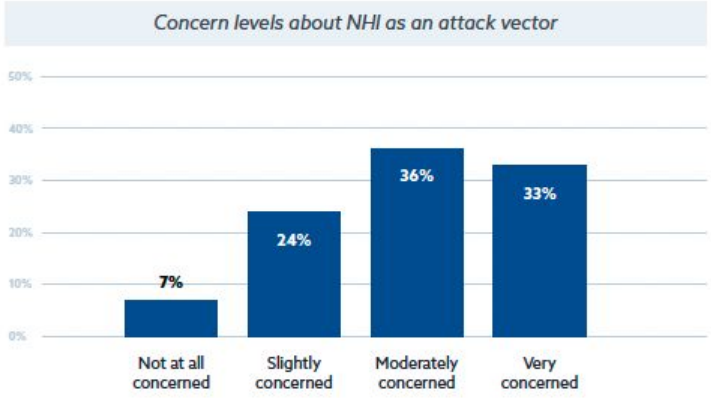


Key Finding: High anxiety, low confidence when securing NHIs

- Comparing Human identities vs Non-human identities
  - Human identity attacks (25% highly confident)
  - NHI attacks (15% highly confident)
- 69% moderately to very concerned about NHI attack vector

Conclusion: Organizations are aware of security implications of NHIs, but don't have the ability to prevent them - Solution awareness





Key Finding: Investment in NHI security capabilities on the rise

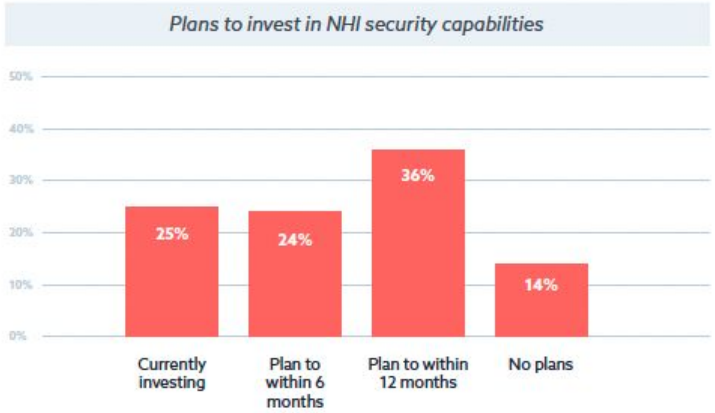
NHI security investment

- 25% currently invested
- 24% planning within 6 months
- 36% planning within 12 months

Searching for wide array of NHI security capabilities

- 26% - Visibility into third party vendors connected via OAuth app
- 26% - Secrets lifecycle management
- 25% - Identity discovery
- 23% - Management of API keys

Conclusion: Understanding of the significance of NHI security and plan to invest accordingly – Strategies like Zero Trust



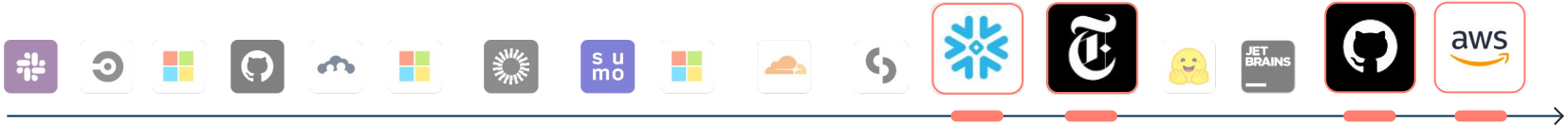
Most important security tool capabilities for NHI security

26%	Visibility into third-party vendors connected via OAuth apps	21%	Automate third-party connectivity	13%	Incident response and remediation
26%	Management of the secrets lifecycle	16%	Access control to sensitive information	9%	Compliance management
25%	Identity discovery	15%	Automated provisioning and de-provisioning of identities	7%	Scalability
23%	Management of API keys	14%	Audit and logging of NHIs	1%	Use level of NHIs
22%	Managing permissions	14%	Identify owners and consumers of NHIs		
22%	Tracking access behavior/ anomaly detection	13%	Policy enforcement		

NHI Attack Surface

FASTEST GROWING ATTACK VECTOR

2023-2024 - At least one publicly known NHI attack per month



Snowflake
May 2024
Hundreds of Snowflake instances were breached by the financially motivated threat actor UNC5537, affecting approximately 165 organizations.

New York Times
Jun 2024
Attackers stole the New York Times' source code by exploiting an over-privileged GitHub token, granting access to all repositories.

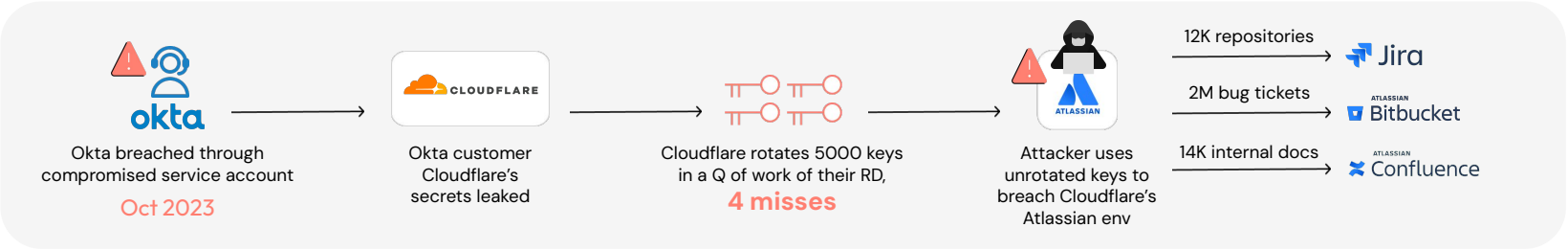
GitHub
Aug 2024
The threat actor Gitloker exploited malicious OAuth apps to target GitHub users, causing significant data loss and ransom demands.

AWS
Aug 2024
Massive NHI Attack: Insecure AWS stored NHIs and machine credentials lead to compromise of 230 Million cloud environments.

It takes 1 vulnerable NHI to breach your organization

BUSINESS IMPACT

The Cost of NHI Breaches

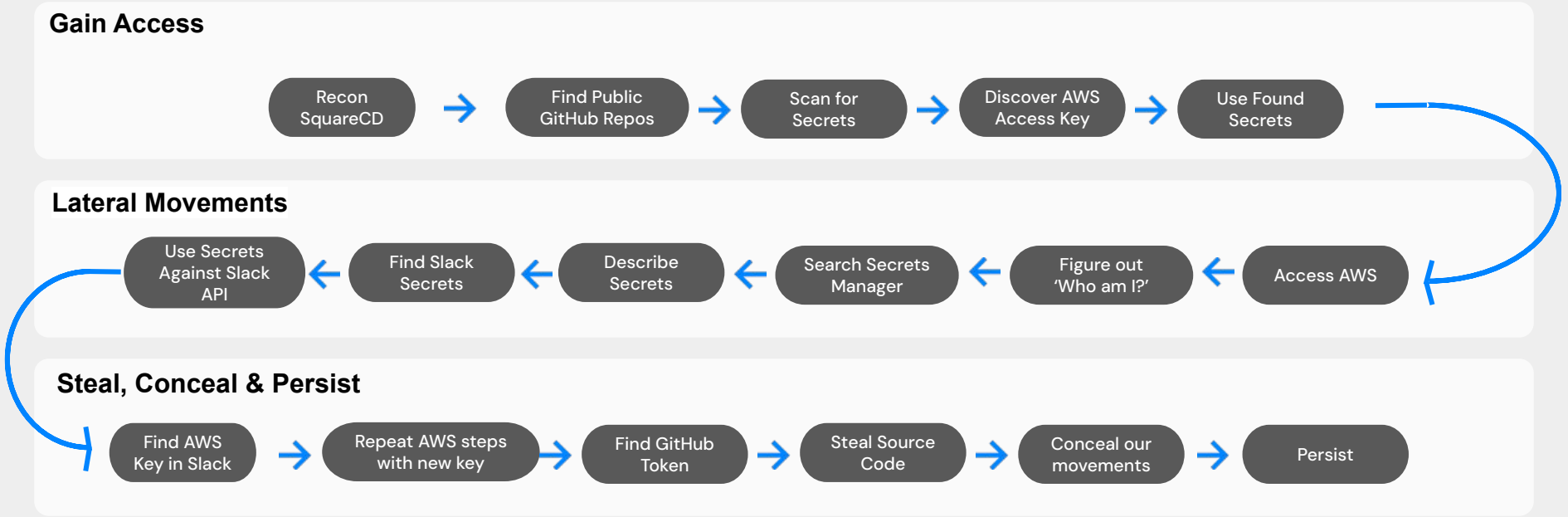


Cost of Risk

It will never happen to me	okta	Customers NHIs were compromised	$B+	**Reputational damage and loss of customers** • Okta's share plummet by 11% and a market cap loss of $2 billion • Compliance fines (stolen customer records) • IR and future mitigation cost - $1-2M
It could happen to me	CLOUDFLARE	Rotate, miss & breached	~$500K-$1M	**Mitigation costs** • IR and Forensic Analysis • Rotating 5,000+ production credentials • System Hardening and Reimaging
Probably already happened	**Thousands of organizations worldwide**	Rotate, miss & dodged	~ $62,500	**IR efforts** • Rotating 5000 keys, 15 min per key. 1250 IR hours

Let’s Attack!

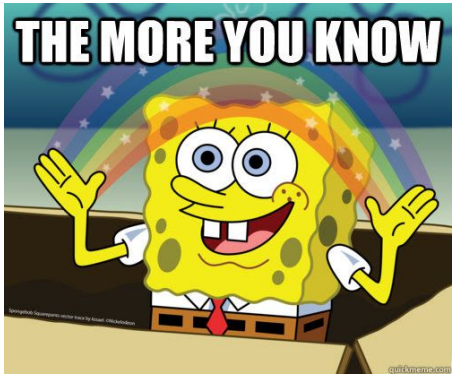
The Attack


Gain Access
Recon SquareCD
Find Public GitHub Repos
Scan for Secrets
Discover AWS Access Key
Use Found Secrets
Lateral Movements
Access AWS
Figure out 'Who am I?'
Search Secrets Manager
Describe Secrets
Find Slack Secrets
Use Secrets Against Slack API
Steal, Conceal & Persist
Find AWS Key in Slack
Repeat AWS steps with new key
Find GitHub Token
Steal Source Code
Conceal our movements
Persist

Environment	Key/Token Prefix	Key Type
Slack	xoxp	OAuth User Access Token
Slack	xoxb	Bot Access Token
AWS	AKIA	Access Key ID
GitHub	ghp_	Personal Access Token (PAT)
Google Cloud Platform	ya29	OAuth 2.0 Refresh Token

POSTMAN

API development platform used to design, build, test, and document APIs



Demo

Attack in a Nutshell

1. Attacker found a leaked secret outside of the main branch within a public repository.
2. Used NHIs to jump between Github, AWS and Slack without ever needing a human credential.
3. Stole source code from a Github repository other than the initial repository that we encountered.
4. Concealed our crime by pretending to have compromised S3 with a data breach, stumbling upon some great material.
5. Used customer keys found in S3 to turn SquareCD into a supply chain attack to their customers.

How prevalent is the issue?

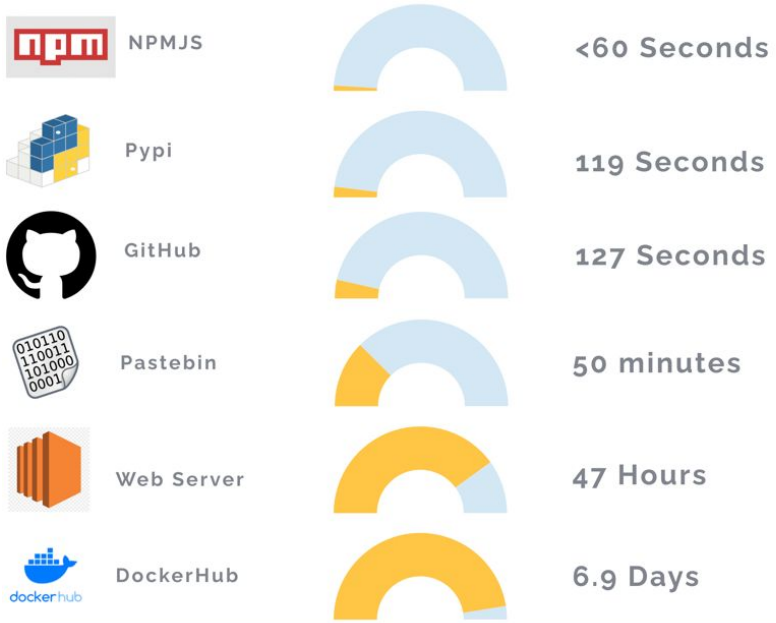
Cybernari Research

Put canary tokens in public places; *self-hosted apps, S3 buckets, SaaS platforms, etc.*

This is how quickly **robotic processes** discovered the keys in each platform.

Next Action Taken:

- GetCallerIdentity
- InvokeModel
- ListSecrets
- ListVaults

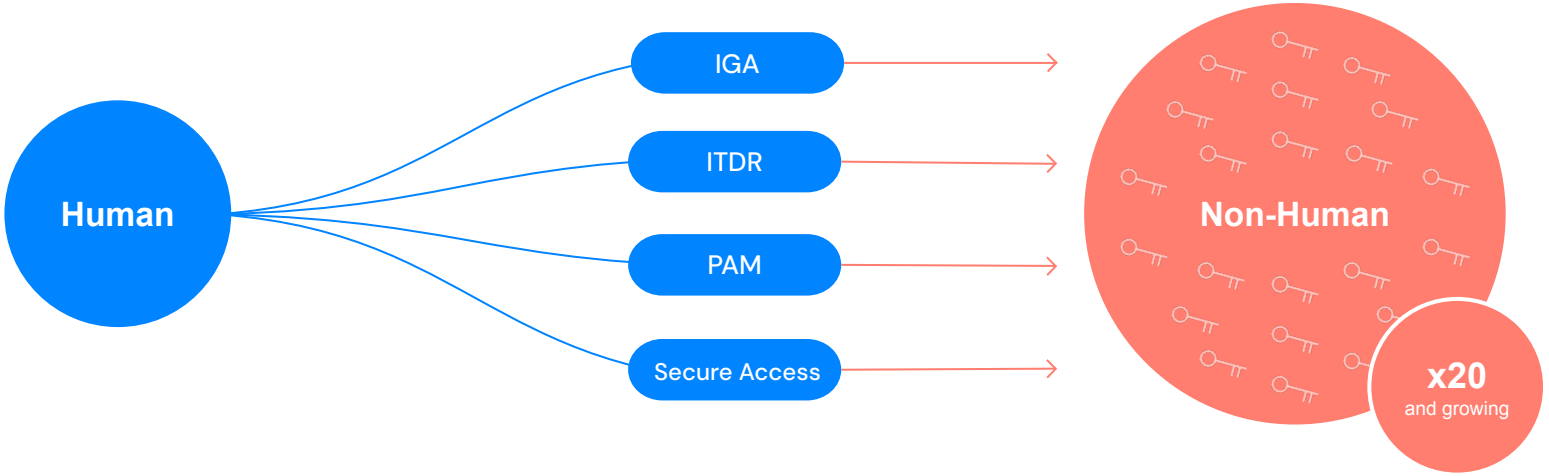


Cybernari, 2024

Astrix Solution

Astrix

Securing Non-Human Identities



Supported Environments:

IaaS

PaaS

SaaS

On-Prem

Vaults

IDP

Astrix

Secure & Manage NHIs, Everywhere.

SUPPORTED ENVIRONMENTS

IaaS

PaaS

SaaS

On-Prem

Vaults

IDP

PRODUCT CAPABILITIES

Inventory

NHI Mapping: accessed resources, permissions, consumers, and third-party vendors

- Connectivity map
- Ownership assignment

Security Posture

- Business & security context
- Risk prioritization

- Redundant/inactive NHIs
- Orphaned NHIs
- Over-privileged
- Connected to untrusted vendor

Non-Human ITDR

- Anomaly detection
- Third-party breach alert
- Secret scanning detection & context of exposed secret
- Policy breach/deviation

- Suspicious geo-location access
- Abnormal API call
- X-employee access secret on vault
- Secret found in external Slack chat

Remediation

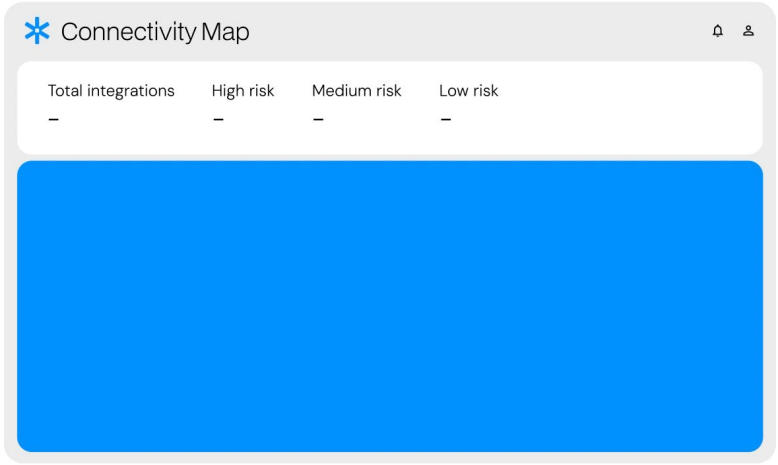
- Automated workflows
- End-user assisted remediation
- Integrations: SOAR/SIEM/IGA/ITSM

- Key rotation
- Contact NHI Owner
- Reduce permissions
- Remove redundant NHI

Identify & Manage NHIs Across All Environments

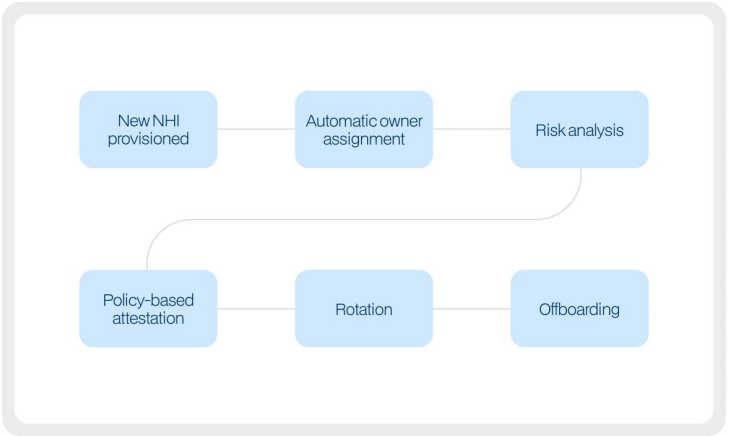
Discover NHIs in near real-time

Continuous & automated inventory and scanning of NHIs like service accounts, OAuth apps, IAM roles, and API keys across IaaS, SaaS and PaaS.



Manage the lifecycle of NHIs

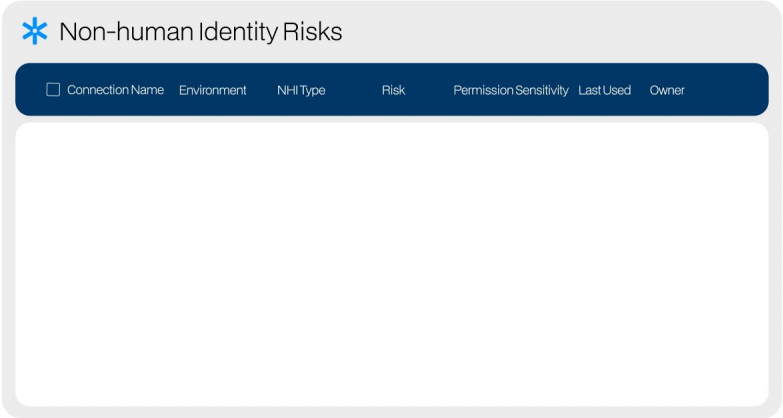
Enable policy-based attestation, alerts, and offboarding of NHIs by managing their lifecycle, from the moment they are created through their entire lifecycle.



Provide Risk Prioritization and Automated Remediation

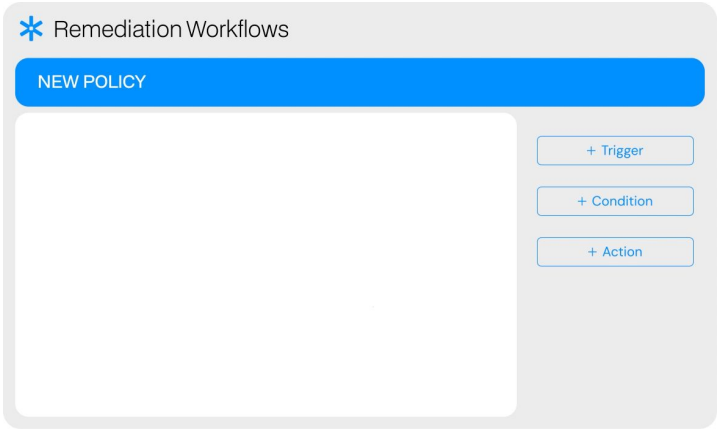
Prioritize NHI risks

Attend to the top 5% risks using threat algorithms based on parameters such as services and resources an NHI can access, permissions, behavioral analysis, and internal or external use.



Automate remediation & integrate with your existing stack

Use out-of-the-box policies, custom workflows and context to remediate NHI risks across your environments. Reduce overhead with native SIEM, SOAR and ITSM integrations.



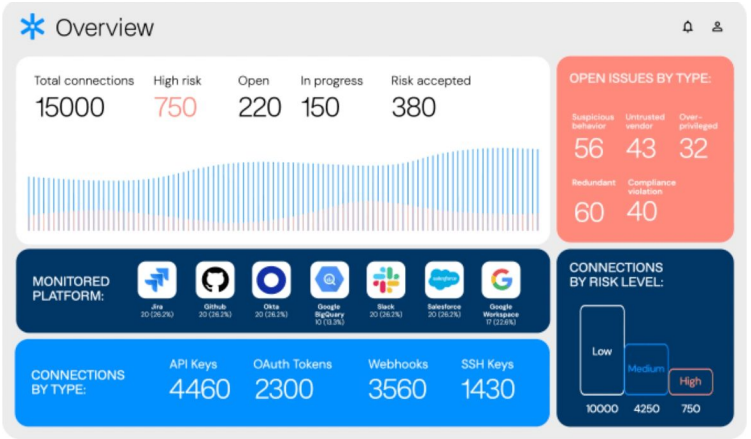
Provide Threat Detection and Behavioral Analysis

Detect suspicious NHI behavior

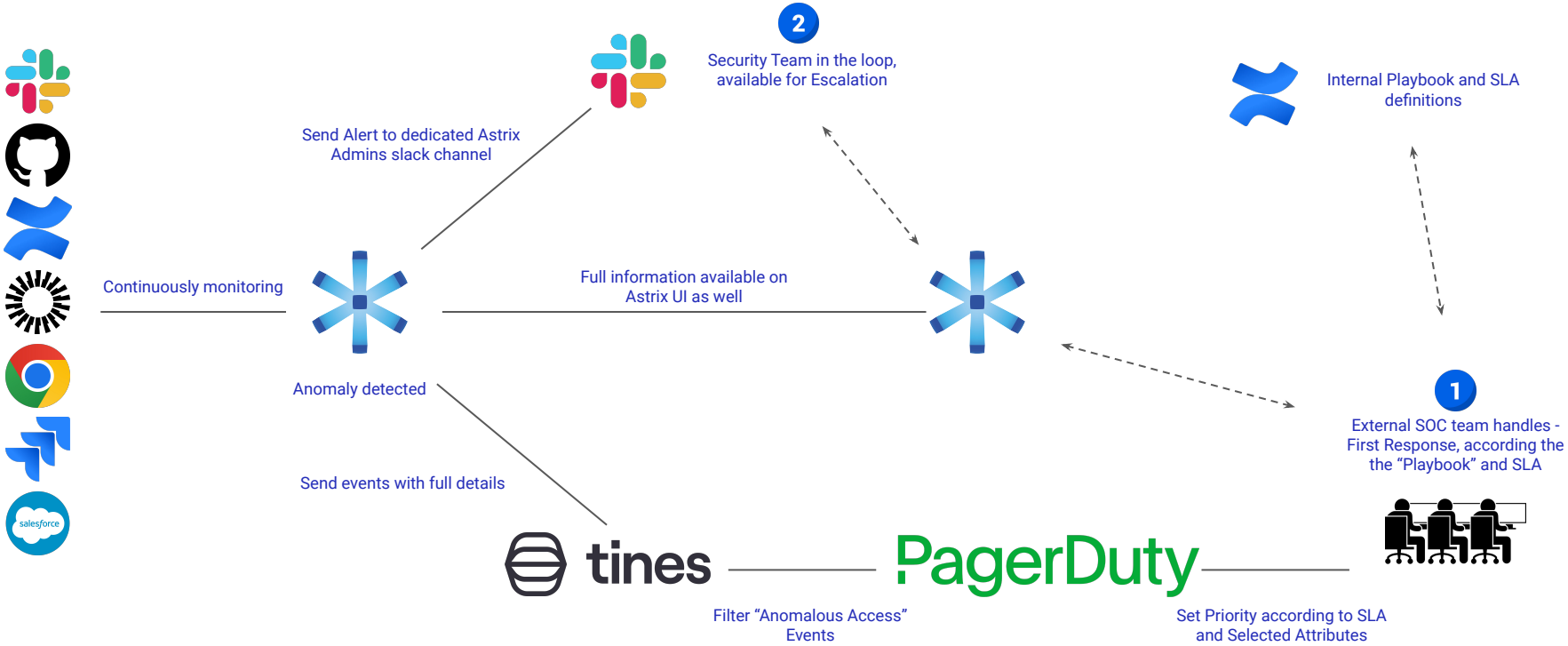
Easily respond to real-time alerts on potential attacks with automated workflows and investigation guides on anomalous NHI activity.

Respond to third-party supplier breaches

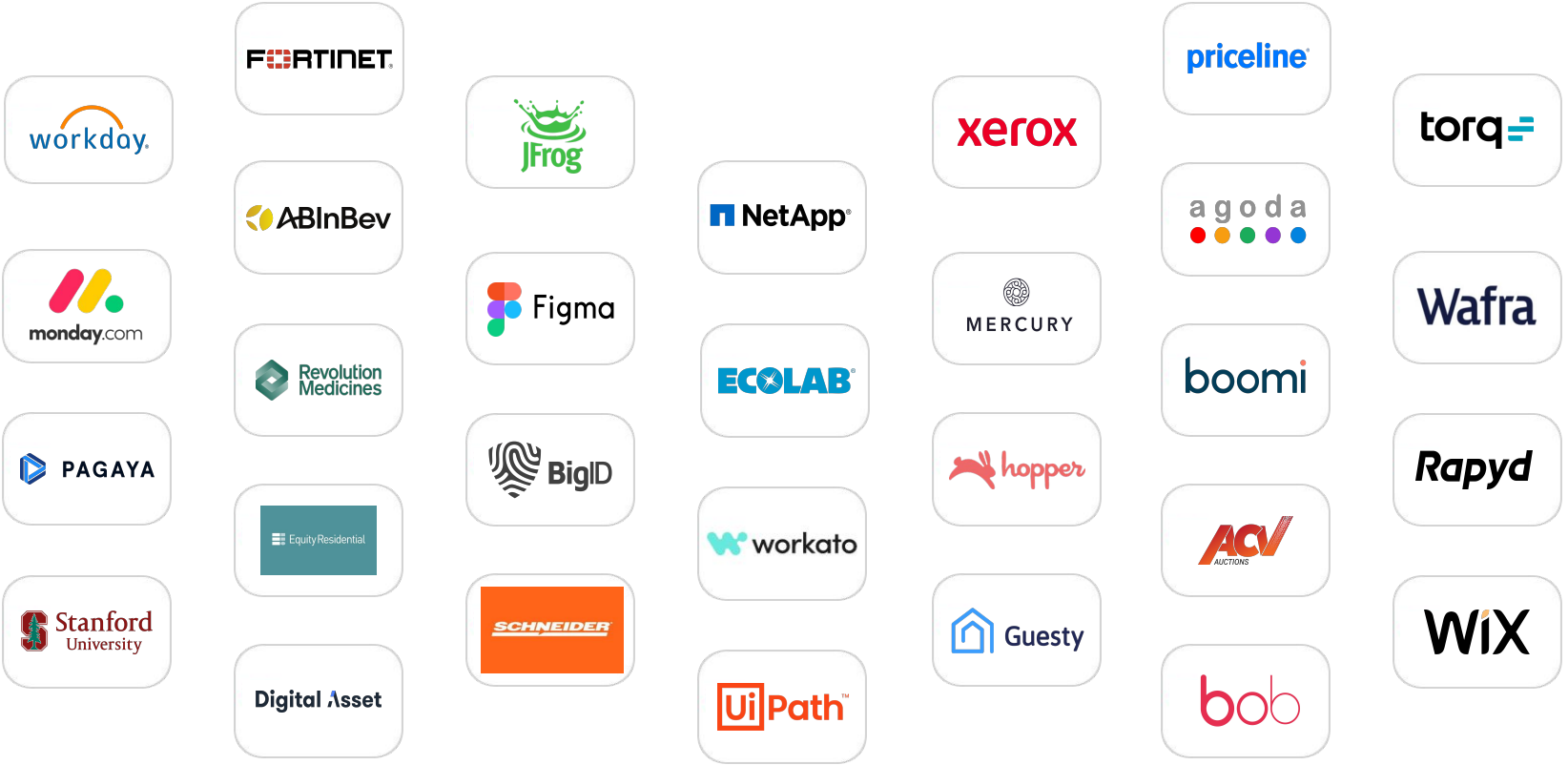
Expedite IR efforts when a vendor is breached. Map every associated NHI, and see everything it's connected to so you can remove or rotate in a jiff.



Anomalous Event Workflow



Astrix Customers



Thank you!

To follow me and/or see relevant content