Navigating NHI (Non-Human Identities) in Incident Response

Astrix

ISC2 CHAPTER | EAST BAY

RSAC Innovation Sandbox 2023 FINALIST

Gartner COOL VENDOR 2023

- What are NHIs? What are the different security implications from traditional human identities?
- Who within an organization is most impacted by the expanded attack surface and complex challenges that NHIs introduce into incident response?
- Where should CSIRTs integrate NHI management within their current processes to effectively mitigate risks?
- When faced with an active incident involving NHIs, what operational and information limitations affect strategies CSIRTs can employ?
- Why is it critical to build CSIRT resilience through post-incident reviews and continuous improvement in the context of NHI security?

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...

CSA Report Key Finding:

Fragmented Approaches Lead to Security Incidents

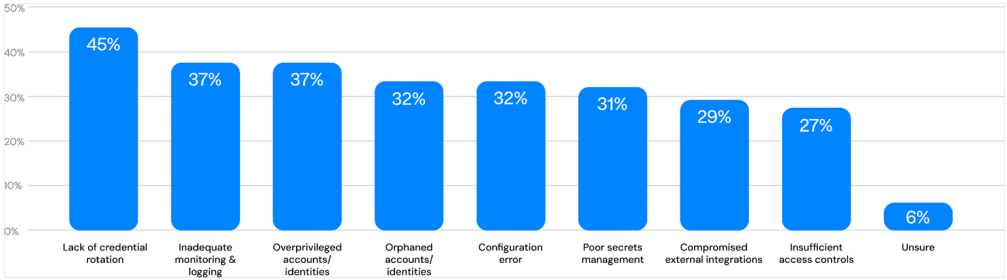
Astrix | CSA cloud security alliance®

ISC2 CHAPTER EAST BAY

Solutions and strategies currently used to manage NHIs

58%	Identify & Access Management (IAM)	35%	Behavioral Analytics & Anomaly detection	20%	Custom Scripts/Tools
54%	Privileged Access Management (PAM)	35%	Auditing & 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 & Management tools		

Causes of NHI security incidents

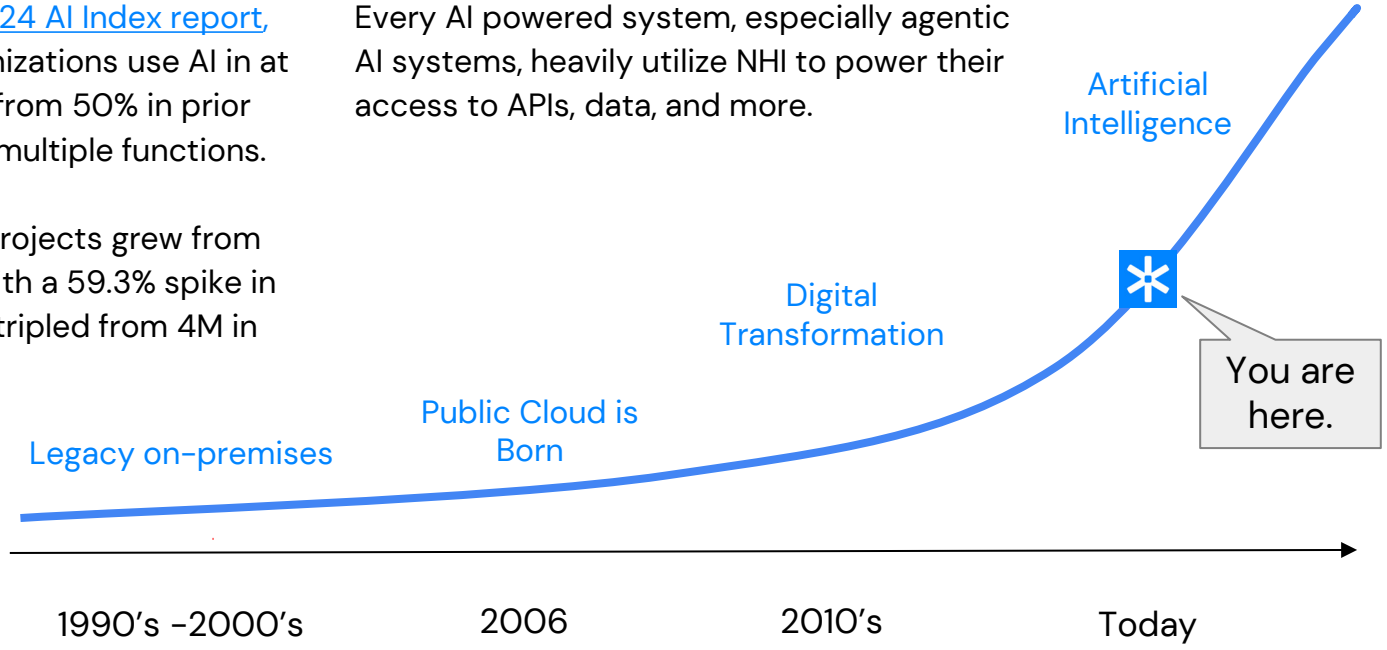


How Did We Get Here?

Stanford University 2024 AI Index report, highlights 72% of organizations use AI in at least one function, up from 50% in prior years. Most using it in multiple functions.

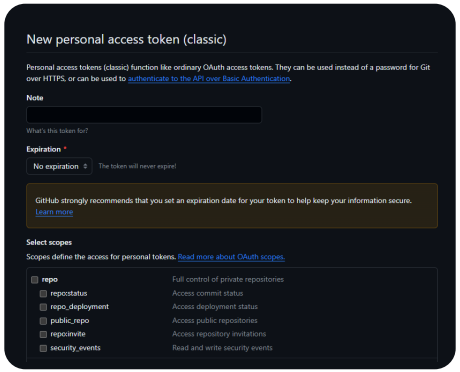
Since 2011, GitHub AI projects grew from 845 to 1.8M in 2023, with a 59.3% spike in 2023. AI project stars tripled from 4M in 2022 to 12.2M in 2023.

Every AI powered system, especially agentic AI systems, heavily utilize NHI to power their access to APIs, data, and more.

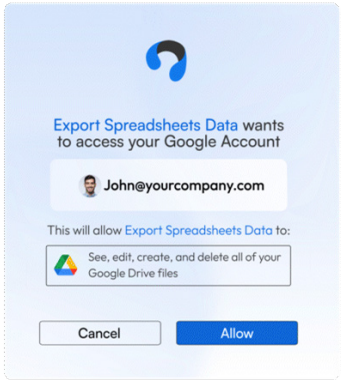


Evolution of NHI Creation

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": "AIDAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:user/division_abc/subdivision_xyz/Bob",
        "CreateDate": "2023-05-24T18:20:17+00:00"
    }
}
```

ISC2 CHAPTER EAST BAY

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.

Th
r
G
c

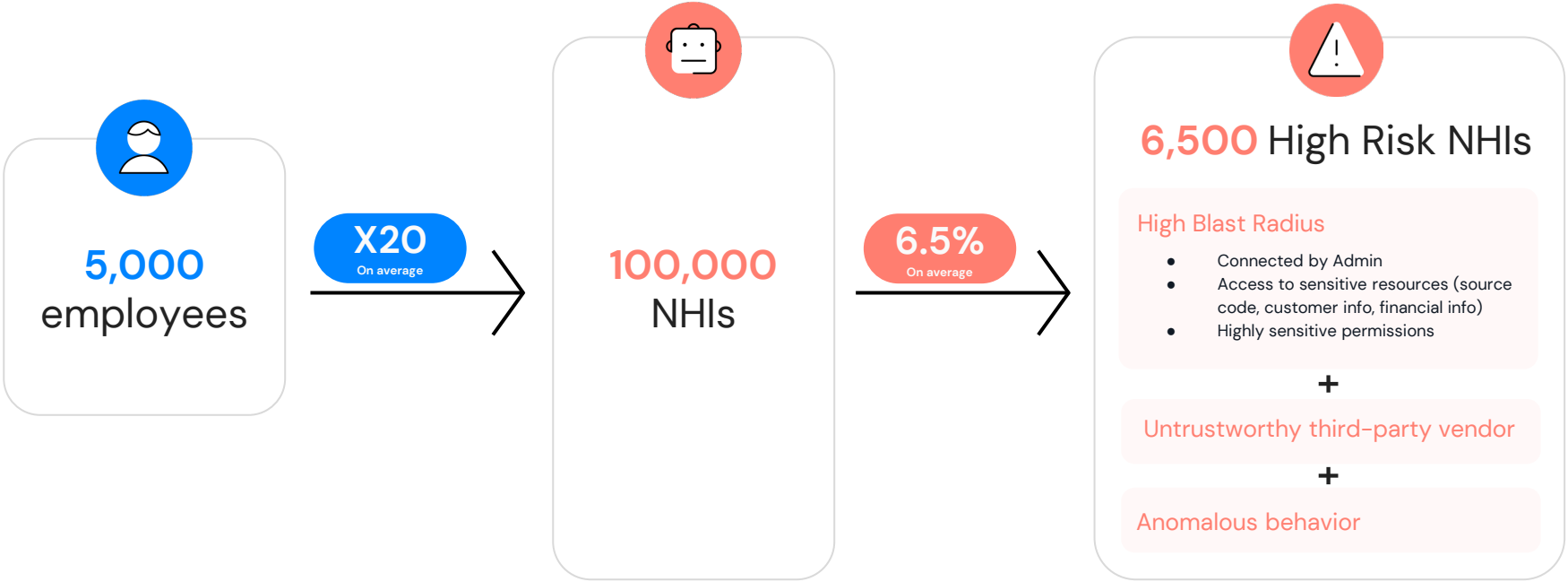
Chinese hackers breach US treasury network, gain access to some files

Third-party cybersecurity provider was compromised after hackers obtained key to override certain systems

It takes 1 vulnerable NHI to breach your organization

BASED ON ASTRIX RESEARCH

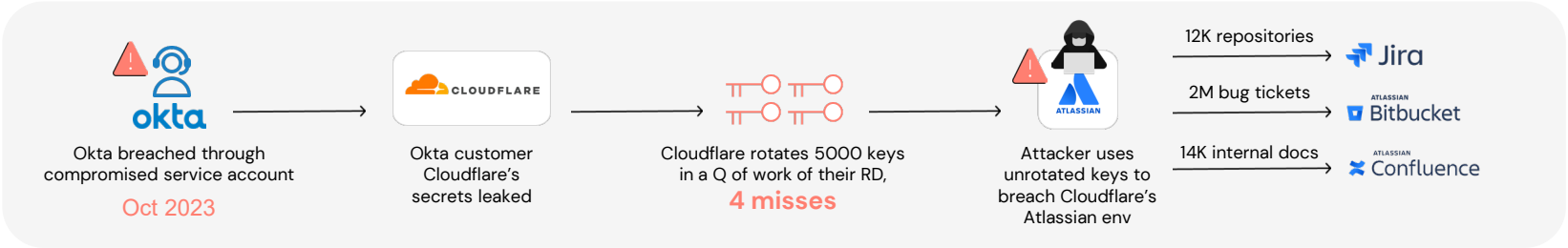
How Big is the NHI Attack Surface



*Based on 20M monitored NHIs

ISC2 CHAPTER EAST BAY

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

Who within an organization is most impacted by the expanded attack surface and complex challenges that NHIs introduce into incident response?

You.

Controlling NHIs is crucial to all security programs

ISC2 CHAPTER EAST BAY

IAM

Extend PAM & IGA programs to NHIs, from inventory and posture to ITDR, lifecycle management and remediation.

*"Astrix strengthens our **identity security program** by providing us with continuous visibility and governance over thousands of NHIs."*

Yaniv Toledano
Global CISO
PAGAYA

AI Security

Gain visibility and security context into all AI agents with access to core environments.

*"With Astrix we can safely leverage the power of AI agents. Astrix is a lighthouse in a sea of **AI integrations.**"*

Gilad Solomon
Head of IT & Security
Guesty

Third-Party Risk

Keep TPRM programs up-to-date with automated discovery of ALL the connected third-party apps and vendors.

*"Astrix helped us catch gaps in our processes, like discovering a vendor that hadn't gone through **TPRM review** during a proof of concept,"*

Kyle Kurdziolek
Director of Cloud Security
BigID

Cloud Security

Secure IAM roles, service principles, and secrets across your cloud production environments and secret managers.

*"Since NHIs are the fabric that connects everything in our **IaaS env.** they're vulnerable security gaps. Astrix is our strategic solution to control and manage these identities."*

Albert Attias
Senior director
workday.

ISC2 CHAPTER EAST BAY

How are you handling NHIs in your organizations

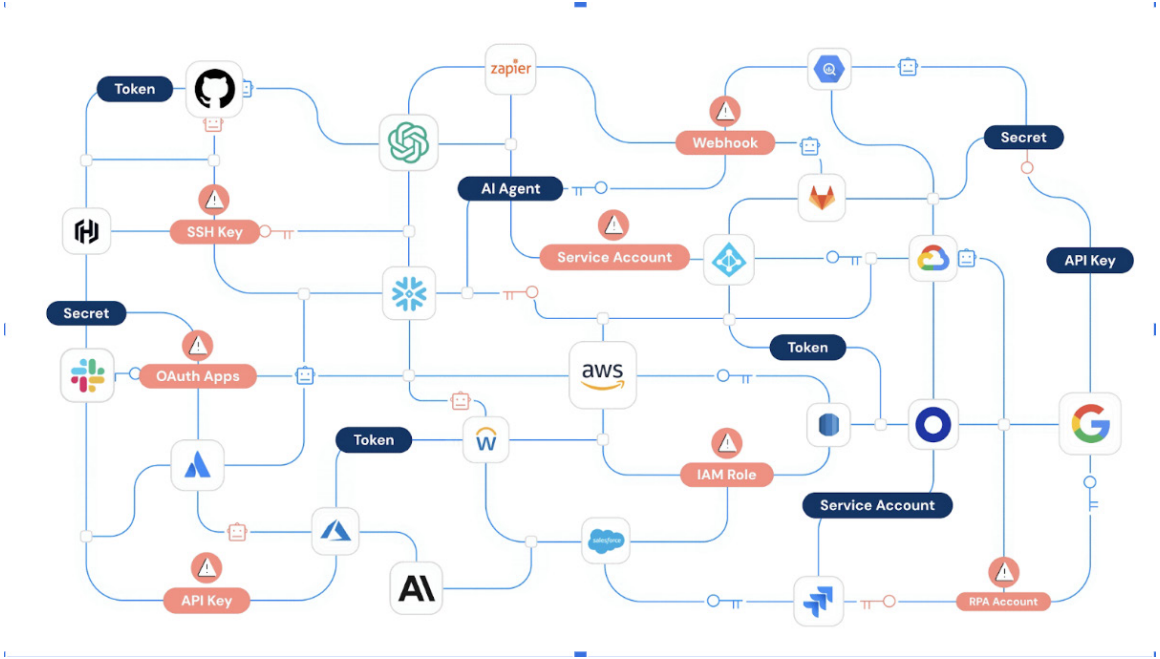
1 in 5

Organizations have experienced a security incident related to NHIs due to:

45% Lack of credential rotation

37% Inadequate monitoring & logging

37% Over-privileged accounts/identities



*Based on a survey of 820 security professionals (by Cloud Security Alliance and Astrix)

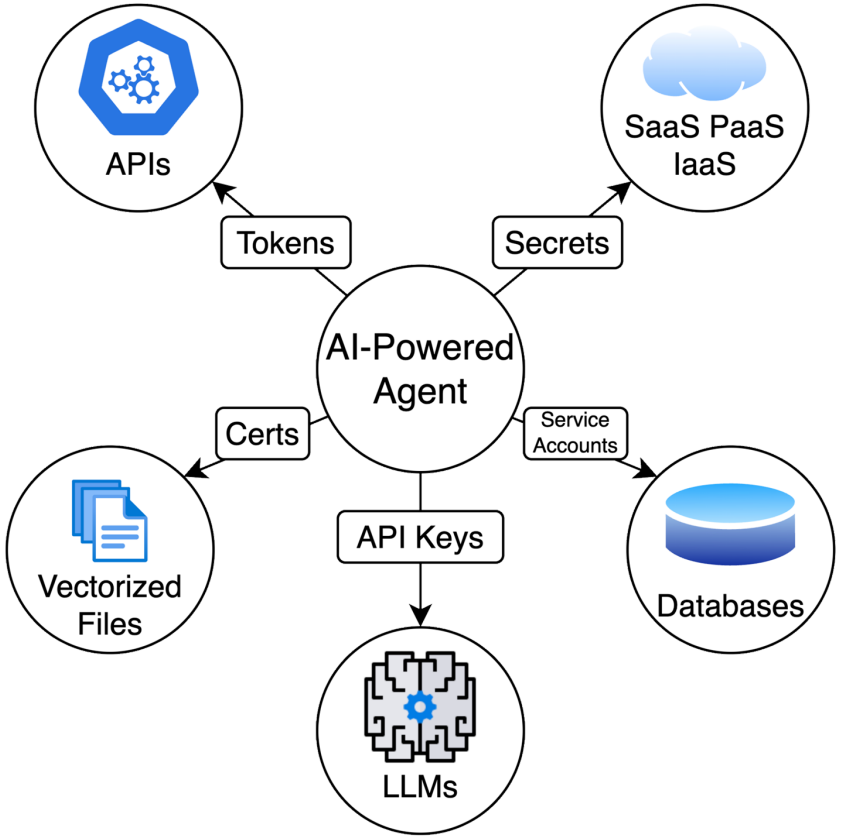
Where Do NHIs Hide? Who Has Them Hidden?

- Application groups create and control the majority of hidden NHIs
  - Worst case they may have them in the applications themselves - hard coded NHIs in the form of API keys, tokens, even passwords
  - Cloud based apps and other IaaS systems will use many of the cloud native secrets solutions, which also tend to be outside the scope of regular processes for most orgs
- Third party integrations also tend to use NHIs and these are often unmanaged
  - Ironically, just about every security, observability, or management tool will be great examples of exactly these sorts of integrations
  - Many folks will create these without knowing (e.g. clicking the allow button), and the access they have is hard to determine
- AI is already becoming a factor here
  - Co-pilots can already borrow the authority of their users through credentials authorized in the form of NHI
  - If you have people making “Custom GPTs” or using any of the computer control systems even experimentally then you have some measure of this

The Role of NHIs in Agentic Systems

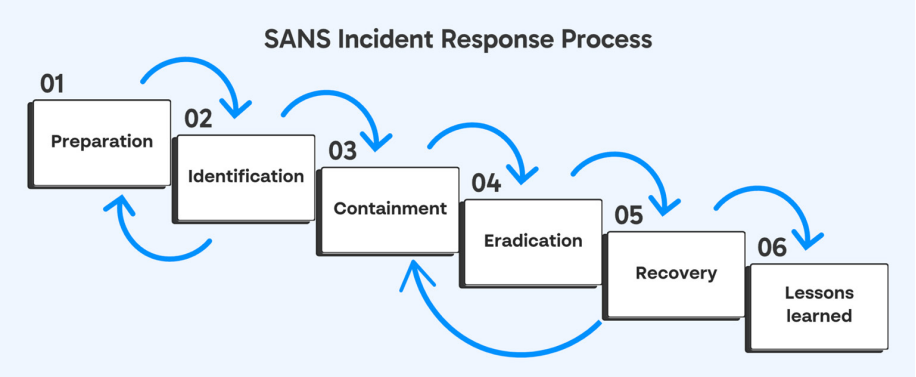
In their "Practices for Governing Agentic AI Systems" paper, OpenAI defines agentic AI systems as those "designed to pursue complex goals with limited direct supervision." The paper emphasizes that these systems "operate by interacting with various components, including traditional IT infrastructures, APIs, and databases, to achieve their objectives." This highlights the composite nature of agentic systems, integrating large language models (LLMs) with conventional IT elements to function autonomously.

NHIs power Agentic AI's access to all the resources the agents need.



Where should CSIRTs integrate NHI management within their current processes to effectively mitigate risks?

Where do NHIs plug in to existing processes?



Ditto for NIST 800-61 R2

1. Prepare For Threats
2. Detect The Threat
3. Analyze/Identify The Threat
4. Contain The Threat
5. Eliminate The Threat
6. Recover And Restore
7. Incident Debrief / Lessons Learned

PURPLESEC

NHIs Impact on CSIRT Processes

1. Prepare For Threats
    - Proactive inventory, posture assessment, governance (ownership assignment, lifecycle management), non-human ITDR - clearly not all of this can be on the backs of the CSIRT

2. Detect The Threat
    - *Timing & Frequency:* Automated processes typically follow predictable schedules. A sudden burst of activity—especially outside expected hours—can indicate compromised NHI credentials.
    - *Volume & Intensity:* Excessive API calls, authentication requests, or data transfers by service accounts or automated systems may signal misuse.
    - *Status Changes:* Anomalous usage patterns, such as repeated failed authentications or logins or access from unfamiliar IP addresses, should trigger further investigation.
    - *Deviation from Access Patterns:* NHIs generally have consistent behavior. Any significant deviation from established baselines (e.g., attempting access to resources they don't typically interact with) may indicate compromise.

When faced with an active incident involving NHIs, what operational and information limitations affect strategies CSIRTs can employ?

NHIs Impact on CSIRT Processes

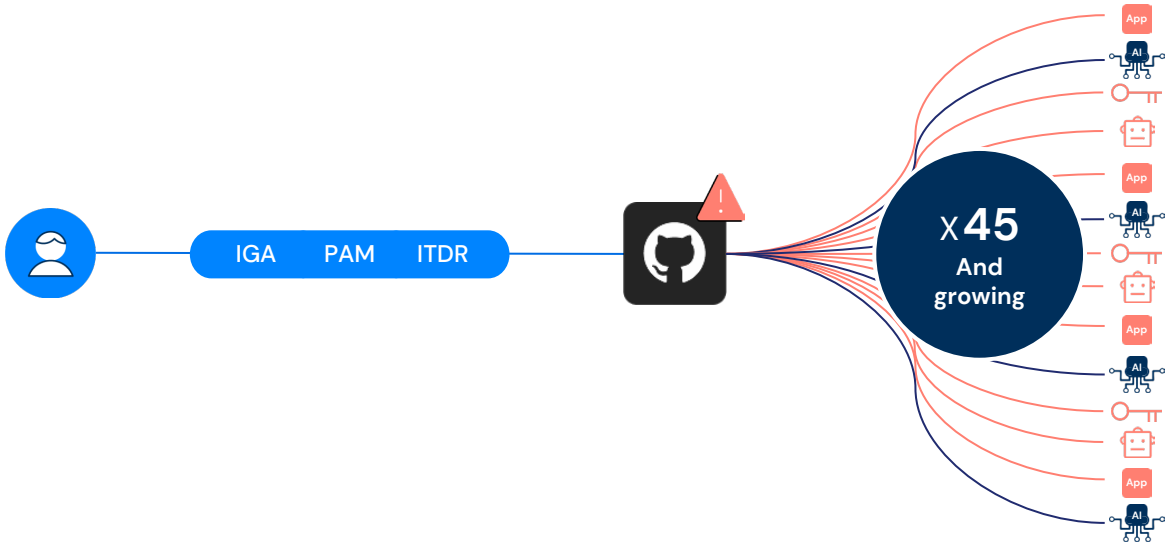
3. Analyze/Identify The Threat
    - This is often the most challenging part with NHI because of the obscurity of much of how these work
        - Bearer tokens won't tell you their source easily
        - Keys are even more opaque
        - IP sources can also shift even if they come from trusted sources
4. Contain The Threat & 5. Eliminate The Threat
    - No person to disable
    - If the NHI is embedded in an application or business process, disabling it is basically stopping the process and rotating may be very difficult
    - If the NHI is a shared credential, this can affect many things
    - Very little insight about preserving forensics for NHIs - no HR/directory

NHIs Impact on CSIRT Processes

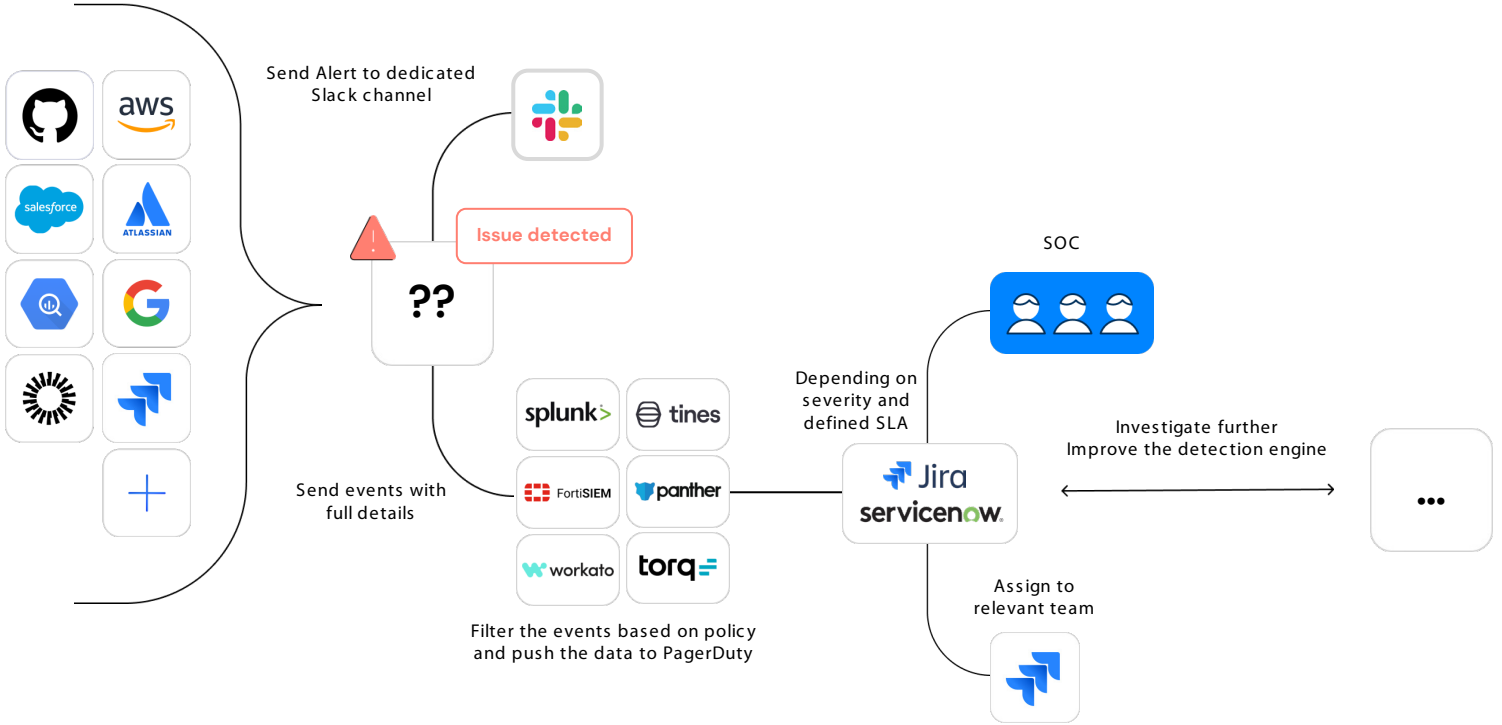
6. Recover And Restore
    - The lack of process and systems can be a positive here - it's easy to generate new NHIs in many instances
    - Distributing new identity information and credentials to all the places affected can be a challenge unless there's a good inventory
7. Incident Debrief / Lessons Learned

NHIs Impact on CSIRT Processes

6. Recover And Restore
    - The lack of process and systems can be a positive here - it's easy to generate new NHIs in many instances
    - Distributing new identity information and credentials to all the places affected can be a challenge unless there's a good inventory



Something that will understand all ***the data*** and do the right thing



Why is it critical to build CSIRT resilience through post-incident reviews and continuous improvement in the context of NHI security?

ISC2 CHAPTER EAST BAY

OWASP Non-Human Identity Top 10

In collaboration with the Astrix Research team!

The Astrix compliance dashboard correlates the organization's security findings with the NHI Top 10 risks

ISC2 CHAPTER EAST BAY

Where Does Your NHI Program Stand?

Do you have a complete and up-to-date inventory of all non-human identities across your systems?	1 No or outdated inventory	2 Partial inventory	3 Complete & updated inventory
Are you confident in your visibility over the activities and access of non-human identities?	1 No visibility	2 Some visibility, but inconsistent	3 Complete & updated inventory
How much of your NHI management is automated? Are you still relying on manual processes?	1 Mostly manual	2 Partial automation	3 Fully automated
Have you implemented automated secret rotation and policy enforcement?	1 No automation	2 Partially automated	3 Fully automated
Are your tools integrated to provide a single view of NHI security, or do you face tool fragmentation?	1 Fragmented' not integrated	2 Some integration, gaps remain	3 Fully integrated
Do you have overlapping solutions that create inefficiencies or gaps in your security posture?	1 Overlapping solutions, causing inefficiencies	2 Some overlap, but manageable	3 No overlaps, streamlined solutions
Can you proactively detect threats and monitor NHI activity across your entire attack surface?	1 Reactive, limited coverage	2 Proactive but not comprehensive	3 Fully proactive and comprehensive
Do you have an established incident response process for NHI-related breaches?	1 No established process	2 Basic process in place	3 Comprehensive, well-established process
Are your NHI processes aligned with compliance regulations and audit requirements?	1 Not aligned with regulations	2 Partially aligned, some gaps	3 Fully aligned with all regulations
How are you managing third-party risk (TPRM) related to non-human identities, particularly across your supply chain?	1 No TPRM process	2 Basic TPRM process in place	3 Fully developed TPRM across the supply

Maturity Levels & Strategic Impact

	CRAWL	WALK	RUN
	10-16 POINTS	17-24 POINTS	25-30 POINTS
SYMPTOMS	• Manual process reliance • Fragmented, overlapping tools • Limited integration • Incomplete NHI inventory • Unmonitored attack surface • Reactive secret scanning and threat detection • Little to no automation for secret rotation and policy enforcement • Lack of coordination and real-time insights	• Partial automation, with manual work still present • Some integration across tools, but fragmentation remains • Incomplete NHI inventory • Gaps in attack surface monitoring • Proactive threat detection but lacking full coverage • Inconsistent automation for secret rotation and policy enforcement • Coordination in place, but insights remain siloed	• Full automation of NHI processes • Complete integration of tools with no fragmentation • Comprehensive NHI inventory with full visibility • Continuous monitoring of the entire attack surface • Advanced threat detection and response in place • Automated secret rotation and policy enforcement • Seamless coordina across all systems
RESULTS	A significant lack of visibility and control over non-human identities leaves critical security gaps. This exposes the organization to higher risks of breaches, operational disruptions, and compliance failures.	Visibility and control over NHIs exist, but gaps remain. Security risks, including breaches and disruptions, persist. Compliance challenges continue, and inefficiencies leave the organization with incomplete protection.	Visibility and control o optimized, minimizing and audit requirement operational disruption benefits from streamli protection across all s

What’s Next on Your NHI Journey?

Turning Insights into Action for a Secure Future

Jonathan Sander

Philosopher Turned Technologist

Astrix

ISC2 CHAPTER EAST BAY