Clutch Launches the NHI Index: A Comprehensive Resource for Securing and Managing Non-Human Identities

The Index is the industry's only centralized resource featuring detailed mapping of hundreds of Non-Human Identities across diverse environments

TEL-AVIV, ISRAEL, October 8, 2024 /EINPresswire.com/ -- Clutch Security, a leading force in Non-Human Identity (NHI) security and management, announced the launch of the NHI Index, a pioneering resource designed to empower security and IT professionals to effectively secure and manage NHIs across diverse environments. The Index features a comprehensive NHI catalog along with essential resources and practical guidance for securing and managing NHIs. By leveraging the NHI Index, security teams can immediately begin implementing changes such as mapping audit sources, adopting ephemeral identities, and minimizing exposure to static NHIs, effectively transforming how organizations protect their digital infrastructure.

> The NHI Index helps teams by mapping audit sources, showing exactly where to look for logs, and ensuring nothing slips through the cracks. Its best practices are key to reducing risk"
>
> *Adam Marre, CISO at Arctic Wolf*

"We identified a critical gap in the understanding and management of NHIs," said Ofir Har-Chen, Co-founder and CEO of Clutch. "The NHI Index is our response to the growing challenges of securing NHIs in today's fragmented enterprise environments. It not only equips security professionals with practical tools and insights but also highlights just how prevalent and integral NHIs are across cloud and SaaS technologies. In many cases, their use is mandatory, embedded within the very services enterprises rely on. By providing this resource, we aim to shed light on the scale of NHI usage and the urgent need for effective management and security. We encourage the community to engage with the NHI Index, share insights, and stay informed on the latest developments in NHI security."

Understanding NHIs and Their Challenges

NHIs refer to digital credentials or entities used by machines, applications, and automated processes to authenticate and perform programmatic operations on various resources. In modern enterprise environments, NHIs are growing at an unprecedented rate, now outnumbering human identities by at least 45:1. This rapid expansion introduces serious security challenges, as NHIs are often dispersed across cloud, SaaS, and on-premises systems. Unlike human identities, they typically lack centralized controls, and frequently hold excessive privileges, which makes them prime targets for exploitation.

Without effective oversight and lifecycle management, NHIs often become stale, inactive, or over-privileged, significantly expanding an organization's attack surface. For instance, many cloud-based NHIs use less than 5% of their assigned permissions, while over 80% remain inactive—creating prime opportunities for privilege exploitation. These risks are not theoretical; recent SEC 8-K filings, including a high-profile case involving Dropbox, have directly linked NHI vulnerabilities to serious security breaches.

Introducing the NHI Index

The NHI Index is a comprehensive resource designed to address these challenges head-on. It provides security and IT professionals with essential tools and insights to navigate the challenges of securing NHIs across diverse and fragmented environments, such as cloud, SaaS, and on-premises systems. More than a comprehensive catalog, the NHI Index highlights the widespread prevalence of NHIs—often an inherent part of modern technologies—and the necessity of managing and securing them. By offering detailed guidance and actionable steps, the NHI Index empowers professionals to proactively secure NHIs, contributing to a more secure and resilient enterprise landscape.

"The sheer volume of NHIs across cloud, SaaS, and on-prem systems creates real challenges," said Adam Marre, CISO at Arctic Wolf. "The NHI Index helps teams by mapping audit sources, showing exactly where to look for logs, and ensuring nothing slips through the cracks. Its best practices guide the shift from static, long-lived identities to ephemeral ones, which is key to reducing risk and enhancing security."

Key Features of the NHI Index Include:

- Detailed NHI Catalog: An exhaustive list of NHIs used across major cloud providers, code repositories, CI/CD solutions, and SaaS applications. Each entry includes critical details such as service names, environments, types of NHIs, and key security features like audit logs, IP allowlists/denylists, and set expiry options.
- Essential Resources for Reducing NHI Attack Surface: Practical guides on establishing OpenID Connect (OIDC) between cloud service providers (CSPs) and version control systems, as well as enabling inter-cloud connectivity using ephemeral keys. These resources, including Terraform files and step-by-step tutorials, help organizations transition from static, long-lived NHIs to ephemeral ones—drastically reducing their attack surface and enhancing their security posture.

The index maps hundreds of NHIs, including over 350 distinct types used by more than 480 cloud services, code repositories, CI/CD solutions, and SaaS applications. While many assume that cloud environments primarily rely on a small set of NHIs, mostly confined to IAM services, the NHI Index reveals a much more intricate landscape, identifying a significant number of NHIs inherent within cloud services themselves, and which are essential for their operation. In total, 144 distinct cloud NHIs were uncovered across over 400 different cloud services.

Unsurprisingly, the most prominent NHIs used within Cloud Providers are those within the Cloud Provider's Identity Access Management (IAM) service, accounting for 65% of NHIs in Amazon Web Services (AWS) and 67% in Google Cloud Platform (GCP). In AWS, 80% of NHIs are audited through CloudTrail, while nearly all GCP NHIs are monitored via Cloud Audit Logs. In Microsoft Azure services, the most prevalent NHIs are those inherent to Entra ID, comprising 33% of the NHIs mapped to Azure services, with 86% audited through Azure Activity Logs.

"The NHI Index is a great resource to drive awareness of the broad range of identities and service credentials that exist," Said Armon Dadgar, Co-founder and CTO of HashiCorp. "One of the biggest challenges facing organizations is secret sprawl and lack of a cohesive approach to managing NHIs. Helping security teams have visibility and control is crucial to reduce the risks inherent to sprawl."

The NHI Index is now live and available at: www.non-human.id

About Clutch
Clutch is the industry's first Universal Non-Human Identity Security Platform, purpose-built for the enterprise. It offers complete visibility through a contextualized inventory, laying the foundation for robust NHI security—including lifecycle governance, risk and posture management, and real-time detection and response. Clutch empowers security teams to extend the same Zero Trust approach they use for their human identities to their Non-Human Identities, by continuously monitoring and validating NHI usage, and facilitating the transition to ephemeral identities. This proactive strategy eliminates security gaps, reduces operational overhead, and enables teams to operate independently and efficiently, without friction.

Tom Sadon
Clutch Security
tom@clutch.security
Visit us on social media:
LinkedIn
Instagram

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.