SamurAI XDR

Identity Management in the Physical and Digital Worlds

Insights from Samurai XDR & NTT Security Holdings

July 30, 2024

Speakers

Paul Asdagi

Senior Director, Product Management
Samurai XDR

NTT Security Holdings

Jeremy Nichols

Director
Global Threat Intelligence Center

NTT Security Holdings

Erin Haynes

Senior Marketing Specialist
NTT Security Holdings

SamurAI XDR

Overview

- The identity threat problem
- Who is being targeted?
- How are hackers breaching identity?
- Digital identities overview in a digital world
- IAM and Cybersecurity
- Intelligence Insights
- Q&A

The Identity Threat Problem

For threat actors, gaining access by compromising credentials removes the need to find more creative ways into a victim's network.

- Exploiting identities requires persistence, but
- It is simpler than exploiting system vulnerabilities

In 2024 84% of identity stakeholders had experienced an incident, up from 68% in 2023

43% of respondents said MFA would have prevented incidents [1]

In 2022, organizations were, on average, using 130 SaaS applications [2]

The average **small business** with under 500 employees used 172 applications in 2023, adding 4.4 new applications every 30 days!

Almost a third of Americans have been victims of identity theft.

[1] Identity Defined Security Alliance
[2] statista.com

Who is being targeted?

Organizations of all sizes, including vendors are being targeted:

- **AT&T and Ticketmaster** both became victims of a breach of the identities of **Snowflake** customers after threat actors compromised contractors working for **Snowflake**. (Subsequently, Snowflake has made MFA mandatory)
- **Okta** had a customer support system exposed the identity data of customers. All users of Okta's Workforce Identity Cloud (WIC) and Customer Identity Solutions (CIS) were impacted
- **Medibank** an Australian Health Insurer was compromised after an attacker stole credentials which were synced (via the browser) to the personal computer of a contractor. Subsequently using these credentials to exfiltrate PII (520GB, 9 Million persons), even after an alert was tripped.
- **Equifax** (2017) – hackers gained access using default login information. **Equifax** was relying on a simple pin for a password. 145 million records were at risk
- **Zoom** has been an ongoing victim of credential stuffing attacks

https://www.tyntec.com/blogs/examples-breaches-multifactor-authentication-could-have-prevented/

How Are Threat Actors Breaching Identity

Cybercriminals are always evolving their strategies, but some common forms of attack have become their mainstays in their arsenal:

- **Credential stuffing** – attackers use botnets to try usernames and passwords from databases of compromised identities across multiple potential victims
- **Password spraying** – attackers systematically try commonly used usernames and passwords to try to gain access to systems
- **Phishing** – attackers target users through email, text messages and other means to trick them into providing credentials or revealing other sensitive information
- **Man in the Middle Attacks** – an adversary intercepts communications, such as login sequences and syphons off credentials

Digital Identities

A **digital identity** is typically defined as a one-to-one relationship between a human and their digital presence

A **digital presence** can consist of:

- multiple accounts
- credentials
- entitlements associated with an individual.

A **digital ID** may be a passport, license, or other printed credential.

A **user** is an actual person operating a resource to which the **digital identity** is assigned (can be a 1: many relationship)

There are two main types of digital identities:

human – (private, partner, employee, customer) allow human users to be assigned access or privileges within a network

machine – endpoints (server, desktop..), IoT, applications, etc

Digital identities can also be assigned to an account

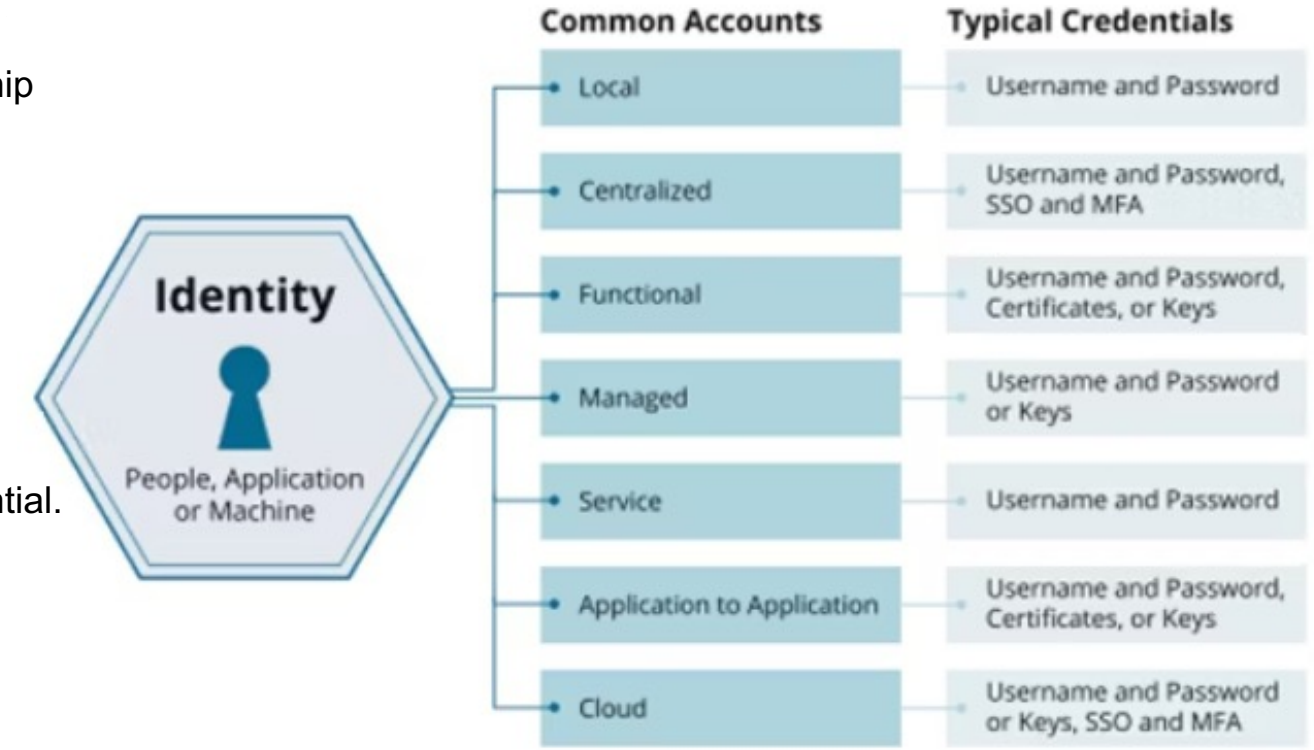
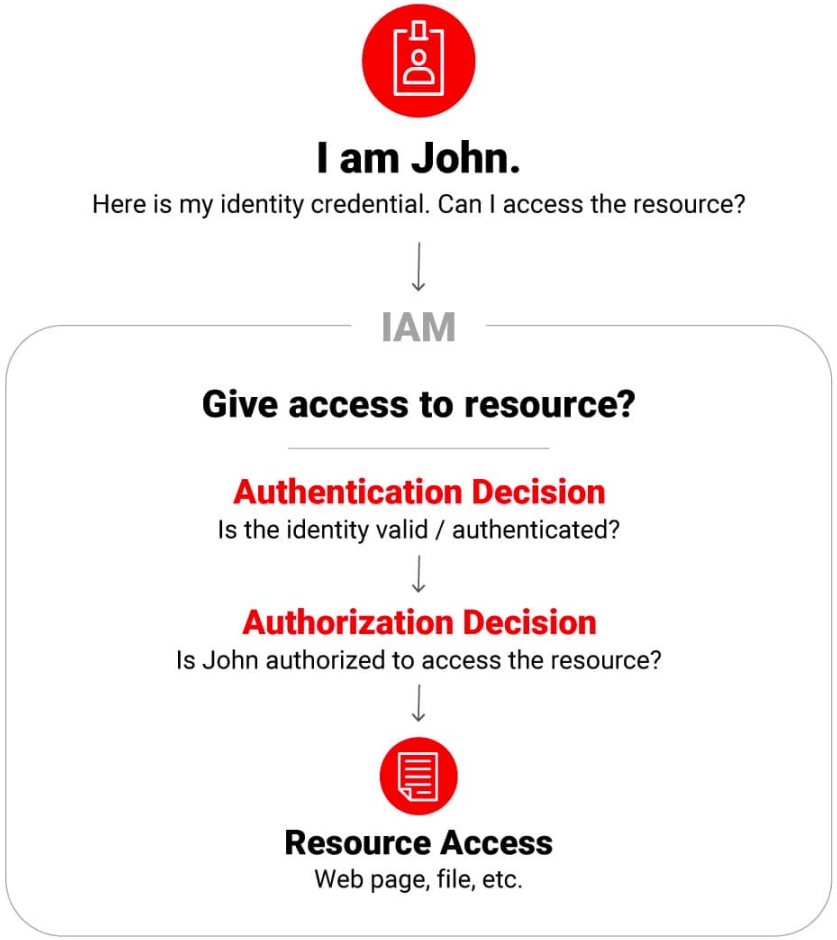


Figure 1: The relationship between identities, accounts, and credentials.(Haber & Rolls, Identity Attack Vectors, 2022)

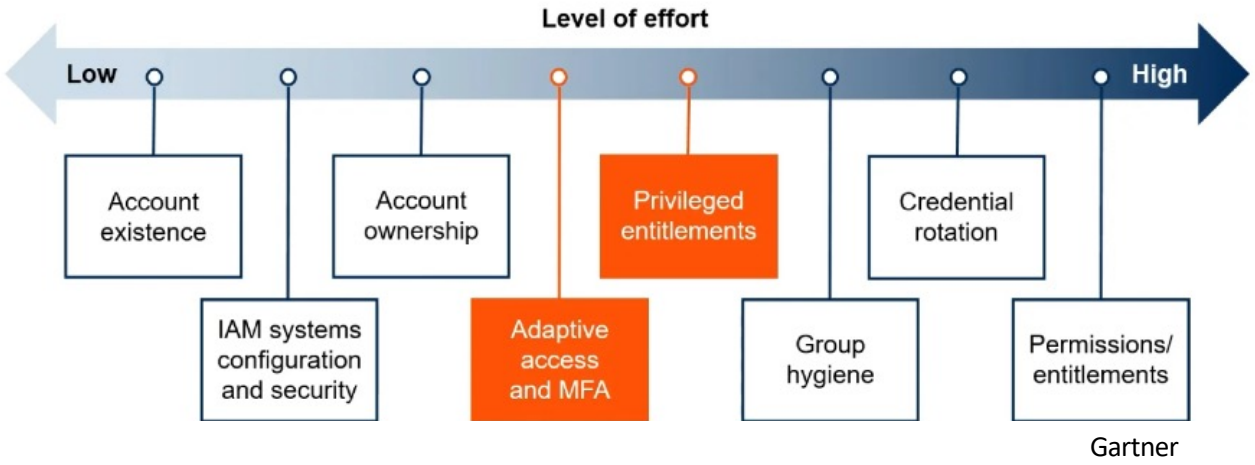
Identification and Authorization in the Digital World

- The requirements we have for managing identity in the digital world in many ways mirror the systems of identity management we have in the physical world
- IAM, provides a framework of systems, policies and procedures
- IAM consists of **five** functions



IAM Journey

- IAM solutions provide us with centralized visibility
- **Correlate** IAM events with applications and infrastructure to generate an **analytics baseline**
- Analytics helps determine good versus bad!
- What about the other events that IAM does not see?



Gartner

IAM supporting cybersecurity

IAM plays a critical role in cybersecurity for several reasons:

- ✓ Protecting Sensitive Data
- ✓ Preventing Unauthorized Access
- ✓ Complying with Regulations
- ✓ Enhancing User Experience
- ✓ Centralized Management and Visibility
- ✓ Protecting Against Credential-based Attacks

Shifts in workplace habits and the adoption of decentralized systems are bringing security and identity closer together.

"Organizations should entrench identity management as part of their cybersecurity foundation…
It [IAM] is the control plane and foundation of cyber security—this is where focus needs to be."

- Gartner

Identity Threat Detection and Response (ITDR) (IAM and XDR) – *future trend*

Integrate

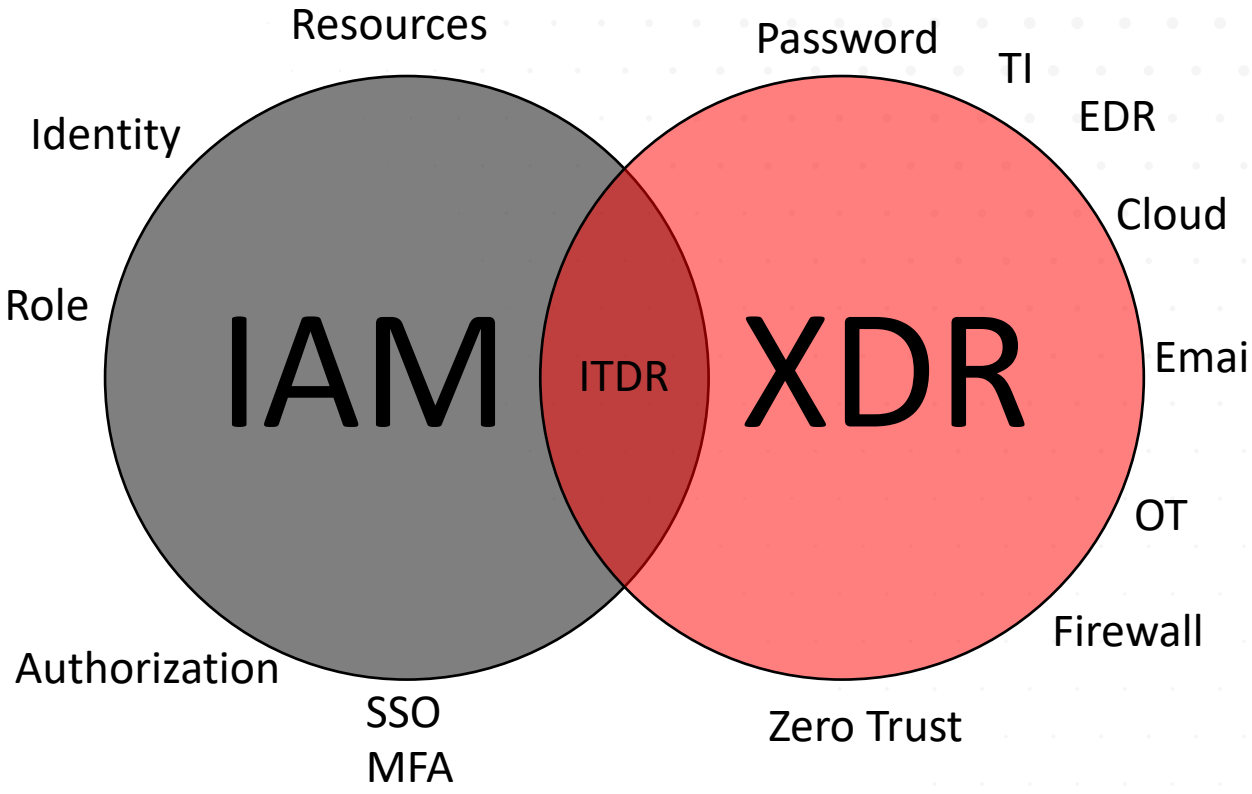
- IAM integrated into all your apps, to remove blind spots
- Use Password Managers where not possible

Contextualize

- XDR to receive telemetry from ALL your Apps – IAM, Password Managers, EUBA, endpoints, edge devices, cloud and Threat Intelligence

Prioritize and Respond

- With full context of threats from all these signals, filter and prioritize so you can respond quickly



Minimize the gap attackers exploit between IAM and other systems.

How to Protect Against Identity Threats

There are a few key measures that organizations should take to protect against identity threats:

- **Enforcing strong passwords** – Without enforcement of strong passwords, users have a tendency to use passwords that are easy to guess
- **Follow the principle of least privilege** – only give users access to the data and systems they need. This way, if credentials are compromised, the blast radius of the attack is minimized
- **MFA** – implementing MFA makes password cracking harder by adding another layer of security. Even if a password is stolen, in most cases the secondary security layer remains intact
- **Security awareness training** - humans are the front line when it comes to many identity threats. By teaching your users to spot phishing attacks and resist social engineering you can turn them into better defenders
- **Password Managers** – Using a password manager prevents password reuse and makes it easier for users to use strong passwords by removing the need to remember passwords
- **Zero Trust** – by implementing zero trust it becomes harder for attackers to move laterally (good for mobile workforce)
- **IAM integrated solutions** – don't let you IAM be an island. Connect you IAM to your security toolset

Identity Cyber Threats

- Phishing
- Credential Stuffing
- Password Spraying
- Social Engineering
- Man in the Middle
- MFA Fatigue

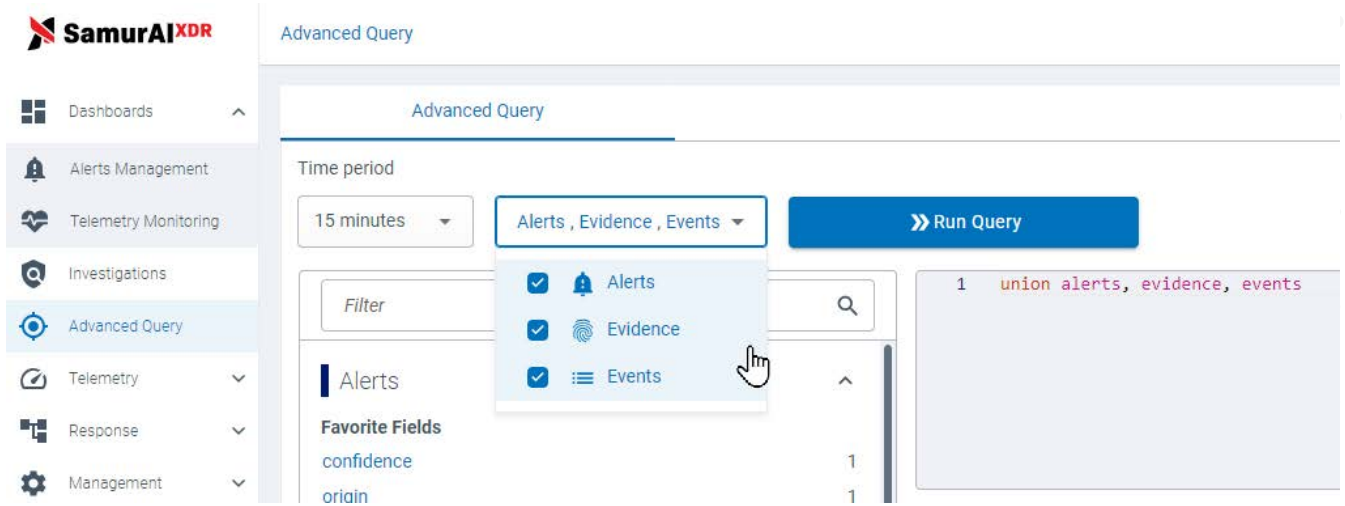
SaaS & Cloud Attacks

"Through 2025, 99% of cloud security failures will be the customer's fault." – Gartner, 'Is the Cloud Secure?'

- **LastPass** – Valid employee credentials and keys used to access third-party cloud-based storage
- **PayPal** – Credential stuffing attack allowed access to user data
- **ChatGPT** – Exploitation of a third-party open-source library
- **AT&T** – Access to Customer Proprietary Network Information gained through vendor systems
- **Salesforce** – Misconfiguration that allowed unauthenticated user access to customer data
- **Dragos** – Compromised personal email of new employee, allowing limited access to 'general use data' in SharePoint
- **MOVEit** – Exploitation of critical SQL injection vulnerability in web application
- **Okta** (Sept 23) – Social engineering of super administration accounts
- **Okta** (Oct 23) – Stolen credentials for case support management system, resulting in suspicious activity of customers such as 1Password
- **Microsoft Cloud** – Forged authentication tokens to access multiple organizations

Value of Identity Provider Logging

- Unusual / impossible logins
- Suspicious source logins
- Multi-factor login changes
- Push notification anomalies
- Unauthorized resource access attempts



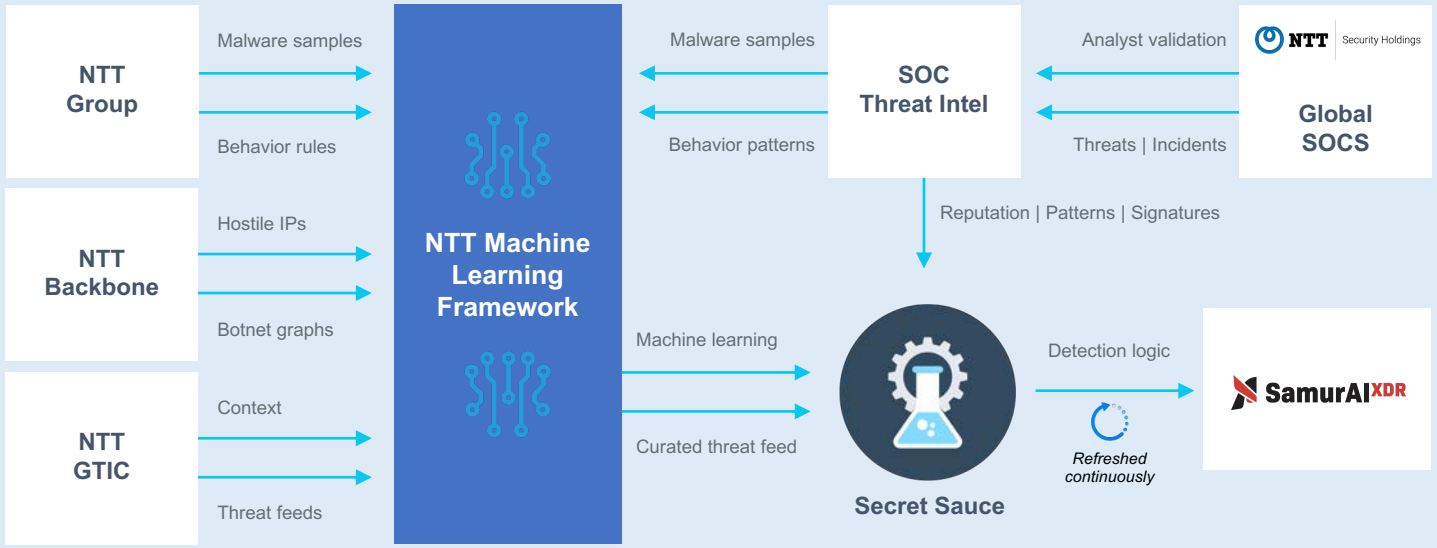
SamurAI XDR

Enrichment & Detections

Threat detection analysis engines use a powerful combination of the following:

- Global data sources via NTT's backbone
- World-class security analysts identifying emerging threats and triaging incident escalations (Samurai MDR, WideAngle)
- NTT GTIC's rich threat research
- Extensive NTT Group collaborative ecosystem of threat feeds combining public/commercial and proprietary sources

Combining global scale with local context for real-time detection and emerging threats



Enhancing Context with NTT Global Threat Intelligence

Collaboration and intelligence sharing platform

Contributing Partners

Microsoft · Recorded Future · FIRST · CYBER THREAT ALLIANCE · VirusTotal · JOINT CYBER DEFENSE COLLABORATIVE

NTT Global Threat Intelligence Platform

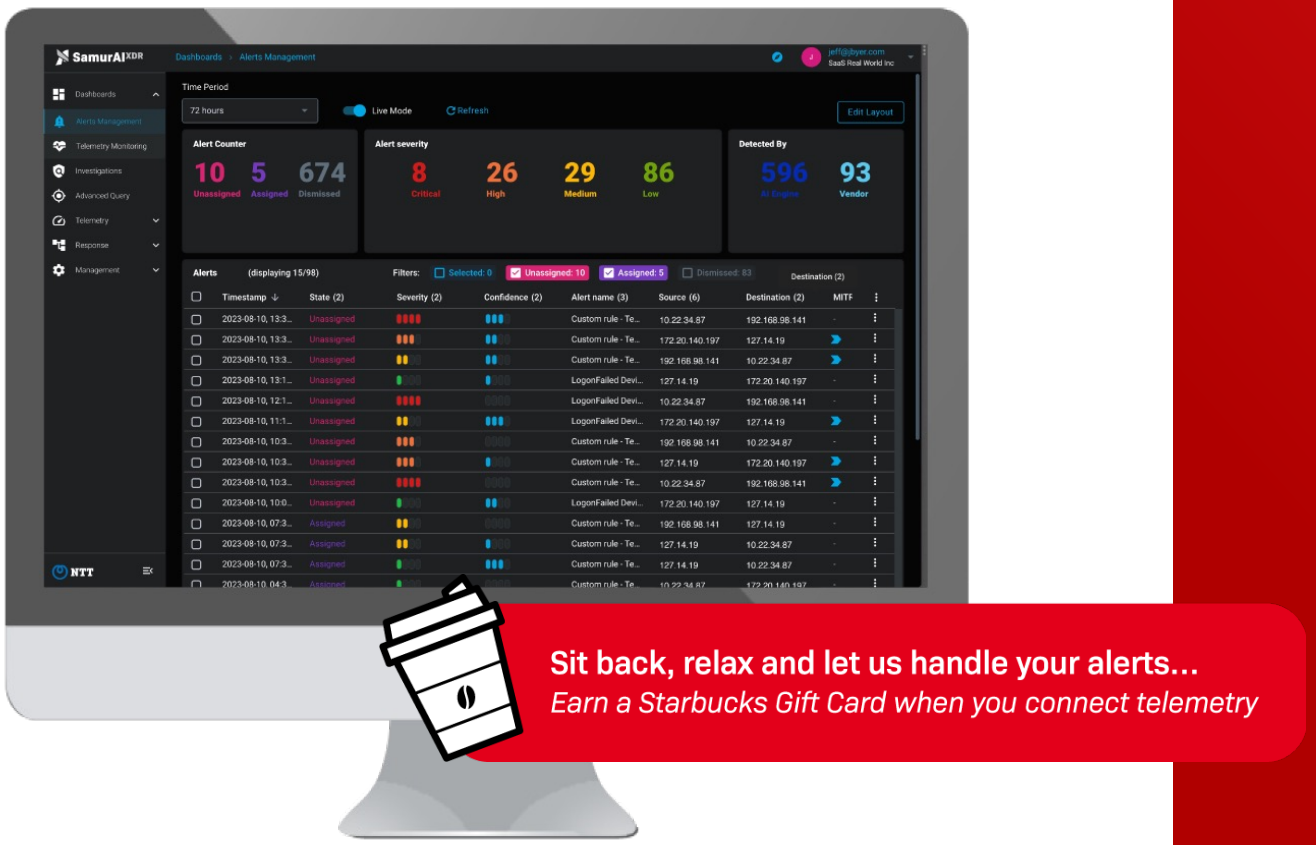
NTT Global Networks
NTT Research
NTT CERT

NTT
Global Honeypot Network
Security Holdings GTIC
Security Holdings SOC
High Confidence Data

Samurai XDR SaaS

Free 30 Day Trial, No Credit Card Required

Go to **samurai.security.ntt** to sign up



Sit back, relax and let us handle your alerts...

Earn a Starbucks Gift Card when you connect telemetry

Recent Integrations

Okta Workforce

1Password for Business

Coming Soon

TrendMicro ApexOne

Microsoft Azure Sentinel

NTT Security Holdings

SamurAIXDR

SamurAI XDR

Q&A

SamurAI XDR

Thank you

samurai.security.ntt