SamurAI XDR

The Future of MSP Security: Embracing XDR Solutions

July 3, 2024

Speakers

Paul Asdagi

Senior Director, Product Management
NTT Security Holdings

Erin Haynes

Senior Marketing Specialist
NTT Security Holdings

SamurAI XDR

Overview

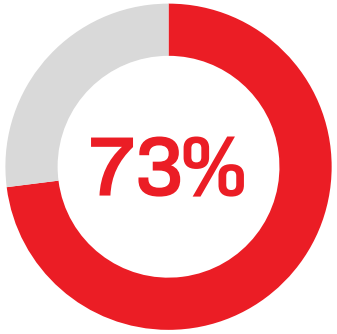
- **Introduction** to XDR
- Current **Threat Landscape**
- **Benefits** of XDR for MSP’s
- **Implementing** Samurai XDR

XDR: Solving the Detection Problem

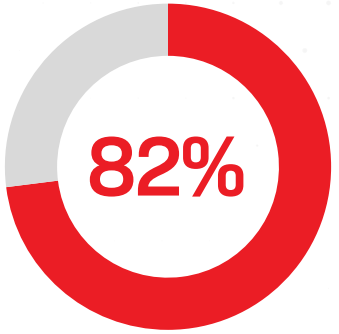
Longstanding solutions—including vulnerability management, SIEM, and SOAR, among others—were too expensive, too hard to deploy, configure, and manage.[1]	XDR provides a path out of the detection and response problem that enterprises increasingly face, by providing a unified threat detection, investigation and response solution.
Security Analysts are on average unable to respond to 48% of alerts. This is up from 41% in 2021.[2]	"XDR, is likely to become the largest single market segment by revenue in enterprise cybersecurity operations (SecOps) by the end of the decade."[1]
No single pane of glass across disparate tools prevents effective correlation.	52% of organizations believe that SecOps is more difficult today than 2 years ago.[3]

[1] Omdia, Sep 2022
[2] 451 Research
[3] ESG : SOC Modernization and the Role of XDR - 2023

Important Stats



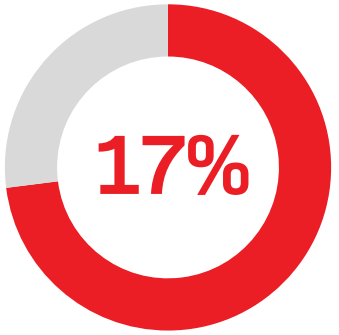
of SMBs experiencing a cyberattack, data breach, or both within a 12-month period



of ransomware attacks were against companies with fewer than 1,000 employees

$3M

Data breaches cost SMBs an average of over $3 million per incident



of small businesses have cyber insurance

Current Threat Landscape

- Growing Importance of IoT Security
- Expansion of Remote Work and Cybersecurity Implications
- Evolution of Phishing Attacks - Use of AI and Improved, Professionalized, and Scaled Phishing
- Taking Advantage of Trust: increasing numbers of breaches occurring through the use of legitimate credentials
- Edge Device Abuse
- Cybersecurity Skills Gap and Education
- Supply chain attacks

Challenges for MSPs

- MSPs have the responsibility to address their clients IT needs, this now, more than ever, **includes Cybersecurity**
- MSPs are under pressure to deliver outcomes, minimize churn while still being profitable (Life time value)
- MSPs are affected by the same issues as their clients, such as, the cost of hiring, training and retaining key resources
- MSPs must Monitor and respond to ALL threats across ALL their clients (environments with different ecosystems) ALL the time
- MSPs need multiple tool sets across clients, creating complexity and inefficiency
- MSPs are worst hit by the prevalence of Ransomware affecting their clients

Introduction to XDR

"XDRs **unify** your security tools into a more **integrated** approach.

They [XDR] **combine** security log data with external **contextual** information in a data analytics engine to provide a common **detection**, **response** and **remediation** capability"

Key Attributes

Centralization of normalized data, the XDR vendors' integration ecosystem.

Correlation of security data and alerts into incidents

A centralized incident response capability that can **change the state** of individual security products as part of incident response

Introduction to XDR

"XDRs **unify** your security tools into a more **integrated** approach.

They [XDR] **combine** security log data with external **contextual** information in a data analytics engine to provide a common detection, response and remediation capability"

Where are you?

XDR Maturity Levels

Level 1	Level 2	Level 3
Data Integration	**Process integration**	**Risk visibility**
• SIEM	• SOAR	• Attack surface management
• Sec. analytics/ML	• Workflow	• Configuration management
• Threat intel	• Playbooks	• Vulnerability management
• Alert management	• Community	• Weighted guidance next steps to secure
• Incident response		• Metrics to compare

Gartner

MSP Alliance – 2024 Predictions

"**XDR Upgrade:** For those of you still using (or selling) legacy anti-virus and firewall technologies, it's time to upgrade your tool belt.

For MSPs, it is considered a current best practice to have some form of XDR technology deployed internally in your MSP practice. For customers, XDR would also be considered a modern-day best practice for any sized organization.

https://mspalliance.com/whats-in-store-for-msps-in-2024/

Benefits of XDR for MSP's

Unified Security: XDR integrates multiple security products into a single platform, Unification helps MSPs detect and respond to threats more efficiently, helps close detection gaps.

Automated Responses: XDR solutions, such as Samurai XDR, often include automation capabilities, which can significantly reduce the workload on security teams by automating threat detection and response processes.

Improved Threat Detection: By correlating data from different sources, XDR enhances the accuracy of threat detection, allowing MSPs to identify and mitigate threats more quickly

Cost-Effective: XDR can be more cost-effective than using multiple, disparate security solutions. It reduces the need for multiple licenses and simplifies management, which can lower overall costs. The more you add, the lower the cost.

Scalability: XDR solutions are flexible and can be scaled up or down based on the needs of the MSP's clients.

Enhanced Visibility: With a unified view of security events, MSPs gain better visibility into their clients' security posture, enabling more proactive threat hunting and thorough investigations. Features like multi tenancy or Kings view provide this visibility across all accounts.

Revenue Rewards: With XDR, service providers can realize revenue with rapid onboarding, and depending on provider, discounts based on increased customer / client base. Supports services growth such as Managed XDR.

Implementing XDR as an MSP

XDR Telemetry: ensure that your chosen partner for XDR has the supported integrations that your clients or customers have (or / and where you can request one to be created at no cost!)

Existing Tools: Ensure the XDR works with YOUR current tool sets, or work with your partner to create a roadmap to support your key systems

Assess and Orient: Have a conversation with your customer about their digital assets, what you monitor and manage today and look to close any gaps for devices not yet monitored. More signals equals better protection!

Educate: Train your team on how to use your XDR, maybe they are new to SecOps if you are moving into providing more Managed XDR type services

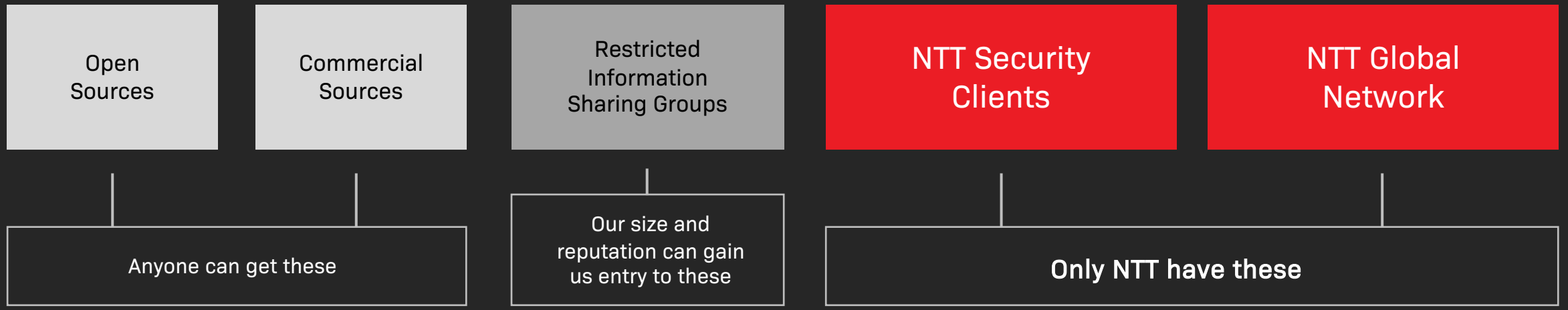
Automate: Leverage the automation capabilities of XDR to reduce manual workload and improve response times

Collaborate: Consider allowing a more transparent view into your service, such as co- manage. XDR is a SaaS that should allow your customers to either be informed or lean in and help if they can.

Support: Before you choose an XDR partner, ask about their program, do they provide training, are there commercial rewards, incentives, etc.

NTT Threat Intelligence

Our threat intelligence is enhanced from what we learn from our own client base. This provides higher quality indicators than publicly available information. Curated intelligence, validated by experts.



- Over **40%** coverage of the Internet
- Analyze **10TB** of data every day
- Validate **1100** security incidents a month
- Analyze **275K** events per second
- Deliver **99%** accuracy

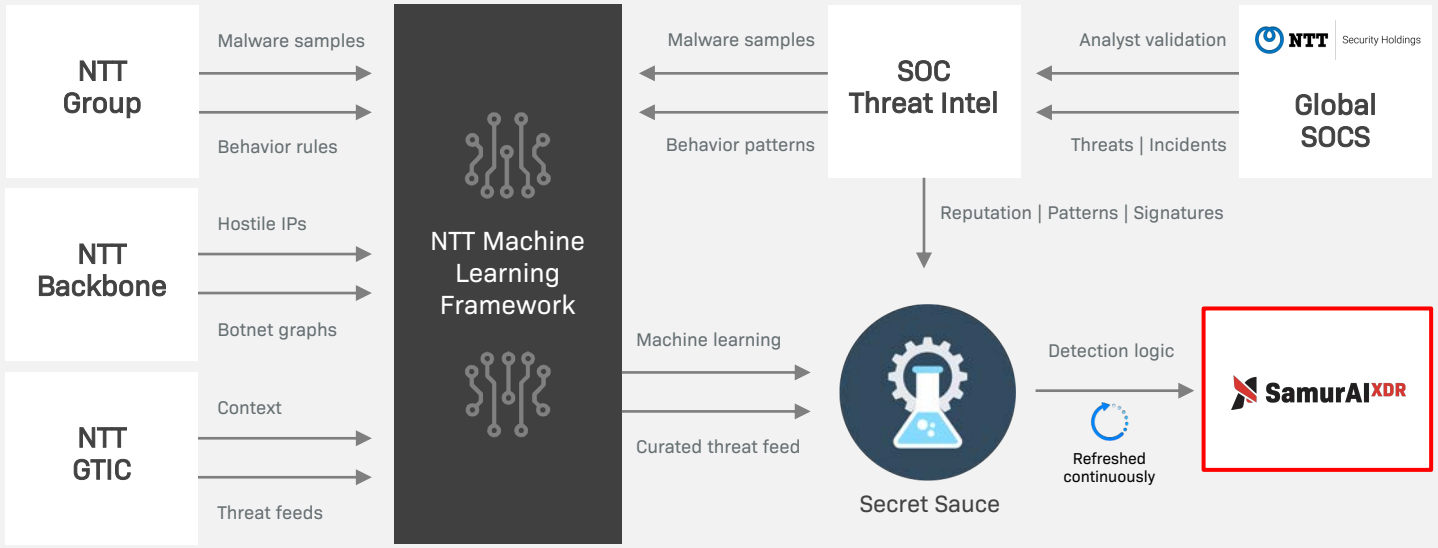
SamurAI XDR

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

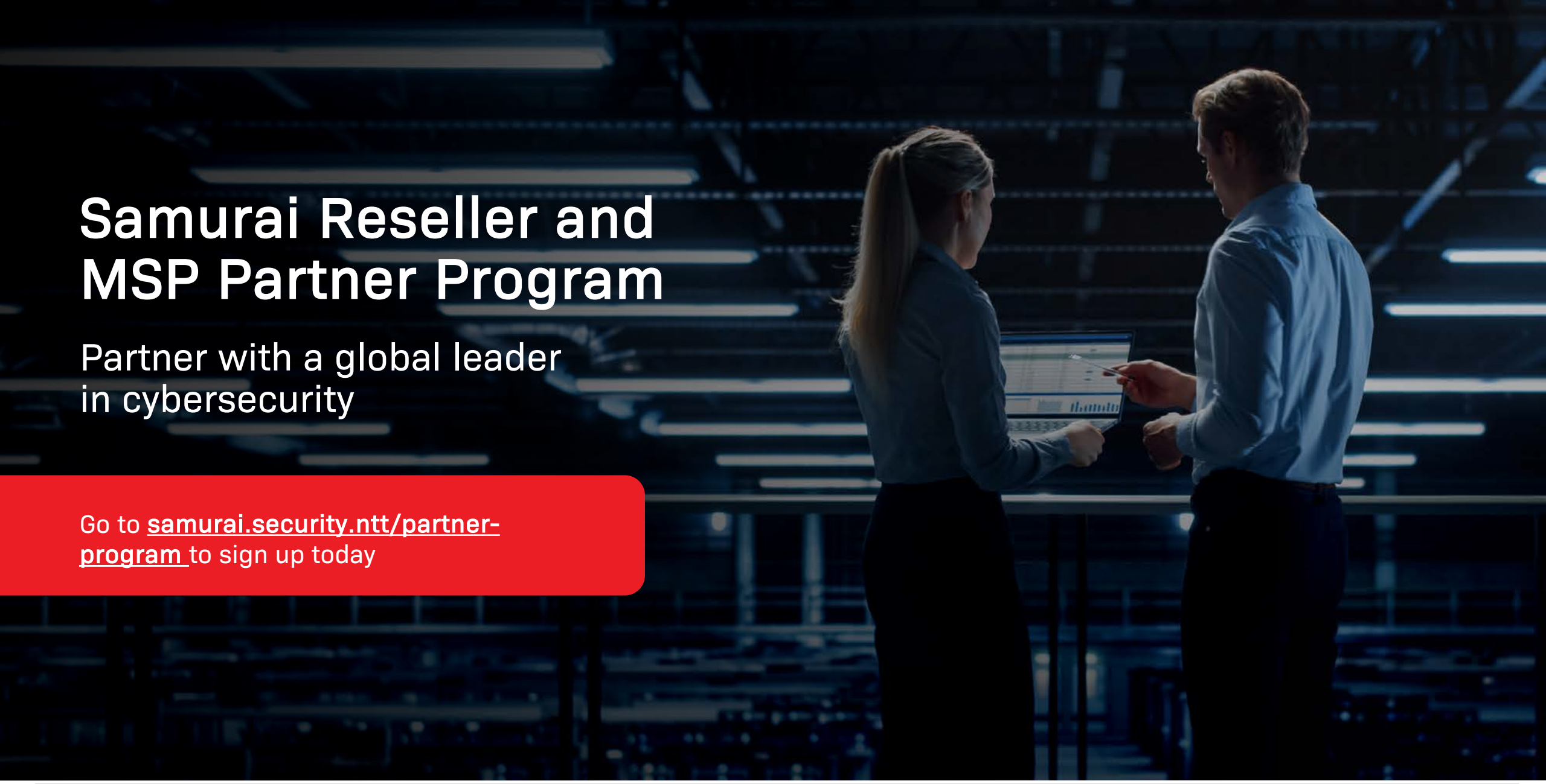
Why Samurai XDR for MSPs?

Trusted Brand

- NTT Security Holdings is wholly owned subsidiary of NTT Group
- Ranked as one the Top 5 (Tier-1) ISPs in the world (owned and operated)
- Consolidated revenues of $80Bn
- Research and development (>2000 employees)
- 40% Internet coverage

Samurai for MSPs

- Open XDR – vendor agnostic ecosystem
- Enterprise grade Threat Intelligence
- Affordable price point $



Samurai Reseller and MSP Partner Program

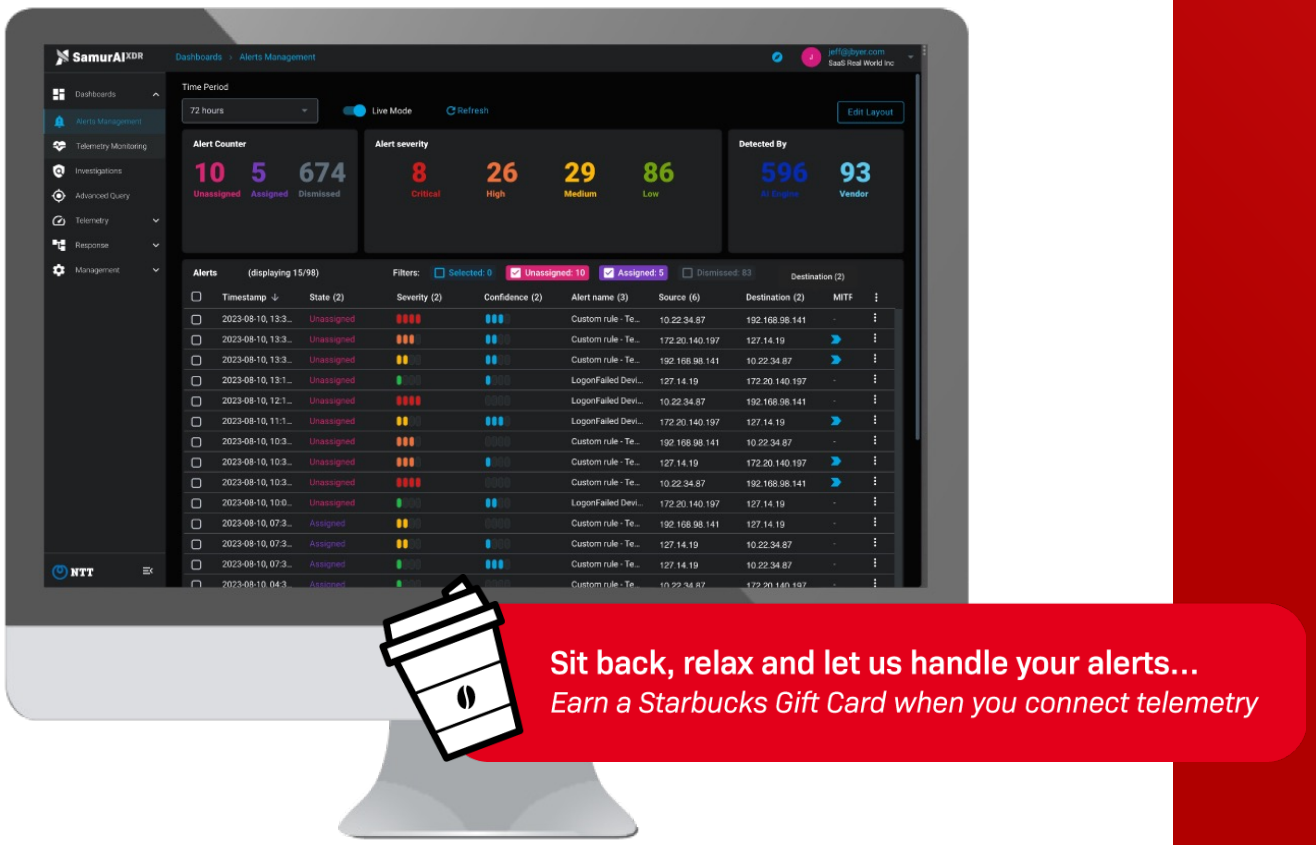
Partner with a global leader in cybersecurity

Go to samurai.security.ntt/partner-program to sign up today

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

NTT Security Holdings

SamurAIXDR

Up Next

WEBINAR

Identity Management in the Physical and Digital Worlds

30 July, 2024 | 08:00 AM PDT

SamurAI XDR

Q&A