Simple cybersecurity in a complex digital world.

SamuraiXDR is a vendor-agnostic, cloud-native, scalable, api-driven, advanced threat detection, and response platform.

It combines world class, cutting edge analytics, machine learning, threat intelligence, and automation to help detect and respond to known and unknown threats.

Guaranteed cloud scalability, flexibility, visibility and real-time actionable insights.

Threats continue to evolve.

Daily, you are faced with multiple alerts from multiple vendors. High volumes of telemetry from disparate sources create gaps in visibility which allow vulnerabilities to be exploited. Where there is a lack of high fidelity alerts, this further increases the need for visibility. Simultaneously, this drives the need for advanced correlation and analytics to investigate all the available telemetry to be able to detect and respond to any threats.

As the threat landscape that may affect your business evolves, so too must your response. You need to be capable of identifying any hidden threats which may impact your business.

Bringing a modern security solution to data intensive challenges.

With a constantly evolving attack surface, increasingly devious attacks and multiple security technologies – each with their own interfaces and telemetry, the ability to detect and respond timeously to threats is no longer the only consideration.

You need a solution that makes sense of all the data, determining the actual threats and establishing an actionable plan for mitigating attacks. Samurai XDR SaaS delivers all that.

Data analyzed. Threats detected. Businesses protected.

9.5TB
data analyzed daily

2.23M
alerts per month

1100
analyst-validated security incidents per month

99%
accuracy of detection

Figures provided from the NTT SOC

“In our first month’s report, we had over **369 million** security logs captured. Through NTT’s systems this was condensed to **637** events of which only **one** needed to be investigated.”

DANIEL TRIBE

Chief Technology Officer | FEX Global

SamurAI XDR

Key capabilities.

- World leading real-time correlation.
- Vendor-agnostic, cloud native and scalable.
- Full environment insights, the entire attack surface is covered; combining data from endpoint, network, host and cloud environments.
- Advanced machine learning analysis of telemetry, enriched by our best of breed threat intelligence.
- High-quality alerting, enriched with contextual information.
- Single pane of glass visibility via an intuitive user interface.
- Simplified detailed investigations of complex attacks.
- Pre-built integrations from a comprehensive array of 3rd party security vendors.
- Key integrations include: Cisco, CrowdStrike, Fortinet, Microsoft, VMware and Palo Alto Networks.
- Support of 150+ vendor product integrations.

Immediate results.

Minimize business impact by disrupting threats early

Reduce risk by detecting threats that could bypass existing controls

Gain cyber resilience quickly with cloud native turnkey solution

SamurAI XDR

Why NTT?

20+ years as a Managed Security Service Provider bundled in one SaaS solution.

- Advanced analytics, machine learning and behavior modeling using human-curated, patent-pending technology to detect threats with near-zero false positives.
- Unique indicators of compromise, exclusively identified from the combined data sourced through the flows of data sampled from the NTT tier 1 Internet backbone, which provides unique visibility into malicious activities across the Internet.
- Extensive relationships with 150+ technology partners in constant development on offerings of security products.
- 73% of all validated security incidents were initially detected with tools and methods developed by NTT that didn't require analyst intervention to detect the threat.
- Extensive threat intelligence information sharing network (Cyber Threat Alliance, US Homeland Security, US JCDC).

1500

enterprise customers rely on NTT to safeguard their digital landscapes and protect them from today's newest and most malicious cyberthreats.

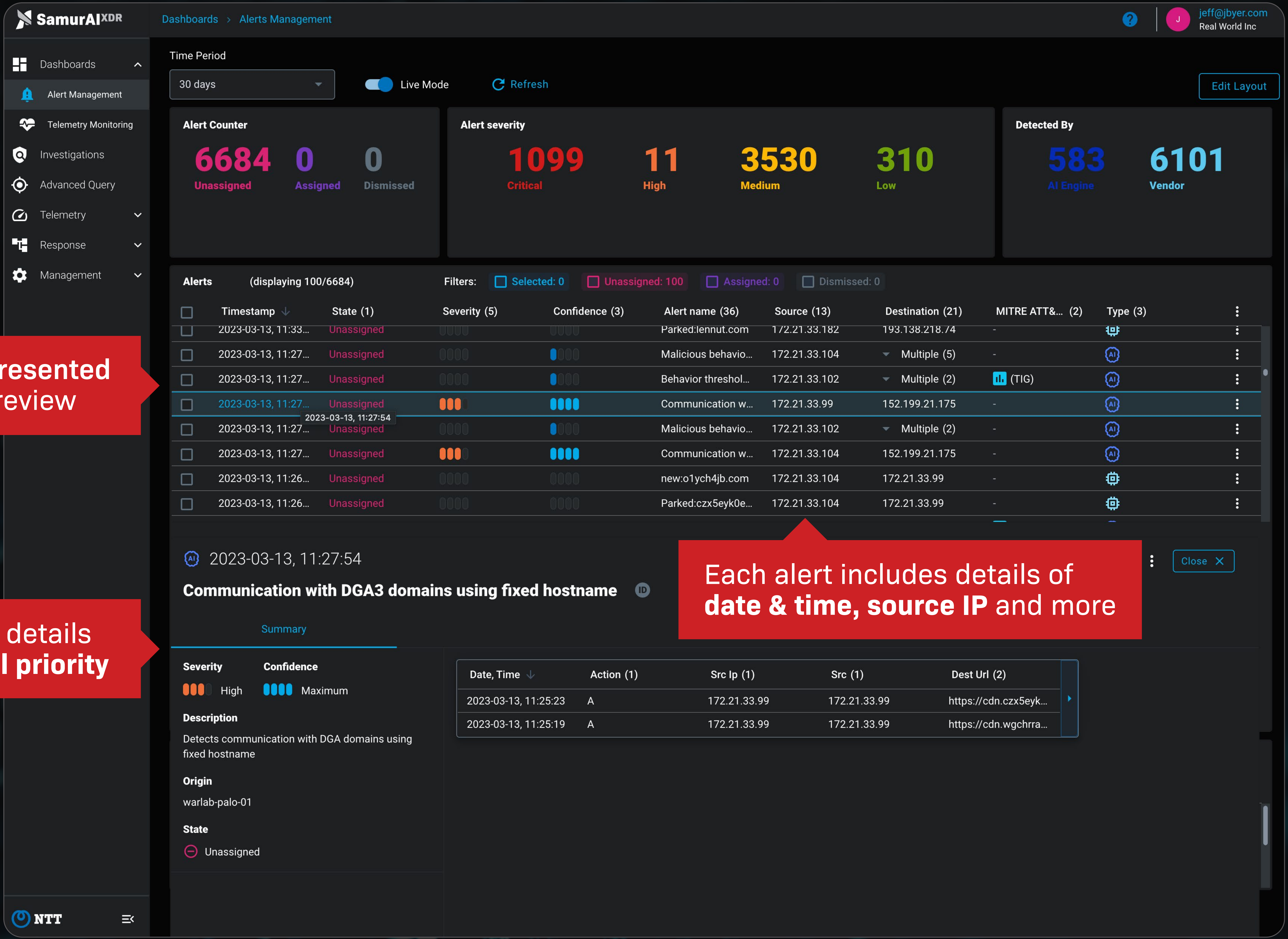
800B+

logs processed per month

> "We have very complex infrastructure with advanced security solutions for endpoints, networks and cloud. NTT provides us with the ability to find the security incidents which would otherwise get missed in endless and seemingly unrelated event data."

FRITZ EKLØFF
Head of IT and Systems
BW Offshore (Norway) AS

SamurAI XDR



Time Period: 30 days

Alert Counter

6684	0	0
Unassigned	Assigned	Dismissed

Alert severity

1099	11	3530	310
Critical	High	Medium	Low

Detected By

583	6101
AI Engine	Vendor

Alerts (displaying 100/6684) Filters: □ Selected: 0 □ Unassigned: 100 □ Assigned: 0 □ Dismissed: 0

□	Timestamp ↓	State (1)	Severity (5)	Confidence (3)	Alert name (36)	Source (13)	Destination (21)	MITRE ATT&... (2)	Type (3)
□	2023-03-13, 11:33...	Unassigned			Parked:lennut.com	172.21.33.182	193.138.218.74	-	▣
□	2023-03-13, 11:27...	Unassigned		▮	Malicious behavio...	172.21.33.104	▾ Multiple (5)	-	AI
□	2023-03-13, 11:27...	Unassigned		▮	Behavior threshol...	172.21.33.102	▾ Multiple (2)	(TIG)	AI
□	2023-03-13, 11:27... 2023-03-13, 11:27:54	Unassigned	▮▮▮	▮▮▮▮	Communication w...	172.21.33.99	152.199.21.175	-	AI
□	2023-03-13, 11:27...	Unassigned		▮	Malicious behavio...	172.21.33.102	▾ Multiple (2)	-	AI
□	2023-03-13, 11:27...	Unassigned	▮▮▮	▮▮▮▮	Communication w...	172.21.33.104	152.199.21.175	-	AI
□	2023-03-13, 11:26...	Unassigned			new:o1ych4jb.com	172.21.33.104	172.21.33.99	-	▣
□	2023-03-13, 11:26...	Unassigned			Parked:czx5eyk0e...	172.21.33.104	172.21.33.99	-	▣

AI 2023-03-13, 11:27:54

Communication with DGA3 domains using fixed hostname ID

Severity ▮▮▮ High

Confidence ▮▮▮▮ Maximum

Description

Detects communication with DGA domains using fixed hostname

Origin

warlab-palo-01

State

⊖ Unassigned

Date, Time ↓	Action (1)	Src Ip (1)	Src (1)	Dest Url (2)
2023-03-13, 11:25:23	A	172.21.33.99	172.21.33.99	https://cdn.czx5eyk...
2023-03-13, 11:25:19	A	172.21.33.99	172.21.33.99	https://cdn.wgchrra...

Alerts are **presented in a list** for review

Each alert includes details of **date & time, source IP** and more

Alerts include details on **threat level priority**

Samurai provides an easy-to-use, easy-to-access, web-based application, with flexible options that can be tailored to meet your unique security requirements.

Samurai XDR SaaS platform-delivered.

- Self-managed service (SaaS).
- Validated alerts. Analysis engine utilizing supervised machine learning.
- Threats curated based on severity level via AI technology.
- Security alerts and investigation.
- Advanced threat hunting.
- Seamless response integrations.
- Detailed response plans.

> “From headline news of attacks targeting critical infrastructure to the unfolding cyber events related to geopolitical conflict, the importance of securing the supply-chain and digital society has never been more critical to business and national economies.”
>
> **NTT SECURITY HOLDINGS**
> Global Threat Intelligence Report

Samurai XDR is supported by NTT’s Global Threat Intelligence Center (GTIC) which provides dedicated R&D capabilities, focused on the development of threat intelligence.

GTIC operates and maintains the global threat intelligence platform which leverages automation to enable machine-to-machine intelligence sharing.

GTIC collects, curates, and integrates threat intelligence from a broad range of sources, including open sources, partnerships and our proprietary intelligence developed through research and analysis of global telemetry.

SamurAI XDR

SamurAI XDR

NTT’s Samurai XDR.

> Threat detection powered by 20 years of advanced artificial intelligence, machine learning models and unique threat intelligence.
>
> Our open XDR self service platform maximizes your security investment by leveraging your best of breed technologies simply! Get the outcome you deserve.

Protect your business with the power of a Samurai.

samurai.security.ntt →