Security is a constant challenge.

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.

NTT | samuraiXDR | Managed Detection and Response samuraiXDR

Threats continue to evolve.

Daily, you are faced with multiple alerts from multiple vendors. This volume of telemetry creates gaps of vulnerability. Where there is a lack of high fidelity alerts, there is an increased need for visibility within the space. Simultaneously, the need increases to be correlating, analysing and investigating all the available telemetry to be able to detect and respond to any threats.
As the threat landscape evolves, so too must your response.
You need to be capable of identifying any hidden threats.

NTT Security Superior Detection:

- 9.5TB data analysed daily.
- 2.23M alerts per month.
- 1100 validated security incidents per month.
- 99% accuracy of detection.

** Data used to train our detection engine, sourced from our managed clients, activity within NTT data lake.

Bringing a modern security solution to data intensive challenges.
With a mobile attack surface, increasingly devious attacks and multiple sources of telemetry, the ability to detect and respond timeously to threats is no longer the only consideration.
You need simultaneously now to be able manage low-fidelity telemetry, volume, as well the low signal to noise ratio and the vulnerability this presents.

Client Values:

- Minimize business impact by disrupting threats early
- Reduce risk by detecting threats that could bypass exisiting controls
- Gain cyber resilience quickly with cloud native turnkey solution

"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

"Access to NTT's global threat detection capabilities, with their global reach, as well as the insights into emerging trends is critical to our overall security strategy."

Tim Hirschl
IT Network Manager EMEA
Synthomer

Key Capabilities

- World leading real-time correlation.
- Endpoint agent. Telemetry integrated with response actions.
- Built in response. Integrated playbook and service desk.
- Full environment insights, the entire attack surface is covered; combining data from endpoint, network, host and cloud environments.
- Proprietary machine learning analysis of telemetry, enriched by our best of breed threat intelligence.

- High-quality alerting, enriched with contextual information from relevant sources.
- Alert enrichment – automatic additional information identification for investigation process.
- Simple point and click responses. Automated playbooks.
- Single pane of glass visibility. Investigations are driven via an intuitive user interface. simplifying detailed investigations of complex attacks (leveraging comprehensive telemetry and evidence).

- Pre-built integrations to a comprehensive array of 3rd party security vendors.
- Key integrations including: Palo Alto Networks, Fortinet, Check Point, Cisco, Okta, Umbrella, Microsoft, Defender, Crowdstrike, Sophos, Trend Micro, Zscaler Proofpoint TAP, Mimecast.
- Support of 150 vendor product integrations.

WHY NTT?

“We have very complex infrastructure with advanced security solutions for end-points, 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

Advanced analytics and Machine Learning including behaviour modelling human curated, patented technology (pending) 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 IP backbone.

Extensive partnerships with 150+ technology partners in constant development on offerings of security products.

Global Honeyport network. Geographically dispersed across multiple regions and multiple cloud providers. Enables early warning and discovery of emerging threats.

Trickbot Commander Controller Servers detection 24h faster than Virustotal (on average).

Over 20 years’ experience in 24x7 Managed Security Services

800+ billion logs processed per month

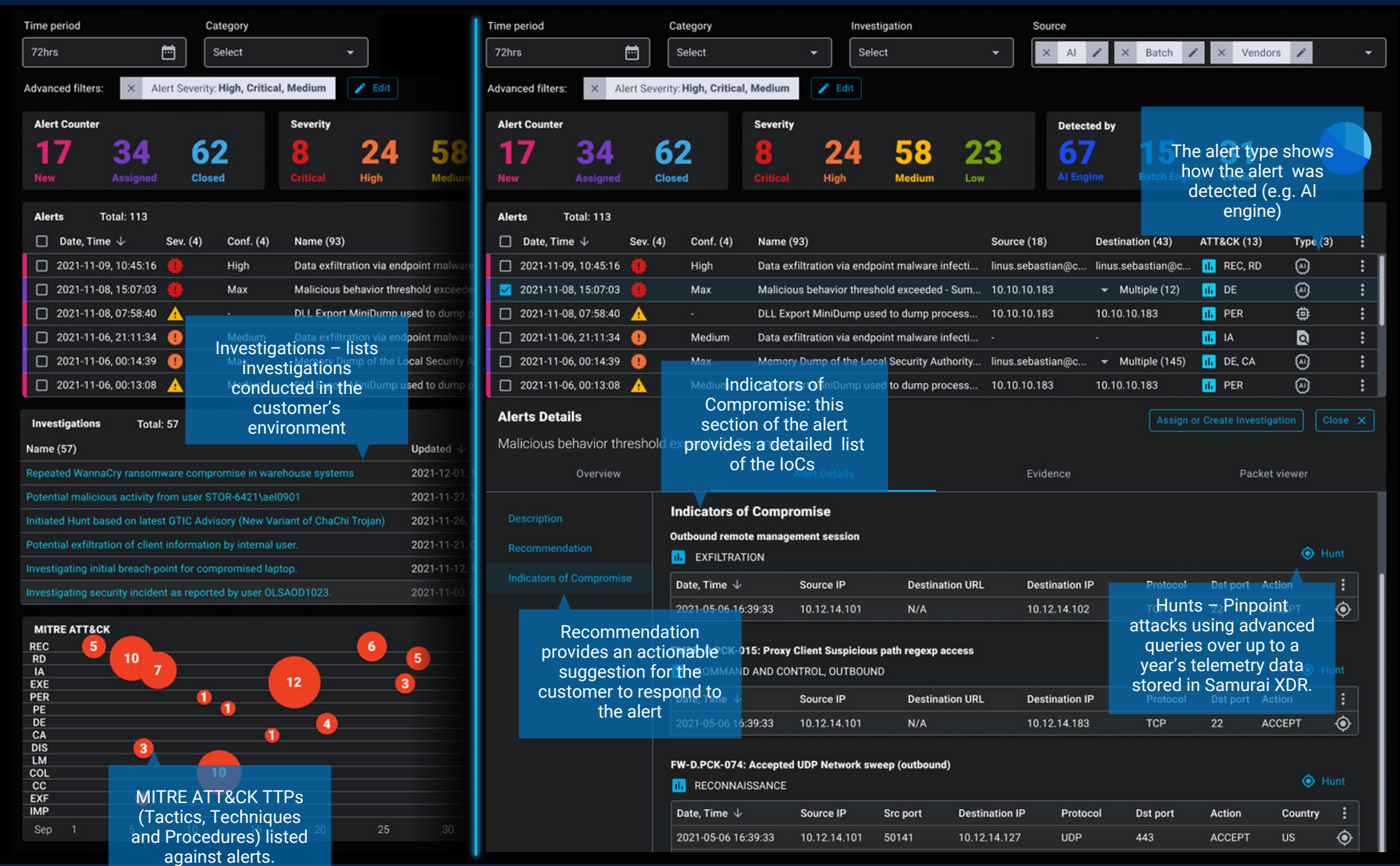
73% of all validated security incidents during 2021 have been initially detected with tools and methods developed by NTT that didn’t require analyst intervention to detect the threat.

Global top 5 Tier 1 IP backbone unique visibility into threat activity over the internet. 40%+ of internet traffic visibility.

Extensive **threat intelligence information** sharing network (Cyber threat Alliance, US Homeland Security etc.)

1500 enterprise customer base experience from securing their environments, and unparalleled early access to threat data.

samurai XDR


Time period
72hrs
Category
Select
Investigation
Select
Source
AI
Batch
Vendors
Advanced filters:
Alert Severity: High, Critical, Medium
Edit
Alert Counter
17 New
34 Assigned
62 Closed
Severity
8 Critical
24 High
58 Medium
23 Low
Detected by
67 AI Engine
Alerts Total: 113
Date, Time
Sev. (4)
Conf. (4)
Name (93)
Source (18)
Destination (43)
ATT&CK (13)
Type (3)
2021-11-09, 10:45:16 High Data exfiltration via endpoint malware infecti... linus.sebastian@c... linus.sebastian@c... REC, RD
2021-11-08, 15:07:03 Max Malicious behavior threshold exceeded - Sum... 10.10.10.183 Multiple (12) DE
2021-11-08, 07:58:40 DLL Export MiniDump used to dump process... 10.10.10.183 10.10.10.183 PER
2021-11-06, 21:11:34 Medium Data exfiltration via endpoint malware infecti... IA
2021-11-06, 00:14:39 Memory Dump of the Local Security Authority... linus.sebastian@c... Multiple (145) DE, CA
2021-11-06, 00:13:08 MiniDump used to dump process... 10.10.10.183 10.10.10.183 PER
Investigations Total: 57
Name (57)
Updated
Repeated WannaCry ransomware compromise in warehouse systems
Potential malicious activity from user STOR-6421\ael0901
Initiated Hunt based on latest GTIC Advisory (New Variant of ChaChi Trojan)
Potential exfiltration of client information by internal user.
Investigating initial breach-point for compromised laptop.
Investigating security incident as reported by user OLSAOD1023.
MITRE ATT&CK
REC RD IA EXE PER PE DE CA DIS LM COL CC EXF IMP
Sep 1 25 30
Alerts Details
Malicious behavior threshold exceeded - Summary
Assign or Create Investigation
Close
Overview
Alert Details
Evidence
Packet viewer
Description
Recommendation
Indicators of Compromise
Indicators of Compromise
Outbound remote management session
EXFILTRATION
Hunt
Date, Time
Source IP
Destination URL
Destination IP
Protocol
Dst port
Action
2021-05-06 16:39:33 10.12.14.101 N/A 10.12.14.102
FW-D.PCK-015: Proxy Client Suspicious path regexp access
COMMAND AND CONTROL, OUTBOUND
2021-05-06 16:39:33 10.12.14.101 N/A 10.12.14.183 TCP 22 ACCEPT
FW-D.PCK-074: Accepted UDP Network sweep (outbound)
RECONNAISSANCE
Date, Time
Source IP
Src port
Destination IP
Protocol
Dst port
Action
Country
2021-05-06 16:39:33 10.12.14.101 50141 10.12.14.127 UDP 443 ACCEPT US
Investigations – lists investigations conducted in the customer's environment
Indicators of Compromise: this section of the alert provides a detailed list of the IoCs
The alert type shows how the alert was detected (e.g. AI engine)
Recommendation provides an actionable suggestion for the customer to respond to the alert
Hunts – Pinpoint attacks using advanced queries over up to a year's telemetry data stored in Samurai XDR.
MITRE ATT&CK TTPs (Tactics, Techniques and Procedures) listed against alerts.

Samurai provides an easy to use, easy to access, web -based platform, with flexible options to choose depending on need, requirement or engagement enabling you to design the right solution for your individual security need.

SAMURAI XDRSAAS PLATFORM-DELIVERED

Self-managed Service (SaaS)
Validated alerts. Analysis engine utilising supervised machine learning. (AI supervision through curation of supervised machine learning technology)
Self-service Security Alert and Investigation
Self-service Threat Hunting
Self-service "Response Workflow" integrations (e.g., ServiceNow, XSOAR, EDR, PagerDuty, etc.)
Self-service Security Incident Response

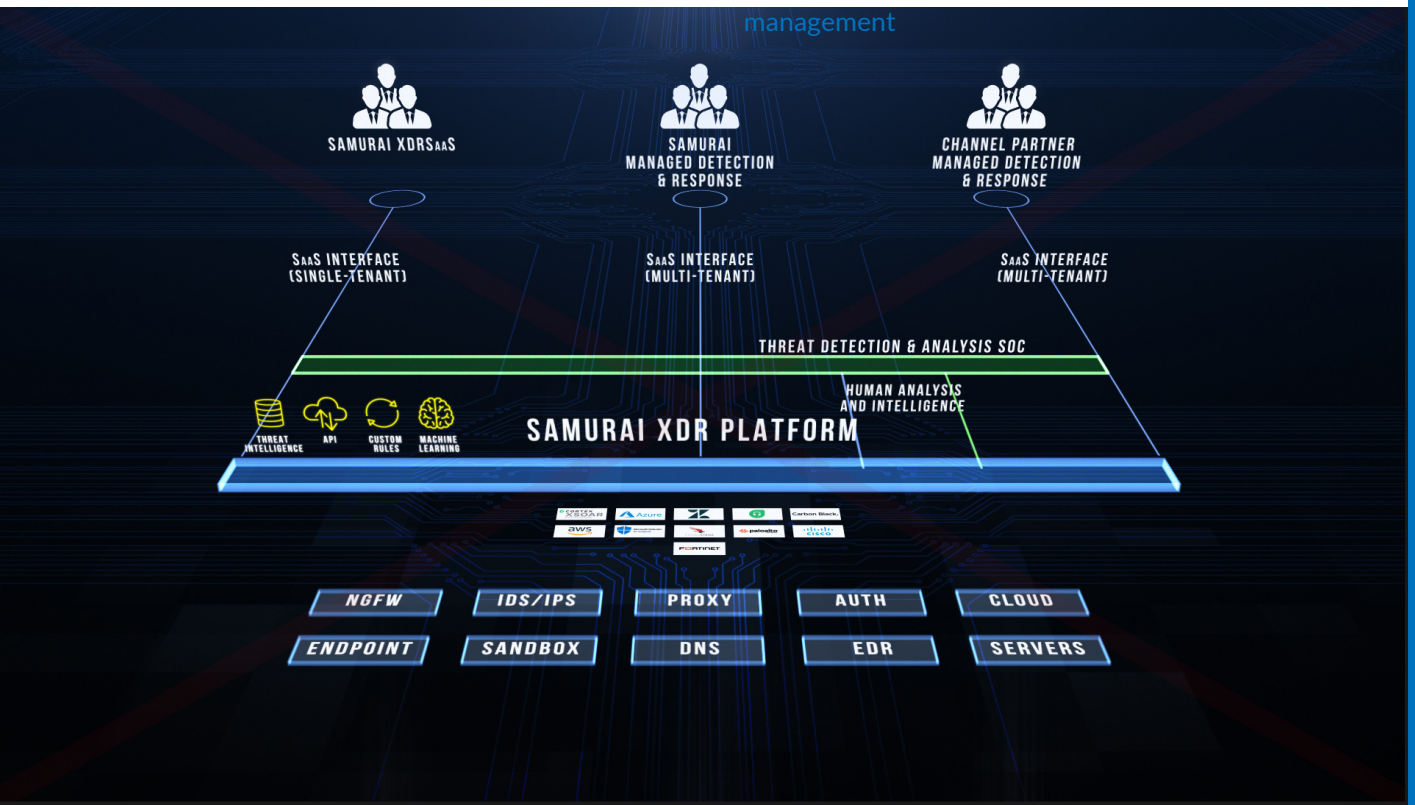
SAMURAI MANAGED DETECTION AND RESPONSE NTTS-DELIVERED

Managed Service Wrapper
ITIL/ITSM Service Management
Customer-specific SecOps (e.g., Security alert investigation, threat hunting, security Incident Report creation, remote Isolation, etc.)
Service Management Portal
Customer-facing Security activities Incident management

CHANNEL PARTNER MANAGED DETECTION AND RESPONSE

CHANNEL PARTNER-OPERATED AND DELIVERED

ITIL/ITSM Service Management
Customer-specific SecOps (e.g., Security alert investigation, threat hunting, security Incident Report creation, remote Isolation, etc.)
Service Management Portal
Customer-facing Security activities Incident management



Samurai XDR and Managed Detection and Response - powered by Samurai XDR, are both uniquely updated and supported by our NTT's Global Threat Intelligence Center (GTIC) which provides dedicated R&D capabilities, focused on the development of Threat Intelligence.
The GTIC operates and maintains the global threat intelligence platform which leverages automation to enable machine-to-machine intelligence sharing.

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

samuraiXDR

NTT's Samurai XDR and Managed Detection and Response - powered by Samurai XDR.

Powered by over 20 years of advanced threat detection across a global security vendor portfolio to develop and train Artificial Intelligence Machine Learning models.
Our XDR platform maximizes your security investment while ensuring that threats are detected, and responses are orchestrated for maximum protection and is available as a self-managed XDR SaaS platform or as a 24x7 analyst based Managed Security Service with Managed Detection and Response powered by Samurai XDR.

NTT | samuraiXDR | Managed Detection and Response samuraiXDR

ISO27001:2013 | ISO22301:2019 | Cyber Essentials Plus