NTT Security Holdings

WEBINAR

# Key Insights on Threat Intelligence and XDR Every Business Needs to Know

# Speakers

**Jeremy Nichols**

Director
Global Threat Intelligence Center

NTT Security Holdings

**Paul Asdagi**

Senior Director, Product Management
Samurai XDR

NTT Security Holdings

**Erin Haynes**

Senior Marketing Specialist
NTT Security Holdings

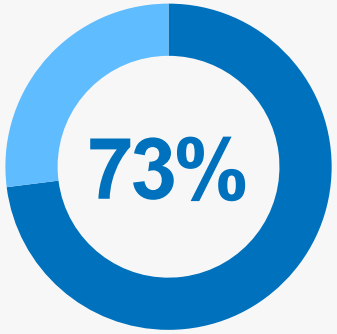
# Overview

Insights from the 2024 **Global Threat Intelligence Report**, with a focus toward SMB issues

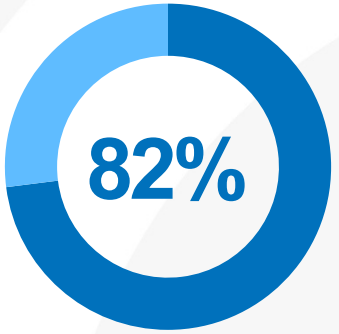
How the **Global Threat Intelligence Center** produces intelligence to support Samurai XDR

How consolidated offerings such as XDR **reduce effort and support SMBs**

# Important Stats



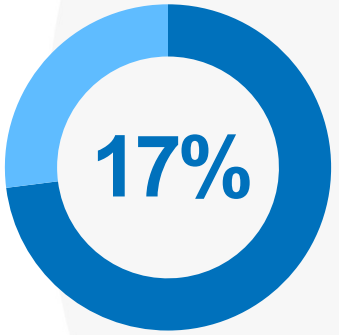

of SMBs experiencing a **cyberattack**, **data breach**, or both within a 12-month period




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**

# SMBs are Exposed to an Ever-growing Number of Threats

- Phishing
- Malware
- Ransomware
- Insider Threats
- Man in the Middle

# How Threat Intelligence and XDR Enhance Small Business Cybersecurity

What is **Threat Intelligence**?

The Role of Threat Intelligence in **Small Business Cybersecurity**

What is **Extended Detection and Response** (XDR)?

The Synergistic Relationship Between **Threat Intelligence and XDR**

Empowering Small Business **Security Teams**

The Unique Advantage of **Samurai Threat Intelligence**

# 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

# Insights from the 2024 Global Threat Intelligence Report

NTT Security Holdings

# Top Attacked Sectors

25.66%
MANUFACTURING

21.42%
TECHNOLOGY

7.94%
PUBLIC

10.20%
TRANSPORT & DISTRIBUTION

10.84%
FINANCE

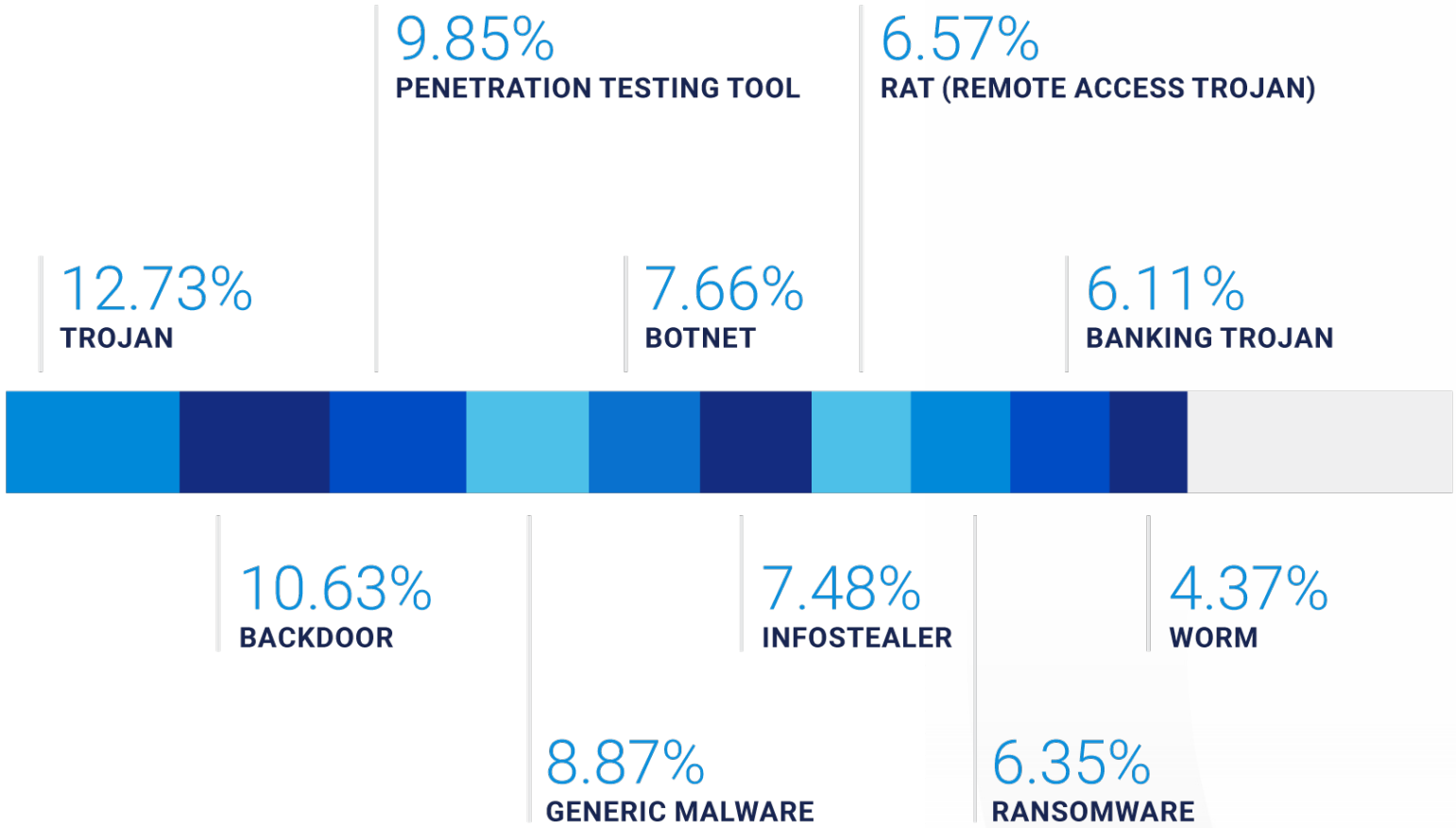
We continue to see attacks against critical infrastructure and supply chains prioritized by adversaries and facing significant risk

Surge in attacks against entities manufacturing components for the energy and mining industries

Over 20% of the attacks observed targeting technology and service providers more than other technology organizations

Finance remains a prime target for financially motivated threat actors

# Malware Telemetry




Malware continues to evolve to gain initial access, evade detection, and maintain persistence

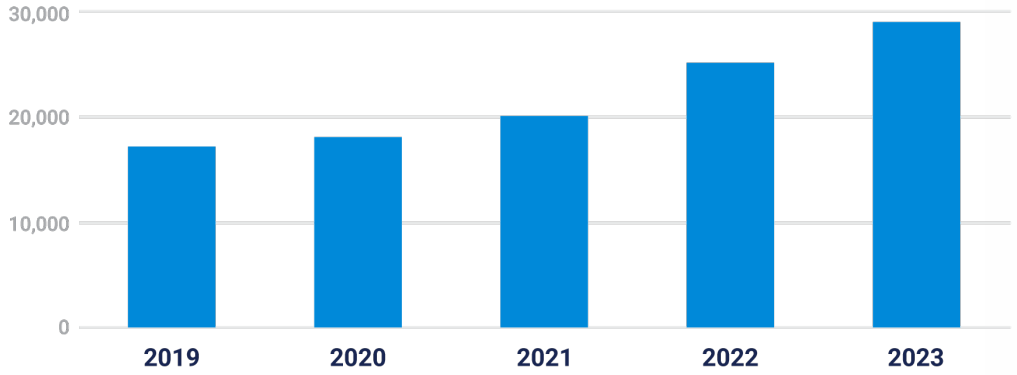
Trojans and infostealers continue to be a major factor

Ransomware detections decreased, with numerous operators shifting away from the traditional encryption and ransom strategy, focusing instead on faster data exfiltration for extortion purposes

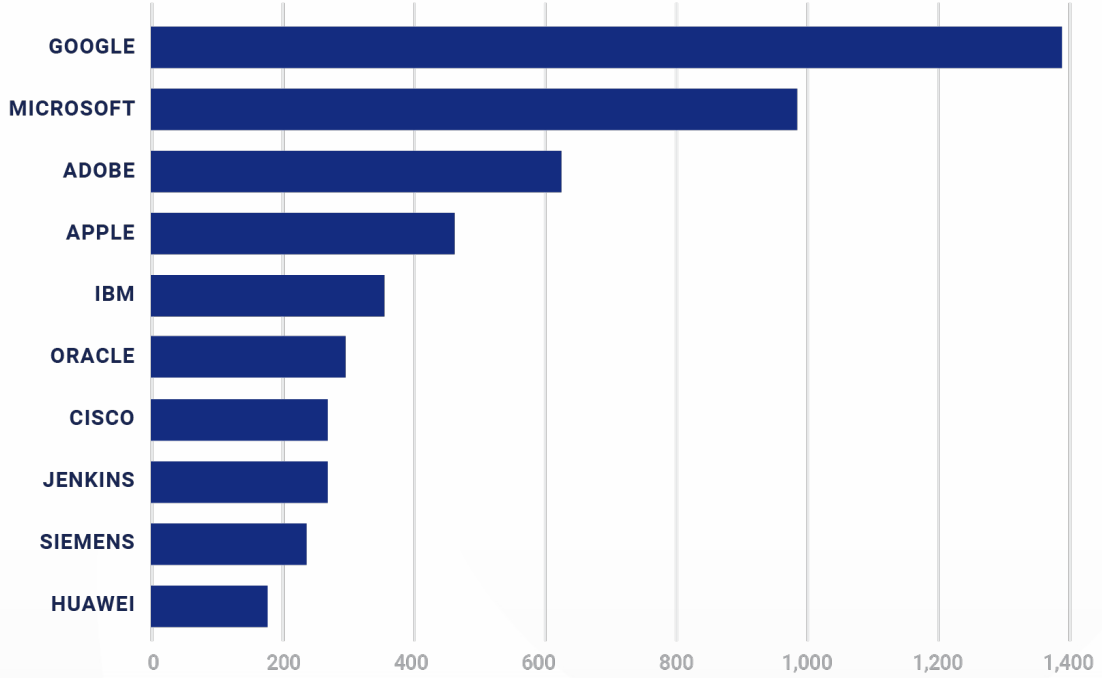
The modularization of malware, and the increase in adversaries living off the land, highlights the need for organizations to have more comprehensive protections in place

# Vulnerability Intelligence

## CVEs by Year

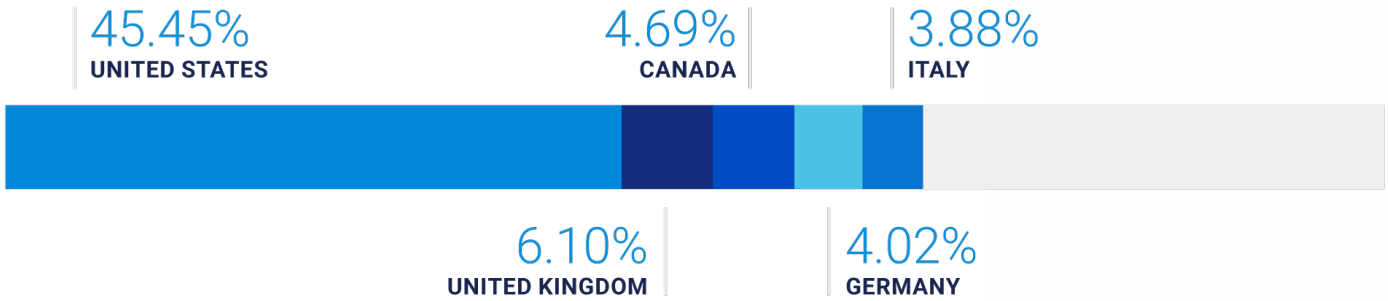


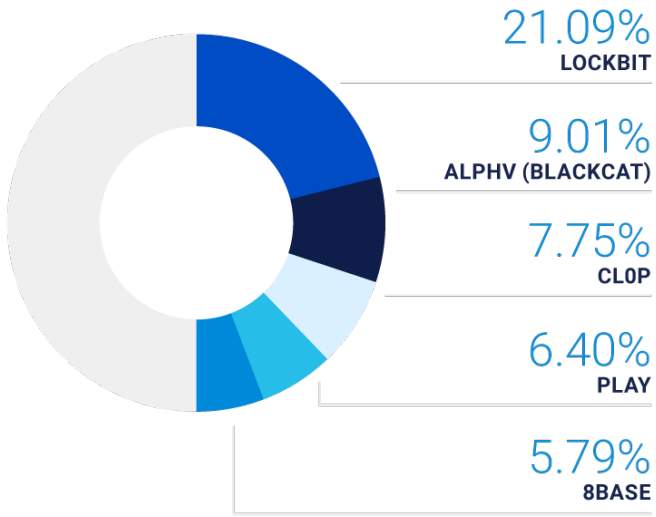

## 2023 CVEs by Vendor

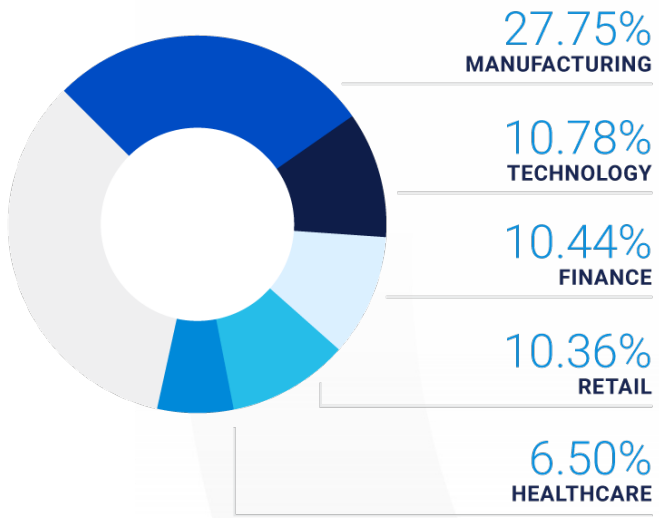



- Vulnerability intelligence is an important aspect of threat intelligence that can provide key data points to help protect your business
- Many of the most popular vendors by market share and reputation are also among the highest in announced CVEs each year
- Popular vendors, Software-as-a-Service (SaaS) and remote management tools are key targets for adversaries looking to maximize victim count with exploitation

# Ransomware Insights




United States and Manufacturing companies top the charts every year

Top targets are organizations that need near perfect uptime

Lockbit claimed the most victims for the second year in a row after ramping up into the top 3 in 2021.

GTIC continues to see small and medium-sized businesses (SMBs) face significant risk, with over 50% of victims we tracked having less than 200 employees and two thirds having less than 500 employees.

# Understanding the Global Threat Intelligence Center (GTIC)

# Overview of the GTIC

Global Threat Intelligence Center
Security Holdings

**Overview of GTIC** and its role in cybersecurity

**Processes and methodologies** used by GTIC to produce threat intelligence

How GTIC's intelligence supports **proactive security measures**

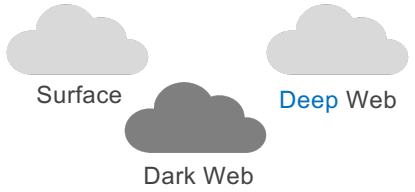
# Samurai Threat Intelligence

## NTTs Global Threat Intelligence Centre

| Collection | Processing & Exploitation | Analysis & Production | Integration & Sharing |
|---|---|---|---|
| Feeds | STIX | Visualization | API |
| Structured Data | Extract, Transform, Load | Pivoting & Relationships | Reports |
| Unstructured Data | TLP & Admiralty Code | TTP Analysis & Attribution | Portal |
| Normalization | Tagging & Categorization | Case / Hunt Investigations | .Dynamic Block List. |
| De-duplication | Enrichments | Intelligence Production | TAXII |

**NTT Global IP Backbone**

**Internet Analysis**




**NTT Sharing Alliances**

NTT Group
CYBER THREAT ALLIANCE
JOINT CYBER DEFENSE COLLABORATIVE
NTT CERT
Microsoft
EUROPOL EC3 European Cybercrime Centre

**Technology Partners**

NTT Group
eclectic iq
Recorded Future
VirusTotal

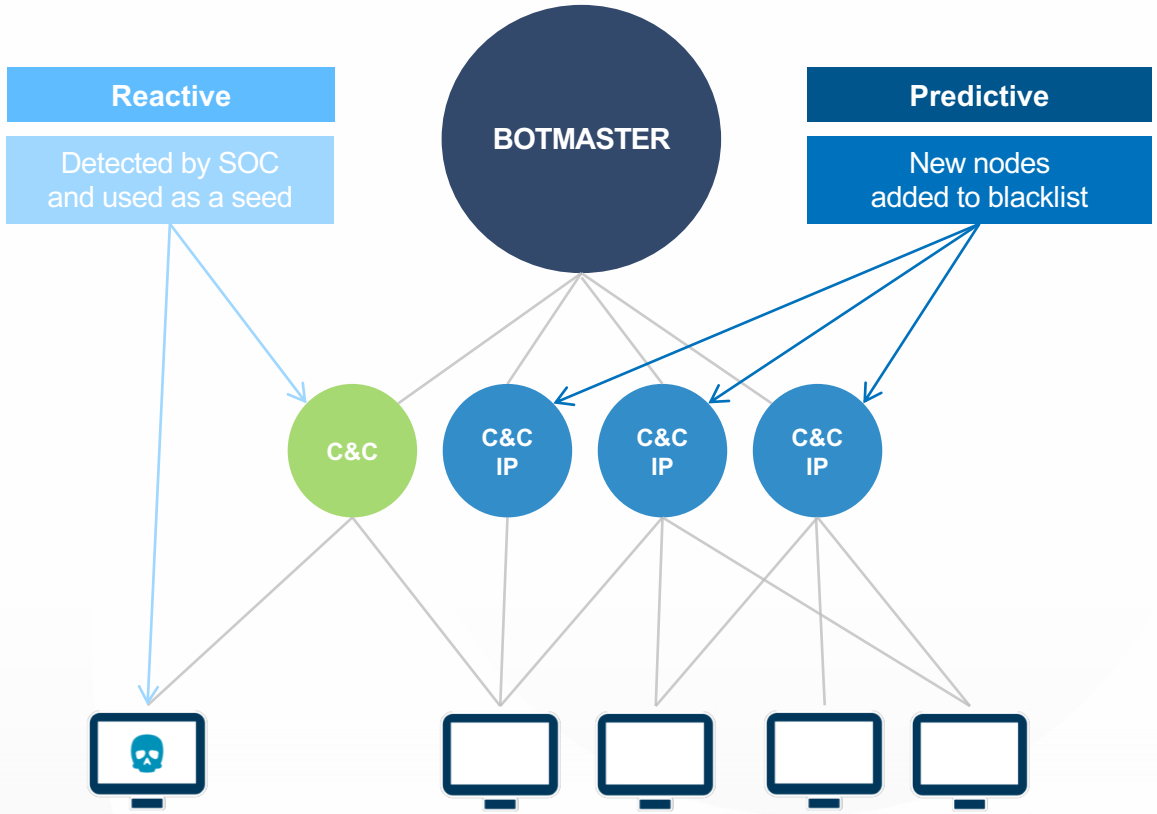
**NTT Honey Net**

- Threat intelligence helps predict, detect, and respond to cyberthreats, while supporting business innovation and risk management.
- NTT stays ahead of the pack by aggressively applying machine learning and threat analysis to its network data.
- **NTT (Tier -1 backbone)** is one of the global top 5 ISPs providing the ability to identify threats seen across its global network
  - Accuracy of 97.4% for machine learning based detection of malicious hosts
  - Detected 20- 30 malicious hosts daily. Some of them were detected 1 - 40 days earlier than VirusTotal
- NTT's strong ability to collate data that others can not from our large network, MSS clients, and comprehensive partnerships.

*As ranked by CAIDA

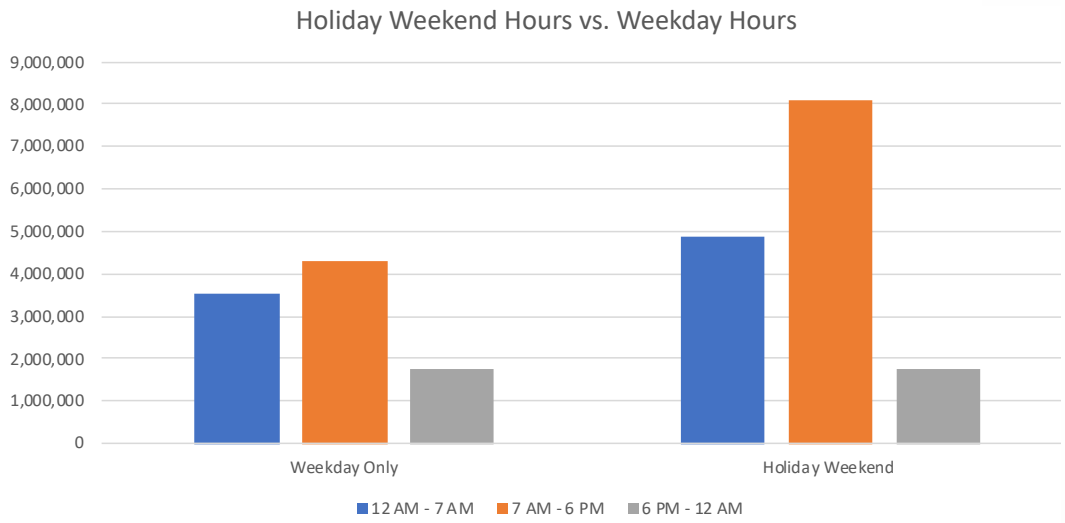
# Tier 1 Backbone Analysis

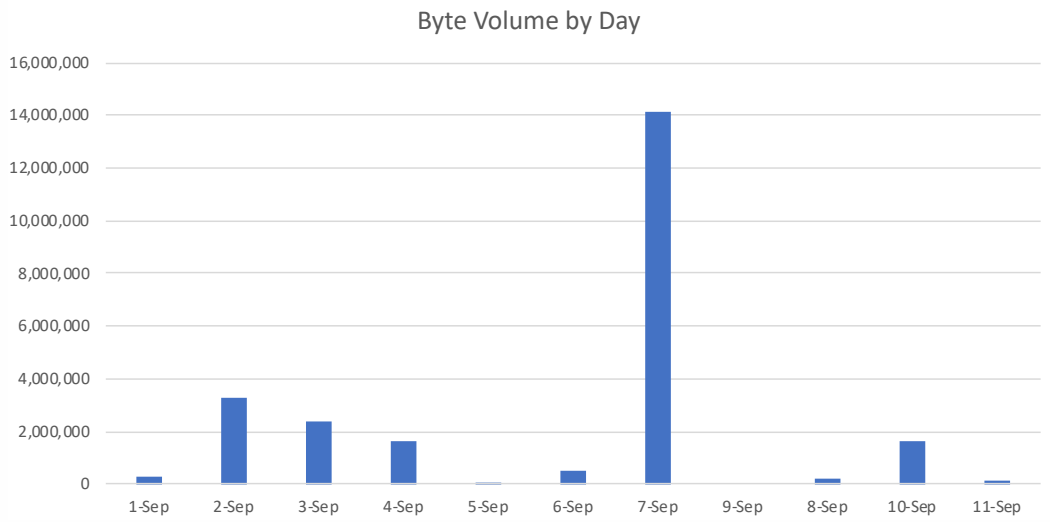
Visualizing Malicious Infrastructure

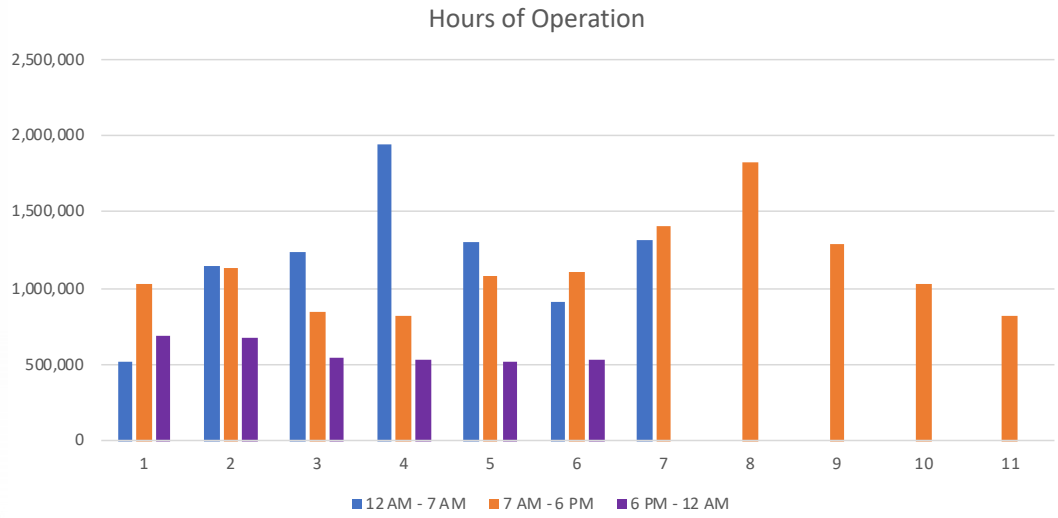


# Tier 1 Backbone Analysis

## Analyzing Traffic Patterns

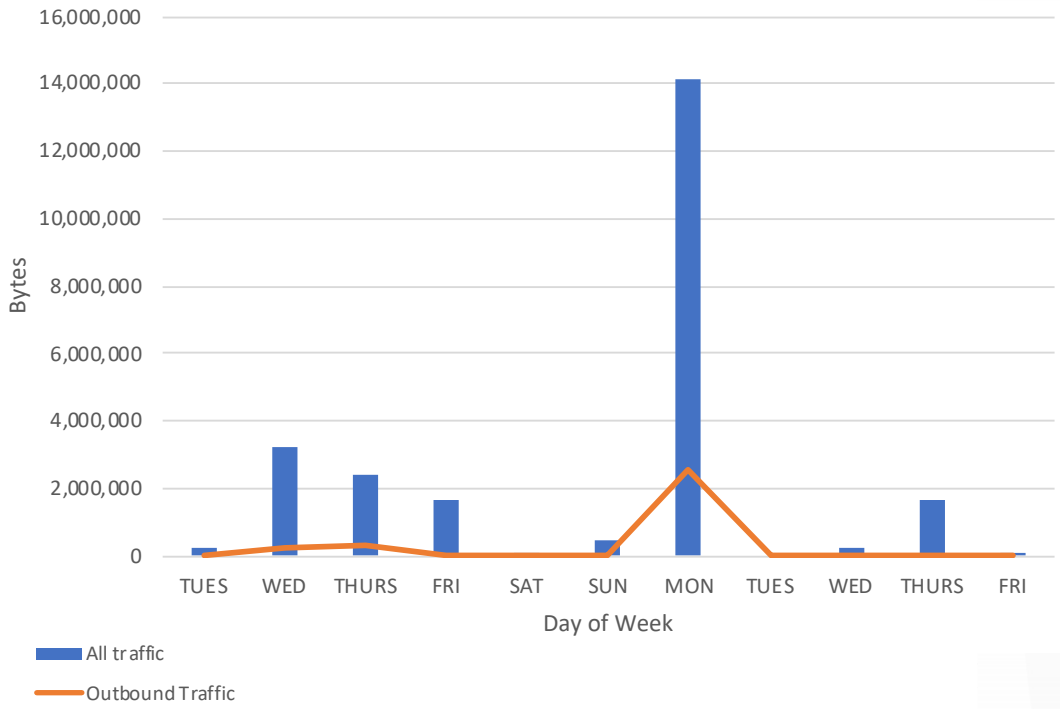


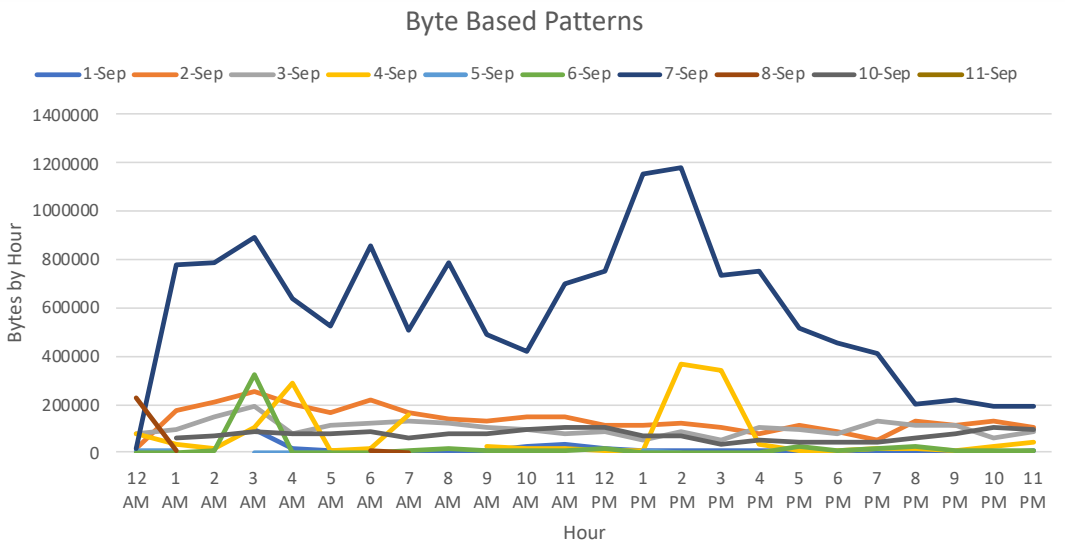



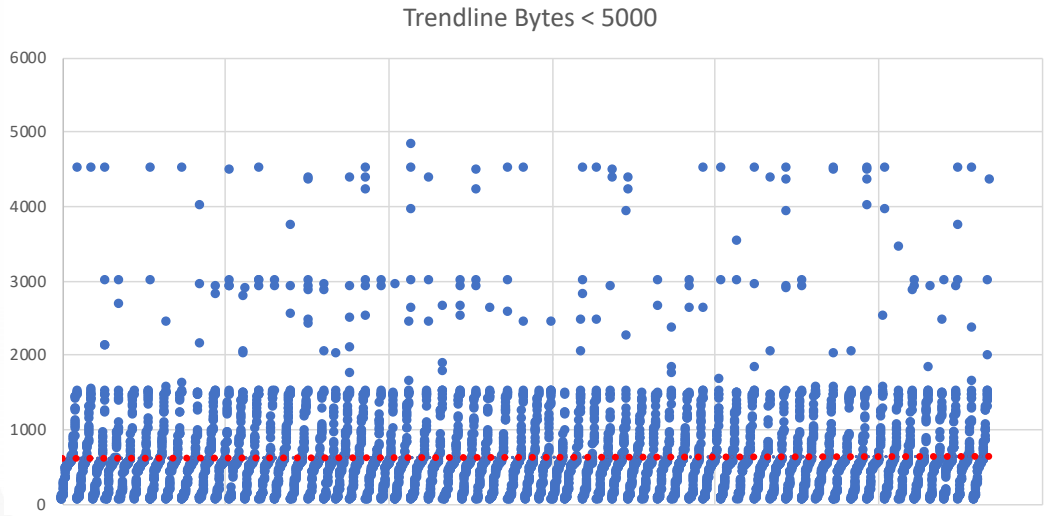



# Tier 1 Backbone Analysis

## Retrohunt



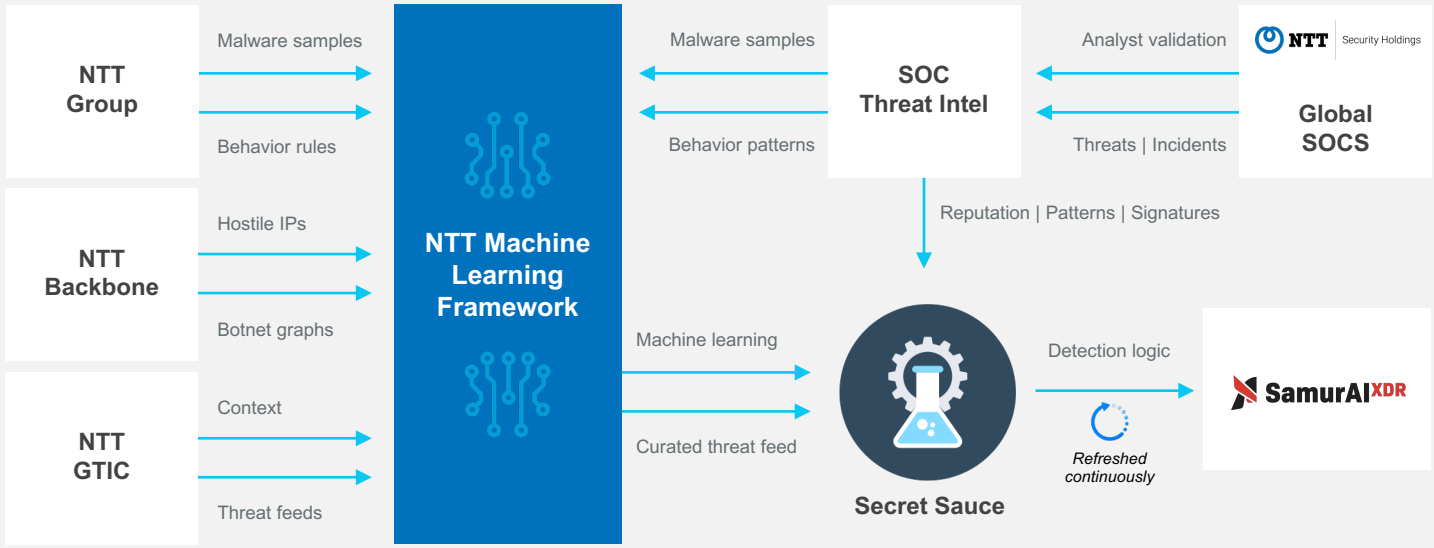
SamurAI XDR

# 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

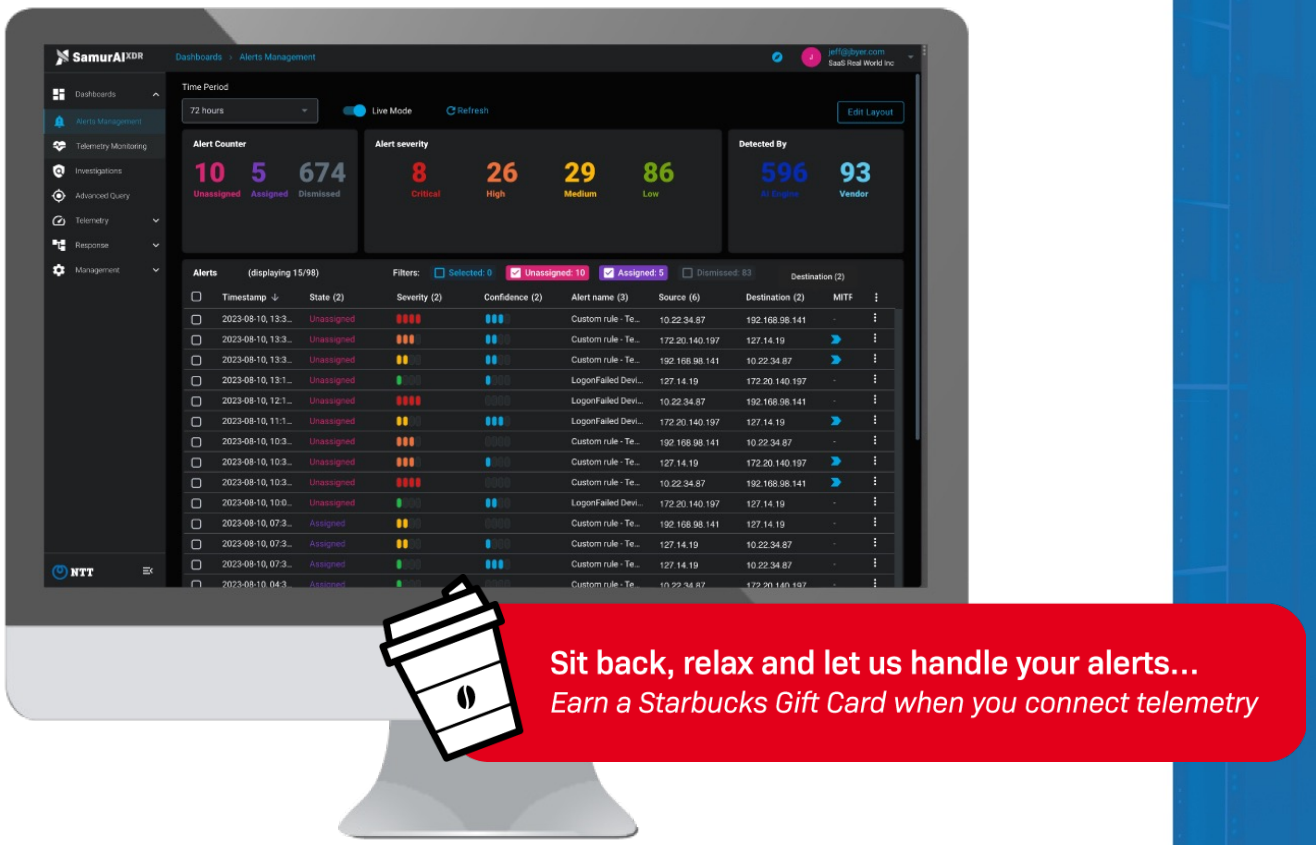
**NTT Global Threat Intelligence Platform**

- 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*

## Up Next

WEBINAR

### The Future of MSP Security: Embracing XDR Solutions

June 27, 2024 | 08:00 AM PDT

NTT Security Holdings

SamurAIXDR

# Q&A Session


# Thank You

**security.ntt**