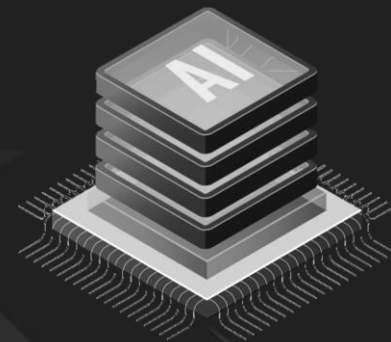# RENEWING SOCIETY THROUGH BUILDING NEW BUSINESSES

## IZAPY

### Comprehensive Ransomware Attack Prevention and Mitigation Solution

**Presented by** - IZAPY, Singapore

**Presented to** - CyberSG TIG
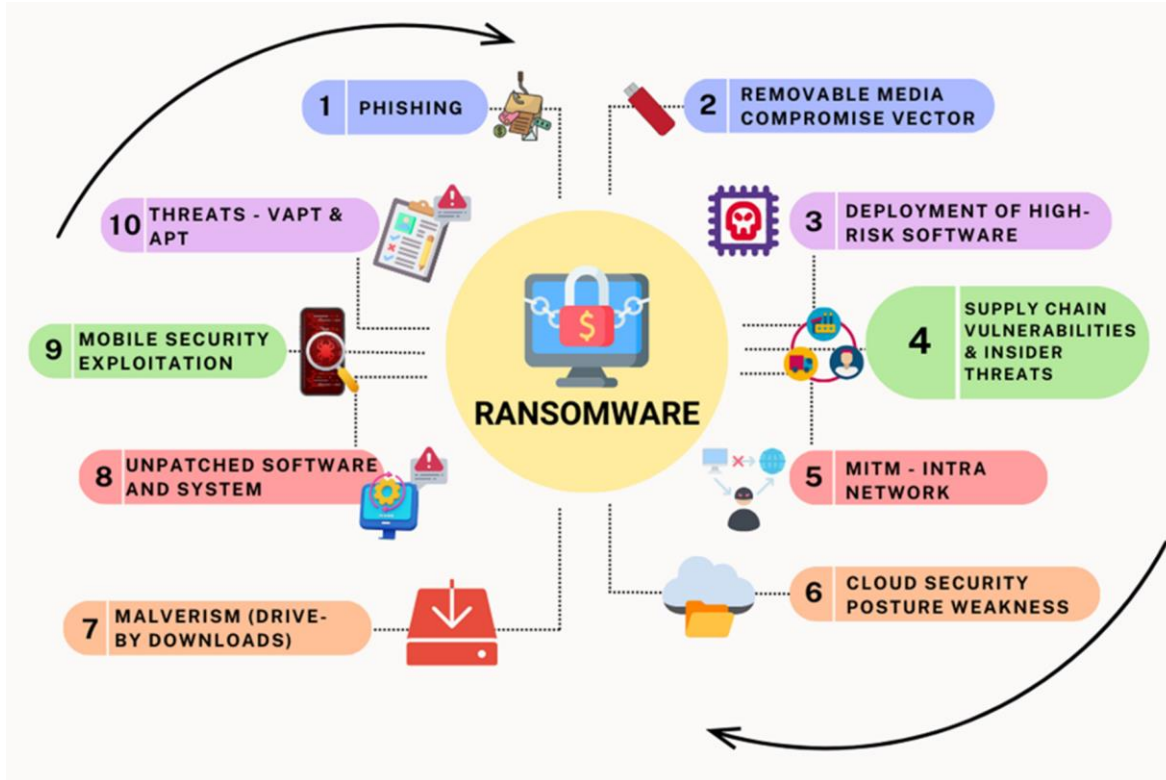
**Date** - 14-05-2025

# Vision & Mission

**VISION**

To pioneer comprehensive ransomware defenses, empowering businesses worldwide to operate safely in the digital and AI era.
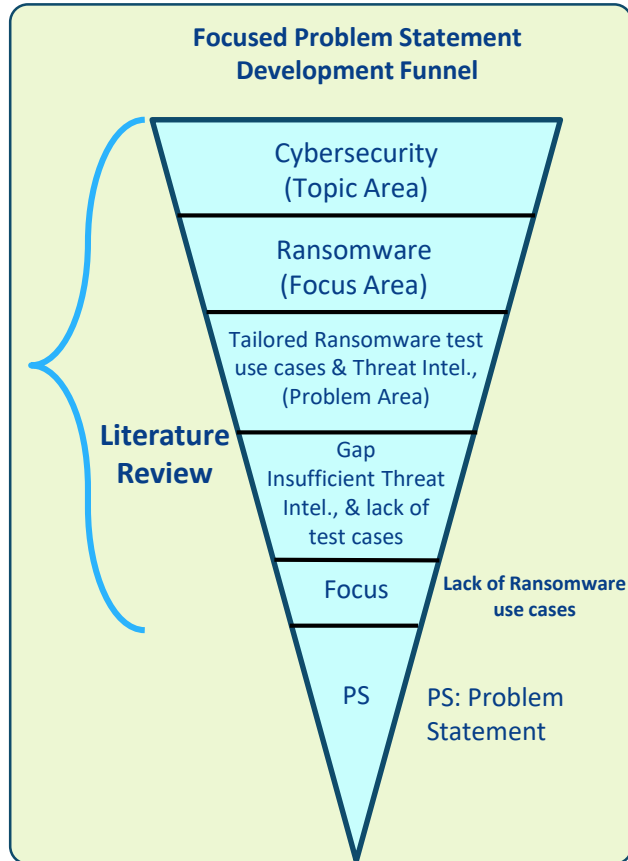
**MISSION**

To offer innovative ransomware defenses that safeguard our clients' operations and data, ensuring their continuous security.

# THE BIG IDEA



We will partner with Partner, providing customized ransomware test use cases and leveraging our tailored threat intelligence capabilities to ensure your EDR, XDR, SOC, Email Gateway, Firewall, End-points, Network Devices and other security tools are ransomware-proof. Our service adds value by proactively testing and validating your defenses in an ongoing process, minimizing the risk of costly breaches.

# Problem / Opportunity



Focused Problem Statement Development Funnel

Cybersecurity (Topic Area)

Ransomware (Focus Area)

Tailored Ransomware test use cases & Threat Intel., (Problem Area)

Gap Insufficient Threat Intel., & lack of test cases

Literature Review

Focus — Lack of Ransomware use cases

PS — PS: Problem Statement

**Problem Statement:**
Lack of comprehensive ransomware threat intelligence feeds and insufficient ransomware test cases render existing security tools and process ineffective. This deficiency leaves organizations vulnerable, as their systems are not adequately tested or prepared to detect and respond to advanced ransomware social disaster, posing significant risks to data security and operational continuity.

**Opportunity:**
Develop a solution that enhances existing security tools with robust threat intelligence and comprehensive ransomware test cases, improving detection, prevention, and response to ransomware attacks. There are 1,700 attacks happened weekly in global level in 2024 and it is considered ransomware attacks on the top.

4

# SOLUTION / BENEFIT



Comprehensive Ransomware Attack Prevention and Mitigation Solution
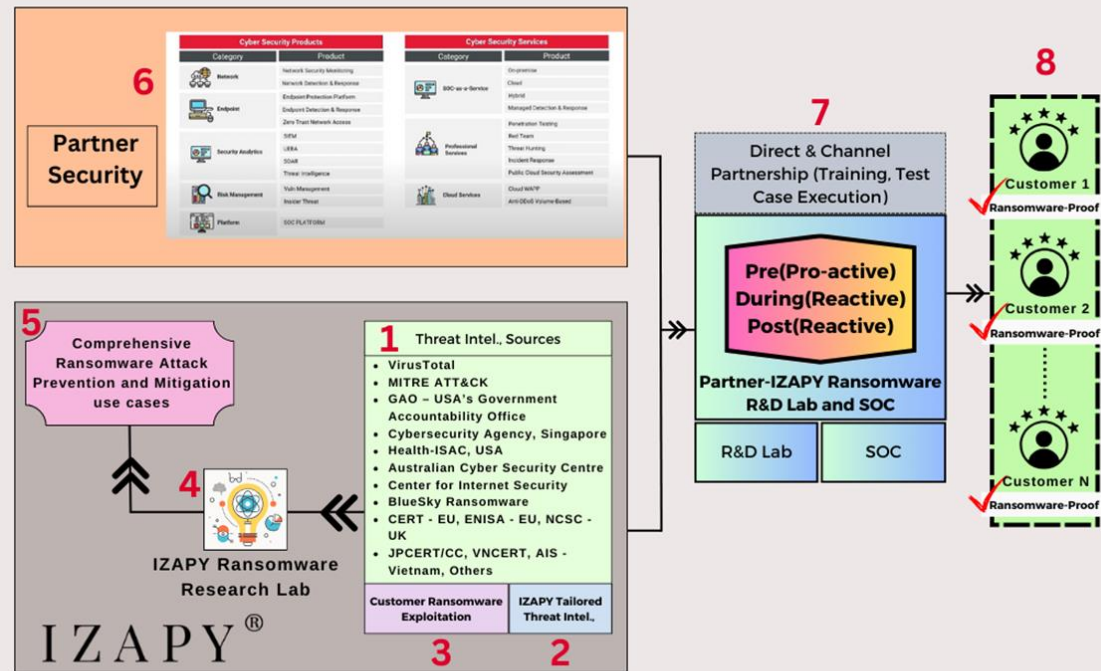
We will collaborate with Partner to deliver customized ransomware test use cases, utilizing our tailored threat intelligence capabilities. This ensures that your EDR, XDR, SOC, Email Gateway, Firewall, End-points, Network Devices and other security tools are fully ransomware-proof. Our solution adds value by continuously testing and validating your defenses, reducing the risk of costly breaches through an ongoing, proactive approach. Eventually we'll build aggregated risk and incident management using Gen AI models.

# COMPETITION /BARRIERS TO ENTRY

## Ransomware Key Use Cases:
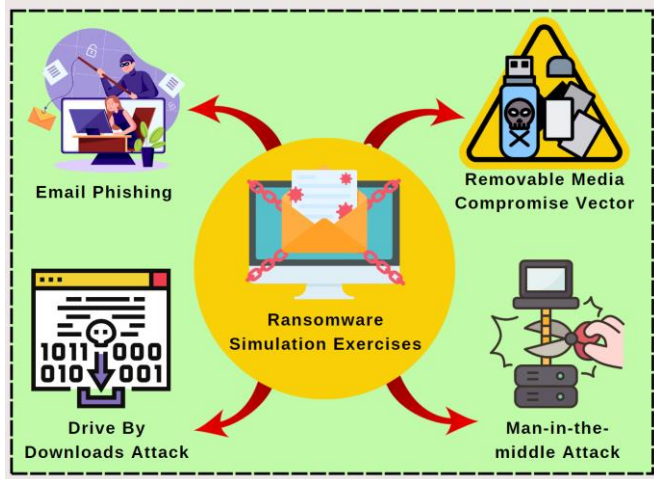


We face minimal competition because of our unique tailored ransomware test cases and 10+ years of developed threat intelligence. Our real-time services and customization create strong barriers, making it difficult for others to compete.

### Ransomware Readiness Assessment

Evaluates the organization's preparedness for handling ransomware threats.

### Ransomware Awareness

Provides training to staff for identifying and preventing ransomware attacks.

### Ransomware Man in Middle Attack

Simulates network-based ransomware attacks to evaluate security measures.

### Simulation Exercise using Sandbox

Tests how defenses perform against controlled ransomware scenarios.

### Ransomware Training & Exercise

Engages teams in practical simulations of ransomware attacks.

### Advanced Ransomware Phishing simulation

Simulates phishing attacks to assess email security effectiveness.

### Ransomware Drive by Downloads

Assesses defenses against ransomware from compromised websites.

### Ransomware IOC Testing

Identifies Indicators of Compromise using market-available ransomware.

### Ransomware Removable Media Compromise Vector

Tests resilience to ransomware introduced via removable media.
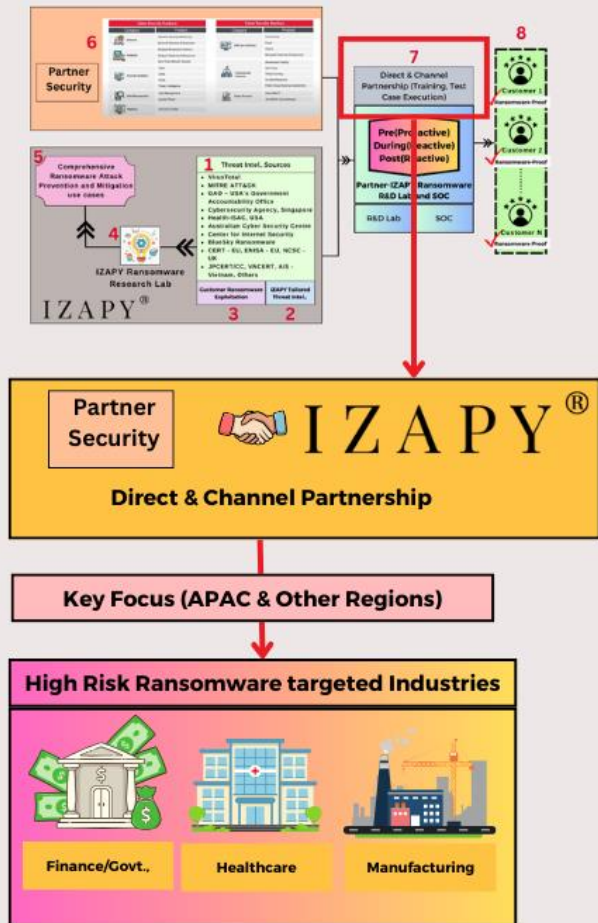
# Business Model
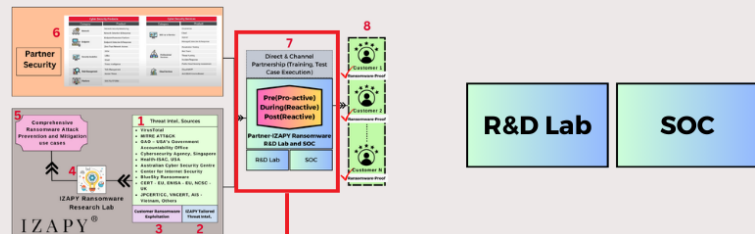


**50 - 80 hrs of Ransomware Retainer Package**

- **Ransomware Awareness - upto 4 Hrs**
- **Ransomware Training - upto 6 Hrs**
- **Ransomware Simulation Exercises**
  - **Ransomware Phishing Exercise - upto 10 Hrs**
  - **Removable Media Compromise Vector - upto 10 Hrs**
  - **Man in the Middle Attack - upto 10 Hrs**
  - **Drive by Downloads - upto 5 Hrs**
  - **Deployment of high risk software - upto 5 Hrs**

| | Free | Plus | Pro |
|---|---|---|---|
| Price | $0 | $1200 | $1920 |
| Customer Support | Email | 9/5 Support | 24/7 Support |
| Retainer Package | Up to 2 Hrs | Up to 50 Hrs | Up to 80 Hrs |
| Ransomware Readiness Assessment | ✓ | ✓ | ✓ |
| Ransomware Awareness | ✓ | ✓ | ✓ |
| Dedicated Security Consultant | ✗ | ✓ | ✓ |
| Simulation exercise using Sandbox | ✗ | ✓ | ✓ |
| Ransomware Training and exercise | ✗ | ✓ | ✓ |
| Advanced Ransomware Phishing Simulation | ✗ | ✓ | ✓ |
| Ransomware Drive by Downloads | ✗ | ✓ | ✓ |
| Advanced Ransomware IOC Testing | ✗ | ✗ | ✓ |
| Ransomware Removable Media Compromise Vector | ✗ | ✗ | ✓ |
| Ransomware Man in the Middle Attack | ✗ | ✗ | ✓ |

*Terms and conditions applicable

**Strategy:** We will focus on industries highly vulnerable to ransomware, including finance, healthcare, and large enterprises. Our approach involves direct sales through cybersecurity partnerships, establishing thought leadership at industry events, and executing targeted digital marketing campaigns.

**Partnerships:** Collaborating with Partner Security and integrating with leading SOC/EDR providers will enhance our market presence and strengthen our credibility. Additionally, we will leverage direct and channel partnerships for training and test execution.

**Strategic Direction:** Direct, Channel Partnership, SOC/EDR + Ransomware value added services, Retainer Model

8

# TRACTION/VALIDATION

Over the past 6 years, we've served more than 30 customers with our ransomware solutions, backed by extensive research. We hold a registered **trademark(AI & Cybersecurity)** in Singapore, **IP registration** in Switzerland, and **ISO 9001** certification. Currently, we are providing ransomware solutions to one of the world's largest financial entities, underscoring our credibility and expertise in the field. Scalable, Repeatable, automation parallel work process for multiple customers.

Leading property, logistics & hospitality – Vietnam, Singapore, UK

Leading power & electric industry – HongKong, Singapore

University & Research Incubation – Singapore, India

Leading Airline in the world - Singapore

Leading Digital Payment and FI - Sigapore

Leading FinTech / Telecom in Asia Pacific – Phillipines, Singapore

Financial Entities – UK, BRICS Countries

Managed IT Service Provider – UK, Australia

REPUBLIC OF SINGAPORE
TRADE MARKS ACT (CHAPTER 332)

REGISTRATION CERTIFICATE

ISSUED UNDER SECTION 15(3)

TRADE MARK NUMBER : 40202022982Y

NAME OF PROPRIETOR(S) : IZAPY Pte. Ltd.

IZAPY

IZAPY is certified by UKAS: Certificate Number: 125522/A/0001/UK/En

UKAS MANAGEMENT SYSTEMS 0043

CERTIFIED QUALITY MANAGEMENT SYSTEM

# FINANCIALS

| | Free | Plus | Pro |
|---|---|---|---|
| Price | $0 | $1200 | $1920 |
| Customer Support | Email | 9/5 Support | 24/7 Support |
| Retainer Package | Up to 2 Hrs | Up to 50 Hrs | Up to 80 Hrs |
| Ransomware Readiness Assessment | ✅ | ✅ | ✅ |
| Ransomware Awareness | ✅ | ✅ | ✅ |
| Dedicated Security Consultant | ❌ | ✅ | ✅ |
| Simulation exercise using Sandbox | ❌ | ✅ | ✅ |
| Ransomware Training and exercise | ❌ | ✅ | ✅ |
| Advanced Ransomware Phishing Simulation | ❌ | ✅ | ✅ |
| Ransomware Drive by Downloads | ❌ | ✅ | ✅ |
| Advanced Ransomware IOC Testing | ❌ | ❌ | ✅ |
| Ransomware Removable Media Compromise Vector | ❌ | ❌ | ✅ |
| Ransomware Man in the Middle Attack | ❌ | ❌ | ✅ |

*Terms and conditions applicable

# KEY TEAM MEMBERS

Our team is highly skilled, with certifications like CEH, OSCP, and CISM. We've achieved top rankings on Google's bug bounty leaderboard and contributed to Facebook's bug bounty program. As a company, we're ISO 9001 certified, hold a trademark in Singapore, and have IP registered with WIPO. This strong foundation allows us to provide top-notch ransomware solutions.

Our global team is made up of 10 skilled members

**Srini Bala**
Singapore
Founder & Partner

**Kenji Sugawara**
Japan
Director

**Todd Facemire**
London, UK
Board Advisor

**Sai**
Bangalore, India
Security Consultant – Cybersecurity &VAPT

**Udhaya**
Bangalore, India
Security Consultant – AI & SOC /DPO (Data Privacy Officer)

**Venki**
Bangalore, India
Security Advisor

**Jana**
Bangalore, India
Delivery Team

# What We Need

1. Partnership with Partner to establish a Ransomware R&D lab and SOC.
2. Funding Support for pilot testing with select customers.
3. Support for ransomware solution collateral preparation.
4. Sales and marketing assistance to build a strong deal pipeline.
5. Engineers to support ransomware solution delivery.
6. High-end laptops and systems for testing.
7. Travel and accommodation assistance for partnership and initial setup.

# SUMMARY / CONTACT

Srini Bala
Founder and Partner
srini@izapy.com
+65 83831592

Sai
Security Consultant
sai@izapy.org
+91 9626660707

Jana
Security Consultant
jana@izapy.org
+918668190446

**IZAPY Pte. Ltd.,
Singapore**
77, High Street, # 09 -
11, High Street Plaza,
Singapore - 179433.

**IZAPY, India**
Salarpuria, 5th Main,
Sector 7, Bengaluru
(Bangalore),
India - 560102.

**IZAPY, Japan**
1-3-6, Hamacho,
Nihombashi, Chuo-ku,
Tokyo, 103-0007,
Japan.

**IZAPY LLC, USA**
16192 Coastal Highway,
Lewes, Delaware 19958,
County of Sussex, USA.