RYUZA SECURITY

CYBER SECURITY SERVICES

PROTECT YOUR DATA.
SECURE YOUR FUTURE.

- Network Security
- Threat Detection & Monitoring
- Vulnerability Assessment
- Penetration Testing
- Data Backup & Recovery

Visit our website
www.ryuzasecurity.com

Table Of Contents

1. Introduction
2. Case Studies
3. VAPT Process Flow
4. Role of AI in VAPT & Cybersecurity
5. Why Choose us ?
6. VAPT Engagement Plans
7. **About Ryuza Red Ops**

Introduction

Our mission is to provide organizations with actionable security intelligence and resilient defence through precision-driven offensive security operations.

About Company

RYUZA SECURITY

We deliver specialized cybersecurity services driven by continuous research, enabling us to provide deeper assessments, greater accuracy, and more effective security outcomes against evolving cyber threats.

In an era of rapidly evolving **AI-driven cyber threats**, attacks are becoming increasingly sophisticated, adaptive, and difficult to detect. Organizations must continuously strengthen their security posture to stay resilient against emerging attack techniques and evolving adversaries.

Forged For Cyber Operations

Case Studies

We will examine real-world case studies to understand the importance of Vulnerability Assessment and Penetration Testing (VAPT) in identifying and mitigating security risks.

Critical Infrastructure Security

Critical infrastructure security is essential because it protects the systems that keep society functioning—such as power grids, water supply, healthcare, transportation, and communication networks.

If these systems are disrupted by cyberattacks or physical threats, the impact can be widespread, causing economic damage, public safety risks, and loss of trust in institutions. Strong security ensures continuity of essential services, safeguards national security, and reduces the risk of large-scale crises.

Cyber Threat Landscape 2025

In 2025, reported cybercrime losses exceeded **US$20 billion** in **FBI complaints**, while independent studies estimate the global economic impact of cybercrime at approximately **US$500 billion** annually. These costs include not only direct financial losses from fraud, ransomware, and data breaches, but also business disruption, recovery expenses, legal liabilities, and long-term reputational damage.

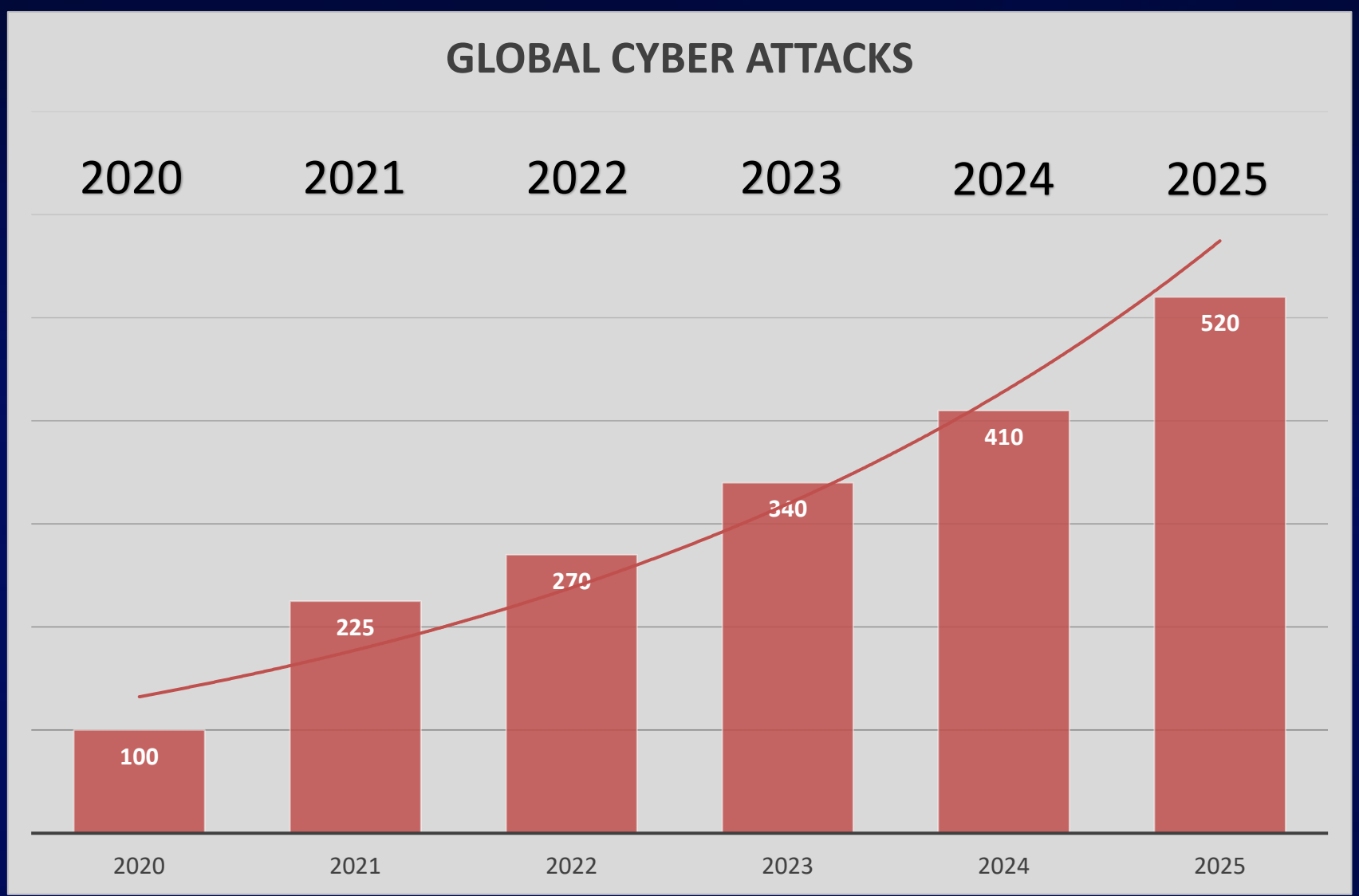
Case Study - Stuxnet (Iran Nuclear Facilities)

Scorch marks at Khojir missile production facility in Tehran, Iran. Credit: Maxar

The Stuxnet attack targeted Iran’s nuclear enrichment facilities by sabotaging centrifuges while reporting normal operations to operators. Widely attributed to nation-state actors, it marked the first known cyber weapon designed to cause physical destruction.

This case fundamentally changed global understanding of cyber warfare and exposed how digital attacks can directly impact physical infrastructure.

Case Study - 5 Years of Cyber Warfare



Indexed trend showing estimated growth in global cyberattack activity from 2020 to 2025 based on multiple industry and government reports.

Case Study - 5 Years of Cyber Warfare

Metrics & Value Figure

METRIC	VALUE
Global cyberattacks increased in 2021 vs 2020	**+125%**
Cyberattacks per organization increased in Q2 2024	**+30% YoY**
Ransomware attacks in 2024	**5,414 attacks** (+11% YoY)
Indian government cyberattacks (2019→2023)	**85,797 → 204,844** (+138%)
FBI-reported cybercrime losses 2024	**$16 billion+** (+33%)
Global cybercrime cost by 2025	**$10.5 trillion annually**
Phishing attacks observed in Q1 2025	**1,003,924+ incidents**

Cyber threats have evolved from isolated attacks into a global digital warfare ecosystem, with attack volumes increasing more than 5× since 2020 and cybercrime projected to cost the world over $10.5 trillion annually.

Case Study - 5 Years of Cyber Warfare

Resources & Links

- ✓ https://aag-it.com/the-latest-cyber-crime-statistics/?utm_source=chatgpt.com
- ✓ https://zerothreat.ai/blog/cyberattack-statistics?utm_source=chatgpt.com
- ✓ https://cyberint.com/blog/research/ransomware-annual-report-2024/?utm_source=chatgpt.com
- ✓ https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents?utm_source=chatgpt.com
- ✓ https://www.reuters.com/world/us/fbi-says-cybercrime-costs-rose-least-16-billion-2024-2025-04-23/?utm_source=chatgpt.com
- ✓ https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/?utm_source=chatgpt.com
- ✓ https://apwg.org/trendsreports?utm_source=chatgpt.com

VAPT Process Flow

The VAPT engagement follows a structured methodology consisting of the following phases.

VAPT LIFECYCLE

1. RECONNAISSANCE

Gather information about the target environment.

2. ENUMERATION

Identify active systems, services and potential entry points.

3. VULNERABILITY ANALYSIS

Scan and identify vulnerabilities in the target systems.

4. EXPLOITATION

Attempt to exploit identified vulnerabilities to gain access.

5. PRIVILEGE ESCALATION

Gain higher level access within the system.

6. REPORTING

Document findings, risks and provide actionable insights.

7. REMEDIATION

Fix vulnerabilities and strengthen security controls.

8. IF REQUIRED

Are issues resolved?

NO

YES

9. RETESTING

Re-validate the environment to ensure vulnerabilities are resolved.

What Client Receives . .

The following deliverables are provided to clients upon completion of the VAPT engagement, depending on the assessment scope and testing requirements

---

✓ **Executive Report**

The Report gives a simple overview of the security weaknesses found during the VAPT assessment and their possible impact on the organization. It helps management understand important security risks and recommended actions in easy, non-technical language.

✓ **Technical Report**

The Technical Report provides detailed information about the vulnerabilities identified during the VAPT assessment, including affected systems, risk severity, and proof-of-concept evidence.

✓ **Risk Matrix**

The Risk Matrix in a VAPT assessment visually shows the severity and impact level of identified vulnerabilities based on their risk to the organization. It helps clients quickly understand which security issues require immediate attention and priority remediation.

What Client Receives . .

✓ **CVSS Severity Scoring**

CVSS Severity Scoring is an industry-standard rating system used in VAPT to measure the severity and criticality of identified security vulnerabilities.

✓ **Proof of Concept Evidence**

Proof of Concept (PoC) Evidence demonstrates how identified vulnerabilities can be exploited, supported by screenshots, payloads, or technical validation findings from the VAPT assessment

✓ **Remediation Guidance & Consultation Evidence**

We provide detailed guidance and consultation support to help you understand identified vulnerabilities, implement security fixes, and improve your organization’s overall security after the VAPT assessment.

“Our team delivers detailed VAPT reports with technical findings, risk analysis, and actionable remediation guidance tailored to your security needs.”

Role of AI in VAPT & Cybersecurity

The VAPT engagement follows a structured methodology consisting of the following phases.

AI in Cybersecurity & Capabilities

✓ **Fully AI-Driven VAPT**
Uses AI and automated tools to identify known vulnerabilities and security weaknesses quickly and at scale. Its effectiveness is limited when dealing with complex, novel, or previously unseen attack scenarios.

✓ **Manual Specialized AI-Assisted VAPT**
Combines human expertise with AI-powered tools to perform deeper security assessments, validate findings, and explore unique attack paths that automation may overlook.

KEY ADVANTAGE

By combining AI efficiency with human creativity and critical thinking, manual AI-assisted VAPT can uncover complex vulnerabilities, business logic flaws, and emerging threats beyond the reach of fully automated testing.

Why Choose Us?

Our services are designed and delivered with precision, ensuring thorough assessments, actionable insights, and effective security solutions.

Overview

Generalized VAPT

A broad security assessment focused on identifying common vulnerabilities across networks, applications, servers, and endpoints. **Focus = Broad Coverage**

Layman Language = A general health check-up that examines your overall body & identifies common health issues.

Real-World Attack Accuracy = ■■□□□

Proactive Threat Protection = ■□□□□

Overview

Specialized VAPT

We Deliver targeted and in-depth security assessment designed for specific technologies, environments or threat scenarios such as critical infrastructure.

Focus = In-Depth Targeted Analysis

Layman Language = visiting a heart specialist for an in-depth examination of a specific medical condition.

Real-World Attack Accuracy = ■■■■□

Proactive Threat Protection = ■■■■□

Certified Professionals

We are a team of dedicated security researchers, combining industry-recognized expertise with continuous research-driven insights to deliver effective, real-world security solutions.

Our team consists of certified cybersecurity professionals accredited by leading certification bodies.

CERTIFICATION BODIES

OFFENSIVE SECURITY	EC-COUNCIL
SANS	ALTERED SECURITY
ELEARN SECURITY	CREST

We Are Precision-Driven Cybersecurity Specialists.

Dedicated Support Services

Our Dedicated Support Services ensure continuous security assistance beyond initial assessments and deployments. Our experts provide ongoing guidance, remediation support, monitoring assistance, and rapid response to emerging security concerns.

Email Support

We provide responsive email-based support and work to resolve client concerns as quickly as possible upon receiving support requests.

Phone Support

We provide responsive email-based support and work to resolve client concerns as quickly as possible upon receiving support requests.

Ticket-Based Support System

A dedicated client portal will be provided, allowing you to securely raise and track VAPT support tickets for technical assistance and remediation support.

Remote Technical Assistance

Remote technical assistance is provided for emergency situations and system-related technical issues identified during or after the VAPT engagement

SLA-Based Support

Support services provided under a predefined Service Level Agreement (SLA) that specifies how quickly and efficiently support will be delivered. SLA-based support ensures that all technical queries, remediation requests, and security concerns are handled within agreed response and resolution timelines.

Security Hardening Support

Security hardening is the process of strengthening systems, applications, networks, and infrastructure by reducing vulnerabilities and minimizing potential attack surfaces.

System Hardening

- Operating System Hardening
- Patch & Update Management
- Registry & Kernel Hardening

Server Hardening

- Web Server Security
- Database Server Protection
- SSH/RDP Security

Network Hardening

- Firewall Configuration
- Router & Switch Hardening
- Network Segmentation
- IDS/IPS Configuration
- VPN Security

Application Hardening

- Secure Application Configuration
- API Security Hardening
- Dependency & Plugin Review

VAPT Engagement Plans

Let’s explore our VAPT engagement plans designed to meet different security requirements, assessment scopes, and organizational needs

Pricing Models

Below are the available pricing and engagement models for our VAPT services, designed to meet different security requirements and organizational needs.

✓ **One-Time Assessment**

A single VAPT engagement conducted to identify and assess security vulnerabilities within a specific system, application, or infrastructure at a particular point in time.

Layman Language – “A one-time security check to find vulnerabilities in your systems or applications.”

✓ **Quarterly Security Testing**

Periodic VAPT assessments performed every three months to continuously identify emerging vulnerabilities and maintain a strong security posture against evolving cyber threats.

Layman Language – “Security testing done every few months to check for new security problems and vulnerabilities.”

Pricing Models

✓ **Annual Security Partnership**

A long-term cybersecurity engagement that provides ongoing security assessments, consultation, remediation support, and strategic security guidance throughout the year.

Layman Language – “A long-term cybersecurity service that provides regular security checks, support, and guidance throughout the year.”

✓ **Retainer-Based Security Support**

An ongoing cybersecurity support model where clients receive continuous access to security expertise, consultation, technical assistance, and rapid response services under a fixed service agreement.

Layman Language – “Continuous cybersecurity help and support whenever you need it.”

Are You Cyber Ready for the Future?

Follow us for more updates on the latest tech trends and insights.

Visit Us On
https://www.ryuzasecurity.com

RYUZA RED OPS

Ryuza Red Ops is a specialized division of Ryuza Security focused exclusively on Vulnerability Assessment & Penetration Testing (VAPT) and advanced red teaming operations. The division is dedicated to identifying security weaknesses, simulating real-world attack scenarios, and evaluating organizational defenses through offensive security methodologies.

By combining technical expertise with intelligence-driven testing approaches, Ryuza Red Ops helps strengthen security posture, improve threat readiness, and enhance resilience against evolving cyber threats.

Connect With Us = https://www.ryuzasecurity.com

Sumant Arora

Computer Scientist

I have strong interest in cybersecurity, red teaming and psychological operations. My interests include cybersecurity research, innovation, and developing creative solutions to emerging digital challenges.

Education

Master of Computer Application

2017 | LPU Distance Education Institute

Bachelor of Computer Application

2014 | Guru Nanak Dev University

Contact

+91 – 7087055115

sales@ryuzasecurity.com

Amritsar, Punjab

(OPC) Pvt Ltd as on JUN 2026

2026

MANAGEMENT PROFILE

Managing Director of Ryuza Security

Year – 2026

I am currently the Director of **Ryuza Security**. I engage in independent research, driven by a strong passion for security, innovation, and solving complex challenges in the evolving digital landscape.

"VAPT is essential because prevention costs far less than recovery after a cyberattack"

Certifications

OSCE | OSCP | OSWP | Offensive Security

eCXD | eCPPTv2 | E learn Security

PSY-OPS | Psychological Operations

Social Media

- **Linkedin** – in/red-dragon
- **Facebook** – sam.arora.0786
- **Instagram** – red_dragon.9
- **Discord** – xx_red_dragon_xx
- **X** – @sumantarora9