CyberHeals

GRC IN THE ERA OF AI AND AUTOMATION

Nizam Mohamed

Co-Founder & Chief Strategic Officer, Cyber Heals

https://www.cyberheals.com/

CyberHeals

What are we Confronted with?

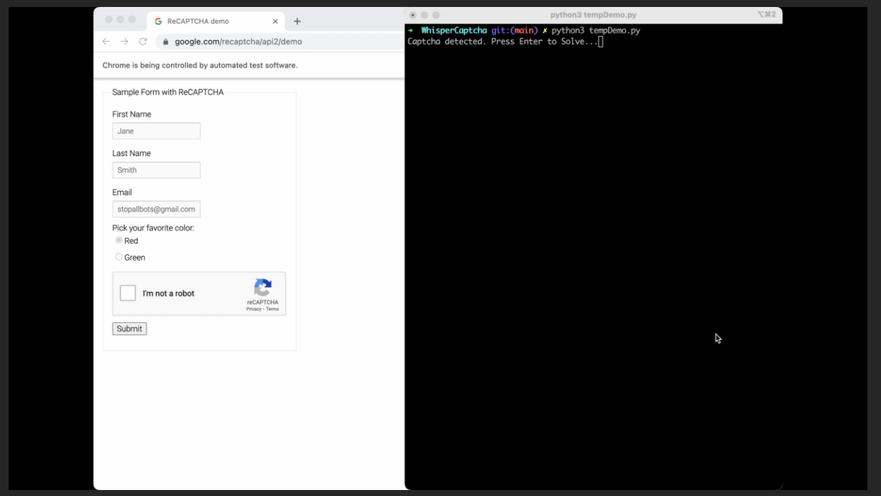
CAPTCHA Busted? AI Company Claims Break of Internet's Favorite Protection System

A software company called Vicarious claims to have created a computer algorithm that can solve CAPTCHA with greater than 90% accuracy. If it's been broken, the entire Internet should probably start transitioning to a new security system. But there would be a silver lining: computationally replicating how humans make sense of images would be a major breakthrough in computer science.

Tech

GPT-4 Hired Unwitting TaskRabbit Worker By Pretending to Be ‘Vision-Impaired’ Human

CyberHeals


ReCAPTCHA demo
google.com/recaptcha/api2/demo
Chrome is being controlled by automated test software.
Sample Form with ReCAPTCHA
First Name
Jane
Last Name
Smith
Email
stopallbots@gmail.com
Pick your favorite color:
Red
Green
I'm not a robot
reCAPTCHA
Privacy - Terms
Submit
python3 tempDemo.py
WhisperCaptcha git:(main) ✗ python3 tempDemo.py
Captcha detected. Press Enter to Solve...


AI-generated image

CyberHeals

The Evolving Threat Landscape

Cyber threats are becoming increasingly sophisticated, with attackers using advanced techniques like malware, phishing, and ransomware to exploit vulnerabilities.

Rise of Advanced Threats

The emergence of AI-powered attacks and sophisticated malware poses significant challenges to traditional security measures.

Data Breaches and Privacy Concerns

Data breaches are becoming more frequent and impactful, exposing sensitive information and jeopardizing privacy.

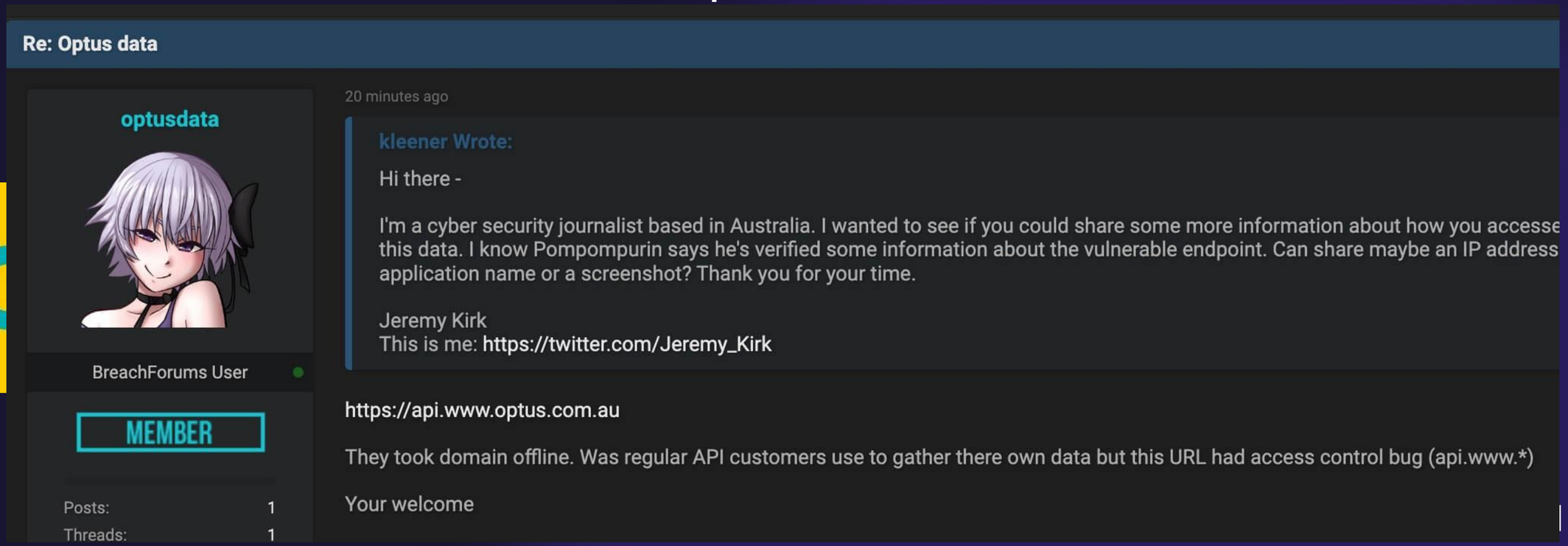
Evolving Attack Vectors

Attackers are constantly seeking new ways to penetrate defenses, utilizing evolving attack vectors and exploiting emerging technologies.

CyberHeals

Optus Data Breach

Impact: 9.8 million customers



.2

million customers

CyberHeals

MediSecure Cyber Security Incident

MediSecure on Wednesday appointed advisory firm FTI Consulting to put into motion administration and liquidation efforts less than a year after it lost a $100 million government contract to supply e-prescriptions to healthcare practitioners.

MediSecure Files for Liquidation Following Major Data Breach

Federal Government Refused to Pay for Bankrupt Firm's Breach Remediation Costs


CyberHeals
RISK
MANAGEMENT
Cyberheals.com

CyberHeals

GRC

- Governance, Risk, and Compliance
- Frameworks, Processes, and Practices recommended by governments and regulatory bodies
- Operate ethically, manage risks effectively, and comply to regulations
- In today's rapidly evolving business landscape GRC has become pivotal to sustaining organizational integrity and resilience.

The Commonwealth Cyber Security Posture in 2023

Content complexity
Moderate

CyberHeals

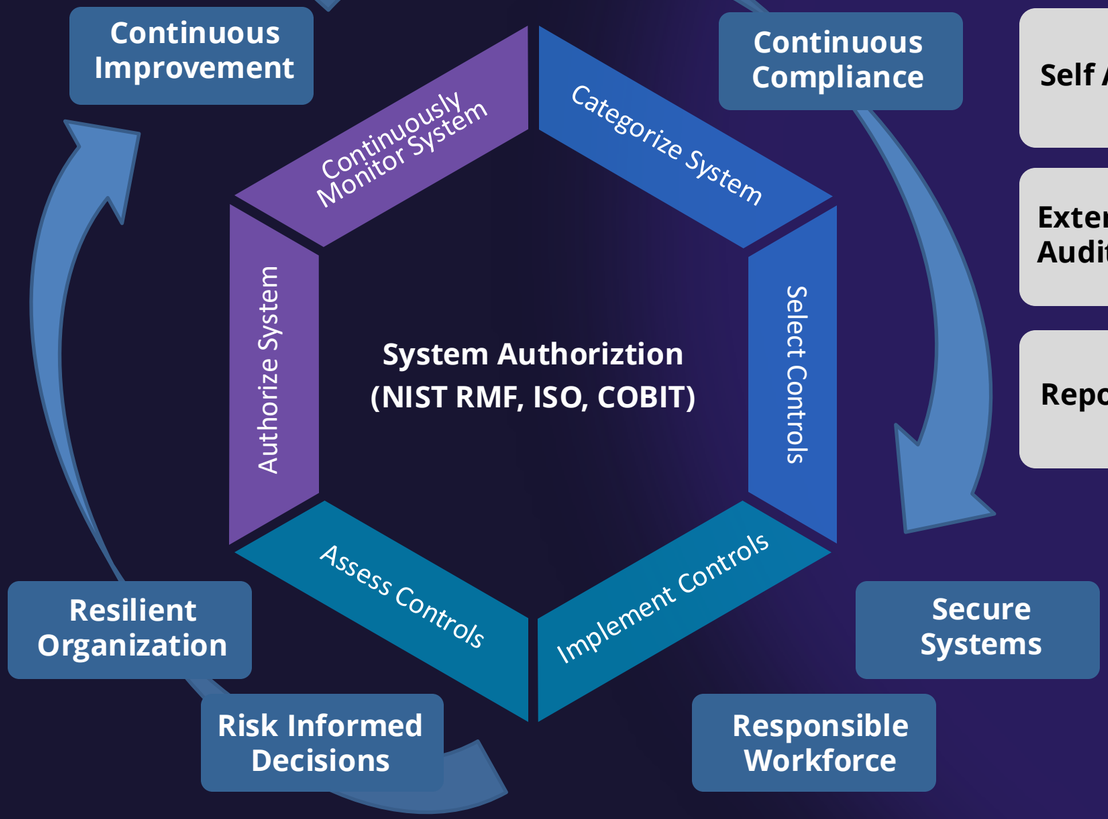
GRC PROCESS

Governance

Statutory/ Regulatory	• Laws • Statutes • Regulations
Standards	• ISO • NIST
Policies	• Organizational • Information Tech • Information security
Contracts/ Commits	• PCI • Customer Contracts • B2B Agreements
Processess & Procedures	• NIST CSF • ISO • Organizational
Controls	• Administrative • Physical • Technical

Risk

Risk Assessment	• Tier 1 - Organization • Tier 2 - Business Lines • Tier 3 - Assets (e.g Systems, People)

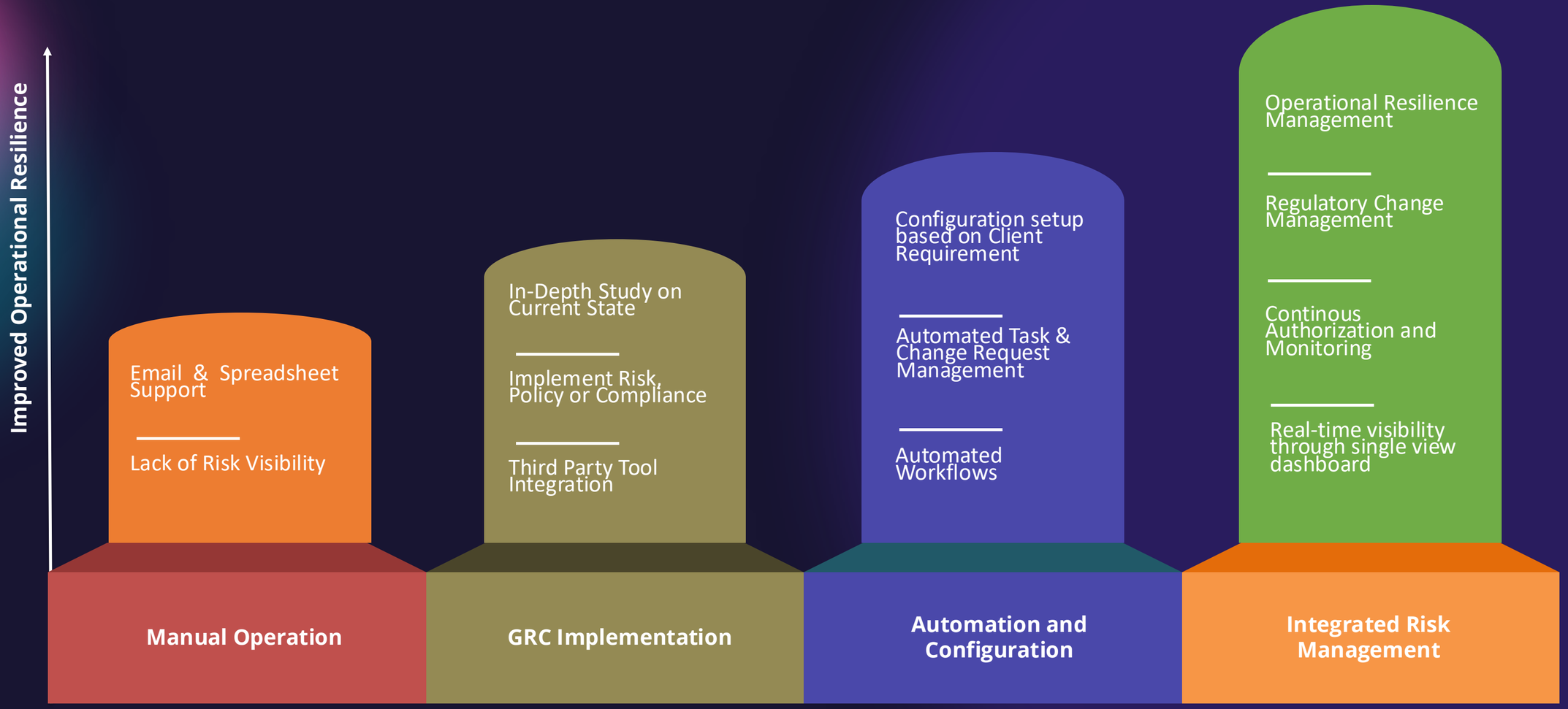


Compliance

Monitor	• Threat Landscape • Implemented Controls • Insider Behavioral Analysis
Self Assess	• Systems • Processes • Audit Preparation
External Audits	• Regulatory Audits • Standards Audits (eg. ISO) • Contractual Audits (eg. PCI)
Reporting	• InternaL • Regulatory Bodies • Customers

CyberHeals

GRC MATURITY LEVELS



CyberHeals

CURRENT STATE OF GRC

Data Silos and Integration Issues

76% of organizations find data silos hinder cross-departmental collaboration

Evolving Regulatory Landscape

45% of companies struggle to keep up with increasing regulations

CyberHeals

CURRENT STATE OF GRC

Resource Allocation and Budget Constraints

63% of organizations plan to increase GRC budgets

Measuring and Tracking GRC Performance

66% of organizations plan to implement additional automation to enhance performance tracking for GRC success

CyberHeals

THE NEED

Real-Time Compliance Updates

A platform that automatically monitors and tracks regulatory changes, updating compliance programs in real-time.

Unified Risk View

A comprehensive system that integrates risk data from various departments to provide a holistic understanding and proactive management of threats.

Enhanced Data Management and Security

Advanced data management systems that ensure the integrity, availability, and confidentiality of data across the organization.

Autonomous Gap and Risk Assessment

AI-driven systems that autonomously identify gaps in compliance and assess risks without manual intervention.

CyberHeals

AI Powered

GRC Automation Applications

SPRINTO

Scrut Automation

Vanta

UltraHeals

CyberHeals

AI-Powered Vulnerability Analysis

AI can automate the process of vulnerability scanning and assessment, identifying weaknesses in systems and applications before they can be exploited.

VULNERABILITY DISCOVERY

AI-powered scanners can identify vulnerabilities in software, hardware, and network infrastructure more quickly and efficiently than traditional methods.

RISK PRIORITIZATION

AI algorithms can prioritize vulnerabilities based on their severity, likelihood of exploitation and impact on the organization.

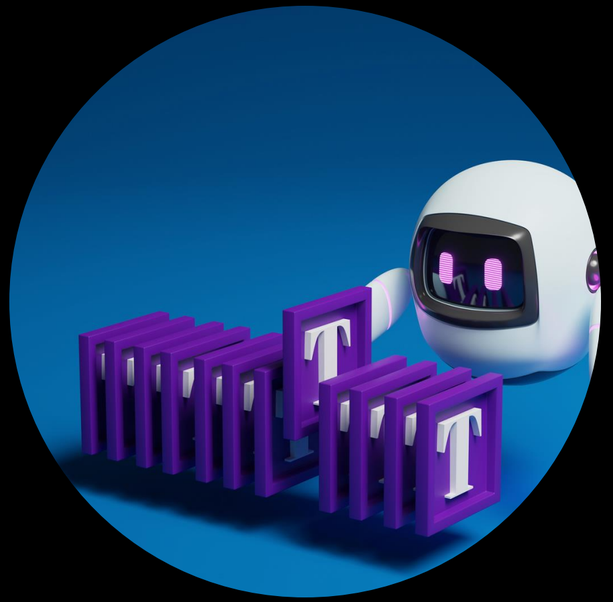
AUTOMATED PATCHING

AI can automate the process of patching vulnerabilities, ensuring that systems are up-to-date and protected againts known threats.

CyberHeals

Automated Incident Response with AI

AI can automate and accelerate the incident response process, enabling faster identification, containment, and recovery from cyberattacks.



Threat Detection

AI algorithms monitor systems and networks for suspicious activity, triggering alerts and initiating automated responses.

Incident Containment

AI-powered systems can automatically isolate affected systems, prevent the spread of malware, and mitigate the impact of attacks.

Recovery and Remediation

AI can help restore compromised systems, identify and remove malware, and implement corrective measures to prevent future attacks.

CyberHeals

COMPREHENSIVE RISK MANAGEMENT FRAMEWORK

Risk Identification

1. Multi-Framework Risk Assessment
2. Holistic Risk Landscape Overview
3. Comprehensive Asset Inventory & Risks

Control Effectiveness Evaluation

1. Assess Control Implementation.
2. Identify Common Controls
3. Evaluate Control Maturity

Unified Reporting

1. Generate Consolidated Reports
2. Clear Risk Visualization
3. Tailored Stakeholder Communication

Actionable Insights & Recommendations

1. Develop Remediation Plans
2. Prioritize Based on Severity
3. Continuous Improvement Steps

CyberHeals

AI IN GRC

AI-Driven Gap Analysis

1

Automatically identifies compliance gaps, ensuring thorough coverage of regulatory requirements.

Smart Policy Creation

2

Tailors policies to your organization's needs, incorporating best practices and standards.

Automated Risk Evaluation

3

Prioritizes risks and provides actionable insights for proactive management.

Vendor Risk Automation

4

Evaluates and monitors third-party vendors, ensuring effective risk management

CyberHeals

AI Powered

GRC Automation Applications

SPRINTO

Scrut Automation

Vanta

UltraHeals

Conclusion and Key Takeaways

Remember, GRC is not just about paperwork and checklists.

It's about creating a culture of

1. Accountability
2. Transparency
3. Proactive Risk Management.

It's about building an organization that can

1. Weather any storm
2. Seize opportunities
3. Achieve sustainable success.