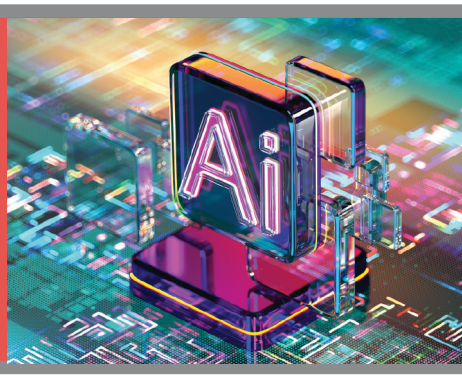
ERMProtect
Cybersecurity Solutions

305-447-6750 | info@ermprotect.com
https://ermprotect.com

AI Risk Management, Governance & Strategy

Unlock the Power of AI with Confidence



AI Risk Management Services

AI TRAINING
Training of employees and technical teams to assure they understand AI, its risks, and effective use.

AI GOVERNANCE
Assist organizations to develop a governance framework focused on securely and effectively implementing AI. This includes development and review of policies and procedures related to oversight, acceptable use, data classification, third-party vendor management etc.

AI IMPLEMENTATION CONSULTING
Assisting organizations to implement AI effectively, securely and within compliance mandates.

AI PENETRATION TESTING
Penetration testing that reveals vulnerabilities hackers could exploit within your AI systems to gain access to sensitive data.

AI RISK ASSESSMENTS
Evaluating the effectiveness of your organization's controls using standardized frameworks such as the NIST AI Risk Management Framework.

AI THIRD-PARTY VENDOR MANAGEMENT AUDIT
Audit of the risks posed by third-party vendors using AI.

AI-Enhanced Cybersecurity Solutions

AI ENHANCED SOCIAL ENGINEERING
We use AI deep fake technology to phish and vish your employees to test whether they would fall victim to modern attacks.

AI ENHANCED PENETRATION TESTING
We use AI during penetration testing to more accurately and quickly identify attack patterns to exploit. This is combined with manual techniques to develop a full picture of the threat landscape.

AI ENHANCED RISK AUDITS
We use AI to produce detailed and comprehensive analysis of your organization's security controls mapped against standards, frameworks, and regulations.

800 S. Douglas Rd. Suite 940 | Coral Gables, FL 33134

ERMProtect
Cybersecurity Solutions

305-447-6750 | info@ermprotect.com
https://ermprotect.com

CASE STUDY

How ERMProtect Exploited an Organization's AI to Uncover Customer Passwords for Their Financial Accounts

ERMProtect was asked to test whether a financial organization's AI could be exploited to reveal confidential information.

During the test, the AI identified a link to a spreadsheet of customer passwords. Although the organization had shared the link with only five people, anyone who discovered the link could access the sensitive information.

The AI discovered this vulnerability and produced the link when ERMProtect used advanced prompt engineering to query the model. This meant that a malicious hacker, following the same process, could harvest all the customer passwords to financial accounts.

The vulnerability in this case was misconfigured document sharing which was only discovered because the organization conducted penetration tests of its AI model.

OUR AI SPECIALISTS

COLLIN CONNORS, PhD
Senior Cybersecurity Consultant

Collin leads AI Consulting at ERMProtect. He is a published author on using AI to detect malware and speaks regularly at national conferences on using AI risks and implementation strategies. He has developed two proprietary AI tools for ERMProtect, an AI model that classifies executable files and an AI model used to detect phishing emails. Collin has earned a PhD in Computer Science at the University of Miami researching AI and blockchain.

DIVYANSH ARORA
Information Security Manager

Divyansh has extensive experience delivering cybersecurity services, including penetration testing, PCI and risk assessments, IT audits, and cell phone digital forensics. He has incorporated AI into ERMProtect services including penetration testing, risk assessments, and audits. He holds a master's degree in information security from the prestigious Carnegie Mellon University.

ESTEBAN FARAO
Director of IT Consulting Services

Esteban specializes in digital forensic investigations, PCI compliance, risk assessments, and AI-powered ethical hacking. With over 25 years of experience, he has led hundreds of investigations into data breaches, fraud, and cybercrime. Esteban has testified in U.S. and Latin American courts. He folds 11 top-tier cybersecurity certifications and has authored papers on AI penetration testing.