Neural Strike

BUSN30135: AI and Financial Information

Team Name: Humorous Judicious Cobra

Team Members

Caesar Lupercal

A strategic leader with years of multi-industry investment experience, growth equity involvement, and senior roles in telecom, film production, and investment banking

Christian Bohren

Founder & Principal Security Engineer at Greatheart, an Offensive Security Enginering Firm, and an MBA candidate at Chicago Booth

Prathamesh M. Saygaonkar

Corporate Strategy and M&A at Danfoss; Equity Research Analyst at Goldman Sachs, and an MBA candidate at Chicago Booth

Terence Fernandes

Over a decade at Visa with experience in a Cybersecurity startup prior, Terence is currently a Cybersecurity Sr. Director leading the global Enterprise, Mobile, IoT & Mac Security. He is a MBA candidate at Booth.

Today's Security Challenges

> **Acute Security Talent Shortage:** Workforce gap of 4.8 million professionals globally

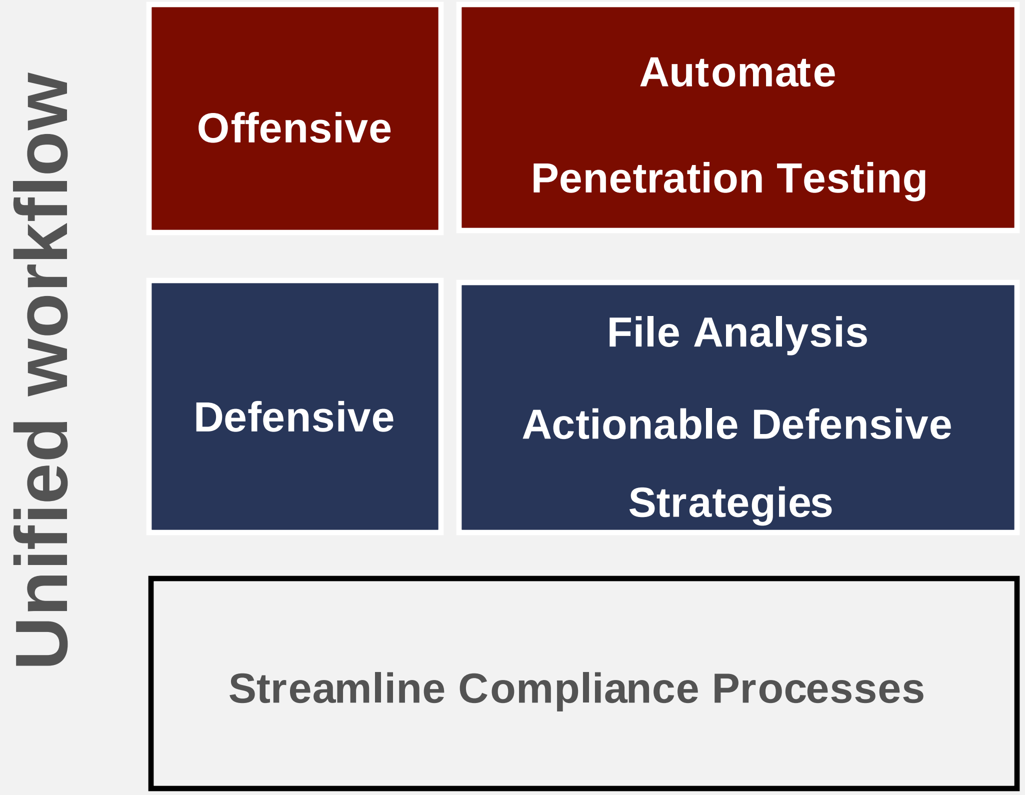
> **Expanding Attack Surface:** Cloud services, IoT, and distributed workforces increase vulnerabilities.

> **Siloed Security Operations:** Traditional separation of Red and Blue teams creates inefficiencies and communication gaps.

> **Compliance Burden:** Mounting regulations like GDPR, PCI DSS, HIPAA demand frequent assessments and documentation.

Neural Strike: Revolutionizing Cybersecurity with AI

AI-driven cybersecurity platform



Unified workflow

Offensive

Automate

Penetration Testing

Defensive

File Analysis

Actionable Defensive Strategies

Streamline Compliance Processes

How do we stand out?

- > **Unified Offense-Defense Platform**
- > **Scoring of generated security strategies recommendation and implementation gaps**
- > **Multiple AI Model Flexibility; No vendor lock-in**
- > **Tool-Specific Action Plans:** Translates strategies into executable commands
- > **Chatbot to answer questions**

CHICAGO BOOTH

HUMOROUS JUDICIOUS COBRA

Why It Matters: Addressing Critical Challenges

The Need for AI-Powered Security

- > AI-driven cyber threats growing in sophistication.
- > Manual penetration testing becoming expensive and time-consuming.
- > Traditional security defenses failing to prevent modern attacks.

Our platform solves these challenges by

- > Bridging offense & defense to provide a unified security approach.
- > Automating security processes to reduce reliance on human expertise.
- > Providing real-time, AI-driven responses to security threats.

How does it work?

Offense: AI-Powered Penetration Testing

Defense: AI-Based Security & Monitoring

> Leverages various LLMs to generate methodologies mapped to industry standards like OWASP and NIST

> Uses multi-model peer-review to evaluate the methodology and tailor it to the use cases and context

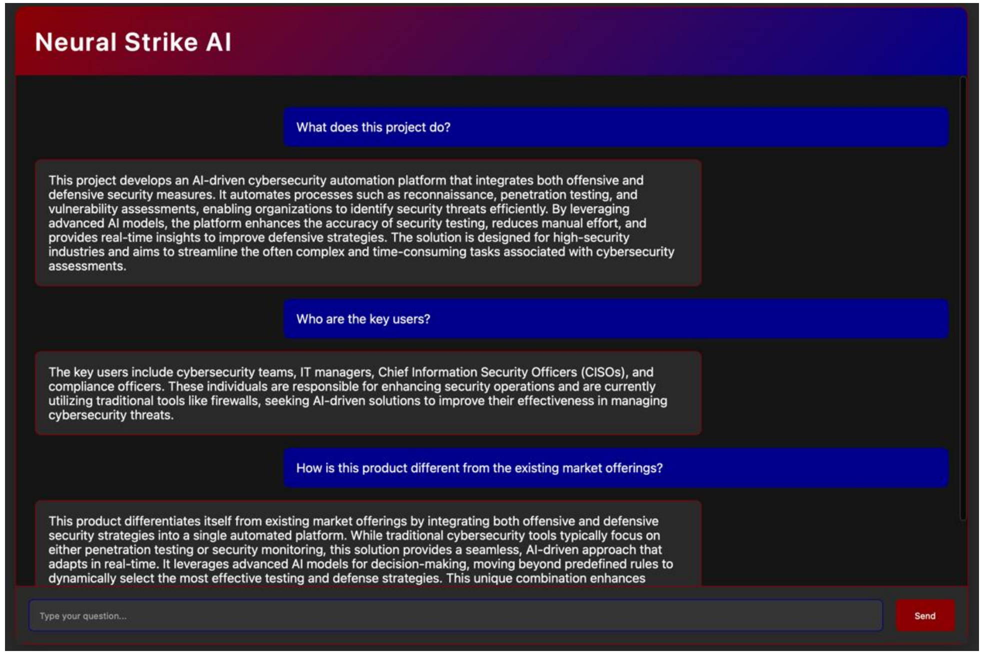
> Guide the analyst through the pen-test process with the option to fully automate it through Agentic tools

Neural-Strike Interactive Assistance Chatbot

Key Features

- Provides real-time guidance on methodology implementation
- Answers technical questions about security tools and techniques
- Helps interpret AI-generated offensive and defensive recommendations
- Offers contextual assistance during penetration testing and hardening activities

"Our integrated chatbot reduces the learning curve for new users while providing advanced teams with immediate access to detailed security information without disrupting their workflow."



Neural Strike AI

What does this project do?

This project develops an AI-driven cybersecurity automation platform that integrates both offensive and defensive security measures. It automates processes such as reconnaissance, penetration testing, and vulnerability assessments, enabling organizations to identify security threats efficiently. By leveraging advanced AI models, the platform enhances the accuracy of security testing, reduces manual effort, and provides real-time insights to improve defensive strategies. The solution is designed for high-security industries and aims to streamline the often complex and time-consuming tasks associated with cybersecurity assessments.

Who are the key users?

The key users include cybersecurity teams, IT managers, Chief Information Security Officers (CISOs), and compliance officers. These individuals are responsible for enhancing security operations and are currently utilizing traditional tools like firewalls, seeking AI-driven solutions to improve their effectiveness in managing cybersecurity threats.

How is this product different from the existing market offerings?

This product differentiates itself from existing market offerings by integrating both offensive and defensive security strategies into a single automated platform. While traditional cybersecurity tools typically focus on either penetration testing or security monitoring, this solution provides a seamless, AI-driven approach that adapts in real-time. It leverages advanced AI models for decision-making, moving beyond predefined rules to dynamically select the most effective testing and defense strategies. This unique combination enhances

"Think of it as having a cybersecurity expert available 24/7 to guide your team through complex security procedures."

Who We Serve: Target Industries & Customers

Industries

- **Finance:** Banks, hedge funds, payment processors (must comply with PCI DSS, SOC 2).
- **Healthcare:** Hospitals, telemedicine providers (need HIPAA-compliant security).
- **Technology:** SaaS platforms, cloud providers, data centers.

Use Cases

- **Automated penetration testing** to find vulnerabilities before hackers do.
- **Continuous security monitoring** for cloud and on-prem infrastructure.
- **AI-driven compliance validation** to meet regulatory standards.

Buyer Personas

- **Cybersecurity Teams** – Need automation to enhance efficiency
- **IT Managers** – Require integrated solutions for security
- **Chief Information Security Officers (CISOs)** – Need proactive security to meet compliance.
- **Compliance Officers** – Ensure regulatory adherence with audits.

Why Our Solution Stands Out

What makes it unique:

Our AI-driven cybersecurity platform is the first to seamlessly integrate offensive and defensive security strategies into a single, automated system.

Key Differentiators

- **AI-Driven Decision Making:** Unlike traditional tools, our platform uses LLMs and machine learning to dynamically adapt security strategies.
- **Automation at Scale:** Combines AI-powered penetration testing with automated security hardening, reducing manual effort while improving accuracy.
- **Self-Learning System:** Continuously improves based on past assessments, making security more adaptive over time.
- **Customizable & Modular:** Works across different security environments, including web applications, cloud infrastructure, and mobile security.

Demo

Thank you!
Q&A