GREG IHESIABA

AI SECURITY | CYBERSECURITY ENGINEERING | INFORMATION SYSTEMS | RISK & GOVERNANCE

DENVER, COLORADO

GEETECH | GEETECHS.COM

I believe the next generation of cybersecurity leadership has to accomplish two things at once: protect the enterprise from rapidly evolving threats and create a secure path for the organization to innovate with AI.

That intersection is central to the work I am building at GeeTech.

I founded GeeTech in 2025 around my background in Information Systems Engineering and Management Information Systems and a belief that sophisticated cybersecurity should translate into practical business protection. As Principal Consultant, I lead work across vulnerability management, incident response, endpoint protection, security operations, compliance, risk assessment, and cybersecurity strategy.

I am also finalizing the **GeeTech Proprietary 8-Layer Cybersecurity Software Package**, an integrated platform designed to bring multiple layers of cyber defense into a structured security ecosystem. The package incorporates capabilities including Vulnerability Assessment, Incident Response Planning, Endpoint Security, security risk assessment, threat detection and prioritization, monitoring, governance support, and remediation guidance.

Building that platform has required me to think beyond individual security tools. It requires looking at how vulnerabilities connect, how risk should be prioritized, how security information should reach decision-makers, how organizations prepare before incidents occur, and how emerging technologies such as AI can strengthen security without creating unmanaged risk.

Through GeeTech, my work includes AI-driven risk assessment and continuous monitoring, vulnerability analysis, SOC investigation, incident response planning, endpoint security, EDR/XDR, phishing analysis, executive security reporting, and compliance readiness aligned with NIST, HIPAA, and ISO 27001.

I understand that an enterprise AI Security program cannot exist solely to restrict technology. It must establish the governance, architecture, controls, risk methodologies, and accountability that allow an organization to use AI responsibly and securely. That means partnering across technology, architecture, engineering, legal, privacy, procurement, risk, and business leadership while maintaining a clear understanding of the evolving threat environment.

I would welcome the opportunity to bring that combination of cybersecurity engineering, AI-enabled security innovation, risk management, product development, and business-focused leadership to your organization and help build an AI Security program capable of protecting the enterprise while enabling what comes next.

Sincerely,

Greg Chizoba Ihesiaba
Principal Consultant
GeeTech

GREG IHESIABA

AI SECURITY | CYBERSECURITY ENGINEERING | INFORMATION SYSTEMS | RISK & GOVERNANCE

DENVER, COLORADO
GEETECH | GEETECHS.COM

EXECUTIVE PROFILE

Cybersecurity and information systems leader specializing in security engineering, AI-enabled cyber defense, enterprise risk management, vulnerability management, incident response, endpoint security, compliance, and secure technology architecture.

Founder and Principal Consultant of GeeTech, a cybersecurity engineering and advisory company launched in 2025 to help organizations identify vulnerabilities, reduce technology risk, strengthen cyber resilience, and establish practical security and compliance programs.

2026 GeeTech Initiative, the **GeeTech Proprietary 8-Layer Cybersecurity Software Package**, an integrated security platform designed to provide organizations with a layered approach to cyber defense across critical capabilities including Vulnerability Assessment, Incident Response Planning, Endpoint Security, risk visibility, and security operations.

Combines Information Systems Engineering and Management Information Systems expertise with a business-focused approach to cybersecurity, translating technical vulnerabilities, emerging threats, regulatory requirements, and security architecture into actionable strategies for organizational leaders.

CORE LEADERSHIP COMPETENCIES

AI Security Strategy & Governance | Cybersecurity Architecture | AI-Driven Risk Assessment | Information Systems Engineering | Enterprise Risk Management | Vulnerability Management | Incident Response | Endpoint Security | EDR/XDR | Threat Detection | Security Operations | Security Policy & Governance | Compliance Readiness | NIST Frameworks | HIPAA | ISO 27001 | Security Assessments | Threat Modeling | Third-Party Risk | Executive Reporting | Security Awareness | Phishing Defense | Data Protection | Security Program Development

PROFESSIONAL EXPERIENCE

GEETECH

Founder & Principal Consultant, Information Systems Engineering & MIS
Denver, Colorado | 2023–Present

Founded GeeTech to deliver practical, enterprise-grade cybersecurity engineering, advisory, risk management, and compliance solutions designed to strengthen organizational cyber resilience.

- Lead cybersecurity strategy, security engineering, risk assessment, solution architecture, and advisory engagements across organizations with varying security maturity levels.
- Translate cybersecurity risk into actionable technical and business priorities, connecting security investments with operational resilience, compliance requirements, and organizational objectives.
- Design layered security approaches addressing vulnerabilities across users, endpoints, applications, infrastructure, policies, processes, and organizational controls.
- Advise organizations on cybersecurity readiness, risk reduction, incident preparedness, endpoint protection, identity security, and security governance.
- Develop executive-facing security assessments, risk prioritization frameworks, remediation recommendations, and implementation roadmaps.
- Integrate technical security considerations into business processes through cross-functional consultation, education, and risk-based decision-making.

AI SECURITY & SECURITY INNOVATION

- Develop AI-enabled approaches to cybersecurity risk assessment, threat detection, prioritization, monitoring, and security decision support.
- Apply AI-driven analysis to identify vulnerabilities, prioritize security exposure, strengthen monitoring, and accelerate remediation planning.
- Evaluate emerging cybersecurity threats and attack patterns to strengthen defensive architecture and organizational preparedness.
- Advance secure, responsible adoption of AI-supported cybersecurity capabilities while maintaining human oversight and risk-based governance.
- Design security approaches intended to evolve with emerging technologies, changing attack surfaces, regulatory expectations, and adversarial techniques

GEETECH PROPRIETARY 8-LAYER CYBERSECURITY SOFTWARE PACKAGE

Product Architect & Security Lead | In Final Development

Leading the strategy, architecture, and finalization of GeeTech's proprietary **8-Layer Cybersecurity Software Package**, an integrated cyber defense solution designed to provide organizations with structured, layered protection and greater security visibility.

The platform incorporates critical cybersecurity capabilities including:

- Vulnerability Assessment
- Incident Response Planning
- Endpoint Security
- Security Risk Assessment
- Threat Detection & Prioritization
- Security Monitoring
- Compliance & Governance Support
- Security Reporting & Remediation Guidance

SELECTED SECURITY PROJECTS

Vulnerability Assessment
Performed security assessment utilizing Nessus and Metasploit, identifying 23 critical findings and developing a prioritized remediation roadmap.

SOC Incident Investigation
Applied Splunk analytics to investigate security events and identify activity associated with a simulated advanced persistent threat scenario.

Healthcare Security Risk Assessment
Conducted a simulated HIPAA-focused cybersecurity gap assessment and developed an 18-item risk register to prioritize remediation.

Network & Packet Analysis
Performed Wireshark-based PCAP analysis to identify suspicious network activity and command-and-control beacon behavior.

Phishing & Social Engineering Analysis
Analyzed phishing communications, identified indicators of compromise, and translated technical findings into security-awareness material.

Security Policy & Governance
Developed security policy frameworks and templates addressing incident response, acceptable use, vendor risk management, access control, and organizational security practices.

TECHNICAL & SECURITY EXPERTISE

Security Operations: Vulnerability Assessment, Incident Response, Threat Detection, Security Monitoring, Risk Assessment, SOC Investigation, Phishing Analysis, Endpoint Security

Security Technologies: Nessus, Metasploit, Splunk, Wireshark, EDR/XDR, MFA, Email Security

AI & Emerging Security: AI-Driven Risk Assessment, AI-Assisted Threat Detection, Security Automation, AI Security Governance, Emerging Threat Analysis

Frameworks & Governance: NIST Cybersecurity Framework, NIST-aligned Risk Management, HIPAA Security, ISO 27001, Security Policy Development, Vendor Risk Management, Compliance Gap Assessment

Executive & Business: Cybersecurity Strategy, Security Architecture, Risk Prioritization, Executive Reporting, Security Roadmaps, Business Risk Alignment, Project Management, Cross-Functional Collaboration.