Gilles S. Biagomba

Philadelphia, PA (484) 619-3275 gilles.biagomba@live.com GitHub LinkedIn

Application, AI/ML, Offensive Security & Cyber Security Leader

Innovative, adaptable, and results-driven Security Engineer with 7+ years of experience specializing in **AI/ML security, penetration testing, application security, and cloud security**. Proven expertise in **identifying and mitigating complex security risks**, securing large-scale AI systems, and collaborating cross-functionally to build resilient security architectures. Strong **problem-solving skills, leadership in high-stakes environments, and ability to bridge security gaps between development and business teams**. Recognized for **mentorship, technical excellence, and strategic thinking** in security initiatives across **Big Tech environments**.

Technology Summary

Certifications:	**Possesses** CB Response Admin, CB Response Advance Admin & **Pursuing** OSWE
Systems:	Windows (e.g., 7-11, Server 2008-2020), UNX/NIX (e.g., RHEL/CentOS, Debian/Ubuntu/kali, BSD, MacOSX)
Languages:	Beginner – Assembler, C/C++, PowerShell, Rust Intermediate – HTML5, Go, Java, JavaScript, Python Advanced – Bash/Shell Fluent – English, French
Software:	AWS, Azure, Burp Suite, Carbon Black, Chatbox AI, ChatGPT, Claude, Checkmarx, Codename Goose, Command Prompt (Windows), Crowdstrike, Cygwin, DeepSeek, Docker, Firefly, Gemini, GCP, Hashcat, Hugging Face, John The Ripper, HP Fortify, Hydra, Kali, LangChain, LangGraph, LangSmith**,** LLM/SLM/VLM, Llama, Metasploit Pro, Molmo LLM, MS Threat Modeler, Nessus, Nexpose, Nmap, Ollama, OWASP Threat Dragon, PE Frame, Qualys, SonarQube, Symantec DLP, Symantec Endpoint Protection, Terminal (Linux), Veracode, Virtual Box, vLLM, VMware Workstation, VS Code, Wireshark
Skills:	Active Directory, AI/ML Security, Application Security, Automation, Bilingual, Blue Team, CI/CD, Cloud Security, Coding, Compliance Auditing, Containerization, Cross-functional Collaboration, Customer Service/Support, DAST, Data Analysis, Digital Forensics, DevOpsSec, DevSecOps , Entrepreneurship, Ethical Hacker, Firewalls, Flexible, IAST, Identity & Access Management (IAM), Incident Response, Information Security, Interpersonal Relationships, Kubernetes, Leadership, LLM, Mobile Applications, Network Security, Offensive Security, OpenStack, Orchestration, Penetration Tester, Physical Security, Policy Writing, Problem Solving, Project Management, Purple Teaming, Quality Assurance, RASP, Red Team, Reverse Engineering, Risk Assessment, Risk Management, Salesmanship, SAST, Scripting, SecDevOps, Secure Code Review, Secure Development Lifecycle (SDL), Security Engineering, Security Management, Security Operations, Self-Motivated, Social Engineering, Software Development, System Administration, Team-Player, Technical Support, Threat Modeling (e.g., STRIDE, PASTA, OCTAVE, MAESTRO, DREAD) , Web Application Security, Zero Trust Architectures
Laws/Regulations:	CCP, GDPR, HIPAA, ISO 27001/2, NIST SP800, OSWAP Top 10, OWASP Top 10 Risks for LLMs , PCI DSS 3.2, SANS Top 25, SOX, WASC Threat Classification v2.0

Professional Experience

Adobe Inc., Philadelphia, PA (January 2024 - Present)

- **Senior Product Security Engineer** - Working on AI/ML security, IAM service revamping, and xR/AR/VR/MR technologies. Conducting static, dynamic, and interactive application security testing (SAST/DAST/IAST). Conducting code reviews across multiple programming languages and negotiating security contracts with third-party software vendors. Experienced in purple team engagements and collaborating with red teams to enhance security posture.
    - Spearheading **AI/ML security initiatives**, ensuring compliance with industry-leading best practices for model integrity, adversarial robustness, and data protection. Developed a comprehensive **AI threat modeling framework**, enhancing the organization's ability to anticipate and mitigate potential AI-specific security threats
    - Led the **revamp of Identity & Access Management (IAM)**, strengthening authentication mechanisms and access control policies across critical systems. Implemented a **role-based access control (RBAC) system**, reducing unauthorized access incidents by 25%
    - Conducting **static, dynamic, and interactive application security testing (SAST/DAST/IAST)** to fortify software against evolving threats. Established an **automated security testing pipeline**, decreasing manual testing efforts by 30% and accelerating release cycles
    - Partnering with development teams to embed **secure coding practices** into the SDLC, reducing vulnerabilities by 40% before production releases
    - Collaborating with **red and blue teams** to identify security gaps, enhance detection capabilities, and refine incident response strategies

Amazon (Consumer Payment), Arlington, VA (June 2022 - December 2023)

- **Application Security Engineer** - Working closely as a dedicated product security engineer with service teams, & technical product managers (PM). Triaging findings in our bug bounty program and conducting security assessments (e.g., code reviews, design reviews, penetration tests) of Amazon Pay products.
    - Led a risk management project in our software development organization to address the security risks of outdated third-party libraries. Initiated a comprehensive audit of our software stack, identified vulnerable components, and established a streamlined process for monitoring and applying security updates. This proactive approach significantly improved our product's security and minimized potential security threats, emphasizing our dedication to protecting customer data and system integrity
    - Improved Amazon Pay security posture by performing a security assessment of new payment instruments (i.e, P2P payment apps, bank debit/transfer services, and cash) to ensure a secure product launch. Performed security consultations with service teams to help address conflicts between product designs and security policies. Assisted with triaging new bug bounty findings by validating findings and working with service teams to resolve the issues. Documented application workflow for bug bounty researchers to help identify targets of interest
    - Implemented and streamlined automated pen-testing framework processes to ensure all applications and services were tested using the same set of tools, and reported using the same reporting template and language. Ensured results from all scanning tools were displayed in one centralized dashboard and data is organized by application or service. This ensured most pentests to be completed within two-to-three-week SLA
    - Documented a 'Dogs Not Barking' strategy on Amazon Pay resulting in raising the security bar by pushing AWS products (e.g., S3, EC2, SNS, etc.) to be configured with secure best practices by default. The document proposed AWS apps and services using third-party software with known vulnerabilities. Lastly, proposed a radical shift in RBAC permissions in Amazon services (e.g., Prime, Pharmacy, Payments, etc.) to help prevent data leakage and limit cross-domain permission abuse
    - Collaborated with the threat intelligence team by creating a dashboard for tracking critical and high CVEs and pairing them to known CPE (Common Platform Enumeration strings) within Amazon Pay. Enabled security engineers to track emerging threats within financial services and e-commerce. Enabling business leaders to make informed decisions– Improving response time to incidents and better workload balancing
    - Assisted in red team operations and campaigns, improved red team engagement process with new tooling process (e.g., gowitness, nuclei, custom scripts). Helped significantly reduce time spent on identifying web services and conducted secure code reviews of web applications written in Java to identify vulnerabilities that can be leveraged by the red team

Comcast Corporation, Philadelphia, PA (April 2021 to June 2022)

- **Senior Offensive Security Engineer** - Working closely with application development teams, product managers (PM), and third-party groups (including the paid bug bounty program) to ensure that Comcast products and services are secure.
    - Administered recruitment engagement, actively contributed to, and participated in community work (i.e., Black Is Tech, IEEE, UTP), and mentorship – Built strong relationships with product development teams and their leadership
    - Directed highly coordinated red team (Mean-Time-Breach) & purple team (Mean-Time-Detect) engagements of the company network and services then conducted security assessments (e.g., code reviews, and static/dynamic testing) of critical systems, cloud services, and internal apps
    - Developed automated security testing and auditing tools (e.g., Odin, Sherlock, and Tron) and advised teams on best practices for secure development of products & services
    - Led platform-specific (i.e., Windows, Linux) & web application security assessments – including reporting zero days and other security-related issues to third-party vendors
    - Identified security risks by conducting security code reviews for applications written in C/C++, Java, Groovy, Golang, Python, and JavaScript.

Comcast Corporation, Philadelphia, PA (April 2019 to March 2021)

- **Offensive Security Engineer** - Analyzed web applications, and remote endpoints (e.g., IoT devices, Windows/Linux servers, etc.) for software defects (vulnerabilities). Recommended ways to mitigate or remediate the risks of findings. Used a combination of automation and manual testing to perform and developed tools and web services to automate workloads.
    - Performed network penetration tests of IoT devices and servers (Linux/Windows) and completed several static and dynamic security assessments of first and third-party web applications, cloud instances, and source code
    - Advised developers and infrastructure teams on remediating security findings and continually provided recommendations for emerging technologies, products, and solutions while maintaining alignment with enterprise needs
    - Collaborated with stakeholders to gather technical requirements, architect solutions, and execute on deliverables
    - Recommended innovative and automated approaches for operational tasks which leveraged available resources and simplified operational overhead – providing measurable impact, scalability, stability, and security
    - Identified opportunities for process improvements and established department standards to ensure comprehensive assessments across various systems and networks

National Board of Medical Examiners, Philadelphia, PA (May 2017 to March 2019)

- **Application Security Analyst** - Analyzed web applications and remote systems for software defects (vulnerabilities). Recommended and developed security measures to protect company digital assets against unauthorized access, modification, manipulation, or destruction.
    - Fielded threat modeling exercises using the STRIDE testing methodology and delivered technical reports/papers on test findings
    - Executed various web application security assessments across multiple architectures and environments and proficiently developed new tools/scripts to automate security testing (See GitHub)
    - Assisted with Vulnerability and Patch Management by providing risk-based patching and boasted value to the organization by leveraging red/blue team experience to highlight security gaps
    - Advised in discovering, implementing, and deploying security appliances (i.e., SIEM, EDR) responded to security-related incidents, and provided thorough post-event analysis
    - Defined, implemented, and maintained corporate security policies to determine the most effective way to protect computers, networks, software, data, and information systems against possible attacks

Protiviti Inc., Philadelphia, PA (Feb 2016 to May 2017)

- **IT Security Consultant** - Participated in multiple client projects across multiple industries such as financial services, and pharmaceuticals. Conducted vulnerability scans and penetration tests of the network and implemented secure changes after submitting the report. Interpreted, and applied standards, policies, and best practices and analyzed threats and vulnerabilities, then designed system security strategy and architecture. Promoted the use of security requirements for the System Development Life Cycle across multiple projects and enterprises.
    - Coordinated PCI vulnerability management assessments using industry-recognized scanning tools and manually tested/validated findings discovered by scanners
    - Managed static and dynamic code analysis to automate the code review process and manually verified findings
    - Participated in red-team engagements of external (internet-facing) & internal (on-premise) infrastructure and used various information-gathering methods (e.g., social engineering, OSINT, scanners) to conduct the assessments
    - Assisted clients with improving their patch management program by interviewing staff and heads of departments to determine specific security issues
    - Delivered detailed technical reports to technical teams and delivered executive-friendly presentations to client stakeholders

David's Bridal Inc., Conshohocken, PA (Sep 2014 to Jan 2016)

- **IT Security Administrator** - Analyzed and consulted on Security-related matters by aiding in troubleshooting network access problems and implementing network security policies and procedures. Ensured network (LAN/WAN, telecommunications, and voice) security access and actively monitored security tools and vulnerability releases.
    - Organized security gap analysis of infrastructure and aided in the acquisition of security products to help fill gaps. Operated with vendor engineers to deploy and implement said security products
    - Collaborated with various teams to resolve security incidents and reported incidents to upper management
    - Created scripts/tools to automate PCI audits, configure upgrades, and harden UNX/NIX-based servers and saved the company time and resources
    - Developed and managed Vulnerability Management program by performing vulnerability scans of corporate and retail networks, used threat intelligence feeds to enhance vulnerability data, and implemented automatic blocking of malicious hosts, and known malicious files (hash/signature-based)
    - Audited & documented best security practices and standards (e.g., PCI 3.0, FISMA/NIST800, SANS Critical Security Controls) and rigorously reviewed new software & technologies

Leadership & Mentorship

- Active mentor in cybersecurity communities, guiding junior security engineers in red teaming, pentesting, and AI security
- Engaged in public speaking at security conferences (e.g., BSides Bucharest), presenting on threat modeling AI and security automation
- Champion of diversity & inclusion in cybersecurity, advocating for equitable access to cybersecurity education and career opportunities
- Advisor to university cybersecurity clubs, providing guidance on curriculum development and hands-on training exercises
- Organizer of local Capture The Flag (CTF) competitions, fostering practical skills and community engagement among aspiring security professionals

Personal Projects & Research

- Anubis Security Tool (Rust) – Developed a malware analysis tool using peframe and CVE-bin-tool, automating security assessments for executable files
- AI Model Security Research – Conducting ongoing research into adversarial ML attacks, model poisoning, and secure AI model deployment strategies
- Threat Modeling the Death Star (BSides Bucharest 2024 Presentation) – Applied STRIDE, DREAD, and PASTA methodologies to analyze fictional and real-world security architectures
- **Odin, Sherlock, and Tron Security Tools** – Developed **custom security automation tools** to enhance vulnerability detection and streamline remediation workflows.

Education

East Stroudsburg University, East Stroudsburg, PA

- **B.S. in Computer Science, May 2014**
    - Concentration in Information Security and a sub-focus in Network Security, Digital Forensics, Policy Writing, and Information System Auditing