# Kendall Hastings

Chattanooga(Open to relocation), TN |423-677-0469 | kendall.hastingscs@gmail.com | [LinkedIn](#) | [Cybersecurity Portfolio](#)

Information Systems Security Officer (ISSO) with over 5 years of experience in IT and software development, currently completing the Google Cybersecurity Professional Certificate. Proven leader with expertise in asset management, Linux, Python, Xcitium, and security procedure development. Seeking a cybersecurity role where I can apply my skills and contribute to organizational growth and stability.

## RELEVANT SKILLS & EXPERTISE

**Tools/Languages:** Linux, Windows, SQL (BigQuery), Splunk, WireShark, Tcpdump, Suricata, Python, ChatGPT, Java, C#, XML, Remote desktop clients such as windows RDP and comodo remote desktop.
**Security Practices:** Information Security, Network Security, Vulnerability Assessment, Threat Analysis, Log Analysis, Security Frameworks and Controls
**Software Platforms:** Google Workspace, Slack, Genuity Ticketing and Asset Management system, Xcitium SIEM, Duo authenticator, Microsoft 365
**Strengths:** Problem-Solving, Attention to Detail, Calmness Under Pressure, leadership, Innovation, process development.

## CYBERSECURITY PROJECTS

**TryHackMe Rooms:** Utilized interactive, gamified virtual environment to enhance practical knowledge and hands-on skills:
- **Linux Fundamentals** (1, 2, & 3) and **Linux Strength Training** - Navigated directories and files, adjusted permissions, analyzed logs, explored common utilities
- **Intro to Logs** and **Log Analysis** - Identified log types, located logs, employed regular expressions (RegEx), and utilized command line and CyberChef for effective log analysis
- **Wireshark Basics** and **Wireshark 101** - Gained proficiency in packet dissection, navigation, and filtering techniques; analyzed ARP, ICMP, TCP, DNS, HTTP, and HTTPS traffic for network troubleshooting and security analysis
- **Windows Fundamentals** (1, 2, & 3) and **Windows Forensics** (1 & 2) - Acquired fundamental understanding of Windows, including file systems, user account control (UAC), control panel, system configuration, security, firewall, registry, and FAT/NTFS file systems; developed skills in accessing hives, utilizing registry explorer, and recovering files
- **Splunk Basics**, **Incident Handling with Splunk**, and **Splunk** (2 & 3) - Developed skills in navigating Splunk; conducting incident handling using Splunk; participated in the Boss of the SOC investigation for security analysis

## PROFESSIONAL EXPERIENCE

**Information system security officer(ISSO)•** *Diversified Supply, Chattanooga, TN*                                    **8/2024-Present**
- Developed and implemented security solutions that reduced phishing incidents by over 70%. Created and delivered security training programs for employees, including live presentations and demonstrations of controls to mitigate external threats.
- Identified and notified management of potential security risks, leading to a reduction in security incidents by over 40%.
- Authored a System Security Plan (SSP) in accordance with NIST SP 800-171 Rev 2, which contributed to securing a bid valued at over $400 million.
- Managed and secured legacy assets by maintaining an inventory and conducting asset security evaluations. Established a partnership with a local disk destruction center, resulting in the removal of over 300 outdated disks and 100 legacy computer models, mitigating risks of data breaches.
- Initiated a data destruction program, achieving 100% compliance with company data protection regulations. Successfully processed over 70 TB of sensitive data, eliminating the risk of data compromise through improper disposal.
- Enhanced helpdesk operations by implementing a unified ticketing system, optimizing workflow processes to reduce response times by 40%, and increasing first-contact resolution rates from 50% to 80%.
- Created comprehensive documentation and training materials for the Genuity Ticketing System, including an interactive FAQ and advanced automations. This led to a 50% reduction in onboarding time for new IT staff and a 30% decrease in repetitive support requests.
- Performed periodic audits of system health and security posture, as well as quarterly risk assessments. Developed specialized training courses to increase security awareness across the organization.

**Java Software Developer •** *Infosys, Remote*                                                                                    **2019 - 2023**
- Designed and developed custom software solutions for over 50 clients, addressing complex business challenges using Java (Spring Boot, Hibernate), with a focus on performance, scalability, and maintaining best practices for secure coding.

- Collaborated with cross-functional teams in an Agile environment, utilizing tools like JIRA and Confluence to efficiently track development progress, while ensuring that product iterations aligned with both business needs and secure development guidelines.
- Developed automation tools and ERP systems, leveraging frameworks like Spring MVC, Spring Boot, and Hibernate, and implemented RESTful APIs to ensure seamless integration with client systems. Applied encryption techniques (AES, RSA) for handling sensitive data.
- Implemented authentication and authorization mechanisms using Spring Security and JWT, ensuring users had the correct access without impacting the performance or functionality of the applications.
- Conducted code reviews using tools like SonarQube to ensure code quality and maintainability, while also identifying and fixing potential vulnerabilities before deployment.
- Optimized and integrated CI/CD pipelines with tools such as Jenkins and Maven, facilitating smoother software releases. Incorporated basic security checks as part of the build process to ensure that software complied with internal and external security requirements.
- Developed software in compliance with industry regulations such as GDPR and ISO/IEC 27001, ensuring data privacy requirements were met, and security risks were minimized.
- Utilized SQL and NoSQL databases like MySQL and MongoDB, ensuring data integrity and applying proper encryption where necessary to protect sensitive information in storage.

**Senior Helpdesk associate** • *Amazon, Remote (Worked at the same time as infosys)*                    **2019 - 2022**
- Connected with over 10,000 end users to resolve complex issues, with a first contact resolution rate of over 70%
- Handled any escalated issues in an efficient and timely manner and had a customer satisfaction rate of over 90%
- Led a team of over 100 associates and resulted in group cooperation and effective solution resolution, contributing to a satisfaction rating among my team alone of over 70%
- Troubleshooted end users systems such as amazon alexa, kindle tablets, amazon firesticks, and third party partner devices.
- Maintained business facing support for employees with technical issues and maintained active directory and onboarding of new users assigned to my group. Also did troubleshooting for VPN issues,  and any internal network issues an amazon associate may have.

---

**EDUCATION, CERTIFICATES, & CERTIFICATIONS**

---

**Google Cybersecurity Professional Certificate** • *Merit America, Remote*                    **12/2024**
- Cultivated holistic understanding of cybersecurity's critical role in organizational security, privacy, and success, including how to systematically identify and mitigate risks, threats, and vulnerabilities
- Gained practical experience with **Linux**, **SQL**, **Python** and utilized **SIEM tools**, **IDS**, and **network protocol analyzers** for proactive threat management
- Applied knowledge to real-world scenarios, developing skills in proactive **threat detection** and **response** through completion of dynamic hands-on projects, including: conducting a simulated **security audit**, responding to a **cyber incident**, analyzing **vulnerable systems**, and completing an **incident handler's journal**

**Woz U Java certification**

**CompTIA A+** • *CompTIA*
Successful candidates will have the following skills:
- Install and configure end-user devices and software.
- Connect devices to networks.
- Perform basic cybersecurity mitigations.
- Troubleshoot common problems to diagnose and resolve issues.
- Demonstrate basic knowledge of scripting, the cloud, and virtualization.

**Harvard university CS50 certification** • *Harvard university*
Develops skills in basic computer-science knowledge.