Joshua Gaede

- Email: Joshua.S.Gaede@gmail.com
- Phone: 010-2841-1408 / +82-10-2841-1408
- Website: https://kalifornia909.info
- Github: https://github.com/zer0sense

Objective

Passionate cybersecurity professional dedicated to lifelong learning and innovative problem-solving. Demonstrated expertise in tackling complex challenges, particularly in large-scale migration and technical issues, to restore business operations. Continuously expanding knowledge of emerging technologies and cybersecurity trends to develop creative solutions that enhance and fortify business security postures.

Key Cyber Security Achievements

- **Offensive Cybersecurity Skills:**
  - Currently ranked in the top 4% of 929,000 users on the hands-on offensive cyber range, TryHackMe.
  - Successfully completed challenges like Advent of Cyber 2020/2021 using chained exploitation techniques and mainstream ethical hacking tools.
  - Proficient in enumerating target machines using tools like nmap, Burpsuite, gobuster, smbclient, and Wireshark.
  - Skilled in exploiting vulnerabilities with techniques such as reverse/bind shells, cross-site scripting, and Metasploit.
  - Experienced in privilege escalation using tools like linpeas and researching software versions for exploitable CVEs on Rapid7 and Exploit-DB.
  - Capable of identifying and exploiting OWASP Top 10 misconfigurations and vulnerabilities, including SQLi, XXE Payloads, and IDOR vulnerabilities.
- **Hands-On Cybersecurity Research:**
  - Configured a type 1 hypervisor to establish a Windows Server 2019 active directory domain for cyber security research, focusing on Windows privilege escalation and exploitation techniques.
  - Actively experimenting with techniques such as SMB relay and LLMNR poisoning to enhance understanding and proficiency in cyber security.
- **Network Security Testing and Evaluation:**
  - Deployed an enterprise firewall to assess Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), DNS blocking, VLAN communication, VPN access, and access control lists for secure and private communication within a home lab environment.
  - Actively learning and implementing industry standards and best practices in enterprise network security.
- **Wireless Security Architecture Simulation:**
  - Simulated the deployment of enterprise wireless security architecture using lightweight access points and a software-based controller to replicate cybersecurity best practices in wireless network deployments.
- **Automation and Playbook Development:**

  - Leveraged Security Orchestration, Automation, and Response (SOAR) technologies to develop and deploy IT and cybersecurity playbooks in a home lab environment, refining techniques before public release via personal GitHub repositories.
- **Infrastructure as Code (IaC) and DevSecOps:**
  - Simulated a DevSecOps infrastructure through docker containerization of enterprise server applications in a self-hosted lab environment.
  - Gained insights into valuable configurations and deployments of infrastructure as code, ensuring the maintenance, operation, and security of containerized applications.

Cyber Security Work Experience

Korea Site Manager

Leidos May 2016 - Present

- **Managed Migration of Electronic Health Records (EHR) Infrastructure:**
  - Led the successful migration of electronic health records server stack and Storage Area Network (SAN) to a new data center location, ensuring the security and integrity of sensitive patient data throughout the process.
  - Coordinated travel logistics and access control measures for travel system engineers, prioritizing security protocols and compliance standards.
  - Collaborated closely with stakeholders to address timeline requirements and logistical considerations for server relocation, with a focus on safeguarding Personally Identifiable Information (PII) during transportation.
- **Revamped Security Protocols and Procedures:**
  - Overhauled outdated work instructions and standard operating procedures to align with cybersecurity best practices, ensuring enhanced security measures across local and enterprise-level operations.
  - Played a pivotal role in reviewing and refining enterprise-level security protocols across a global coverage area, reinforcing data protection measures and compliance standards.
- **Oversaw Security Operations in High-Risk Environments:**
  - Managed personnel, operations, and customer relations for all medical facilities in the Republic of Korea, prioritizing cybersecurity measures to safeguard critical health data.
  - Supervised a team of 7 individuals to support cybersecurity initiatives in the region, implementing robust security controls and incident response protocols.
- **Implemented Access Management Controls:**
  - Administered Identity Access Management (IAM) functions, ensuring secure creation, deactivation, and auditing of user accounts to the electronic health record database.
  - Reviewed audit logs and access records to identify and mitigate potential security risks, maintaining strict access controls for sensitive medical records.
- **Mitigated Security Incidents and Restored System Access:**
  - Troubleshot and resolved application misconfigurations swiftly after system migrations, minimizing downtime and revenue loss for the largest military hospital in South Korea.
  - Provided instrumental support in cyber awareness training and reporting, mitigating potential PHI/PII leakage risks and ensuring compliance with HIPAA regulations.
- **Maintained Data Security and Compliance:**
  - Maintained zero findings in the operation and maintenance of data classification standards, ensuring HIPAA compliance of electronic health records across a global network of sites.

  - Spearheaded the pilot of enterprise-wide security protocols, covering over 140 site locations worldwide and reinforcing data security practices.
- **Facilitated Secure Communication Infrastructure:**
  - Provided vital support in establishing secure communication channels for proprietary lab instruments, ensuring continuous patient care and data integrity for the largest US military hospital in South Korea.
  - Played a key role in facilitating connectivity for new COVID-19 lab testing instruments to electronic health records, enhancing productivity and result accuracy amidst operational challenges.

CYBER SECURITY ENGINEER

Root Access Protection June 2021 - Present

- **Establishment of Key Performance Indicators (KPIs) for Security Maturity:**
  - Contributed to establishing and prioritizing Key Performance Indicators (KPIs), reporting, and metrics to assess the cybersecurity maturity of Root Access Productions and its subsidiaries.
  - Played a key role in developing metrics to track the effectiveness of cybersecurity initiatives and identify areas for improvement.
- **Technical Expertise in Security Technology:**
  - Provided technical expertise and advisory services on various aspects of security technology, including network security, platform security, and security frameworks.
  - Offered strategic guidance and recommendations to enhance the security posture of clients, leveraging industry best practices and cutting-edge technologies.
- **Partnership Development and Relationship Building:**
  - Coordinated partner agreements and established business relationships to bolster the quality and credibility of the Cyber Insecurity stream and community.
  - Successfully secured partnerships with Fortune 100 companies and Series A startups, fostering collaboration and knowledge exchange in the cybersecurity domain.
- **Mitigation Strategy Analysis and Enhancement:**
  - Collaborated with the Root Access protection team to analyze and review mitigation strategies, providing valuable insights and recommendations for improvement.
  - Offered guidance and assistance in enhancing mitigation strategies to effectively address emerging threats and vulnerabilities.
- **Content Creation and Industry Engagement:**
  - Utilized Open Source Intelligence (OSINT) techniques to gather information and create engaging content on a wide range of cybersecurity topics.
  - Developed talking points for Twitch streams targeting industry professionals, providing valuable insights to an audience of 16K viewers monthly and meeting key performance indicators for stream partners, including Fortune 100 companies.

Other Professional Experience

TRICARE BENEFICIARY SERVICE REPRESENTATIVE

Leidos March 2015-May 2016

- **Effective Communication:**

  - Conducted engaging public briefings to educate 2500 active duty military personnel on the medical benefits offered by Tricare (military health insurance), demonstrating strong public speaking skills.
  - Delivered one-on-one counseling sessions to address the individual needs and concerns of military members regarding their benefits, showcasing empathy and active listening.
- **Customer Service:**
  - Acted as a customer educator, providing personalized assistance and guidance to military members, ensuring they were well-informed about their entitlements and benefits.
  - Distributed marketing materials and utilized technological self-service aids to facilitate access to Tricare benefits, prioritizing customer satisfaction and convenience.
- **Organizational Skills:**
  - Implemented efficient file management systems to organize and maintain active files for 2500 active duty service members, demonstrating meticulous attention to detail.
  - Managed logistics for enrollment forms, ensuring compliance with HIPAA regulations for the storage and shipping of sensitive documents, highlighting a commitment to data security and compliance.

ACMI POD LOADER

Cubic Worldwide Technical Service August 2013-March 2015

- Training facilitator providing support of critical United States Air Force pilot training. Allowing instrumental review and planning to ensure offensive advantage and air dominance while minimizing risk. Facilitated combat exercises of large scale training operation to include US and foreign military.

SENIOR AIRCRAFT ARMAMENT MAINTENANCE SUPERVISOR

United States Air Force September 1999-August 2013

- **Operational Enhancement and Data Analysis**
  - Utilized specialized tools and conducted functional tests to enhance the operational capabilities of multiple United States Air Force aircraft.
  - Provided comprehensive support for both scheduled and unscheduled maintenance of all weapons system components, ensuring optimal performance and reliability.
  - Compiled and analyzed data to generate detailed reports on daily aircraft operations, including manpower allocation, scheduling efficiency, and mission accomplishment metrics, enabling senior leadership to make informed decisions.
- **Documentation Management and Safety Compliance**
  - Maintained meticulous documentation and reviewed aircraft maintenance logs to track all maintenance events and identify discrepancies, prioritizing aircraft reliability and safety for flight operations.
- **Leadership and Team Management**
  - Demonstrated leadership and training abilities by overseeing teams ranging from 3 to over 200 members.
  - Developed and managed workplace shift schedules for twenty-four-hour operations, including appointment coordination, vacation planning, and personnel rotation.
  - Mentored junior military members to succeed in their military careers and prepared them for transition to civilian life.
- **Training Program Development and Improvement**

  - Revamped workplace training programs by implementing on-the-job training initiatives, streamlining the qualification process for employees, and boosting productivity and quality standards in a fast-paced aircraft maintenance environment.

Education and Training

- CISCO Certified Entry Networking Technician (CCENT)
- CompTIA Security +
- CompTIA Network +
- CompTIA A +
- **University of Maryland Global Campus**
  - Computer Science Major (1 semester)
  - Languages learned
    - Python
    - Java

Online Courses Completed

- **ITproTV**
  - CCNA 200-301
- **CBT Nuggets**
  - CCNA 200-301
- **TCM Security Academy**
  - Practical Ethical Hacking
- **INE**
  - Penetration Testing Student