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

Joshua Gaede is a cyber security professional who is a life long learner and innovative thinker. Joshua Gaede has proven to be a critical asset in unique challenges presented in large scale migration technical issues and challenges to restore business operations . His enthusiasm continually grows his awareness of new technologies and cyber security news to bring creative solutions to improve and strengthen business security postures.

Key Cyber Security Achievements

- Currently top 4% of 929,000 using the hands-on offensive cyber range,TryHackMe. Utilized chained exploitation techniques to successfully complete Advent of Cyber 2020/2021 and other challenges. Demonstrated experience with mainstream ethical hacking tools and techniques.
  - Enumerating target machines using nmap, Burpsuite, gobuster, smbclient, and wireshark.
  - Exploitation of vulnerabilities by using reverse or bind shells, cross-site scripting, and metasploit
  - Privilege escalation with tools such as linpeas to find SUID binaries, and researching specific software versions for exploitable CVE's on Rapid7 and Exploit-DB
  - Identify and exploit OWASP Top 10 misconfigurations and vulnerabilities such as SQLi, XXE Payloads, and IDOR vulnerabilities.
- Configured type 1 hypervisor to set up Windows Server 2019 active directory domain used for cyber security research for Windows privilege escalation and exploitation. Actively using techniques such as SMB relay and LLMNR poisoning.
- Deployed enterprise firewall to evaluate IDS/IPS, DNS blocking, VLAN communication, VPN access, and access control lists for secure and private communication to my home lab. Learning and developing techniques and industry standards of enterprise environments.
- Simulated enterprise wireless security architecture deployment utilized lightweight access points and a software based controller to simulate cyber security best practices in wireless deployments.
- Utilized SOAR and other automation technologies to develop and deploy IT and cyber security playbooks on a home lab prior to making available to the public via personal Github.
- Simulated Dev Sec Ops infrastructure through docker containerization of enterprise server application on self hosted lab environment. Learning valuable configurations and deployments of infrastructure as code to maintain,operate, and secure containerized applications.

Korea Site Manager

Leidos May 2016 - Present

- MManaged the successful migration of electronic health records server stack and SAN to new data center location at new physical data center location.

- – Coordinated travel requirements, facilitated access control requirements, and logistical support for travel system engineers.
  - – Collaborated with customer for timeline requirements, logistical requirements for server relocation, and proper transportation of PHI removable media.
  - – Point of contact for scheduled downtime coordination, planning, and system restoration of electronic health records to users within downtime window.
- Revamped outdated work instructions and standard operating procedures for local site reference and training. Individually requested to review enterprise level work instructions and standard operating procedures across contract coverage area worldwide.
- Oversaw personnel, operations, and customer relations for all medical facilities in the Republic of Korea. Manages a team of 7 individuals to support the ROK.
- System Administrator responsible for verifying scheduled backup completion, and applying backup templates. Monitor system performance, and responsible for outage or degradation reporting. Accomplish functionality and confidence tests for storage server and database functionality ensuring system reliability and availability of the electronic health record database supporting 1300 users.
- Operation oversight and execution of Identity Access Management (IAM) functions to include creation, deactivation, and auditing of 1300 user accounts to the electronic health record database by using role-based access controls. Reviewed audit logs of users accounts and access logs for stale accounts and inactivity policy enforcement. Controlling access to critical personal health records for past and present military service members and families (hundreds of millions of records).
- Troubleshot and resolved application misconfiguration after Medical Country of Origin Information (MedCOI) application migration to restore access to the electronic health records to the medical community of 1300 users within an hour. Patient care and medical availability minimally impacted for the largest military hospital in South Korea, and minimized the estimated $23,000 per hour loss in revenue.
- Customer support oriented with daily tasks such as isolating, diagnosing, and resolve PC, printer, network, software, and database access issues. Escalating issues not able to be locally resolved to outside agencies with accuracy and information needed to resolve the issues. Individually responsible for the closure of 2000 trouble tickets in 2021. Highlighted for excellence in customer service by customer feedback.
- Aided in cyber awareness training and reporting of any possible PHI/PII leakage of sensitive medical records or personal identifiable information. Adverting additional business operations costs of HIPAA violation fines of $50k per violation with over 10 possible leakages avoided.
- Compliance driven. Maintained zero findings in the operation and maintenance of data classification standard and its use in the storage and transmission of sensitive documents to meet HIPAA compliance of electronic health records. Hand selected to pilot enterprise-wide work instructions and standard operating procedures covering over 140 site locations with worldwide coverage.
- Provided instrumental support to provide communication of proprietary lab instruments to the electronic health record database, and providing vital continuous patient care for the largest United States military hospital in South Korea. Was key in establishing short notice support of new COVID 19 lab testing instruments connectivity to electronic health records to increase productivity and result accuracy. Responsible for coordinating the effort of establishing communication of new lab analyzer and re-establish existing lab analyzers during hospital relocation to new location in a different city. Facilitating accurate and reliable testing of over 30k patients.

CYBER SECURITY ENGINEER

Root Access Protection June 2021 - Present

- Help establish and prioritize Key Performance Indicators, reporting, and metrics to track maturity of Root Access Productions and its subsidiaries.
- Provides technical expertise and advice on various areas of security technology, including: network security, platform security, and security frameworks in a consulting capacity.
- Coordinate partner agreements and establish business relationships to enhance the quality of the Cyber Insecurity stream and community. Securing partnerships with fortune 100 companies and series A startups.
- Interface and coordinate with Root Access protection team to analyze and review mitigation strategies. Provided guidance and assist when strategies need to be enhanced for potential clients.
- Using OSINT information gathering techniques, created talking points on a wide range of cyber security topics with industry professionals for Twitch streams. Provided vital insight of an audience of 16K viewers monthly and meeting key performance indicators for stream partners including of fortune 100 companies.

Other Professional Experience

TRICARE BENEFICIARY SERVICE REPRESENTATIVE

Leidos March 2015-May 2016

- Customer Educator delivered public briefings to educate 2500 active duty military on medical benefits offered by Tricare (military health insurance). Public briefer of audiences in excess of 200 personnel, and offered one-on-one counseling to educate military members on their needs and concerns for their benefits.
- Responsible for distributing marketing material to ensure target populations are informed of entitlements provided by Tricare. Provided information for technological self-service aid for retirees in order to maintain benefits for life.
- Efficiency oriented by completely revamping and maintaining active file management for 2500 active duty service members assigned to the location. Including logistics preparation of enrollment forms to the national archive for members that depart for all members that rotate through the location following HIPAA compliance for storage and shipping of sensitive documents.

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

- Used custom tools and functional tests to provide superior offensive capability of multiple United States Air Force aircraft. Provided support of schedule and unscheduled maintenance of all weapons system components, and ensuring the most capable and reliable weapons system. Computed data to communicate statistic regarding all aspects of aircraft daily flying to include

man hours used, scheduling effectiveness, and created custom reports, allowing senior leadership to have insight into daily mission accomplishment.
- Documented and reviewed aircraft maintenance logs for inclusion of all maintenance events and discrepancies. Ensured aircraft reliability and safety for flight.
- Leader and Trainer of teams of 3 to groups of over 200. Created workplace shift schedule for twenty-four hour operations to include appointments, vacation forecasting, and on-boarding/off-boarding rotations. Mentored junior military members in being successful in military career and preparing them for post-military preparations.
- Restructured workplace training program through on-the-job training provisions. Allowing for expedited job qualification of employees. Thereby, increasing productivity and quality of overall product in a high demanding operation tempo of aircraft maintenance.

Education and Training

- CISCO Certified Entry Networking Technician (CCENT)
- CompTIA Security +
- CompTIA Network +
- CompTIA A +

TCM Security Academy

Practical Ethical Hacking

INE

Penetration Testing Student