Trenton Williams

706-975-5431
trentonwilliams1@icloud.com
github.com/tw181802
https://www.linkedin.com/in/trenton-williams-74a381254
Active Security Clearance
Byron, GA

EDUCATION

Gordon State College, Bachelor of Science	2017
freeCodeCamp, JavaScript Algorithms and Data Structures	2022
Sololearn, Python Core	2022

CERTIFICATIONS

CISSP - Certified Information System Security Professional
CEH - Certified Ethical Hacker
CompTIA Security+
CompTIA Linux+
CompTIA Pentest+
CompTIA CySA+
CompTIA Network+
eJPT - Junior Penetration Tester
eCPPT - Professional Penetration Tester
eWPT - Web Application Penetration Tester
BTL1 - Blue Team Level 1
Google Cybersecurity Certification
Google IT Support Certification
Azure 900 Fundamentals
Qualys Vulnerability Management
ISO 27001 Information Security Associate
ISC2 Certified in Cybersecurity

PROJECTS

Project: Implementing a SOC and Honeynet in Azure
Source: github.com/tw181802/Cyber-Course
Platforms and Technology Used: Azure Virtual Machines, Microsoft Sentinel (SIEM), Log Analytics

EXPERIENCE

Company: Log(N) Pacific 12/1/2023 - Present
Title: Cyber Security Support Engineer

- Implemented secure cloud configurations using Azure Private Link, Network Security Groups, Microsoft Defender for Cloud, and Azure Regulatory Compliance for NIST 800-53, resulting in a 30% reduction in security incidents.
- Troubleshooted and supported Microsoft Azure services, including Microsoft Sentinel (SIEM), Virtual Machines, Azure Monitor, and Azure Active Directory, resolving 65 issues per week on average.

- Developed KQL queries to support Log Analytics workspace and Microsoft Sentinel, resulting in 15 new SIEM dashboards and workbooks.
- Implemented a SOC and Honeynet in Azure and imported logs from Event Viewer to analyze threat actors.
- Automated playbooks and processes via Security Orchestration, Automation, and Response (SOAR).
- Monitored various email accounts for phishing attempts using phishing campaigns to increase overall email security.
- Leveraged specialized threat intelligence sources, including MITRE ATT&CK and Open-Source Intelligence (OSINT).
- Improved incident triage, containment, and recovery strategies with 30% faster resolution using the Diamond Model and Cyber Kill Chain.
- Configured and fine-tuned Microsoft Defender to detect and prevent malware, ransomware, and other threats reducing false positives by 20%.
- Designed and implement improvements to logging, data pipelines, integrations. and automation to expand response capabilities.
- Employed Deep Packet Inspection (DPI) techniques for granular analysis with Wireshark and Suricata.

Company: Robins Air Force Base 10/23 - Present
Title: Security Analyst

- Resolved over 90% of the trouble tickets assigned to me over the phone, saving time and resources for both the customers and the IT team.
- Utilized DameWare® and RDP to perform remote fixes for customers who gave permission for remote administration. Completed over 50 remote fixes in the past month, improving the efficiency and security of the IT service delivery.
- Used ServiceNow and Remedy/ITSM to verify and document the resolution of over 100 problems with the customers in the past year, ensuring the quality and accuracy of the IT service delivery and customer satisfaction.
- Distributed over 100 computers for Tech Refresh and over 60 pieces of equipment for new employees annually from the Depot, ensuring the availability and readiness of the IT resources for the customers and the IT operations.
- Delivered written technical solutions and evaluations on over 50 IT requirements documents of new technologies, downward directed programs, RAFB unique requirements in the past year, demonstrating my technical expertise and analytical skills.
- Made recommendations to the Government as to the feasibility of implementation into the existing network environment, supporting the IT decision making and planning process.

Company: WP Engine **09/22 - 10/23**
Title: Technical Support

- Provided Tier 1 IT support and advanced to Tier 2 within 3 months.
- Directed front-end website development using WordPress and other editing software to increase profit margins by over 15%.
- Leveraged mastery of HTML, CSS, and JavaScript to build top quality code for diverse projects.
- Oversaw back-end development using PHP to maintain website integrity, security, and efficiency cut down performance time by 35%.
- Scanned sites for malware and vulnerabilities and delivered clean-up and recommendations for over 100 companies.
- Developed and maintained custom bash scripts to automate routine tasks such as log rotation, backups, and system health checks.
- Reduced manual intervention by 80%, resulting in improved system reliability and reduced downtime.
- Tuned MySQL database queries to enhance performance and reduce query execution time.
- Implemented indexing strategies, resulting in a 30% reduction in page load times for our web applications.
- Administered multiple WordPress sites, ensuring seamless updates, plugin management, and security patches.
- Collaborated with the development team to troubleshoot issues and optimize site performance.
- Managed Linux servers (Ubuntu, CentOS) in both on-premises and cloud environments.

- Implemented security best practices, including firewall rules, user access controls, and regular patching.
- Acted as the primary point of contact for customer support inquiries via Zendesk.
- Resolved technical issues promptly, maintaining a high customer satisfaction rate.
- Decreased page load times by 30%, resulting in improved user experience and higher conversion rates.
- Ensured seamless domain resolution for internal and external services.
- Mitigated DNS-related outages, preventing revenue loss, and maintaining brand reputation.

Company: Junior System Administrator 08/14 - 09/22
Title: Gordon State College

- Automated software processes using SCCM resulting in 20% decrease in workload and increasing productivity.
- Developed multiple solutions for patch management, application deployments and updates to secure over 1000 computers.
- Created a backup recovery plan to ensure that availability was not compromised, and performance continued.
- Monitored server resources and processes to ensure we maintained 99% uptime.
- Managed multiple user accounts, passwords, privileges, and access control while installing hardware and network infrastructure.
- Utilized Powershell scripts to automate to repetitive tasks such as file backups or system maintenance to increase efficiency.
- Documented all activities and reduced support tickets by 25%.
- Installed, configured, and maintained Windows Server operating systems (2008/2012/2016/2019).
- Achieved a 25% increase in system reliability and availability due to streamlined configurations and proactive monitoring.
- Configured Group policy settings to enforce security measurement to improve security posture by 40%.

SKILLS AND TECHNOLOGIES

Microsoft Office Suite, Help Desk, Ticketing System, Azure, Network Security Groups, Firewalls, ACLs (Access Control Lists), Virtual Machines, Virtual Networks, Cloud Computing, Active Directory, File Permissions, Windows 10, SIEM, Sentinel, Cisco Networking Essentials, Linux, PowerShell, Nmap, Splunk, Phishtool, Git, Docker, TravisCI, Google Cloud Platform, VS Code, Visual Studio, PyCharm, IntelliJ, Eclipse, AWS, tcpdump, Snort, pfSense, Bitlocker, Nessus