Brad Getchell | Security Engineer | San Antonio, TX

Brad@Getchell.Work | Getchell.Work/LinkedIn
Security Clearance: DOD Top Secret - SCI | **8570 Level:** IAM 3

Technical Skills

Strong: Tanium, HBSS/Trellix, Nessus/Tenable/ACAS, Splunk, SIEM, Microsoft 365, Windows, Group Policy, Active Directory, Defender, DNS, Nginx, Proxy, Reverse Proxy, Cloudflare, Proxmox, Docker, Container, Portainer, Node Red/Node.js, Home Assistant, Ubiquiti/UniFi, VirusTotal, Firewalls, Vulnerability Scanning/Management, Endpoint Security, Problem Management, Incident Response, Intrusion Prevention, Intrusion Detection, Insider Threat, Security Engineering.

Experienced: AWS, Azure, Google Cloud, SolarWinds, Netcool, LogRhythm, Elastic Stack/Kibana/ELK, SOAR, Wuzah, Grafana, Linux, SSO/SAML/OpenID, MECM/SCCM, Keycloak, Kubernetes, CrowdSec, Container Scanning, Regex, Python, Apache, Agile/Scrum, Jira, GitHub, GitLab, Git, Cisco, Network Design/Architecture, Automation, NIST 500-53, RMF, Disaster Recovery, Digital Forensics, Pentest

Certifications

Certified Information Systems Security Professional (CISSP)
CompTIA CASP+, PenTest+, CySA+, Security+
Tanium Certified Operator (TCO)
LogRhythm Security Analyst (LRSA)
DISA ACAS Operator and Supervisor
AWS Certified Cloud Practitioner
Splunk Core Certified Power User
ITIL® Foundation Certificate in IT Service Management

Education

Bachelors | Texas A&M University-San Antonio **05/2018**
Major: Bachelor of Applied Science – Information Security & Assurance
Honors: Magna Cum Laude

Roles and Responsibilities

Cybersecurity Engineer **02/2021 to Present**
GDIT | 16AF/A6IR, San Antonio, TX | Full-Time | 40 hours per week

- Conducted vulnerability scans and assessments to identify potential security risks and developed mitigation strategies based off vulnerability findings to reduce risk.
- Served as a Cybersecurity SME/Consultant to Air Force Intelligence Community Delegated Authorizing Officials (DAOs) and the Incident Response Center (IRC) for 200+ sites.
- Developed and maintained security policies and procedures in accordance with NIST 800-53 to support secure operations and reduce the risk of security incidents.
- Collaborated with cross-functional teams to implement network security controls, such as intrusion prevention and detection systems, to improve the overall security posture of the organization.
- Conducted supply chain security assessments to identify and mitigate risks in the supply chain.
- Maintained up-to-date knowledge of emerging security threats, trends, and technologies, and recommended improvements to security infrastructure.
- Monitored enterprise security and networks, responding promptly to security incidents, and providing timely and accurate status reports.
- Used Tanium, HBSS/Trellix, ACAS/Nessus, and Splunk identify to create dashboards for leadership, maintain situational awareness, and identify/remediate potential threats based off latest Indicators of Compromise.
- Improved and automated endpoint vulnerability quarantine efforts by 75% across the enterprise to reduce risk.

TTP Development Analyst **11/2020 to 02/2021**

CNF Technologies | 90COS/CYK, San Antonio, TX | *Full-Time | 40 hours per Week*

- Constructs and maintains a multi-system virtual environment for testing and evaluation of tactical solutions.
- Develops solutions in Microsoft Windows PowerShell; prepares PowerShell modules and documentation for delivery to customers.
- Collaborate on all stages of systems development lifecycle, from requirement gathering to production releases for Tactics, Techniques, and Procedures (TTP)

Enterprise Problem Manager **05/2019 to 10/2020**

GDIT | 690NSS/AMAC, San Antonio, TX | *Full-Time | 40 hours per Week*

- Worked closely with Incident Response Teams, and Problem Response Teams to identify and resolve the major various issues across the enterprise that required industry experts (EX: Microsoft, F5, Tanium).
- Led a COVID-19 Remote Access Stabilization team to deploy VPN capabilities enterprise wide within two weeks to ensure mission capabilities during pandemic.
- Led a Ready Operational and Lethal IT (ROle-IT) project to improve user experience and identify ways to improve login time by reducing unnecessary GPOs, startup apps, scripts, and endpoint tool confliction.
- Used Tanium to collect system metrics to help AF Leadership make critical decisions.
- Assisted organizations to deploy various applications and fixes using Tanium, SCCM, and GPO
- Managed the Known Error Database to provide workarounds and solutions for the enterprise.
- Worked with various boundary and infrastructure teams to resolve routing and firewall issues.
- Monitored critical Air Force assets using SolarWinds and Netcool to provide real time alerts to the various Network Operation Squadrons across the enterprise.
- Monitored, identified, analyzed, documented, and reported Air Force enterprise level degradations and outages.

System Administrator **09/2018 to 05/2019**

Obxtek | AFMOA, San Antonio, TX | *Full-Time | 40 hours per Week*

- Interfaced with Air Force Medical Operations Agency and Department Health Agency customers and systems to resolve all endpoint and network issues.
- Created scripts to automate vulnerability patching, software audits, active directory queries, software installs, and computer inventories.
- Improved refresh process by 80% setting up Windows 2012 R2 server that automated deployment services.
- Remediated vulnerabilities by identifying and installing relevant software, patches, and updates.
- Used Remedy trouble ticketing solution to accurately track and update service tickets to completion.
- Deployed and managed a windows deployment server to PXE boot systems, transfer profiles and install drivers.

College, Home Labs, and Non-Profit Volunteer **01/2014 – 07/2018**

- Developed practical skills through establishing a home lab environment, replicating real-world cybersecurity scenarios to investigate vulnerabilities and implement security measures.
- Enhanced understanding of cloud security through hands-on projects on cloud, implementing and testing security controls to protect cloud-based resources.
- Participated in national hacking competitions such as Capture The Flag (CTF), honing penetration testing and ethical hacking skills, and collaborating with a team to solve complex cybersecurity challenges.

United States Army **01/2009 – 01/2014**

Wheeled Vehicle Mechanic | *Full-Time | 40+ hours per Week*

- Supervised a 12-member maintenance team mentoring and developing squad members.
- Performed detailed preventive and warranty service maintenance on $60M of equipment.
- Conducted wheeled vehicle recovery operations.
- Deployed to Afghanistan earning the Army Commendation Medal for my efforts on defending the base perimeter.