Tyler Feldstein

CONTACT

763-772-5471

TylerFeldstein@gmail.com

Sioux Falls, SD

linkedin.com/in/tylerf1110

EXPERIENCE

Senior Cyber Security Engineer | Everbridge **July 2021 – Present**

Architected and automated Security Operations and Incident Response (SOAR) capabilities, integrating security automation within cloud-native CI/CD environments across AWS, Azure, and GCP in a FedRAMP-accredited environment. Designed and deployed automated threat detection, incident response playbooks, and security infrastructure as code (IaC) solutions using Terraform, Kubernetes, and GitLab/GitHub Actions. Architected and deployed a Zscaler VPN, enhancing secure remote access and enterprise network security. Led security architecture efforts to enhance endpoint protection, IDS/IPS, and SIEM integrations, driving enterprise-wide security automation, compliance, and resilience through advanced security engineering principles.

Senior Cyber Security Architect | WBD **July 2021 – September 2024**

Served as the primary security architect for Warner Bros. Discovery, enhancing enterprise security by developing and enforcing secure configuration policies, cloud security strategies, and infrastructure hardening initiatives. Led the deployment of security automation and infrastructure-as-code (IaC) solutions using Terraform, ensuring security was embedded into cloud and on-prem environments from the ground up.

Conducted regular security audits and vulnerability assessments across WBD's global network infrastructure, utilizing tools such as SentinelOne, Brinqa, Nessus, and Splunk to proactively identify and mitigate risks. Designed and implemented firewall policies, intrusion detection systems (IDS), and VPN gateways to bolster network security and prevent unauthorized access.

Developed and maintained security policies, standards, and guidelines, ensuring alignment with compliance frameworks such as NIST, ISO 27001, and SOC 2. Led threat modeling exercises and security architecture reviews for new IT infrastructure components, collaborating with cross-functional teams to evaluate risks before deployment. Leveraged APIs and scripting (Python, Bash) to automate security processes, integrate tools, and generate executive-level security reports on network security posture. Provided expert guidance on securing hybrid cloud environments across AWS, Azure, and GCP, enhancing WBD's ability to defend against emerging cyber threats.

Senior Cyber Security Architect | CACI **January 2020 – September 2022**

Served as the primary architect for the mission support directorate (MSD) within CBP to develop a secure cloud infrastructure to assist with modernization efforts. Provided cybersecurity consulting to assist with the newly implemented AWS environment. This included the implementation of a brand new Gitlab pipeline that would serve as the CI/CD that would push containers to multiple VPC's and Kubernetes clusters that served as the DEV, PRE-PROD, and PROD environments for the newly implemented services. Assisted with the implementation of fortify on all dev's computers as well as SAST/DAST within Gitlab as the master branch was committed. Implemented Aquasec and Nessus Security Center to add to the multiple layers of security.

Assisted with monitoring efforts to include multiple instances of ELK that could also be fed to the enterprise SPLUNK for the threat hunters to monitor.

Senior Cyber Security Consultant | T-Mobile (Contracted) **June 2019 – January 2020**

Designed and implemented scalable security solutions to protect T-Mobile's 5G telecommunications infrastructure, ensuring secure communication from Radio Access Network (RAN) sites to subscriber databases. Led security automation efforts by integrating Kubernetes, Docker, and CI/CD pipelines, embedding security into the DevSecOps lifecycle. Conducted technical security assessments, vulnerability testing, and secure code reviews, leveraging tools such as Tenable, Qualys, OpenVAS, and Fortify to identify and remediate threats.

Performed risk analysis and penetration testing, validating security posture against evolving threats. Enforced compliance with PCI-DSS, SOX, and CCPA, ensuring regulatory alignment across cloud and on-premises environments. Developed threat intelligence reports and implemented MITRE ATT&CK-based detection strategies to strengthen T-Mobile's cyber resilience. Leveraged AWS, Azure, and GCP security best practices to enhance cloud security architecture and harden infrastructure. Collaborated with engineering teams to integrate security controls within Terraform-based infrastructure-as-code (IaC) deployments. Strengthened intrusion detection and prevention by optimizing firewall architecture, log management (ELK, Splunk), and endpoint security solutions. Maintained an adaptive security posture by continuously evaluating emerging threats and implementing proactive defenses.

Chief Information Security Officer | US Army (UTARNG) **August 2016 – June 2019**

Designed and orchestrated the installation of a tier 3 private cloud infrastructure consisting of over 1.5 Terahertz of processing, 12 terabytes of ram, and 1 petabyte of usable storage. The private cloud was built with Vmware Vsphere that housed over 800 VM endpoints which provided zero client access to multiple employees in several geographical regions.

Redesigned the data center network infrastructure to provide more efficient communication between virtual servers and zero client endpoints. The network infrastructure consisted of several Cisco Nexus 7000 series switches spanning down to multiple Nexus FEX switches to provide access for the dozens of layer 2 access switches. Maintained several Type-1 encrypted lines creating VPN pipelines to several off-site CONUS locations.

Directed the implementation of a complex threat hunting infrastructure consisting of multiple Bro, Suricata, and Silk sensors placed in strategic locations. Built several ELK stacks to store and compute the data against custom rules written directly from CVE publications on MITRE. Installed an ACAS client that housed several Nessus scanners in order to scan systems at regular intervals, thus ensuring the systems were within compliance with the government's NIST policies. Routinely lead and participated with penetration teams searching for potential vulnerabilities in the infrastructure.

Wrote several policies and procedures to ensure the infrastructure maintains compliance with the Risk Management Framework (RMF). Routinely ensured that the policies were being enforced by conducting audits. Designed a COOP (Continuity of Operations Plan) that would ensure the private cloud would maintain a 99.99% uptime in the event of a system breach or a natural disaster.

25 CMF Information Technology Instructor | US Army (UTARNG) **July 2015 – October 2018**

Army instructor for MOS 25B (Information Technology). Teaching students in areas such as CCNA Routing and Switching Network administration, MCSA Server 2008, 2012, and 2016 administration, CompTIA Security+, Certified Ethical Hacking, and CompTIA Advanced Security Practitioner. Managed 8 physical servers running Windows Server 2012 in an N-tier design. Also designed and managed a 6 server virtualization cluster running VMware VShphere that hosts an excess of 400 virtual machines (VM's).

Information Technology Specialist (MOS 25B) | US Army (UTARNG) **June 2011 – June 2021**

Managed a variety of networks for the National Guard, including layer 3 switches and routers using protocols such as: OSPF, EIGRP, BGP, DTP, 802.1x, Tacacs+, VTP, GRE, IPSEC, ISAKMP, ACAS.
Managed multiple servers running Windows Server 2008 and 2016 with 1000s of active directory users.

EDUCATION

M.S. Cyber Security and Information Assurance @ Capella University **May 2019 – June 2020**

Accreditation Board for Engineering and Technology (ABET) Masters program located in Minneapolis, MN. Specializing in Cyber Security and Information Assurance. Presidents List. Graduated with a 4.0 GPA.

B.S. Cyber Security and Information Assurance @ Capella University **Feb. 2018 – Dec. 2018**

Graduated on an accelerated path while maintaining a 4.0 GPA

CERTIFICATIONS

	Acquired
ISC2 - Certified information Systems Security Professional (CISSP) | 651013	**September 2018**
GIAC - Certified Intrusion Analyst (GCIA) | Analyst #13476	**February – 2018**
CompTIA advanced Security Practitioner (CASP+) | 2ZXXTGJPECB1QNWJ	**July – 2018**
EC-Council Certified Ethical Hacker (C|EH) | ECC13384335519	**December – 2017**
Cisco Certified Network Associate (CCNA) - R&S | COMP001021082447	**May – 2017**
VMware Certified Professional Network Virtualization (VCP-NV)	**July – 2018**
CompTIA – Pentest+ | FW3ZGQNM7311Q7SQ	**MAY – 2020**
CompTIA - Security+ | CESFKQ5MFHE4S75H	**November – 2016**
CompTIA - Network+ | HJT1ET6HBCE11SSM	**October – 2016**
CompTIA - A+ | HHDGYX3EPPF42C5F	**November – 2016**
Splunk – Core Certified User	**March – 2020**
DOD Cyber Crimes Unit (DC3) – Discovery and Infiltration (DCI)	**June – 2019**
Perched – Threat Hunter using RockNSM and Kibana	**July – 2019**