Trevor Martin

Sr. Cloud Security Engineer

AZ, United States | hello+wells@trevorm.tech | social.0xtrev.com

Accomplished Security Professional & Technologist with a track record of leading enterprise identity & security initiatives.

Key Skills & Qualifications

- 5 years of experience implementing, integrating, monitoring and securing Azure offerings
- 2 years of Purple Team expertise, covering penetration testing strategies, current trends, tools, and protocols.
- Technology-agnostic skill set with a strong understanding of implementing cloud architecture, the risks and pitfalls.
- Practical experience using PowerShell/bash, Python, C++ with the agility to adapt to new languages swiftly.
- Skilled in assessing security platform efficacy, writing custom detections, and performing threat modeling.
- Keen interest in keeping up with global trends and security events on X, Reddit, and other less known platforms.

Experience

Sr. Cloud Security Engineer – Wells Fargo (Hybrid) — **April 2024 – Now**

- Led efforts to enumerate and migrate users relying on weak MFA methods to MS Authenticator, targeting >40k users
- Participated in Conditional Access Policy review, troubleshooting and implementation
- Performed evaluation of Privileged Identity Management implementation in Azure
- Leveraged PowerShell to generate various reports, and evaluate overall Azure security posture

Security Engineer - Kudelski Security (Remote) — **March 2022 – April 2024**

- Responsible for full scope operations to support, configure, and integrate platforms, systems, and software between a variety of environments: Microsoft Defender XDR, Sentinel, CrowdStrike, Hunters XDR, Claroty, Tenable (SC+IO), LogRhythm(+cloud), Splunk(+cloud), Zabbix, Grafana, Docker, Ansible, Active Directory, Entra, Azure, AWS, Gitlab.
- Recognized as a Subject Matter Expert (SME) on internal and selected technologies, providing critical support and solutions for broader MDR operations teams.
- Authored SOPs, technical documentation, and training presentations for Junior Analysts and Engineers.
- Improved onboarding processes & project planning framework, facilitating more accurate business analysis.
- Facilitated cross-department collaboration through purple team assumed breach exercises, leveraging crackmapexec, responder, nmap, burp, and other open-source tools to identify gaps in security posture.
- Received 2023 “MDR Excellence” award for outstanding initiative, performance, and leadership.

Security Analyst - Kudelski Security (Remote) — **September 2021 – March 2022**

- Triaged, investigated, and responded to alerts & events across all supported SIEM & EDR technologies in a global multitenant environment. Performed real-time response, containing threats, and preventing lateral movement.
- Performed OSINT research to identify emerging threats, constructed proactive threat hunts with queries for multiple SIEM stacks to be executed by global CFC teams on a weekly basis.
- Performed basic maintenance and tuning on LogRhythm XM & distributed SIEM deployments.
- Leveraged Python & Gitlab to globally decrease false positive detection rate via whitelist updates.

System Administrator (Lead) - Sony Interactive Entertainment (Remote) — **June 2019 – August 2021**

- Technical Lead for global internal support group, managing technology for all SIE employees, contractors, and vendors.
- Responsible for Azure and On-prem Active Directory administration.
- Created streamlined escalation channels for internal teams, greatly improved Tier-1 FLR as a result.
- Guided Service Desk through transition to full remote during initial months of the Covid-19 pandemic.
- Coordinated with InfoSec, Platform Engineering & broader Applications teams to ensure consistent & clear SOP for onsite and remote help-desk teams.

System Administrator - Copperhead Diesel (Onsite) — **June 2012 – May 2019**

- Served as the principal Security Administrator and Technology Consultant for the largest Diesel-only shop in AZ.
- Guided technical architecture through different phases of company growth & multiple site migrations.
- Supported all staff infrastructure & endpoints in a primarily Windows-based environment.
- Created & maintained a profitable, secure online storefront using open-source technology & PaaS.
- Automated social media flows and increased engagement, ultimately driving online sales & local brand recognition.

Certifications

- CompTIA Pentest+
- CompTIA Security+
- CompTIA A+
- LogRhythm Deployment Engineer

Hello,

I am writing to express my enthusiasm for an open Lead Information Security Engineer role within our Security family at Wells Fargo. With over five years of experience in cloud security and hands-on expertise in Azure at Sony and Kudelski Security, I am eager to leverage my skills to enhance the security posture of our cloud solutions as the bank further embraces modern computing methods.

In my current position as a Sr. Cloud Security Engineer at Wells Fargo, I have led initiatives to migrate Azure users to stronger MFA methods and reviewed Conditional Access Policies, significantly impacting our Azure security landscape. My role has given me a thorough understanding of our environments, internal change processes, and the obligations we adhere to as a heavily audited financial institution with a global footprint. This familiarity further enables me to design, implement, and manage secure cloud solutions that meet our stringent compliance requirements and maintain the integrity of our systems.

My background includes two years of Purple Team experience at a global Managed Security Services Provider, where I honed detection and vulnerability management skills across dozens of diverse customer environments as a Security Engineer. At Kudelski Security, I also supported secure integrations to and from Azure, authored SOPs, and facilitated cross-departmental collaboration. This experience has provided me with a comprehensive understanding of the modern security landscape, challenges at scale, and the ability to anticipate and mitigate threats as they evolve.

I am particularly skilled in:

- Adapting detection and testing methodology to new environments and emerging threats
- Investigating and performing RCA in Azure in response to incidents or findings.
- Monitoring and analyzing evolving threats, TTPs, and threat actors in real time through OSINT/CTI.
- Staying abreast of the constantly evolving Azure platform, frequenting Microsoft Learn & Blogs.
- Leveraging my exceptional soft skills to collaborate effectively and empower adjacent teams and peers.

My proficiency in wielding languages such as PowerShell, Python, bash, and C++ allows me to quickly adapt to new use cases, methodologies, and platforms. My certifications, including CompTIA Pentest+ and Security+, further attest to my dedication to continued education and expertise in the field.

Security is not just my career, but also a personal passion. I am strongly invested in staying up to date with the latest trends, tools, and threat intelligence, regularly engaging with security communities on platforms like X and Reddit. Outside of work, I enjoy reading breach reports and technical analysis blogs, building and breaking my lab, and pursuing new technical certifications. My genuine interest in security, coupled with my ability to balance multiple priorities in a fast-paced environment and my collaborative nature, makes me an ideal candidate for this role.

Thank you for considering my application. I look forward to the opportunity to discuss how my experience and skills align with the goals of your team and contribute to the continued success of Wells Fargo.

Best,

Trevor Martin

Sr. Cloud Security Engineer, CNVP

CompTIA

Trevor Martin

has successfully completed the requirements to be recognized as

COMP001021596875
CANDIDATE ID

January 26, 2024
CERTIFICATION DATE
EXP DATE: 01/26/2027

TODD THIBODEAUX, PRESIDENT & CEO

Code: LGLLW6362F1Q1WGW
Verify at: http://verify.CompTIA.org

CompTIA

Trevor Martin

has successfully completed the requirements to be recognized as

CompTIA Security+ CERTIFIED · CE

CompTIA OFFICIAL GLOBAL SKILL CERTIFICATION CERTIFIED

COMP001021596875
CANDIDATE ID

March 28, 2021
CERTIFICATION DATE

EXP DATE: 01/26/2027

TODD THIBODEAUX, PRESIDENT & CEO

Code: VDJVJB9FQHVEQHWX
Verify at: http://verify.CompTIA.org

CompTIA

Trevor Martin

has successfully completed the requirements to be recognized as

COMP001021596875
CANDIDATE ID

October 25, 2020
CERTIFICATION DATE

January 26, 2024
RENEWAL DATE

January 26, 2027
EXPIRATION DATE

TODD THIBODEAUX, PRESIDENT & CEO

Code: X6JW2VTPSCE1QSS1
Verify at: http://verify.CompTIA.org


LogRhythm
Certification
Trevor Martin
for the successful completion of
LogRhythm Deployment Engineer - LRDE Certification
06/23/2022
Grantor
Barry Krauss
Director, Training and Enablement
LogRhythm
University