Ted Summey
Driving Cybersecurity Leadership and Innovations
Knoxville, TN 37918
+1-574-780-0875
tsummey@tsummey.com
https://www.linkedin.com/in/tedsummey
https://tsummey.github.io/tsummey_portfolio

PROFESSIONAL SUMMARY

With over 25 years of experience in architecting, deploying, and securing enterprise-level systems, I am driven by a passion for self-growth and a proactive approach to mastering new and evolving technologies. Throughout my career, I have built scalable infrastructures, automated enterprise processes, and transitioned legacy systems to hybrid and cloud-integrated solutions, always staying ahead of industry trends to address emerging challenges. My commitment to learning is exemplified by completing MIT's Professional Program in Applied Data Science, earning certifications in AWS and Microsoft Azure, and independently acquiring expertise in AI-driven tools. These efforts highlight my initiative in tackling complex systems and adapting to changing technological landscapes to deliver impactful solutions. I thrive on applying this continuous growth mindset to implement innovative strategies that optimize operations, strengthen security, and drive organizational success in an ever-changing digital environment.

AREAS OF EXPERTISE

Strategic Security Planning | Cross-Functional Leadership and Collaboration | Executive Communication and Risk Management | Stakeholder Engagement (Technical and Non-Technical) | Mentoring and Team Development
Product Development and Placement | Cost Optimization in Cloud Environments | Compliance Governance (HIPAA, PCI, FFIEC) | Security Frameworks (NIST CSF, NIST AI RMF, OWASP Top 10, OWASP Top 10 AI/ML, MITRE ATT&CK, MITRE ATLAS, ISO 27001, CIS Benchmarks) | Data Residency and Sovereignty | Security Governance | Advanced Detection and Response (MDR, XDR, ADAR) | Application Security Architecture | SaaS and PaaS Security | API Integration and Security
Cloud and Hybrid Cloud Architecture (AWS, Azure) | Workflow Automation | SIEM and Cloud-based SIEM (Microsoft Sentinel, Securonix, Fluency, AlienVault, Elastic) | Python for Operations, AI Modeling, and GenAI | Incident Response Automation | Managed Security Operations | Threat Intelligence and Analysis | Incident Investigation and Reporting | Emerging AI Toolsets.

SELECTED ACCOMPLISHMENTS

- Evaluated, Designed, and implemented RBAC controls for Securonix using Python and AWS Athena, improving application security and maintaining operational integrity.
- Resolved a potential data breach for Verizon, working with legal teams to confirm no breach occurred through detailed analysis and reporting, alleviating significant organizational concerns.
- Developed analysis of the BlueLeaks breach using Python, streamlining data extraction and impact assessment for the Las Vegas Metropolitan Police Department and Southern Nevada Counter Terrorism Center (SNCTC), confirming minimal risk exposure.
- Architected Microsoft Sentinel-based MXDR solutions, automating 80% of security operations and enhancing threat detection capabilities.

- Reduced AWS operational costs by $12,000/month through cloud resource optimization and advanced cost-monitoring strategies.
- Integrated SOAR with Securonix, leveraging APIs and Python to automate workflows, boosting efficiency and response times.
- Published DHS cyber threat advisories, translating complex risks into actionable insights shared with nationwide fusion centers.
- Applied HIPAA and PCI compliance frameworks, ensuring data security, audit readiness, and organizational adherence to regulatory standards.
- Identified inequities in workforce development, advocating for equitable pay adjustments and mentoring team members, fostering a more inclusive and high-performing team environment.

PROFESSIONAL EXPERIENCE

Senior Manager, Product Management and Development

Verizon Business | Knoxville, TN | 07/2022 – 09/2024

Led the development of advanced security solutions, focusing on automation, cost optimization, and compliance to enhance operational efficiency and threat detection.

- Designed and implemented Microsoft Sentinel-based MXDR solutions, automating 80% of security operations and enhancing threat detection capabilities.
- Reduced AWS operational costs by $12,000/month through resource optimization and advanced monitoring strategies.
- Developed and implemented RBAC controls for Securonix using Python and AWS Athena, improving application security and operational efficiency.
- Collaborated with Securonix to resolve critical integration issues, bridging technical gaps and improving cross-functional team collaboration.
- Conducted a potential data breach investigation in partnership with Verizon's legal team, confirming no breach occurred and alleviating organizational concerns.
- Proactively earned AWS and Microsoft Azure certifications, enhancing team capabilities and ensuring successful delivery of cloud security solutions.

Senior Solutions Engineer

CyberClan | Vancouver, BC | 02/2021 – 07/2022

Transformed MDR services to enhance security operations, scalability, and client outcomes, integrating advanced SOAR solutions and streamlining workflows to meet enterprise needs.

- Designed and implemented SOAR technologies with Securonix, leveraging Python and APIs to automate workflows, boosting threat detection and response efficiency.
- Conducted incident analysis for BlueLeaks, using Python to streamline data extraction and confirm minimal risk exposure for key stakeholders, including the Southern Nevada Counter Terrorism Center (SNCTC).
- Migrated cloud-based MDR solutions from Securonix to Fluency, enhancing scalability and operational effectiveness.
- Optimized Salesforce workflows for lead generation and incident management, improving operational efficiency across the enterprise.
- Collaborated across engineering, security, and sales teams to align technical advancements with strategic business goals, delivering tailored solutions for clients.
- Demonstrated cultural awareness by learning basic French phrases to connect with French-Canadian clients, fostering better relationships and customer satisfaction.

Cyber Threat Intel Analyst 4 / Senior Sales Engineer

ZeroFOX (acquired LookingGlass Cyber) | Baltimore, MD / Arlington, VA | 06/2019 – 02/2021

Advanced national cybersecurity efforts by delivering actionable threat intelligence, safeguarding critical systems, and supporting enterprise clients through technical and sales expertise.

- Conducted BlueLeaks incident analysis, automating data extraction with Python to streamline impact assessments for law enforcement and mitigating risks.
- Published DHS cyber threat advisories on HSIN, delivering actionable intelligence to nationwide fusion centers and enhancing external threat visibility.
- Generated leads for enterprise accounts using Salesforce, ZoomInfo, and LinkedIn Sales Navigator, significantly expanding the sales pipeline.
- Designed and managed product demonstration environments, aligning technical solutions with client needs and driving new business opportunities.
- Delivered impactful presentations at global cybersecurity events, including Black Hat and MENA ISC, enhancing client engagement and brand visibility.

Senior Solutions Engineer

Giant Oak, Inc. | Arlington, VA | 12/2018 – 06/2019

Contributed to the development, sales, and implementation of AI/ML-driven platforms for combating financial fraud, supporting federal and enterprise clients with innovative solutions.

- Enhanced keyword recognition in the GOST (Giant Oak Search Technology) platform by developing advanced regular expressions, improving search accuracy and usability for financial fraud detection.
- Self-taught Python to automate workflows, including creating scripts to migrate data from JIRA to Salesforce, increasing operational efficiency and reducing manual workloads.
- Managed trade shows and client demos, delivering impactful presentations to organizations such as the DoD, IRS, and U.S. Secret Service, showcasing GOST's capabilities.
- Transformed trade show engagement strategies, leveraging attendee data and targeted communications to significantly increase booth traffic and generate new business opportunities.
- Provided continuous feedback to align product offerings with cutting-edge industry trends, enhancing GOST’s competitive edge in the marketplace.

Senior Director, Solutions Engineering, Americas

BlueVoyant | New York, NY | 05/2018 – 10/2018

Led the Solutions Engineering team across the Americas, delivering advanced security solutions tailored to client needs while supporting the development of managed detection and response (MDR) services.

- Deployed tools like Carbon Black (EDR), AlienVault (SIEM), and Demisto (SOAR) to strengthen client security operations and mitigate risks.
- Designed and maintained proof-of-concept environments, ensuring effective client demonstrations and alignment of technical solutions with strategic goals.
- Directed pre-sales engineering efforts, collaborating with account executives to scope opportunities and deliver impactful presentations to enterprise clients.
- Contributed to the transition of MDR backend systems, supporting the migration from AlienVault to an Elastic (ELK) stack to improve scalability and performance.
- Participated in incident response engagements, providing guidance to clients on remediation and security enhancements.

Senior Solutions Engineer

Trustwave | Chicago, IL | 08/2012 – 08/2015, 08/2016 – 05/2018

Partnered with enterprise clients to identify cybersecurity gaps, optimize solutions, and deliver secure, scalable infrastructures for a wide range of industries.

- Managed enterprise customer accounts using Salesforce, scoping opportunities and creating statements of work (SOWs) for penetration testing, PCI assessments, and endpoint security.
- Led deployment of Trustwave agents across 14,770 endpoints, identifying and escalating critical SIEM issues, resulting in resolution by MSSP architects.
- Designed and maintained a demo environment for product demonstrations, reducing costs and enhancing client engagement through up-to-date, cost-effective simulations.
- Supported Black Hat and other trade shows, delivering presentations, product demonstrations, and strategic insights to enterprise customers.
- Implemented McAfee NSP appliances to resolve contractual misunderstandings and bring critical security systems into production.
- Recognized as a Star Performer in 2017 for exceptional performance and contributions to sales engineering efforts.

Manager, Information Security and Architecture

Vidant Health | Greenville, NC | 08/2015 – 08/2016

Directed information security engineering and compliance efforts, improving threat detection, reducing vulnerabilities, and aligning operations with healthcare regulatory standards.

- Reduced cyberattacks by 80% through proactive vulnerability management, ransomware mitigation strategies, and misconfiguration remediation.
- Conducted merger and acquisition risk assessments, identifying and mitigating critical third-party risks to safeguard patient data and operational integrity.
- Ensured compliance with HIPAA and PCI standards, strengthening data security governance and audit readiness across the healthcare network.
- Applied LEAN Six Sigma principles to streamline operational processes, reduce waste, and improve efficiency.
- Advocated for equity and professional development, mentoring team members toward certifications like CISSP and securing salary adjustments to retain top talent.
- Stopped active phishing campaigns targeting critical systems, preventing data breaches and maintaining system integrity.

EDUCATION

- Bachelor of Science in Business Management | Western Governors University | 08/2017 – 05/2020
- Associate of Science in Computer Science | Indiana University South Bend | 08/1998 – 05/2004

CERTIFICATES

- Certificate of Completion in Applied Data Science | MIT Professional Education | 05/2022 – 08/2022
- AWS Certified Cloud Practitioner | AWS | Expires: 12/2025
- Microsoft Certified: Azure AI Fundamentals | Microsoft | Expires: 06/2026
- Microsoft Certified: Security, Compliance, and Identity Fundamentals | Microsoft | Expires: 06/2026
- Microsoft Certified: Azure Fundamentals | Microsoft | Expires: 10/2025