# Ted Summey

Driving Cybersecurity Leadership and Innovations

Knoxville, TN 37918
+1-574-780-0875
tsummey@tsummey.com

## PROFESSIONAL SUMMARY

Seasoned cybersecurity leader with 25+ years of expertise in designing, deploying, and safeguarding enterprise systems. Known for driving innovation through scalable infrastructure solutions, process automation, and seamless transitions to hybrid and cloud environments. A lifelong learner with certifications in AWS, Microsoft Azure, and MIT's Applied Data Science program, I excel in leveraging emerging technologies, including AI, to address complex challenges. Focused on delivering strategies that optimize operations, fortify security, and drive success in an ever-evolving digital landscape.

## AREAS OF EXPERTISE

Leadership and Collaboration

Cross-Functional Collaboration | Mentoring and Team Development | Strategic Security Planning | Technical and Non-Technical Communication | Executive Stakeholder Engagement | Change Management Leadership | Workforce Equity Advocacy | Continuous Learning Advocacy | Team Upskilling and Certification Support | Conflict Resolution and Mediation | Scalable Process Design | Strategic Vision Implementation | Event Security Planning and Coordination | Operational Efficiency Leadership | Crisis Management Leadership | Organizational Resilience Building | Cross-Departmental

Threat Detection and Response

Threat Detection and Response | Extended Detection and Response (XDR) | Incident Response Automation | Threat Intelligence Analysis | Incident Investigation and Reporting | Cyber Threat Group Analysis | SOAR Integration and Optimization | Ransomware Mitigation Strategies | Proactive Threat Containment | BlueLeaks Data Breach Analysis | External Threat Landscape Monitoring | Zero-Day Threat Analysis | Fusion Center Collaboration | DHS Advisory Publishing | Supply Chain Attack Investigations | Endpoint Threat Management | Phishing Attack Prevention and Analysis | Election Security Threat Investigations | Real-Time Threat Visibility Enhancement

Governance, Compliance, and Risk Management

Security Framework Compliance (HIPAA, PCI) | Data Security Governance | Regulatory Compliance and Audits | Cybersecurity Risk Assessment | Vulnerability Management | RBAC Implementation | Merger and Acquisition Risk Assessment | Third-Party Risk Management | Compliance Readiness and Gap Analysis | Regulatory Audit Preparation | Policy Development and Enforcement | Incident Risk Mitigation | Security Awareness Program Development | HIPAA Audit Safeguarding | Proactive Risk Identification | Data Retention Policy Oversight | Enterprise Compliance Road mapping | Regulatory Change Adaptation

Cloud and Workflow Optimization

SaaS, PaaS, and IaaS Security | Cloud-Based SIEM and SOAR | Workflow Automation with Salesforce | Salesforce for Incident Management | Cost Optimization in Cloud Environment | Hybrid Cloud Security Design | Cloud Resource Utilization Audits | Multi-Cloud Strategy Implementation | Automated Incident Triage Systems | API Integration for Workflow Enhancement | Scalable Cloud Architecture Planning | Serverless Workflow Design | Cloud Dataflow Optimization | Cloud-Based Threat Intelligence Platforms | Salesforce Process Automation | Cloud Migration and Modernization | Secure Dataflow in Cloud Environments

SELECTED ACCOMPLISHMENTS

Threat Detection and Response
- Reduced ransomware risks by 80% in 3 months via improved protocols and vulnerability management.
- Mitigated a phishing attack targeting 14,000+ users, reducing recovery time by 50% with DNS fixes.
- Enhanced threat detection for 10+ clients by deploying a Microsoft Sentinel-based MXDR solution.
- Automated incident triage via SOAR, cutting response times by 40% and boosting containment rates.
- Published 10+ DHS advisories on ransomware and supply chain attacks, impacting 200+ agencies.

Governance, Compliance, and Risk Management
- Achieved 100% compliance with HIPAA, PCI-DSS, and FFIEC for 10+ audits across 3 organizations.
- Designed RBAC in Securonix, securing 500+ roles and eliminating 95% of unauthorized access risks.
- Directed incident response for a suspected breach, confirming no data loss and saving $500K+ in costs.

Leadership and Collaboration
- Secured a $10K (14.71%) pay raise for a team member, enhancing equity and morale organization wide.
- Mentored 5+ team members, guiding 2 to achieve CISSP certifications and fostering career growth.
- Trained 15+ cross-functional teams on security protocols, reducing human error incidents by 30%.

Cloud and Workflow Optimization
- Saved $12K/month by optimizing AWS resources, reducing cloud costs by 15% over six months.
- Led cloud migration efforts for 3 major platforms, improving operational efficiency by 25%.
- Spearheaded cost-saving measures in cloud ingestion, reducing unnecessary events by 20% for clients.
- Deployed Zero Trust Architecture for 3 hybrid-cloud environments, mitigating 25+ insider threats.

---

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, streamline threat detection, and reduce operational risks
- Automated 80% of security operations via Sentinel MXDR, boosting detection accuracy by 30%.
- Cut AWS costs by $12K/month, reducing cloud expenses by 15% through resource optimization.
- Implemented RBAC in Securonix, securing 500+ roles and cutting access risks by 95%.
- Resolved integration issues, improving reliability by 20% and enhancing cross-team collaboration.
- Investigated a breach, confirming no data loss and saving $500K+ in legal and remediation costs.
- Reduced event processing by 20%, cutting ingestion costs while maintaining detection integrity.
- Earned AWS and Azure certifications, applying skills to optimize operations and cut cloud costs.
- Ensured 100% compliance deploying Sentinel MXDR, meeting regulatory and audit requirements.

Senior Solutions Engineer
CyberClan | Vancouver, BC | 02/2021 – 07/2022
Transformed MDR services to enhance security operations and market positioning, achieving scalable solutions with Fluency and leading tools like CrowdStrike. Revolutionized incident response by integrating SOAR with Securonix Snypr, boosting threat detection and operational efficiency for enterprise clients.
- Led team collaboration to align tech advancements with business goals for enterprise clients.
- Designed MDR solutions, boosting threat detection by 30% and enabling 20% faster incident response.
- Integrated SOAR with Securonix, improving detection accuracy and operational efficiency by 25%.
- Automated triage systems, introducing sandboxing to reduce containment times by 40%.

- Led the migration from Securonix to Fluency, ensuring scalability and improving client satisfaction.
- Developed backend Python scripts, enhancing SOAR workflows and enabling seamless tool integrations.
- Introduced cross-functional initiatives with engineering and sales, driving 15% revenue growth.
- Used CrowdStrike and AlienVault integrations to deliver tailored solutions for enterprise security.

Cyber Threat Intel Analyst 4 / Senior Sales Engineer
ZeroFOX (acquired LookingGlass Cyber) | Baltimore, MD / Arlington, VA | 06/2019 – 02/2021
Directed strategic threat intelligence initiatives, including the BlueLeaks response, safeguarding law enforcement and higher education systems. Stationed in the Southern Nevada Counter Terrorism Center collaborating with DHS, FBI, TSA, Dept of Treasury, Depart of Energy, LVMPD and CISA to publish critical advisories, enhancing national cybersecurity and threat visibility across key sectors.
- Led BlueLeaks response, automating data analysis and safeguarding Nevada law enforcement systems.
- Authored DHS advisories, shared nationally, raising preparedness for ransomware and supply chain threats.
- Strengthened statewide cybersecurity, improving critical infrastructure visibility and response capabilities.
- Delivered intelligence for 5+ threat groups, providing actionable insights to protect Nevada's key sectors.
- Collaborated with federal and state agencies to mitigate risks to law enforcement and education systems.
- Conducted election security assessments, identifying vulnerabilities and publishing findings to DHS.
- Provided in-depth risk analyses on ransomware targeting schools, enhancing state-level response strategies.
- Integrated intelligence tools like Cyveillance, improving external threat visibility for key stakeholders.
- Developed Python tools to streamline BlueLeaks data analysis, reducing assessment time by 40%.

Senior Solutions Engineer
Giant Oak, Inc. | Arlington, VA | 12/2018 – 06/2019
Enhanced a DARPA-derived SaaS solution for financial fraud detection, collaborating with the DoD, IRS, Department of Treasury, and Secret Service. Refined open web search and analytics capabilities, enabling federal agencies to identify and mitigate fraud with greater precision and efficiency.
- Improved fraud detection by refining platform algorithms, boosting anomaly detection accuracy by 20%.
- Partnered with IRS and Treasury to align solutions with agency needs, enhancing fraud mitigation efforts.
- Delivered tailored demos for federal clients, showcasing SaaS capabilities for mission-critical challenges.
- Developed advanced regex scripts, enhancing platform search precision and reducing false positives.
- Led proof-of-concept initiatives, demonstrating scalable innovations to meet federal security goals.
- Optimized SaaS usability, reducing client onboarding time by 15% through user-driven design refinements.
- Created Python scripts for seamless data migration, improving operational efficiency during transitions.
- Enhanced web analytics for open-source intelligence, aiding federal agencies in combating complex threats.

Director, Solutions Engineering, Americas
BlueVoyant | Henderson, NV | May 2018 – October 2019
Led a solutions engineering team to deliver advanced MDR and threat intelligence solutions, enhancing detection and response for enterprise and government clients. Partnered with federal agencies and stakeholders to mitigate complex threats, drive regulatory compliance, and implement scalable security strategies across diverse industries.
- Directed a team delivering MDR services, improving detection and response for enterprise clients.
- Integrated proprietary tools into client environments, boosting threat resilience by 25%.
- Partnered with DoD and enterprise leaders to mitigate advanced threats and ensure compliance.
- Designed scalable security solutions, tailoring strategies to unique client and industry needs.
- Fortified cybersecurity postures, reducing vulnerabilities and enhancing response readiness.
- Streamlined security workflows, cutting incident response times by 30% through automation.

- Led client engagements to align regulatory compliance efforts with business security strategies.
- Oversaw deployment of Carbon Black and XSOAR tools, optimizing EDR and SOAR capabilities.

Senior Security Solutions Engineer
Trustwave | Henderson, NV | August 2016 – May 2018
Managed cybersecurity operations at Trustwave, enhancing managed threat detection, response, and compliance solutions. Partnered with enterprise clients to optimize threat intelligence workflows and implement scalable security strategies tailored to diverse industries.
- Led managed threat detection, boosting cybersecurity resilience for 10+ enterprise clients.
- Strengthened compliance programs, ensuring PCI-DSS and GDPR readiness across multiple sectors.
- Streamlined threat intelligence workflows, cutting response times by 30% and improving accuracy.
- Designed scalable security solutions, tailoring deployments to meet client needs and regulations.
- Supported PCI audits for Fortune 500 clients, reducing compliance gaps by 20%.
- Enhanced EDR systems, improving endpoint protection across 15,000+ client devices.
- Deployed advanced SIEM tools, improving threat visibility and analysis capabilities by 25%.
- Delivered tailored security training, reducing user-driven vulnerabilities by 15%.

Manager, Information Security Engineering and Architecture
Vidant Health | Greenville, NC | August 2015 – August 2016
- Reduced ransomware risks by 80% via incident response and proactive vulnerability management.
- Ensured 100% HIPAA compliance, safeguarding patient data and achieving full audit readiness.
- Secured a 14.71% pay raise for a top performer, fostering equity and boosting team morale.
- Mentored team members, guiding 2 toward CISSP certification and professional advancement.
- Designed scalable systems, improving security architecture across 10+ healthcare facilities.
- Stopped phishing campaigns, reducing breaches by 30% through improved threat response protocols.
- Applied LEAN principles, cutting operational inefficiencies by 20% across security processes.
- Conducted vulnerability scans, reducing unpatched systems by 25% to strengthen overall security.

Manager, Information Security Engineering and Architecture
Trustwave | Henderson, NV | August 2012 – August 2015
Led security engineering at Trustwave, implementing advanced threat detection and vulnerability management solutions. Supported enterprise clients with scalable cybersecurity architectures, optimized incident response, and ensured compliance with frameworks like PCI-DSS. Collaborated across teams to deliver tailored strategies that enhanced resilience and efficiency.
- Designed advanced threat detection systems, reducing incident response times by 30%.
- Optimized workflows, improving threat containment efficiency by 25% for enterprise clients.
- Ensured PCI-DSS compliance, achieving 100% audit readiness for high-profile client environments.
- Developed scalable security architectures, tailoring solutions for 15+ diverse enterprise clients.
- Reduced unpatched vulnerabilities by 40% via proactive vulnerability management strategies.
- Strengthened cross-team collaboration to deliver solutions aligned with client business goals.
- Implemented advanced SIEM tools, boosting detection accuracy and response coordination by 20%.
- Delivered security training, reducing client-side misconfigurations by 35%.

---

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

---

SOCIAL LINKS

- LinkedIn - https://www.linkedin.com/in/tedsummey/
- Portfolio - https://tsummey.github.io/tsummey_portfolio/