# Ted Summey


**Cybersecurity Leader | Architect | Engineer & Data Scientist**

Knoxville Metropolitan Area

Email: tsummey@tsummey.com

Experience: LinkedIn Profile | Portfolio


---

## SUMMARY


Dynamic Cybersecurity Architect with over 25 years of comprehensive experience in building, scaling, and optimizing cybersecurity frameworks and architectures for both enterprise and federal clients. A proven leader in designing and implementing cloud-based security architectures (AWS, Azure), with a specialty in MDR/XDR solutions, zero-trust architecture, and AI-driven threat detection. Leveraging deep expertise in compliance management across key standards such as NIST CSF, ISO/IEC 27001, PCI-DSS, GDPR, and HIPAA, I excel at crafting solutions that align security with business goals and regulatory demands.

I have consistently driven innovation by incorporating AI/ML technologies to enhance threat detection, incident response automation, and security posture management. Through this integration, I have successfully reduced operational costs by $12K per month while increasing detection accuracy by 30%. My cross-functional leadership skills have led to successful collaborations with C-Suite executives, federal agencies like CISA and DHS, and large-scale enterprise clients, enabling business growth and ensuring robust cyber resilience.

In my roles, I've championed the integration of Security Orchestration, Automation, and Response (SOAR) platforms, optimizing security workflows and streamlining incident management. By fostering a proactive security culture, I have led efforts in disaster recovery planning, business continuity management, and large-event cybersecurity strategies, securing critical infrastructure for events like BlackHat, DEF CON, and RSA.

I'm equally adept at guiding technical teams and collaborating with business units to create scalable, compliant, and cost-effective security architectures. My expertise extends to pre-sales consulting, helping organizations tailor their security strategies to meet unique client needs, while also leading cybersecurity awareness programs and developing technical training for cybersecurity professionals. With extensive hands-on experience in SIEM, EDR, SOAR, and cloud-native security solutions, I am committed to delivering security-first innovations that protect against evolving threats and drive operational efficiency.


Key Achievements:

- Architected MDR/XDR solutions for enterprise and federal clients, driving 30% improvements in threat detection and cutting response times using AI/ML automation.
- Successfully led security compliance efforts across HIPAA, PCI-DSS, GDPR, and ISO 27001, passing federal audits with top marks.

- Reduced operational costs by optimizing cloud resources, saving $12K per month through AWS audits and policy enforcement.
- Partnered with DHS and CISA to develop cyber awareness advisories and enhance national cybersecurity efforts.
- Designed and led disaster recovery and business continuity plans, ensuring uptime and operational resilience during high-stakes events.
- Integrated SOAR with Securonix and Sentinel, revolutionizing incident response workflows and boosting operational efficiency for global teams.
- Delivered impactful pre-sales technical consulting and client engagement, driving business success and securing multi-million-dollar projects for Fortune 500 clients.

## AREAS OF EXPERTISE

Enterprise Cybersecurity Architecture | Cloud Security (AWS, Azure) | AI & Machine Learning Integration | MDR/XDR Design & Deployment | Zero Trust Architecture | Security Orchestration and Automation (SOAR) | Threat Intelligence & Incident Response | External Threat Landscape Monitoring | Endpoint Detection and Response (EDR) | Security Operations Center (SOC) Leadership | Disaster Recovery & Business Continuity Planning | Large Event Cybersecurity Planning | Incident Response Automation | Managed Security Operations | Extended Detection and Response (XDR) | Data Science for Security Operations | Root Cause Analysis & Collaborative Problem Solving | Executive Communication & C-suite Risk Management | Cross-functional Team Leadership | Compliance with Regulatory Frameworks (ISO/IEC 27001, NIST CSF, PCI-DSS, HIPAA, GDPR) | Risk Management & Merger/Acquisition Cybersecurity Review | Cloud-based Managed Detection & Response (MDR): Microsoft Sentinel, Securonix, Fluency, SecureWorks | Threat Research & Vulnerability Management | Pre-Sales Technical Consulting | Security Automation with Python, KQL, PowerShell | Security Analytics & Dashboard Development (Elastic, Logstash, Kibana) | Document Classification & Data Security | Employee Learning & Development | Compliance Auditing & Regulatory Success (NIST, FedRAMP, HIPAA, GDPR) | Public Cloud Security Architecture (AWS, Azure) | Incident Response Playbook Design | Cybersecurity Training for Large Events (BlackHat, RSA) | Security Awareness Training | Disaster Recovery Planning & Business Continuity Management | SOAR & SIEM Integration | Collaborative Problem Solving & Executive Leadership

## SELECTED ACCOMPLISHMENTS

- **Architected Scalable MDR/XDR Solutions:** Spearheaded the global development and enhancement of MDR/XDR services at Verizon, improving threat detection by 30% and reducing operational costs by $12K monthly. Integrated SOAR platforms such as Microsoft Sentinel to automate incident response workflows and secure cloud environments.

- **Proactive Risk Mitigation:** During a potential merger, conducted a cyber risk review and identified significant security risks, resulting in the decision to fail the partner's risk assessment. This decision shielded the organization from exposure to a major data breach involving over two million protected health records, which later made national news.

- **Incident Response Leadership:** Responded to a command-and-control attack at a university integrated with a healthcare organization's network. Disconnected the affected machine, enforced multi-factor authentication (MFA), and blocked network integration until vulnerabilities were removed, preventing a wider breach.

- **BlueLeaks Incident Analysis:** Led the assessment of the BlueLeaks data breach targeting law enforcement agencies, including the Southern Nevada Counter-Terrorism Center (SNCTC). Developed a Python-based scraping tool to safely analyze the 260GB data leak, which helped contain the risk without exposing systems to malware and provided accurate reporting on the leak's true impact.

- **Phishing Attack Mitigation:** Neutralized a phishing attack targeting over 14,000 employees by leveraging DNS redirection and internal message routing, preventing data loss and malware infection across the organization's infrastructure. The attack was fully mitigated within hours, avoiding potential ransomware spread.

- **Optimized Remote Access Security:** During a remote access attack on a healthcare partner's network, implemented MFA, isolated the attack, and conducted a full audit to secure the organization's systems. This swift response ensured that no further compromise occurred and led to the adoption of stricter security policies.

- **Cybersecurity for Large-Scale Events:** As Senior Information Security Engineer for Caesars Entertainment, secured high-profile events like DEF CON and the World Series of Poker by managing event security, conducting real-time risk assessments, and leading the Cyber Security Incident Response Team (CSIRT) to ensure zero cybersecurity incidents.

- **Advanced Threat Detection and Automation:** At CyberClan, transformed the MDR service by integrating SOAR with Securonix Snypr, automating incident triage, and deploying zero-day sandboxing for rapid threat analysis. This improved scalability, performance, and threat intelligence.

- **Security Automation and Compliance:** At Trustwave, architected and deployed SIEM solutions with Splunk and Carbon Black to enhance real-time threat detection and compliance with PCI-DSS standards. Led the integration of MDR services to reduce incident response times by 30%, ensuring robust protection across North American organizations.

## CERTIFICATIONS

**Microsoft Certified: Azure AI Fundamentals | Microsoft |** Jul 2024

**Microsoft Certified: Security, Compliance, and Identity Fundamentals | Microsoft |** Jun 2024

**Microsoft Certified: Security, Azure Fundamentals | Microsoft |** Oct 2023

**AWS Certified Cloud Practitioner, Amazon Web Services |** Dec 2022

## EDUCATION

**Certification Applied Data Science** | MIT Professional Education | Mar 2022 – Aug 2022

**Bachelor of Science Business Management** | Western Governors University | Aug 2018 – May 2020

**Associate of Science Computer Science | Indiana university South Bend | Jan 1998 – Dec 2004**

## EXPERIENCE

**Senior Manager - Product Development & Management |** Verizon Business | July 2022 – 9/2024

As Senior Manager at Verizon, I led the strategic development of MDR/XDR services and architected advanced cloud security solutions across global teams. I improved operational efficiency and threat detection through the integration of AI-driven automation, while also driving compliance and collaborating with C-suite executives to align security strategies with business goals.

Key Responsibilities and Achievements:

- Led the architecture and deployment of global MDR/XDR services, improving threat detection accuracy by 30% and reducing response times using AI and automation technologies.
- Achieved $12K monthly savings through cloud optimization and AWS resource audits, ensuring cost-efficient security operations.
- Designed and implemented Microsoft Sentinel components, integrating SOAR to automate security workflows and enhance incident response.
- Collaborated with cross-functional teams to align security strategies with business objectives, ensuring compliance with ISO/IEC 27001, NIST CSF, and GDPR.
- Led technical teams in the integration of KQL queries and JSON configurations to improve log analytics and overall system performance.

**Senior Solutions Engineer** | CyberClan | Feb 2021 – Jul 2022

In this role, I pioneered advanced MDR services and automated incident response systems, significantly improving security operations and scalability. I collaborated with cross-functional teams and customers to design tailored security solutions, driving operational efficiency and enhancing product positioning.

**Key Responsibilities and Achievements**:

- Led the development of an advanced **MDR platform**, integrating **SOAR** with **Securonix Snypr** and other security tools to automate **incident triage** and response.
- Transitioned the **MDR platform** from **Securonix** to **Fluency**, improving **scalability**, **performance**, and **threat intelligence** capabilities.

- Implemented zero-day **sandboxing automation** via **Any.Run**, ensuring rapid threat containment and analysis.
- Spearheaded **product positioning** efforts, enhancing sales growth by aligning security operations with customer needs.
- Collaborated with global teams to integrate **SOAR** with **CrowdStrike** and **AlienVault**, enabling comprehensive threat intelligence

**Cyber Threat Analyst** | ZeroFOX | Jun 2019 – Feb 2021

As a Cyber Threat Analyst, I played a pivotal role in leading high-profile cybersecurity investigations, including the response to the BlueLeaks breach. I collaborated with multiple law enforcement agencies and developed automated tools to assess and contain threats, protecting critical infrastructure and sensitive information.

Key Responsibilities and Achievements:

- Led the response to the BlueLeaks breach, working with Southern Nevada Counter-Terrorism Center (SNCTC) and law enforcement agencies to mitigate risks.
- Developed a Python-based scraping tool to safely analyze 260GB of exposed documents, avoiding malware exposure and ensuring accurate assessment of the breach's impact.
- Authored cyber awareness advisories for CISA and DHS, enhancing national cybersecurity posture through detailed threat assessments and proactive advisories.
- Collaborated with CISA and DHS to assess and neutralize critical cyber threats, protecting sensitive law enforcement data.
- Improved external threat visibility by conducting deep analysis on threat groups using ScoutPrime and delivering actionable intelligence.

**Senior Solutions Architect** | **Giant Oak, Inc.** | Dec 2018 – Jun 2019

At Giant Oak, I was responsible for optimizing client security strategies through the integration of AI/ML-based solutions and behavioral science, particularly for financial fraud detection. I led proof-of-concept environments and collaborated with key federal agencies, including the U.S. Secret Service, to enhance security screening and develop innovative security tools.

Key Responsibilities and Achievements:

- Spearheaded the deployment of Giant Oak Search Technology (GOST), an AI/ML-driven tool designed to detect financial fraud, improving the accuracy of behavioral pattern analysis.

- Collaborated with the U.S. Secret Service to develop an automated screening solution using GOST, significantly improving the efficiency and accuracy of top-secret clearance screenings.
- Migrated the organization's workflow from JIRA to Salesforce, optimizing cross-functional operations and enhancing client engagement.
- Developed advanced regular expressions to improve search accuracy, enabling more precise fraud detection and pattern recognition for government and financial clients.
- Led the creation of proof-of-concept environments, showcasing customized security strategies that enhanced client confidence and supported pre-sales efforts.
- Presented tailored security demos to key stakeholders, delivering expert consultations on search strategies and technical requirements.
- Managed trade show operations, overseeing everything from floor design to product presentations, ensuring successful client interactions.

**Solution Engineering, Americas** | **BlueVoyant** | May 2018 – Oct 2018

As Senior Director at BlueVoyant, I led Solutions Engineering efforts across the Americas, delivering highly customized security solutions for enterprise clients. My role focused on integrating cutting-edge security technologies such as EDR, SOAR, and SIEM, while driving client success and aligning security strategies with business goals.

**Key Responsibilities and Achievements**:

- Led a **high-performing Solutions Engineering team**, delivering tailored security solutions for Fortune 500 companies across North and South America.
- Architected and deployed key security tools, including **Carbon Black** for **endpoint detection and response (EDR)**, **Demisto** (now Cortex XSOAR) for **SOAR**, and **AlienVault SIEM**, to enhance threat detection and response capabilities.
- Spearheaded the deployment of **Illusive Networks** for **deception-based defense**, improving the organization's ability to detect lateral movement by attackers.
- Developed and delivered **impactful presentations and demos**, showcasing customized security strategies that led to increased client confidence and project wins.
- Created and managed **proof-of-concept environments**, ensuring effective demonstrations of security solutions that addressed client-specific challenges.
- Consulted with executive leadership on **product positioning** and strategy, ensuring that the sales engineering efforts aligned with BlueVoyant's business goals and market needs.
- Mentored and developed the **Solutions Engineering team**, fostering talent and encouraging career growth, ensuring that the team stayed ahead of emerging security technologies.

**Senior Security Solutions Architect** | **Trustwave** | Aug 2016 – May 2018

At Trustwave, I designed and implemented advanced SIEM and MDR solutions to enhance threat detection and response capabilities for North American clients. I led the integration of multiple security platforms and ensured compliance with PCI-DSS and other regulatory frameworks.

**Key Responsibilities and Achievements**:

- Architected and deployed **SIEM solutions** using **Splunk** and **Trustwave Intellitactic**, improving real-time **threat detection** and response by 30%.
- Integrated **MDR services** with tools like **Carbon Black** and enhanced security incident response times by 30% through automation.
- Implemented **secure web gateways** and **email security** protocols, reducing phishing and malware risks by over 40%.
- Conducted **PCI compliance management** and security training, ensuring clients maintained regulatory standards and reduced non-compliance risks.
- Led **proof-of-concept environments**, demonstrating the effectiveness of customized security solutions for enterprise clients

**Manager, Information Security Engineering and Architecture | Vidant Health |** Aug 2015 – Aug 2016

As Manager of Information Security Engineering and Architecture at Vidant Health, I led the Security Operations, Engineering, and Compliance teams, driving initiatives to secure critical healthcare infrastructure. I was responsible for overseeing incident response, vulnerability management, and ensuring compliance with HIPAA and PCI-DSS standards, all while improving the organization's overall security posture.

**Key Responsibilities and Achievements**:

- Managed cross-functional teams in **Information Security Engineering**, **Architecture**, and **Compliance**, implementing security strategies to protect healthcare data and systems across the organization.
- Led **incident response planning** and **forensics** efforts during critical security breaches, mitigating threats, reducing downtime, and safeguarding patient data.
- Achieved an **80% reduction** in cyber-attacks by addressing system misconfigurations, strengthening security protocols, and proactively identifying vulnerabilities.
- Successfully mitigated **active phishing attacks**, implementing **real-time threat management** to protect sensitive patient information and ensure compliance.
- Managed **Intel Security Nitro SIEM**, **Secure Web Gateway (SWG)**, and **Secure Email Gateway (SEG)**, optimizing threat detection and response capabilities across Vidant's extensive network.

- Spearheaded vulnerability scanning, patch management processes, and compliance efforts, ensuring continuous protection against evolving threats and adherence to **HIPAA** and **PCI-DSS** regulations.
- Collaborated with HR and legal teams to identify severe security risks during mergers and acquisitions, helping to shape organizational security decisions.
- Applied **LEAN Six Sigma Green Belt** principles to streamline security processes, enhancing operational efficiency, and reducing waste.

**Information Security Advisor** | **Trustwave** | Aug 2012 – Aug 2015

As an Information Security Advisor at Trustwave, I led technical engagements with enterprise clients, designing and implementing tailored cybersecurity solutions to enhance threat detection and ensure compliance with industry standards. My role involved managing MSSP operations, optimizing SIEM configurations, and deploying endpoint security across large infrastructures, all while providing strategic security consultations to ensure alignment with business objectives.

**Key Responsibilities and Achievements**:

- Led **onsite engagements** with customers, guiding them in the design and implementation of customized security solutions, ensuring alignment with **business objectives** and **security standards**
- Deployed **SIEM solutions** (Splunk, Trustwave Intellitactic), improving **threat detection** and response capabilities across 14,770 endpoints.
- Successfully integrated **endpoint security** across enterprise environments, significantly reducing **vulnerability exposure** and enhancing network protection.
- Managed **MSSP operations** for enterprise clients, ensuring effective security solution deployment and ongoing management across diverse customer environments.
- Implemented **Unified Threat Management (UTM)** systems, including **Web Application Firewalls (WAF)** and **M86 Secure Web Gateway**, strengthening **perimeter defenses** against cyber threats.
- Conducted **penetration testing** and **vulnerability assessments** using tools like **DbProtect**, ensuring the security of databases and other critical infrastructure.
- Directed **incident response planning** and conducted forensic investigations, minimizing downtime during breaches and ensuring swift recovery.
- Delivered **security awareness training** to internal teams and client organizations, fostering a proactive cybersecurity culture and reducing human error risks.
- Developed **proof-of-concept demonstrations**, showcasing the effectiveness of proposed security solutions and driving client engagement.

**Senior Information Security Engineer** | **Caesars Entertainment, Inc.** | May 2012 – Jul 2012

In this role, I was responsible for securing high-profile events and managing real-time risk assessments during major operations such as **DEF CON** and the **World Series of Poker**. I developed and implemented comprehensive security measures to protect critical infrastructure.

**Key Responsibilities and Achievements**:

- Led information security strategy for **10 major Las Vegas casino-resorts**, including **DEF CON** and **World Series of Poker**, ensuring zero major cybersecurity incidents.
- Managed real-time **risk assessments** and **incident response** for large events, protecting high-value assets and critical infrastructure.
- Implemented advanced **security controls** for **data center operations**, ensuring continuous protection of critical infrastructure during high-profile events.
- Conducted **network security assessments** and real-time risk mitigation for exposed **RJ45 ports** in public venues, ensuring no unauthorized access.
- Collaborated with the **Cyber Security Incident Response Team (CSIRT)** to effectively respond to potential threats and ensure event safety.