Shaun A. Stanley

San Diego, CA

Profile

Cloud & Security Specialist with 20+ years of experience in enterprise IT and cybersecurity, specializing in pre-sales technical leadership, solution architecture, and Microsoft cloud security. Proven track record of delivering customer-centric, scalable, and secure solutions using Microsoft Defender, Sentinel, Azure AD, and Purview. Skilled in translating business needs into technical strategies, conducting technical workshops, resolving blockers, and accelerating digital transformation through hands-on collaboration. Cleared to support mission-critical projects in classified environments.

Security, Cloud, and AI Highlights

- Pre-Sales Enablement: Led customer-facing technical engagements—including PoCs, demos, and architecture design sessions—for secure cloud adoption and Zero Trust frameworks using Microsoft security tools (Defender, Sentinel, Entra, Azure AD).
- Customer Success Engineering: Developed and implemented Microsoft security solutions that improved detection accuracy by 35% and reduced incidents by 50%, ensuring alignment with compliance mandates and industry frameworks.
- AI-Driven Automation: Deployed AI-based threat intelligence and automation via Azure OpenAI and Cognitive Services to reduce manual analysis by 40% and increase decision accuracy by 25%.
- Cost & Performance Optimization: Drove cloud modernization efforts by leveraging Azure-native features, reducing costs by 30%, and improving system uptime to 99.99%.
- Security Architecture: Implemented Zero Trust architectures, integrated DLP, and executed posture assessments and remediation strategies using Defender for Cloud, Sentinel, and Conditional Access.

Skills

Azure	Sentinel	Microsoft Defender XDR
Azure AD	Copilot	Conditional Access
Entra	Zero Trust	SIEM
Identity Governance	SQL	MFA
DLP	PoC Development	Customer Engagement
Threat Modeling	Solution Selling	Continuous Learning

Professional Experience

Microsoft, **Security Solution Area Specialist** | San Diego, California — 09/2025 to Present

Drove cybersecurity and compliance engagements for regulated customers, specializing in Microsoft government cloud environments, and aligned secure cloud adoption strategies with complex regulatory frameworks to enable compliant collaboration, reduce risk, and support business transformation across commercial and sovereign architectures.

- Advised organizations on identity, data protection, and endpoint security, supporting over 4,000 Microsoft 365 GCC High licenses to enable compliant collaboration across regulated environments.
- Led customer workshops and technical engagements that accelerated Microsoft 365 and Azure Government adoption, contributing to $7M+ in security and cloud billings.
- Translated complex security, compliance, and licensing concepts into clear, executive-level guidance that influenced strategic investments and reduced organizational risk.

Microsoft, **Technical Program Manager** (Fellowship) | San Diego, California — 05/2025 to 08/2025

Led the end-to-end program management of global Wi-Fi 6 deployment across Microsoft's worldwide campuses, coordinating cross-functional teams to upgrade and install thousands of wireless access points, resulting in enhanced network performance, increased device capacity, and improved end-user experience.

- Collaborated with regional site leads, network engineers, and vendors to standardize deployment plans and ensure minimal disruption to business operations during the rollout.
- Utilized Agile methodologies and internal project tracking tools to manage timelines, risk mitigation, and stakeholder communications, driving on-time delivery across 30+ international locations.

FLEET CYBER OPERATIONS – INTEGRATED PLANNING ELEMENTS (CO-IPE), Deputy Director | South Korea 11/2022 to 05/2025

Collaborated with combatant command headquarters to integrate offensive and defensive cyber operations with traditional military activities. Deploy comprehensive, intelligence-driven cyber defense infrastructure, neutralizing advanced persistent threats and ensuring the continuous integrity and availability of critical military communication networks. Coordinate with national and international cyber defense partners to share threat intelligence, vulnerability assessments, and exploit mitigation knowledge.

- Enhanced Security Operations Center (SOC) capabilities as Deputy Director by implementing advanced threat-hunting techniques, machine-learning-driven anomaly detection, and proactive incident response protocols, resulting in the early identification and neutralization of multiple Advanced Persistent Threats (APTs) targeting critical mission systems.
- Enhanced cyber defense posture using SIEM and automation that improved threat detection speed by 30%, quickened response times by 25%, and reduced vulnerabilities by 40%.

USS ANCHORAGE (LPD-23), Cyber Officer| San Diego, California 08/2020 to 11/2022

Led a multidisciplinary information technology team to execute comprehensive network and cybersecurity operations aboard a San Antonio-class amphibious transport dock. Conducted vulnerability assessments and secure code development, and risk analyses to identify security weaknesses and enhance defensive measures. Deployed security patches and software updates in alignment with Department of Defense cybersecurity standards. Trained and mentored junior personnel to strengthen capabilities in threat identification and response.

- Implemented a Zero Trust security framework aboard the Naval ship, segmenting network access, enforcing multi-factor authentication, and continuously validating user/device trust to eliminate lateral movement and significantly reduce attack surface against advanced threats.
- Developed PowerShell scripting training plans, cybersecurity contingency plans, and cyber warfare tactics to prepare for potential conflicts in the cyber domain.

NAVY SPECIAL WARFARE UNIT TWO, Director of Communications | Stuttgart, Germany 06/2017 to 07/2020

Managed information technology programs as Computer Network Defense Manager, leading a team of three military personnel, nine civilians, and two contractors. Managed communications and information flow during joint combined exercise training with European partners. Documented and monitored security plans to support operational readiness and mission success. Authored cyber security policies and developed protective measures to secure sensitive information.

- Maintained Authorization to Operate (ATO) through continuous monitoring with tools including eMASS, SPLUNK, ACAS, and Wireshark.
- Collaborated with stakeholders such as DoDIN, USCYBERCOM, and ARCYBER to identify project requirements, establish acceptance criteria, and define goals and milestones.

COMMANDER TASK FORCE SEVEN TWO, Director of Communications | Atsugi, Japan 06/2014 to 06/2017

Directed operations for a key U.S. Navy 7th Fleet unit under Patrol and Reconnaissance Wing ONE, conducting maritime surveillance, reconnaissance, and bilateral training exercises throughout the Indo-Pacific. Supervised over 30 military, DoD civilian, and IT contractor personnel. Oversaw incident response activities, investigated security-related incidents, and implemented corrective measures. Produced weekly, monthly, and on-demand project documentation, briefing senior executives on threats and countermeasures.

- Audited vulnerability and conducted IAVA compliance scans using the Risk Mitigation Framework and eMASS, achieving a 98% DoD compliance rate.
- Developed Information Systems policies, drafted and reviewed Memoranda of Agreement, managed Certification and Accreditation processes, and composed required Body of Evidence documentation.

EDUCATION & CERTIFICATIONS

EXCELSIOR UNIVERSITY, Bachelor of Science
Information Technology

- Active Top Secret/SCI Clearance w/ CI Polygraph
- Certified Information Security Manager (CISM)
- Project Management Professional (PMP)
- Certified Ethical Hacker (C|EH)
- CompTIA CySa +
- CompTIA Security +
- **Microsoft**
  - **Fundamentals AZ-900, AI-900, SC-900**
  - **Associate AZ-104, AZ-500, SC-300**

PROJECTS

Enterprise Data Loss Prevention (DLP) Implementation

Led the deployment of enforcing a comprehensive DLP solution across Flank Speed, integrating Microsoft Purview and Azure Information Protection to classify, monitor, and secure sensitive data. Implemented automated policies to prevent data exfiltration, achieving a 45% reduction in security incidents and ensuring compliance with NIST and DoD standards while enabling secure collaboration for over 400,000 users.

Enterprise Endpoint Hardening with SCCM and McAfee Integration

Engineered and deployed secure Group Policy Objects (GPOs) at scale using System Center Configuration Manager (SCCM) to enforce enterprise-wide security baselines across classified and unclassified enclaves. Developed custom configuration baselines and task sequences to standardize firewall settings and BitLocker enforcement across geographically dispersed nodes.