Sam S. Jobes – CISA, CISSP

(512) 400-8883
sjobes@yahoo.com
https://www.linkedin.com/in/samjobes
https://technosec.info

Professional Summary

Senior level solutions-oriented security professional with proven experience developing secure processes, policies, and architecture for business. Disciplined, results-driven, security leader, highly proficient at executing security and compliance initiatives within a globally diverse organization. Adept at translating complex concepts into actionable strategies, leveraging 18+ years of security experience to bridge the gap between technical and executive teams. Passionate about driving innovation and fostering a culture of security-first mindset.

Expertise

- Secure Network and Cloud Architectures
- Endpoint Security Management
- Vulnerability Management
- Security Analysis and Research
- Intrusion Detection and Prevention
- Risk Management
- Project Management
- Security Information Event Management (SIEM)
- Security Configuration and Tuning
- Data Loss Prevention
- System/OS Hardening
- IT Governance and Security Compliance
- Policy, Standard, and Procedure Development
- Audit and Assessment

Application & Platform Knowledge

- Microsoft Sentinel
- Microsoft Azure
- Citrix (DaaS & VDI)
- McAfee (ESM, ePO)
- Rapid7 (Insight IDR)
- Tenable (Nessus, EP)
- Microsoft Defender (Identity, Endpoint, Azure)
- Amazon Web Services
- RSA (NetWitness)
- Palo Alto (Next-Gen FW, Panorama)
- Cisco (Firepower, StealthWatch, Umbrella)
- SailPoint (Identity, SSO)
- CrowdStrike
- CyberArk (PAM)
- VMWare (ESX, vSphere)
- Trend-Micro (ATP, Deep Discovery, IPS)
- ZScaler – Zero Trust (ZTE, ZIA, ZPA)
- Burp Suite, Nmap, Wireshark, tcpreplay, etc.

Major Accomplishments

- ✓ Led numerous incident response (IR) engagements, successfully restored business-critical systems and data for high-profile clients affected by ransomware attacks.
- ✓ Migrated MSSP's SIEM platform from co-located US data centers to AWS, enhancing scalability, reliability, and performance for AT&T's managed security service provider consultancy.
- ✓ Enhanced up-time of critical security event monitoring and logging platforms, ensuring uninterrupted service availability.
- ✓ Increased efficiency in security event monitoring, improving case generation and response times through process optimizations.
- ✓ Achieved compliance with multiple government and industry standards, including ISO 27001, SOC2, CMMC, HIPAA, and PCI through comprehensive assessments and process improvements.
- ✓ Drove significant risk reduction by implementing architectural changes focused on segmentation, redundancy, and zero-trust principles.
- ✓ Played a key role in securing state government infrastructure from over one billion cyberattacks per day through advanced IPS full-packet inspection configuration changes, enhancing security capabilities during critical election period.

Career Highlights

Security Architect | Incident Response (IR) Engagement Lead – Dell Technologies (Jul 2022 – Jun 2024)

Managed engagement teams of up to 15 engineers, successfully restoring business-critical systems and data within days following serious security events. Conducted initial damage assessment and scoping for ransomware incidents affecting millions of dollars in operations. Initiated containment and eradication strategies, simultaneously coordinated triage and forensics work streams based on critical infrastructure prioritization, regulation and client requirements.

Mentored and supported Dell analysts and forensic engineers across all IR work streams during engagements. Co-facilitated daily/hourly status meetings, enhancing client decision-making processes with real-time updates on milestones. Served as a subject matter expert (SME) in C-suite discussions, successfully securing additional resources for storage, networking, and forensics to a reduce in incident recovery time. Delivered tailored closeout presentations, advocating for the implementation of recommended security measures for continued risk mitigation. Offered strategic guidance to corporate legal teams during negotiations based on forensic findings and provided detailed reporting to insurance providers.

Co-developed internal automation tools using SharePoint and Microsoft Power Platform, significantly reducing manual processing times. Designed playbooks and workflows for engineers in various subject matter areas. Contributed to the ideation and development of new client-facing security products, as well as providing valuable feedback to enhance existing solutions.

Security Architect | Engineer – Spirit AeroSystems (Jun 2021 – Jun 2022)

Led the setup and configuration of Microsoft Sentinel, Defender for Cloud Apps, Identity, and Endpoint, securing over 5,000 devices within Azure GCC-High for global operations. Collaborated with IT to develop a hybrid multi-cloud architecture (Azure, AWS, Office 365, SAP HANA), increasing operational efficiency and reducing infrastructure costs.

Implemented Cisco Umbrella, successfully offloading 100% of DNS traffic from AD servers globally, improving security response time and reducing DNS-related vulnerabilities and threats. Managed the rollout of Cisco Stealthwatch, FirePower, CyberArk, and SailPoint, securing privileged server

access, corporate network and resource access, and effectively segmenting legacy manufacturing systems and networks.

Supervised global refresh of PaloAlto firewalls, taking advantage of server clustering and Panorama to reduce panes of glass for enhanced security monitoring. Led the Spirit Security Change Board, implementing new change controls and spearheaded an effort to streamline, document, and update existing corporate firewall rules. Acted as SME, advising on policy, standards, and compliance, resulting in improved regulatory adherence across all business units in an effort to comply with recent changes to government contractor requirements (CMMC).

Contract Security Consultant (HIPAA and Data Privacy) – Self Employed (Oct 2020 – May 2021)

Delivered comprehensive security consulting for 5+ law firms, ensuring 100% HIPAA compliance and improving overall IT infrastructure security. Assessed business systems and processes, resulting in a reduction of data breach risks, strengthening the integrity and availability of client data used in legal representation. Conducted IT audits across multiple firms, identifying critical vulnerabilities in existing infrastructure and implementing policy and hardware changes. Installed and configured security hardware/software, identified and remediated system vulnerabilities, improved overall system reliability and up-time. Developed IT security policy and provided contract recommendations, resulting in cost savings and reduced third party provider risks.

SIEM & Security Infrastructure Engineer – Team Lead – AT&T (Oct 2019 – Aug 2020)

Led a team of 8 engineers for SIEM operations, managing multi-tenant security services for 20+ global clients, and acted as SME for McAfee SIEM and ePO services. Assisted in the migration of a SIEM platform to AWS from 3 legacy data centers, improving system reliability and reducing overall operational costs.

Provided SME support for SOC 2 audit preparation, improved overall compliance and reduced security gaps. resulting in successful certification. Conducted comprehensive gap analysis for risk and compliance across 10 client environments, identified and remediated major vulnerabilities, reducing compliance-related risks.

Authored security procedures, policies, and business continuity documentation, improving overall regulatory compliance and streamlining security response processes. Developed playbooks for security analysis, triage, and incident response, improving response times and ensuring consistency across security operations teams globally.

Senior Security Engineer – AT&T (Oct 2018 – Oct 2019)

Delivered expert security consulting services for the State of Texas DIR. Deployed TrendMicro/TippingPoint IPS systems with full 10G inspection at multiple perimeter gateways, enhancing network defense capabilities. Configured and tuned all IPS/IDS systems, optimizing traffic inspection and increasing intrusion detection accuracy. Acted as SME for IPS/IDS operations, leading deployments and threat investigations.

Conducted threat research and threat hunting, identifying unique threats, preventing multiple major security incidents affecting state-critical infrastructure. Co-designed and configured multi-tap architecture, enabling continuous network recording and improving packet inspection efficiency, enhancing incident response times. Monitored and advised on DDoS mitigation strategies provided by CenturyLink across carrier backbones, reducing the impact of DDoS attacks and safeguarding critical infrastructure against service disruptions.

Product Designer, Developer, Business Analyst, & Course Author – AdamsArcher, Inc. (Oct 2017 – Sep 2018)

Designed and integrated systems for online course publishing via learning management system, providing user management and payment processing. Authored first in a series of security, ethics, and compliance courses for Texas attorneys, reaching over 20 law firms, improving regulatory compliance (HIPAA). Produced, directed, and developed interactive online security courses accredited by the State Bar of Texas, facilitating continuing education for 200+ attorneys and legal professionals.

Senior Technical Solutions Consultant – TippingPoint/HP/Trend-Micro (Mar 2011 – Sep 2017)

Supported IPS, next-gen firewall, and advanced threat appliance deployments for over 1,000 global clients. Delivered expert troubleshooting and network defense guidance to Fortune 500 companies and governments during active attack scenarios. Developed tailored configuration and filtering strategies for clients, optimizing network traffic flow and enhancing security efficiency based on unique topologies and architectures. Conducted root cause analysis for network-down events, implementing permanent fixes that improved system reliability across client environments.

Developed internal infrastructure for reproducing complex issues, reducing troubleshooting times and facilitating proof of concept deployments for 20+ customer environments. Co-developed internal and external testing and data gathering tools, improving product testing efficiency, enabling faster identification of system configuration issues. Authored more than 50 configuration and troubleshooting guides, improving support team efficiency, enabling faster resolution of customer issues.

Cyber Security Lead – Delivery Center Operations Americas – Accenture (Aug 2008 – Dec 2010)

Managed a team of 12 security analysts and IT technicians across North and South America, to ensure the protection of sensitive client data. Led audit preparations for 10+ delivery center clients, ensuring 100% compliance with HIPAA, PCI, and SOX regulations. Enforced security policies across the Americas region. Developed and led security training sessions for new hires, improving security awareness and reducing policy violations. Rolled out security initiatives that contributed to successful ISO 27001 certification for global delivery centers. Managed the deployment of security applications and hardware across multiple regions, improving threat detection capabilities and reducing vulnerabilities in client networks. Represented the “Americas” in change review meetings, advocating for security changes that resulted in a significant reduction in security risks across the region's IT infrastructure.

Security Analyst – MainNerve, Inc. (Nov 2006 – Jul 2008)

Assisted clients with custom security appliance installation and configuration, reducing security vulnerabilities and improving system stability through regular patch management. Contributed to the design of FreeBSD-based security appliances, enhancing intrusion detection capabilities and overall effectiveness. Conducted market analysis for new security product components, identifying key features that increased customer interest and contributed to the successful launch of two new products. Performed wireless penetration tests and vulnerability assessments for clients across multiple states, identifying critical security gaps and reducing vulnerabilities through remediation efforts. Produced executive reports detailing critical vulnerabilities and security deficiencies, leading to the implementation of the recommendations and reducing potential risks for clients.

Education

Master of Science in Computer Networking – Capella University, 2005-2007
Bachelor of Business Administration in Finance – University of Texas at Austin, 1997

Certification

Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)
CompTIA A+
CompTIA Network+
CompTIA Security+