JASON BLUE

Chantilly, VA | (703) 424-6206 | tzachyb@gmail.com | https://www.linkedin.com/in/tzachyb

PROFESSIONAL SUMMARY

A Senior Principal Program Manager and Technical with greater than 20 years' experience in cybersecurity and information technology. Focused on mitigating insider threat risks and detecting suspicious cyber activity. Key architect and technical lead for several complex enterprise-wide projects with a unique ability to intuitively grasp overall system designs to quickly contribute at both macro and micro levels, as well as perceive the impact on the enterprise landscape and strategic vision. Individual contributor, as part of a team, and in leadership roles, adept at collaborating with teams at all levels and throughout the organization.

KEY ATTRIBUTES

Data Analysis / Security Analytics	Program Management
Collaborative Leader	Establish Strong Partnerships
Strong Communication/Organizational	Intuitive Thinker

PROFESSIONAL EXPERIENCE

Securonix, Inc, Addison TX (Remote) 2020 - 2023

Plan and manage the Security and Information Event Management (SIEM) transition program for largest customer to date. Continued to facilitate and oversee both greenfield and brownfield projects of other large enterprises. Initiated transfer to address post-project obstacles and opportunities for greater reliability, operations and security maturity, and customer satisfaction.

Principal Operations Engineer / Cloud Operations Shift Leader (2022 – 2023)

- Member of leadership team transforming Cloud Operations from a function-based to market-based support paradigm and structure.
- Minimized risk to the legacy (on-premise customers) revenue stream concurrently with significantly reducing the support resources allocated to it.
- Led the US-based large-enterprise Operations team. Reduced ticket handoffs, backlogs, and overall resolution time via staff development, mentoring, and creations of custom dashboards.

Senior Principal Program Manager / Service Delivery Manager (2020 – 2022)

- Managed a top 10 bank's SIEM transition, oversaw professional services team and coordinated joint efforts with customer's program management, technical, cybersecurity, and governance teams. Achieved full payout of milestone-based incentives.
- Managed a large bank's transition from on-prem SIEM, User Entity Behavior Analytics (UEBA), and Incident Management product. Greenfield implementation completed within three months. Contributed to incident management integration and automated workflows in collaboration with a third-party vendor, receiving customer appreciation for on-time delivery.
- Championed internally on behalf of customers including priority of support tickets, delivery on contractual commitments and development of product enhancements and third-party integrations.
- Advised customers across multiple sectors and geographical zones on technical approaches to enhance the value and efficacy of their Security Operations and Insider Threat efforts.

BAE Systems, Herndon/Reston VA 2005 - 2020

In-sourced and centralized all IT services and continued as the IT lead solutions architect for endpoints. Transferred to cybersecurity to design, implement, and manage the Insider Threat program. Promoted the Litigation Support, Investigations/Forensics, and Security Awareness teams and efforts.

Technical Director *I (2016 - 2020)*

- Reduced insider threat detection and escalation from a week to a day.
- Oversaw the development of a corporate-wide insider case tracking solution that replaced distinct

business function solutions, manual reporting and data sharing processes.
- Collaborated on the design of new and updates to existing on-site and cloud-based enterprise solutions to ensure they meet our security standards and requirements.
- Established strong partnerships with vendors and negotiated license upgrades, training, and implementation support with over $1M in savings.

Program Manager II *(2013 – 2016)*
- Established the Cybersecurity program responsible for Insider Threat detection and Data Loss Prevention (DLP) services across BAE Systems' US operations' 35K+ IT-enabled insiders at 6-% less staff/cost than peers.
- Demonstrated strong program safeguards of the confidentiality, privacy, and civil rights of insiders. Instrumental for human resource, legal, and other functions to share protected information.
- Implemented standard practices and collaborated to establish corporate policies for proactive monitoring of high-risk insiders.
- Developed expertise in all aspects of Securonix's UEBA and its components as well as McAfee's DLP solutions. Recognized as a subject matter expert (SME) for Insider Threat programs and solutions both within the company and externally.

Program Director *(2008 – 2013)*
- Architect and owner/service delivery manager of the End User Computing Shared Service and a team of over twenty engineers..
- Anticipated need and drove effort to replace the automated configuration management solution. Identified opportunities that saved the corporation an additional $450K.
- Led software reclamation efforts that achieved $2M cost avoidance in Microsoft desktop licenses.

Principal Secure Systems Engineer *(2005 – 2008)*
- Responsible for team that transitioned multiple AntiSpyware, AntiVirus, and Hard Disk Encryption solutions to a single corporate standard Endpoint Protection solution.
- Developed vision and plan for the desktop management services that would be offered as part of a three-year activity to in-source and consolidate the IT functions across 50K+ seats.
- Integrated staff at different US locations into a single synergetic team.

OTHER RELEVANT EXPERIENCE
The MITRE Corporation, McLean VA — *Various Titles*

EDUCATION/TECHNICAL

Carnegie Melon's Software Engineering Institute, CERT ***Insider Threat Program Manager***
Insider Threat Defense Group, **Insider Threat Program Development / Management / Insider Threat Detection & Data Analysis**
The MITRE Corporation, ***Management Development and Project Management***
ITIL Foundation ***Certified Change & Release and Agree & Define Practitioner***
George Mason University, Fairfax, VA, ***Math & Computer Sciences***

TECHNICAL
Technical Leader and System Architect | SQL and scripting Languages | Linux/UNIX and Microsoft Operating Systems | Insider Threat Analytics | UEBA Solutions | Securonix SNYPR Certified Administrator, Data Integrator, Content Developer, and Security Analyst | Microsoft Certified Professional

National Insider Threat Special Interest Group (NITSIG) Advisory Board Member
DoD Secret Clearance (inactive)
Fluent in Hebrew