Cell: 1+ 586.549.7324 Email: kos@semonski.com

KOS SEMONSKI

SUMMARY

Dynamic and motivated professional with a proven record of achieving effective outcomes while building highly respected relationships. Extensive experience in information systems security, peer and subordinate mentoring, strategic planning, operational assurance, and project management methodologies.

Expert Enterprise IT security specialist with 20+ years of leadership and success spanning business operations, and global network vulnerability management, mitigation & remediation.

Experienced holistic security practitioner for systems assurance & hardening, security policy design, and security audit governance & compliance.

EDUCATION

Master of Science, Davenport University 2011
Information Assurance, with Distinction (4.0 GPA)

Bachelor of Science, University of Maryland 2007
Info. Sys. Mgmt. Magna Cum Laude (3.96 GPA)

CERTIFICATIONS

Certified Info. Sys. Sec. Professional (CISSP) 2013
ISC^2

Certified Ethical Hacker (CEH) 2016
EC Council

Certificate of Cloud Security Knowledge (CCSK) 2014
Cloud Security Alliance

Six Sigma Blackbelt 2008
Acuity Institute

MEMBERSHIPS

InfraGard, FBI & Private Sector Partnership 2012
Member St. Louis Chapter

Domestic Security Alliance Council (DSAC) 2019
Member

EXPERIENCE

AT&T (Retired)

Principal – Cyber Security	2012 – 2022
Sr. Manager Enterprise Performance & Compensation	2009 - 2012
Sr. Manager Data Analytics	2000 - 2009
Technical Field Support Manager	1997 - 2000

Grantham University

Part Time Adjunct Instructor, College of Info. Technology	2013 – Present

KOS
SEMONSKI

Cell: 1+ 586.549.7324 Email: kos@semonski.com

NARRATIVE of EXPERIENCE

- Provide change leadership and management as a principal member of AT&T's Vulnerability Management System platform by establishing and nurturing collaboration & consensus amongst diverse internal organizations each having competing goals and distinct budgetary considerations. Requires establishing and maintaining relationships with internal Business Units, documenting existing & targeted information asset inventories, and evolving current and desired security requirements & access models across the internal and Enterprise Cloud network spaces.

- Active member of AT&T's Security Scanning and Vulnerability Management Team tasked with reducing AT&T's total risk exposure by partnering with internal business organizations to actively scan network endpoints, databases, and applications using industry leading security scanning tools and frameworks. Actively engage, consult, guide and mentor internal business units regarding IT security best practices and policies.

- Develop and mentor a team of Security Managers producing coordinated, repeatable, accurate, and dependable monthly executive dashboards illustrating AT&T's Total Enterprise IT Security Posture. Required activities include designing, consolidating, managing, and implementing standardized metrics reporting systems. Effort is ongoing and has currently reduced monthly man-hour requirements from > 300 hours to less than 24 hours (90% + reduction).

- Lead manager for AT&T CSO internal security compliance and audit response team: tasked with guiding business units through comprehensive risk analysis exercises, providing audit scope grounding & containment, and assembling & presenting audit requested data, analysis & narratives.

- Participate with and provide technical support for St. Louis technology laboratory with hands on instruction, learning, research and testing of emerging and existing information technologies including: 4G & 5G infrastructures, SIEM platforms, vulnerability & malware assessment tools, firewalls, routers, switches, network analysis systems, etc.

- Representative for internal AT&T Technology Strategies & Standards (TSS) committee providing technical review and oversight of existing and proposed IT architectural specifications in relation to internal policies & directives, contractual obligations, legal obligations, and industry leading organizations, frameworks, and best practices

- Conceived, designed, and implemented an automated data-mining analytic system that monitors Internet news and blog traffic to identify emerging global events or technological threats in relation to AT&T's products and / or services. Initial cost savings exceeded $400,000 with sustained ongoing savings of $120,000 + annually.

- Conceived, designed, and implemented RSA / Archer application to track identified cyber threats to AT&T mobile endpoint information assets and provide integration with existing compliance and policy directives and platforms. Initial cost savings $150,000 + with sustained annual efficiencies est. at $200,000 annually.