ERIK VADNAIS

Cloud Security I Program Management, CISSP, SCSA

[clipper311@protonmail.com](mailto:clipper311@protonmail.com)

*OBJECTIVE*

PROGRAM MANAGER - Seeking long-term engagement to provide guidance, stimulation and support to teammates, while working through delicate issues to focus on program objectives.

*CLEARANCE*

Secret Security Clearance (granted 2006, DoD), NACLC, & DHS Headquarters’ Badges SUMMARY

Mr. Erik Vadnais is a Certified Information Systems Security Professional (CISSP) and project management professional with more than 20 years of Information Technology (IT) experience, more than 15 years of program and project management experience, and 14 years of Information Security (InfoSec) experience within a variety of large to mid-sized IT programs that operate cloud computing, financial, and hosting systems. He has more than 6 years of cloud-enabling technology experience designing, implementing and auditing cloud policies and infrastructure in multi-tenant ISP data center/cloud computing environments. He possesses a demonstrated history of contributing to the roll out of large-scale technical programs such as Private, Public and Hybrid Cloud Computing programs at Fortune 500 companies, such as HP, Harris, and AT&T, and the Department of Defense.

*EDUCATION*

* MBA Student, Embry/Riddle Aeronautical University, FL
* MS, Technology Management Graduate, George Mason University, VA
* BA, Journalism Graduate, University of Minnesota
* Print & Broadcast Journalism Graduate, DINFOS, Ft. Meade, MD

PROFESSIONAL EXPERIENCE

**Peridot** 2016-Present

Cloud Security Architect

DEPARTMENT OF DEFENSE, DEFENSE HEALTH AGENCY (DHA). KSJ CONTRACT

* Serve as senior cloud security architect to DHA, one of the largest health care systems in the world, which serves 55 hospitals and 600 clinics, employs 150,000 workers, and provides care for 9.6 million members in the military’s health plan under a $2 billion IT budget.
* Consultant to the Military Health System (MHS) on Risk Management Framework (RMF),

FISMA, FedRamp, FedRamp+, and the DoD Cloud Security Requirements Guide (SRG), to protect both Personally Identifiable Information (Pll) and Protected Health Information (PHI).

* Identify and develop cloud migration plans for up to 50 legacy healthcare apps under the Health IT (HIT) Directorate deployed in DoD/DISA, and commercial cloud vendors.
* Lead technical cloud service hosting working groups and integrated product teams moving toward a cloud-based computing model across multiple DoD medical applications.
* Conduct cloud technology assessments, AoA, trade studies, and cost modeling, business case assessments, and return on investment analyses supporting cloud computing.
* Deploy IA, cybersecurity, network transport, and general systems engineering support to DoD, DHA, and commercial Cloud Service Providers (CSPs) regarding cloud computing, security, hosting, network, and system security for protecting sensitive medical information between DoD, healthcare providers, and other partners such as the Veteran’s Administration.

**Vimro LLC** 2012-2016

Cloud Security Program Manager I Cloud Security Architect

AT&T INTEGRATED CLOUD (AIC) & OPEN STACK IAAS CLOUDS / AT&T CONTRACT

* Managed cloud security governance and strategic direction for AT&T OpenStack clouds across 15+ DevOps teams, CSO, Compliance and Chief Privacy offices.
* Led AT&T cloud security compliance efforts supporting best practices and regulatory requirements for OpenStack cloud across multiple security frameworks to include ISO 27001, HIPAA (HiTrust), PCI-DSS 3.1, SOX, NIST (FISMA/FedRAMP), and data privacy laws.
* Directed client engagement with the help of Accenture, Arista, Basho, Cisco, CloudScaling, Dell, Dyn, Ericsson, IBM, Mirantis, Nicira, OpsCode, PagerDuty, Quanta, SourceFire, SuperMicro, TrustWave, Veris, and VMWare, while supporting >200 internal apps and >50,000 VM's.
* Aligned laaS security to include server deployment (Ubuntu/Red Hat/CentOS linux), IPS (SourceFire), DDoS, firewall, multi-factor access control (RSA), risk management (McAfee MVM, Tenable), anti-virus (ClamAV), inventory control, PenTest, application scanning (HP Weblnspect), and static code analysis (Fortify), with corporate compliance goals.
* Well versed in all phases of the SDLC, including Agile and Scrum methodologies; as Scrum Master, executed regular scrum call and took status of AT&T cloud security delivery.
* Managed company Cloud Security Practice, forged partnerships, and developed and implemented cloud security solutions, to include using Cloud Security Alliance controls.

**GOVPLACE** 2011-2012

Sr. Program Manager

DHS ICE. TSA, & CIO CONTRACTS

* Communicated with senior level customers, vendors and executives to manage the contract relationship and to maintain a high level of customer satisfaction by delivering on all aspects of the ICE/Archer eGRC contract.
* Managed and communicated the accomplishments of contract goals and objectives to drive profit maximization and contract growth.
* Led interdepartmental matrixed team to ensure delivery performance to SLA, profitability of projects on the program and customer satisfaction.

**APEX SYSTEMS** 2011

Project Manager I Cloud Computing Security SME

HARRIS CORP. CYBER INFORMATION SYSTEM (CIS) CONTRACT / HEWLETT-PACKARD

* Served as a Cloud Security SME contributing to the roll out of a large-scale technical program with BMC, VMWare, EMC, Hewlett-Packard and Harris partners.
* Created policies to guide Harris in implementing a secure multi-tenant private/hybrid cloud configuration-secure Infrastructure as a Service (laaS).
* Communicated info to include audit/compliance, virtualization, system security, anti-virus, IDS, vulnerability scanning, network security, SAN Security, hardened OS's, and security technologies like those from VMWare, McAfee, RSA, Tenable, Harris SignaCert, IBM AppScan, Novell IAM, NitroSecurity SIEM, and Splunk.

**ALTA IT** 2011

Project Manager I Security SME

US ARMY. DEFENSE LOGISTICS AGENCY (DLA) HQ. FT. BELVOIR, OPS CONTRACT/BAE

* Led 15-person contract to migrate 3,500 DLA HQ assets to Windows 7 in more than 5 locations utilizing Federal Desktop Core Computing (FDCC) image.
* Successfully upgraded 114 assets during pilot phase, which include project planning, execution, and status reporting to senior agency operations management and enterprise executives.
* Provided IA expertise as field site project manager for the Command Cyber Readiness Inspection (CCRI) conducted by DISA on behalf of the United States Cyber Command (USCYBERCOM).