Sr. IT Risk Analyst - Consultant Sr. IT Risk Analyst - Consultant Sr. IT Risk Analyst - Consultant - iptiQ America Life & Health Totowa, NJ More than 10 years' experience as a Senior/Lead/ advisor role with ownership and accountability in Risk & Compliance, Security Architecture, Implementation and Risk Analysis. Influencing skills result oriented, time management and proven ability to work with senior management in a matrix organizational structure. Strong understanding and experience of IT Security Standards, Data Protection and Network Security Tools & Analysis, Vulnerability Assessment and Penetration testing tools. Worked with Splunk, QRadar, RSA envision SEIM tools, Packet analysis, Active Response, and Regulatory Compliance. Successfully achieved and led organization wide risk and compliance and data protection program/ initiative based on ISO/IEC 27001, 17799 / BS 7799, PCI-DSS, COSO ERM and NERC regulatory compliance frameworks. Knowledge of GDPR and BCR requirements. Server farm / network infrastructure consulting IS Audit/ Gap analysis based on industry best practices, OSSTMM, NIST SP800-53, CIS - Critical Security Controls and GRC tools. Quick learner, strategic thinker, mentor, proactive, team player with excellent written & oral communication. Industries include Electric Utilities, Retail, Government, Insurance, Payroll/Finance, Telecom, Pharmaceuticals and Engineering & Hospitality. Authorized to work in the US for any employer Work Experience Sr. IT Risk Analyst - Consultant iptiQ America Life & Health - Armonk, NY March 2019 to Present Helping Deputy CISO and working for GRC program - security audit/controls assessment to achieve certifications of HIPAA, PCI - DSS, SSAE 18 (SOC 2) and NYDFS - NYCRR-500 using HITRUST My Csf. Performing related assessment activities utilizing HITRUST My CSF tool, and working with Cyber Security, Infrastructure technology and Business staff on completing the assessments and evidence collection. Work with external auditors to address the gaps and work towards above certifications. Environment: Cloud environment - Azure, Dell Boomi & Okta, HITRUST My Csf Sr. Information Security Governance & Risk Analyst - Consultant MTA January 2015 to December 2018 Worked as a Risk Analyst & Internal Controls program management coordinator based on COSO ERM Framework for MTA IT divisions. Built COSO ERM Internal Control framework using GRC tool and based on ISACA, CIS Critical Security Controls, PCI and NIST SP 800 53. Perform testing

of Internal Controls, risk identification and remediation. Aided/guidance to various process owners for improvement of MTA IT Internal Controls Tasks performed: ? Prepare monthly reports with risk and controls status and dashboards for compliance activities. Presented findings to management. ? Monitor all IT groups to ensure they follow established standards, policies and procedures. ? Design work flow and integration for all the business process of MTA IT to GRC. ? Created and helped to established business process for all IT division and overseeing testing of the Internal Controls. ? Perform risk analysis for gaps and corrective action plans for risk mitigation for security enhancements. ? Manage/ maintain GRC tool to annual update and mapping the Internal Controls with risk scoring of all the business process with Information Security policies, standards and procedures. ? Organize and conduct annual training for about 35 Internal Controls testers using GRC tool. ? Risk scoring/ matrix and creating & tracking KPI & KRI of all important and critical business processes and business impact on all business processes. ? Contribute for developing Information Security policies, procedures and processes. ? Annual maturity assessment using SEI CMM methodology to improve quality of Internal Controls. ? Manage audit workflow in tracking Audit open items, remediation and coordination with IT and Internal/ External auditors for regulatory and compliance. ? Perform Vulnerability Assessment and testing of Internal Controls for following key process (few listed) with evidence gathering and detail reviews, organizing the evidence in presentable format. MTA - New York, NY January 2014 to December 2018 Sr. Information Security Architect/ Analyst - Consultant January 2014 to December 2014 01/14 - 12/14) Worked on CISO deliverables as a Lead for vendor's presentation and report generation with detail comparison, analysis and solutions for decision making for various following security tools (Data protection and risk management tools): Exabeam UBA, Palo Alto, Splunk, McAfee DLP etc. as part of risk management and technology upgrade. Led project of Exabeam UBA, Palo Alto Firewalls, Splunk and McAfee Data Loss Prevention from POC and contributed for security architecture and implementation. Led project to analyze the data protection technology and performed POC for Application Control (Bit9+Carbon Black) and Avecto. Review McAfee Antivirus / DLP - ePO and Fire eye for threat analysis Ran and reviewed Splunk queries for threat analysis for network attacks,

viruses, mal ware, SPAM, phishing and other intrusions. Environment: Splunk SIEM, McAfee DLP, and Antivirus, Malware protection -Fire eye, Palo Alto, Exabeam UBA, Cisco Firewalls, Information Security Governance, Risk & Compliance, Internal Controls program, PCI, SOX, COSO- ERM, CIS - Critical Security Controls, NIST - SP 800 53, COBIT, Oracle GRC tool, Qualys, Cloud Computing Sr. Information Security Analyst- Consultant ADP Inc - Roseland, NJ July 2013 to November 2013 Project: RSA enVision integration, RSA DLP tuning, Log extraction Performed integration of new devices and troubleshooting on RSA enVision. Performed security analysis and monitoring on RSA Archer. Worked on Greenplum using sql statements for device verification/ duplication and analysis for RSA enVision sites. Prepared weekly event analysis, substantiation and reporting for RSA DLP using crystal reports for management, verifying false positives and true positives for tuning with Vontu. Contributed for extraction of forensic log and content search using scripts and working with other groups. Environment: RSA EnVision, RSA Archer, Green plum, RSA DLP, Vontu, SOX, CIS, NIST Sr. Information Security Consultant/ Architect Bed Bath and Beyond - Union, NJ February 2013 to June 2013 Project: Network Architecture for PCI Network Segmentation, PCI Risk and Compliance. Led the project and worked on building secure network design and architecture for PCI Zone. Led the team and successfully achieved management goal of migration of applications, database and servers (PCI assets) to PCI zone. Led and worked with team to secure / hardening of Application, Database, Linux and Windows servers and network components based on vulnerability analysis results. Worked on RSA DLP scanning for event analysis and worked for threat mitigation. Worked with other groups to support incident response and security analysis for threat mitigation. Environment: PCI, SOX Cisco ASA, Nexus 7k, AlgoSec, Blue coat proxy, RSA two factor authentication, RSA DLP Sr. Security Consultant / Analyst SONY Corporation America - Park Ridge, NJ November 2012 to February 2013 Project: Multiple (National/ International) NOC Operation and design Took ownership and led project of Skybox Security for Firewall Assurance and achieved goal of well organizing firewall rules for PCI Compliance. Built firewall rules ASA 5580, Cisco PIX, Checkpoint R 70 SPLAT, Nokia IP series using Provider-1, Nokia Voyager for IP series. Worked on Blue Coat Proxy SG and Blue Coat Reporter for logging

for PCI compliance. Took ownership and configured RSA enVision SIEM for security analysis and incident response for PCI compliance. Environment: PCI Compliance, Checkpoint R65, Provider-1 platform, Nokia IP series appliance, Blue Coat SG appliance, Skyboxview Firewall assurance, Cisco ASA and Cisco PIX firewalls, IPSec L2L VPN Lead Information Security Consultant / Analyst High Security Zone Datacenter - Parsippany, NJ May 2012 to October 2012 Project: Accountable and ownership of building High Security Zone Datacenter infrastructure and operation of multiple (National/ International) NOC for PCI compliance Successfully led and built PCI network segmentation in abbreviated time and received management appreciation to achieve major milestone of PCI compliance. Led the project and worked with Cisco ASA firewalls (Single& multimode, transparent & routed), design, build and maintained seven (7) IPsec L2L VPN's between High Security PCI Zone & MPLS cloud Firewall in active/ standby environment. Designed and implemented VLan on Core Cisco 6500 and Nexus 7k series for wireless users as a part of network segmentation and isolated them from PCI high zone by creating IPSec L2L VPN and firewall ACL. Integrated all network, security devices, servers and critical applications to IBM QRadar. Environment: PCI & SOX compliance, Production and Co-lo Datacenter environment, Global network MPLS infrastructure, Cisco ASA 5540, 5550, 5585 Firewalls (Transparent, Routed, Multimode), Cisco ACE Load balancers, Nexus Core 5500 / 7000 Switches, Cisco 6500 series Core and IDF distribution, Cisco 3700 series, Cisco 3800 series ISR, Cisco Security Manager for configuration and log management, IBM QRadar SIEM, IPSec L2L VPN, GRE over IPSec VPN, Cisco Core 6500, EIGRP, BGP, MPLS, Service Now for Change Management, MS Visio Sr. Information Security Consultant UIL Holding Corp - Shelton, CT October 2011 to March 2012 Project: UI Technology Center Network Security Data Center Operations Contributed towards NERC Compliance for CIP (Critical Infrastructure Protection) regulatory compliance with NERC and "Service Now" Change Management process for infrastructure change and updates Worked on RSA envision to create custom alerts, tuning of existing alerts, creating dashboard view for reporting, event analysis and remediation of Security Alerts and events of Cisco ASA, IPS, routers, Blue coat proxy, McAfee End Point Antivirus, Oracle database and Windows and AIX servers.

Worked on detail packet analysis and forensics using RSA Event Explorer by creating Event Traces from various device and Server groups for threat/log analysis and creating appropriate custom alerts and Correlated Alerts for enVision SIEM. Lead team for daily operation and maintenance creating new firewall rules of Cisco ASA and Palo Alto firewalls in active/ standby and VPN. Maintained existing VPN and installed/ configured seven (7) new IPSec L2L VPN for various site offices and group of companies. Lead team on Cisco IPS 4240 (Intrusion Prevention/ Detection) for daily operation, monitoring and signature tuning and creating action filters using Cisco Security Manager. Environment: NERC CIP Regulatory Compliance, Cisco ASA firewalls, IPSec L2L VPN, Cisco IPS 4240, Cisco TACACS+, PA 2050/2020 (Palo Alto Networks), RSA enVision SIEM, RSA Event Explorer, Regular and Correlated Alerts creation from RSA enVision SIEM, Blue Coat Proxy Sr. IT Security Analyst (Consultant) Wyndham - Parsippany, NJ May 2011 to August 2011 Project: Infrastructure Stability program for PCI Security Compliance Performed gap analysis and study of existing Enterprise Monitoring Tools configuration for systems, database and applications for high availability, better performance, PCI compliance. Performed study and gap analysis of implemented capabilities for all systems, applications, and database components, find gaps and suggest better options with remediation strategy plan. Authored EMT Gap Analysis and Enterprise Monitoring Vision document presented to management. Environment: PCI Compliance, Windows, Linux, AIX, servers; Applications -Tomcat, .Net, Java, Databases - Oracle, Informix, DB2, SQL, Monitoring Tools - Applications Manager, Oracle Enterprise Manager, Sentinel from Server Studio Lead Consultant - Information Security Analyst Pioneer Data Systems Inc June 2010 to April 2011 Lead team June 2010 to April 2011 of engineers and performed daily operation, installation and maintenance of various device and servers including Cisco ASA Firewall ACL change, IPSec L2L VPN planning design and implementation, change in Crypto map entries, editing of ports, IP or subnets etc. Reviewed and implemented improved access control on Cisco IDS as per company's security policy. Reviewed root and other user accounts in Linux systems and implemented improved permissions and access controls as per company's security policy and performed server hardening. Improved and updated user access and permission on Windows server after review of

Active Directory environment as per security policy. Environment: Cisco ASA 5520, Cisco IDS, Enterprise Linux with High Availability, Windows AD, Information Security policies and procedures and compliance, vulnerability assessment, Nessus, Nmap Sr. Consultant - Network Security Engineer/ Architect/ Security Analyst AT&T - Florham Park, NJ August 2006 to August 2009 Sr. Security Analyst Cisco, Checkpoint August 2006 to August 2009 Worked on the same project two separate time periods: 08/06 - 08/09 & 02/10 - 05/10 Project: Secure Data center implementation for SEIM (Security Event and Incident Management System) Platform, to process log feeds and generate meaningful and actionable security alerts (Threats) in near real time on the web portal based on Intellitactics NSM. Sr. Security Analyst: Worked as an Incident Response Security Analyst by monitoring and working on suspicious activity and security Alerts generated on SIEM portal. Performed deep inspection and analysis for supplemental details and device logs for security threats; take necessary actions or more investigation using ARIN/APNIC databases, AT&T's vulnerability resource portal and various resources. Sr. Network Security Engineer: Involved in Network design and implementation of Secure Datacenter. Implemented SEIM platform with integration of various logs of Cisco, Checkpoint, IDS/IPS, Antivirus. Performed implementation and maintenance of Checkpoint NGX R-65 VPN1 on SPLAT in High Availability environment. Implemented security access controls, roles and permission in the systems and security devices in compliance with the company's security policy, standards, directions, procedure and consistency. Involved in implementing/ configuring Red Hat Linux ES/ AS servers and network/ firewall configuration with proper access controls and resource permissions and alert management using Nagios. Worked with some shell and pearl scripts for automation. Environment: Red Hat Linux ES servers with High availability, Open LDAP for authentication, Microsoft Active directory infrastructure, Checkpoint NGX R65 XL Firewalls on SPLAT, VMWare ESX 4.0, Cisco VPN 3000 Concentrators, Cisco PIX, Routers, Switches, KVM Switches, Daytona, Shell Scripts/ Pearl Scripts, SSH, VPN, VLAN, Nagios, Intellitactics NSM 5.7 (SIEM), SOX compliance framework Consultant - Security Architect Cap Gemini - Dallas, TX March 2006 to May 2006 Client: TXU- A Utility Company of Texas. Project: To evaluate existing Network infrastructure and security policies by performing

gap analysis, risk assessment and vulnerability analysis using commonly available tools for NERC compliance. Design and improve new secure network architecture, implementation plan and deploy improved organization for NERC CIP Standards. Identified Cyber Assets in the office and plant. Performed annual qualitative and technical Risk Analysis. Conducted penetration testing and Vulnerability Assessment for existing network /server/ Wireless infrastructure, using GFI Lan guard, Superscan, Nmap, Nessus, ethereal, etc. Report generated and prepared a plan with remediation strategy using CVE database, US-Cert and product website reference. Reviewed documentation of Network/Server infrastructure documentation, log retention practice and gap analysis between implemented controls and documents. Remediation plan provided. Information Security Consultant Indus Face Consulting - IN April 2005 to January 2006 Education BS in Physics in Physics South Gujarat University

Name: Debra Frey

Email: andersonsamantha@example.com

Phone: (384)529-1290