Steven Mayson

E-mail: info@stevenmayson.com
Cell: 214.310.9865

Summary

Steven has spent nearly a decade in cybsersecurity specializing in Guardium and QRadar working for Bank of America, AIG, Visa as a customer of IBM and later as a provider of managed security services for IBM supporting numerous customers: Horizon Blue Cross Blue Shield, Clarient Global (a subsidiary of Depository Trust & Clearing Corporation), Viewpointe, American Express, Anthem, State of California Medicaid Management Information System (CA-MMIS), AECOM, CenturyLink, IBM Business Continuity & Resiliency Services or BCRS, L.L. Bean, State of Arizona, Parkland Hospital, Cleveland Clinic, CapitalOne, Banco, Brighthouse, TD Bank, First Bank, Meijer, MetLife Tribeca, Northern Trust, AIG, and Sysco Foods) supporting Guardium, QRadar, Tripwire, and Vyatta firewalls with multi-disciplinary roles as Engineer, SME, Architect, Solution Architect, Developer, Trainer, and Tech Lead.

Though many accomplishments have been achieved in his tenure at IBM for six years, the most notable being:

- Reverse Engineered a complicated Python script written by a prior developer that talks to the Ariel db via Python requests module and prepares event data processed by configured Building Blocks and Rules for ingestion by another system called ICD (IBM Control Desk) that automatically creates compliance tickets for ACAT compliance team, corrected small handling issues, and added multi-tenancy selection capability.
- Developed several Bash and Python scripts that add, remove, or disable log sources directly touching the QRadar database prior to the new Log Source Management app having this capability.
- Reverse Engineered the QRadar database and related processes to the WinCollect agent without any formal training from IBM and developed a Python script that automatically removes all relevant pieces of information so that an agent may be registered as brand new again. This capability still does not exist in the latest QRadar version.

Skills

Cybersecurity

Symantec Vontu Enforce DLP Systems	Guardium Data Encryption
RADWare Content Distribution	InfoSphere Sensemaking
RADWare SSL Decryption/Accelerators	QRadar SIEM (7.2.x, 7.3.x, 7.4.x)
FireEye Malware Scanning Systems	Tripwire Enterprise
Imperva DBAM	Cisco ASA NGFW w/ FirePOWER Services
Guardium DBAM (7, 8, 9, and 10)	Vyatta Firewalls (5400, 5600)
Guardium for Applications	Cisco ASA 5500s
Guardium for Files	ASG Firewall (Sophos UTM)
Guardium Data Redaction	

Router Experience

Cisco 1800s
Cisco 2500s
Cisco 2600s
Cisco 2800s
Cisco 3600s
Cisco RV340

Switch Experience

Cisco Catalyst 2900s
Cisco Catalyst 3500s
Cisco Catalyst 6500s

Desktop/Server/OS Experience

Windows (95, 98, 2000, XP, Vista, 7, 8.1, 10)
Maintenance, security, and performance
Software and hardware upgrading
Troubleshooting, repair, i.e. soldering
Hard drive encryption
Debian Linux
Ubuntu Linux
Unix (OpenBSD/FreeBSD)
Red Hat Enterprise Linux 5, 6, and 7

Programming & Scripting Languages & IDEs

Python
Bash
Expect
IntelliJ IDEA

Entry Level Machine Learning with Python

Linear Regression	Decision Trees
Logistic Regression	Random Forests
Multi-Class Classification	Natural Language Processing
Support Vector Machines	
Naive Bayes	

Entry Level Data Analysis and Visualization with Python

Pandas Series & DataFrames
Matplotlib
Seaborn

Employment Experience

Artech Information Systems (contractor) | IBM
September 2, 2014 – Present – Solution Architect | Guardium & QRadar Architect

Steven is the Guardium & QRadar Architect responsible for IBM Security Guardium & QRadar SIEM on the Delivery & Transformation team within IBM alongside many security technology experts with a wide range of specializations that provides operational documentation, planning, and steady-state support for numerous fortune 500 companies.

Steven also functions as the Expect, Bash, and Python developer for customized enterprise security management solutions.

Delivery & Transformation, a part of Global Technology Services, delivers managed security services with their exceptionally unique skill sets to design, deploy, and maintain client environments.

Talent Burst (contractor) | Visa, Inc
August 27, 2013 – August 27, 2014 – Sr. Security Engineer (Guardium Administrator)

Steven was a Sr. Security Engineer specializing in Guardium, a Database Activity Monitoring security tool at Visa, Inc. based out of Visa's flagship datacenter dubbed OCE, Somewhere on the Eastern Seaboard.

Steven was the liaison responsible for interfacing with Visa's service desk for serviceability of the Guardium infrastructure and was instrumental in streamlining that requirement.

He customized numerous PCI-DSS compliance requirements including anomaly detection alerting, audit process jobs for SQL activity reporting, classification of sensitive data, S-TAP Serviceability, developed rudimentary Expect scripts to interface with Guardium for information gathering or modify configuration changes leveraging GuardAPI.

Modis (contractor) | AIG Global Services
March 7, 2013 – August 6, 2013 – Sr. Security Engineer (Guardium Administrator)

Steven supported engineering for Guardium.

Insight Global Inc. (contractor) | HP Enterprise Services/Bank of America
December 21 2011- Jan 14 2013 - Security Operations Engineer (Guardium Administrator)

Steven supported operations for multiple cybersecurity vendors: Guardium, Vontu, Radware, Fire Eye, and Arbor.

Education

I pride myself on being self-taught in everything that I do.

Certifications

- Cisco Certified Entry Networking Technician (CCENT) - 2010

Blog

- https://www.stevenmayson.com/post/monitoring-ibm-aix-servers-with-qradar