Brian DeMaio

NYC Metro Area – NJ | www.briandemaio.com | brian529@gmail.com | www.linkedin.com/in/brian-demaio/

Summary

A Cybersecurity Operations Center Infrastructure Engineer with over four years of combined security and IT experience in the financial industry. A proven ability in responding to cyber threats, onboarding security tools and logs, and developing custom alerting use cases and infrastructure. I am seeking a new role to build upon my existing knowledge, with opportunities for leadership development.

Key Skills

- **Tools:** Splunk, IBM Resilient, Microsoft 365 Defender (Including MDE, MDI, MDO, MDC, and MCA), AWS GuardDuty, GCP Security Command Center, Imperva, Zscaler, Bluecoat, Qualys, Jira, and ServiceNow
- **Languages:** SPL, KQL, HTML, Python and PowerShell

Education

MASTER OF SCIENCE | UNIVERSITY OF MARYLAND GLOBAL CAMPUS

- Major: Cybersecurity Technology

BACHELOR OF APPLIED SCIENCE | UNIVERSITY OF MARYLAND GLOBAL CAMPUS

- Major: Cybersecurity Management and Policy

Experience

CYBERSECURITY OPERATIONS SPECIALIST | PRUDENTIAL FINANCIAL | NEWARK, NJ | OCT 2020 – PRESENT

- Vital member of the Cloud and Endpoint CSOC Sub-Team, leading data onboarding, log troubleshooting, use case development, and training.
- Operationalized various security tools including Imperva, Defender for Identity, Defender for Cloud, and Zscaler while curating their output to minimize false positive alerting.
- Spearheaded the creation of several custom use cases such as heartbeat alerts to detect logging outages and the creation of an AWS account lookup file to enrich GuardDuty and CloudTrail alerting.
- Authored multiple internal documents outlining processes, procedures, and guidance for CSOC analysts to follow when responding to specific incidents and alerts.
- Developed and led a Cloud and Endpoint Sub-Team training program which resulted in the successful onboarding and quick assimilation of CSOC processes for new team members

INFORMATION SECURITY SR. ASSOCIATE | PRUDENTIAL FINANCIAL | ROSELAND, NJ | APRIL 2019 – PRESENT

- Manager of daily Qualys operation tasks including purging stale assets, troubleshooting authentication failures, deploying appliances, configuring test environments, and maintaining tags and asset groups.
- Enhanced cloud capabilities through the establishment of new AWS procedures including monthly AMI verification scans, implementation of Qualys EC2 connectors, and identification of missing cloud agents.
- Developed Python and PowerShell scripts to facilitate vulnerability scanning automation and on-demand host-based scans for increased team efficiency.
- Collaborated with DevSecOps team on the design of a new Remediation Hold Portal to refine our exceptions database process and improve remediation timelines.

IT INFRASTRUCTURE ASSOCIATE | PRUDENTIAL FINANCIAL | ROSELAND, NJ | JAN 2018 – APRIL 2019

- Provided Tier II IT customer support for users across multiple internal business units while maintaining an incident SLA of 90.8%.
- Managed the inventory and accounting of a high-value electronics depot with zero incidents.
- Performed bulk builds of PCs for deployment to end-users while meeting urgent migration deadlines.
- Led staff training for new team members on virtual desktop environments, PC builds and ServiceNow.

AVIONICS TECHNICIAN | U.S. AIR FORCE | MILDENHALL, UK | JUNE 2012 – SEPT 2017

- Performed over 3000 scheduled and unscheduled maintenance actions on KC-135 aircraft.
- Instructed and supervised junior technicians on troubleshooting, repairing, and performing operational and preventive checks on aircraft wiring, flight controls, stabilization systems, and avionics systems.