David S. Graham
231 7th St. SW
Pine Island, MN. 55963
(612) 552-6013
dgurehamu@outlook.com

Experience:

Aviator Security 7 / 20 – present
Consultant

Providing software development and cloud deployment services for a motorcycle import and distribution corporation in Taiwan.

3M 10 / 17 – 6 / 20
Cyber Threat Detection Specialist

Led the design and development of SIEM and SOAR solutions at 3M, and served as a mentor and escalation resource for the SOC. Spearheaded efforts to increase the efficacy and decrease the volume of security alerts by developing custom event processing solutions using Python, Go, Kafka, NiFi and Elasticsearch, and implementing an agile rule development process. Worked extensively with business units to facilitate the exchange of business and security concerns, and ensure the protection of critical information and assets. Defined security requirements for application migration to Azure and AWS, and led a POC for ArcSight to Azure Sentinel migration. Assisted with intelligence gathering, incident handling, and investigations of multiple advanced threat actors.

Quanterus 10 / 15 – 8 / 17
Developer and Co-founder

Led a diverse start-up team from idea to minimum viable product for a cloud-based application to simplify information security risk management while maintaining ISO and NIST standards. Developed a full stack solution with a proprietary graph database using javascript, python, and PostgreSQL.

Code 42 10 / 11 – 10 / 15
VP of Security

Joined a fast-growing SaaS company as their first security hire. My experiences ranged from conducting the company's first security assessment and writing its first security policy, to hiring and leading a team that maintained all aspects of physical and technical security, achieved ISO27001 certification, participated directly in CrashPlan product development, and provided support and consultation for sales teams and customers. Some of my major initiatives included driving significant changes in the security functionality of our core product, spearheading security-related business development, and bringing the company into PCI and HIPAA compliance.

Stellar Dynamic 4 / 09 – 10 / 11
Consultant

Provided security consulting services for application development and AWS cloud deployment.

MoneyGram International 6 / 04 – 4 / 09

Security Architect

Worked with business units to define IT architecture, led vulnerability assessments and incident response, provided security guidance for application development, and trained security analyst staff. Designed and deployed a Syslog-NG cluster to centralize logging for thousands of devices, a Nessus SecurityCenter and Scanner infrastructure, and led POCs for AIX to Linux migration. One of my major contributions was the development of a transaction monitoring and fraud detection application leveraging c and Postgresql for event processing and alerting, and PHP for the NOC and Executive dashboards.

ING 2 / 01 – 4 / 04

Senior Network Security Consultant

Responsibilities included security architecture, vulnerability assessment, incident handling, intrusion and forensic analysis, IDS management, policy creation, security consultation for the enterprise software architecture group, and assisting project managers assigned to information security projects. Co-developed an in-house SIEM solution for large-scale network assessment, asset identification / tracking, and analysis utilizing Perl, PHP, and SQL.

Webhelp 3 / 99 – 2 / 01

Security Manager

Was responsible for the design, implementation, and management of security infrastructure. Designed and deployed a global IPSec VPN to connect corporate LANs, co-location facilities, partner networks, and call centers utilizing Cisco PIX firewalls and Cisco routers. Designed and deployed a global IDS infrastructure. Daily responsibilities included vulnerability assessment, intrusion analysis, incident handling, firewall administration, policy creation, security product research, and tracking patch levels. Absorbed roles for infrastructure architecture and network administration.

Certifications:

GIAC Certified Detection Analyst (GCDA #144) 2018

(ISC)^2 Certified Information Systems Security Professional (CISSP #59124) 2004

GIAC Certified Intrusion Analyst (GCIA #208) 2000

My practical assignment was selected for publication in the book "Intrusion Signatures and Analysis" Sams, 2001.