MARK D. GRAY

MARKDALTONGRAY@GMAIL.COM

315-935-9627

OBJECTIVE

Thrives in environments that require improvising, adapting, and overcoming challenges in order to ensure mission success.

CERTIFICATIONS

GSE
CISSP
CCNAS
RHCE
CEH
OSCP
GASF

EXPERIENCE

AT&T, DIRECTOR- CYBERSECURITY

Feb 2016 – Current

-Develops knowledge about cyber adversaries and their motivations, intentions, and tactics that are collected, analyzed, and disseminated in ways that benefit security and business staff.

-Oversee operations for 100+ AT&T MTDR customers, to include solution implementation, incident response activities, and SoC monitoring.

-Provides threat detection, network security, intelligence production, and process automation in support of both U.S. Government and commercial clients.

-Automated the deployment of cyber threat intelligence across multiple databases with a fully-developed analytic process.

-Correlated actionable security events from a large number of data sources by utilizing unique association techniques.

-Developed analytical products that resulting from the fusing of enterprise and all-source intelligence.

-Development of analysis tools and techniques for analysts to interact with logging solutions.

-Lead threat hunting activities in government and commercial sector services.

SANS, SECURITY ENGINEER

Sept 2014 – Feb 2016

-Plan, implement, install, and operate intrusion detection technologies for company network.

-Detect, assess, and report network vulnerabilities.

CLEARANCE

TS/SCI DoD & DHS

PUBLICATIONS

Shell Scripting for Reconnaissance and Incident Response

Effective Windows Monitoring Guidance

Defining the "R" in Managed Detection and Response (MDR)

-Research and development of technology used in SANS courses.

-Course content creation and quality assurance.

USMC, INTELLIGENCE SPECIALIST

Feb 2011 – Current

-Collected, processed, and reported to higher command on raw information leading to mission critical intelligence.

-Developed greater regional, political and social awareness of region and knowledge of regional threats.

-Delivered actionable intelligence for ongoing Cyber missions.

-Operationalized the intelligence component of USMC Cyber Protection Teams.

-Conducted vast research through all-source fusion in support of the Tactical Fusion Center (HUMINT/CI, SIGINT, OSINT, MASINT, IMINT).

EDUCATION

B.S COMPUTER SCIENCE
M.S COMPUTER SCIENCE EST. 2020

Georgia Institute of Technology

TECHNICAL PROFICIENCIES

Analysis Tools: Cuckoo, Bro, Snort, SiLK, Tcpdump, Wireshark, SANS SIFT Kit, OSquery

SIEM Tools: AlienVault, ELK, Splunk, ArcSight

Languages: Bash, C, PowerShell, Python

Cloud Solutions: AWS, Azure, GCP