Michael Griffith

CYBER SECURITY ANALYST

Rancho Cordova, CA | 601.832.0111 | GrLffLth82490@gmail.com

Experience

CYBER SECURITY ANALYST | CALIFORNIA DEPARTMENT OF TECHNOLOGY
2022 – Present

Monitor Security Operations Center (SOC) technologies, encompassing a range of elements such as intrusion detection and protection devices, host-based protection technologies, 0-day and Advanced Persistent Threat (APT) technologies (such as sandboxing, behavioral monitoring, etc.), packet capture and metadata analytic systems, Data Loss Prevention (DLP) technologies, email hygiene systems, and more. Investigate alerts in Sentinel queue using vulnerability assessment and open-source tools, Splunk, Wireshark, CrowdStrike, Riverbed, TippingPoint and Intrusion Detection systems. Utilize expertise in recognizing indicators of compromise and threats to identify attacks or compromised assets. Communicate with multiple agencies Information Security Officers to alert them of exploits.

TARGET DIGITAL NETWORK ANALYST | 149TH IS CA AIR NATIONAL GUARD
2021 – 2024

Conducted advanced analysis of digital network communications to identify foreign military capabilities, intentions, and cyber threats in support of national security objectives.
Exploited foreign network infrastructure using classified SIGINT systems to provide real-time intelligence to combatant commands and national-level agencies.
Leveraged tools such as XKeyscore, MARINA, PINWALE, and Wireshark to discover selectors, map communications patterns, and identify threat actor TTPs.
Collaborated across IC partners including NSA, and CYBERCOM to fuse SIGINT with OSINT for comprehensive intelligence assessments.
Produced classified reporting and intelligence products aligned with Intelligence Community Directive (ICD) 203 standards, driving informed decision-making at the strategic and operational level.
Performed metadata analysis and content exploitation on foreign networks, discovering new targets and expanding existing target sets.
Trained and mentored junior analysts in TDNA methodologies, SIGINT tools, and OPSEC procedures, enhancing overall mission capability.
Operated in secure, compartmented environments with Top Secret/SCI clearance; ensured strict compliance with legal authorities and oversight protocols during intelligence collection and analysis.

FUSION ANALYST | 149TH IS CA AIR NATIONAL GUARD
2018 – 2021

Integrated multi-source intelligence (SIGINT, GEOINT, and OSINT) to produce actionable intelligence assessments supporting national security and interagency decision-making.
Provided fused intelligence products that informed strategic planning, policy development, and operations across defense, intelligence, and homeland security sectors.
Collaborated with federal agencies and intelligence community (IC) partners to share intelligence, align mission objectives, and ensure unity of effort.
Authored finished intelligence reports and briefings for senior leadership, ensuring timely, mission-relevant insights with clear, data-driven recommendations.
Operated within SCIF environments and maintained strict compliance with classification guidelines, handling highly sensitive material under TS/SCI clearance.
Supported counterterrorism, counterintelligence, and cybersecurity initiatives by synthesizing intelligence from multiple domains and regions.
Maintained current knowledge of global security developments, regional threats, and adversary TTPs to support dynamic threat forecasting.

Education

Analysis and Production Apprentice Course – United States Air Force
CompTIA Security+ SY0-701
Network +
Microsoft Security, Compliance, and Identity Fundamentals (SC-900)
Microsoft Security Operations Analyst (SC-200)
Microsoft Azure Fundamentals (AZ-900)

Skills & Abilities

- Strong grasp of security technologies, frameworks, and best practices
- Dependable team-oriented professional
- Strong written and verbal communication skills
- Performs efficiently in high-pressure, fast-paced environments