**Gina Napier**

Senior Cyber Security Engineer Advisor| Active DoD Clearance

T: 619-888-0061| Email: [napier.gina@gmail.com](mailto:napier.gina@gmail.com)

## Profile Overview

Results-driven Senior Cyber Security Engineer with 9+ years of experience in the design, implementation, and maintenance of security measures and cyber tools that protect DoD IT national security systems and networks from cyber threats. Expertise includes vulnerability management, SIEM management, incident response, and secure system design, with a proven track record of improving security posture in federally regulated environments. Holds active TS/SCI Clearance and current IASAE II (DoD 8570/8140) relevant certifications such as CISSP, CISA, CYSA+, AWS Cloud Practitioner, Linux + and Splunk Certified Admin.

## Education

* Master of Science (MS) in Cyber Security - Excelsior College, Aug 2015 – Aug 2018
* Bachelor of Science (BS) in Cyber Security - University of Maryland University College, Aug 2008 - Aug 2013
* Code Fellows Python Software Development Boot Camp - Feb 2022 – Sept 2022

## Certifications

|  |  |  |  |
| --- | --- | --- | --- |
| **Certifying Body** | | **Certification** | **Validity Period** |
| EXIN | ITIL Foundations V3 | | Nov 2013 - Present |
| CNSS | DIACAP Entry-Level Navy Validator | | April 2014 - Present |
| Microsoft | MCP: Windows 7 (70-865) | | April 2014 - Present |
| ISC2 | Certified Information Systems Professional (CISSP) | | June 2015 - Present |
| ISACA | Certified Information Systems Auditor (CISA) | | Oct 2017 - Present |
| Microsoft | MTA (98-389): Introduction to Programming Using Python | | Sept 2018 - Present |
| CompTIA | Linux+ | | Sept 2019 - Present |
| Microsoft | MTA (70-480): Programming in HTML5 with JavaScript & CSS3 | | Sept 2019 - Present |
| Splunk | Splunk Core Certified Power User | | April 2020 - Present |
| Comptia | Cybersecurity Analyst (CySA+) | | Dec 2020 – Dec 2026 |
| Splunk | Splunk Enterprise Certified Admin | | Feb 2022 – Feb 2025 |
| AWS | Certified Cloud Practitioner | | April 2024 – April 2027 |

## Experience

### Cyber Engineer Advisor, General Dynamics Information Technology (Feb 2023 – Present)

* Leads container security integration efforts and advises product teams on implementing security within the SDLC in accordance with NIST 800-160 to meet federal security requirements within the cloud environment.
* Develops and maintains system testing and validation procedures for containers and host systems to support white-box testing and black-box (SAST/DAST) testing tools such as NESSUS (ACAS), Anchore, Twistlock (Prisma Cloud), and SonarQube.
* Conducts vulnerability scanning, patch management, and continuous monitoring using tools like Nessus/ACAS, and McAfee ePO/HBSS, ensuring readiness for VA and federal systems.
* Works as part of the platform security teams to address application security vulnerabilities internal systems and third-party software to enhance the overall security of cloud-based applications.
* Implements security designs to support the server and application of STIGs and other security configuration/automation effort using Bash, Python and PowerShell, reducing manual intervention in patching and security threat detection.
* Manages SIEM agent integrations and creates dashboards to support continuous monitoring and incident response efforts.  
  Performs identity and privilege access management across a variety of tools, (including Keycloak, AWS IAM and Anchore), to support data access and protection requirements.

### Cyber Security Splunk Engineer, Miracle Systems (Jan 2022 – April 2022)

* Managed and performed security monitoring and incident response activities, identifying indicators of compromise and coordinating responses to resolve cyber defense incidents, including data exfiltration and cross-site scripting (XSS) attacks.
* Administered and optimized SIEM (Splunk) for threat intelligence and incident response, driving improvements in SIEM coverage, operational efficiency and refining detection and response processes.
* Developed and implemented security policies and Data Loss Prevention (DLP) mechanisms across cloud environments, leveraging AWS services to enhance security and compliance.
* Led vulnerability management and incident handling efforts to remediate threats, conducting forensic analysis and improving host/endpoint security through proactive monitoring and response.
* Collaborated with DevOps and platform teams to deploy security technologies, executing vulnerability assessments with tools such as ACAS/Nessus and ensuring the alignment of security objectives.
* Served as a primary point of contact for security technology vendors, overseeing vendor relationships and integrating solutions to enhance security monitoring and response capabilities.
* Documented processes and developed developing RMF assessment and authorization artifacts in accordance with NIST SP 800-37.

### Course Creator and Blog Author, Infosec Institute (Mar 2021 – Present)

* Authors technical blogs on NoSQL databases and cybersecurity best practices.
* Develops instructional materials, proficiency assessments and curriculum to communicate complex concepts using learning assessment tools and techniques.
* Recommends revisions to learning materials and curriculum, press outreach, learner engagement and more.

### Sr. Information Security Analyst, General Dynamics (Nov 2020 – Apr 2021)

* Led cybersecurity audits and vulnerability assessments across 20,000+ applications and systems using tools like Nessus(HBSS), Trellix(McAfee), and QRadar.
* Designed and implemented security controls standard operating procedures for secure network system operations to identify possible security violations.
* Acted as the SME for Trellix (formerly McAfee) administrator to implement technical security policies to support DLP (Data Loss Prevention) controls for data-at-rest and data-in-transit.
* Managed incident response and insider threat initiatives by training new CSSP security analysts in cyber incident handling procedures 24/7 NOSC (Network Operation and Security Center) environment.
* Reviewed security designs and DFDs (Data Flow Diagrams) and provided feedback to support accreditation activities aligned with ISO 27001/2, FISMA NIST 800\* series Rev 5 and NIST CSF frameworks.
* Conducted independent comprehensive assessments of management, operational, and technical security controls and to determine identify gaps in security architecture.

### Computer Network Defense (CND) Specialist, Anistar Technologies /C4 Planning Solutions (Jul 2019 – Nov 2020)

* Conducted vulnerability assessments and security audits across DoD environments, ensuring compliance with DISA STIGs and NIST RMF.
* Served as the Subject Matter Expert (SME) for HBSS (McAfee/Trellix), overseeing system administration. incident management processes and compliance strategies.
* Generated custom audit and compliance reports to enhance visibility into network security status
* Performed comprehensive analysis and assessment of vulnerabilities using vulnerability management and penetration testing tools, implementing corrective actions in line with DISA requirements, NIST RMF, NIST SP 800-53, STIGs, SCAP, IAVAs, and JFHQ-DODIN OPORDs/FRAGOs.
* Served as the Subject Matter Expert (SME) for HBSS (McAfee/Trellix) endpoint protection, overseeing system administration and maintenance operations in accordance with organizational compliance strategies.

### Sr. Security Engineer, Vortechx/KeyW Corporation (Oct 2017 – Mar 2019)

* Identified and managed OS and application vulnerabilities using custom security scripts and DoD-approved security tools (ACAS, McAfee/Trellix, QRadar) to mitigate threats to DoD Army Intelligence systems.
* Developed and automated vulnerability remediation efforts across 16 virtual servers (Windows, Linux & Solaris), coordinating patch management and validation activities to support IAVAs, STIG and JFQH-DoDin cyber and operational orders.
* Developed technical documentation and architecture & design papers, including patch installation instructions, and participated in international panels to provide expertise and presentations on cybersecurity matters.
* Identified, documented, and remediated information system vulnerabilities using tools like Nessus, DISA STIGs, DISA STIG Viewer, and SCC (SCAP Compliance Checker), ensuring compliance with DoD security standards.
* Prepared and presented detailed technical security reports to colleagues and senior management, facilitating informed decision-making and reinforcing the organization’s security posture.

### Cyber Information Assurance Analyst, Northrop Grumman (Apr 2015 – Sept 2017)

* Supported the RMF process for IS accreditation to obtain an Authority to Operate (ATO), by conducting system security and vulnerability analyses and risk assessments.
* Selected and implemented applicable security controls within the SSP for the IS, and supported the development, review, and approval of Security Assessment Plans (SAP) to govern the assessment of IS security controls.
* Performed periodic audits of vulnerability and compliance scans of IT systems, using tools like ACAS/NESSUS, Trellix/HBSS, and QRadar), ensuring ongoing compliance and identifying vulnerabilities within the system.
* Acquired and maintained critical RMF-related accounts, including Enterprise Mission Assurance Support Service (eMASS) accounts, to support the accreditation and assessment processes.
* Managed user account access requests and
* Performed data sanitization procedures servers and products to support mission-critical data disposal policies, guidance, and procedures, including device data sanitization to ensure secure removal of sensitive information.
* Conducted risk analysis of intelligence and radar systems, applications and software and recommends risk mitigation strategies.

### IT Specialist, Yoh- A Day & Zimmermann Company (Oct 2014 - Mar 2015)

* Installed, configured, troubleshot, and maintained hardware, software, and administers system accounts.
* Trained end users on the proper use and management of system resources, software applications and data backup & recovery.
* Identified issues and provided maintenance/support for network devices, applications, and peripheral equipment for end users.
* Prepared and inventoried software and hardware documentation in support of proper change management procedures.

### Military Police Officer, United States Navy (May2008 - Nov2011)

* Provided physical protection for U.S. critical infrastructure and cleared service members, and managed access controls for DoD facilities.
* Trained sailors in physical security protocols, including crowd control and riot prevention.
* Conducted preliminary investigations and handled digital evidence to support investigations relating to Uniform Code of Military Justice (UCMJ) violations.
* Designed and assigned user access control mechanisms to provide least privilege to physical facilities (including the generating and issuance of keycards, contractor IDs, passwords and pins).

## Specialty Areas

|  |  |  |  |
| --- | --- | --- | --- |
| * Cyber Defense Analysis | * Incident Response & Incident Management | * Endpoint Security | * Vulnerability Analysis & Management |
| * Risk Management | * Security Education, Training, and Awareness (SETA) | * Systems Security Analysis | * Secure Software Development |
|  |  |  |  |

## Community Contributions

## Publications

* MongoDB (part I): How to design a schemaless, NoSQL database. Published Oct 04, 2022 by Infosec Institute. Article: [Find out how you can use MongoDB to design a schemaless, NoSQL database.](https://resources.infosecinstitute.com/topic/mongodb-part-1-how-to-design-a-schemaless-nosql-database/)
* MongoDB (part II): How to manage data using CRUD operations. Published Oct 06, 2022. Infosec Institute. Article: [Find out how to manage data in a MongoDB database](https://resources.infosecinstitute.com/topic/mongodb-part-2-how-to-manage-data-using-crud-operations/).
* MongoDB (part III): How to secure data. Published Oct 18, 2022 by Infosec Institute. Article: [Learn how to secure data in a MongoDB database.](https://resources.infosecinstitute.com/topic/mongodb-part-3-how-to-secure-data/)

### Boards

### CISSP Exam Developer | (ISC)² 2022 Exam Development Board

* Contributed to the official development and review of CISSP certification exam questions, ensuring alignment with current industry standards and the (ISC)² Common Body of Knowledge (CBK).
* Applied expertise in cybersecurity to create and validate content that reflects real-world security challenges and best practices, helping to maintain the integrity and relevance of the CISSP certification.