Cyber Defense Analyst

Hiring organization
Agile Defense

Job Location
Washington, D.C

Base Salary
$ 62500 - $ 112500

Date posted
June 13, 2024

Apply Now

Description

At Agile Defense we know that action defines the outcome and new challenges require new solutions. Thatâ⍰⍰s why we always look to the future and embrace change with an unmovable spirit and the courage to build for what comes next.Our vision is to bring adaptive innovation to support our nation’s most important missions through the seamless integration of advanced technologies, elite minds, and unparalleled agilityâ⍰⍰leveraging a foundation of speed, flexibility, and ingenuity to strengthen and protect our nationâ⍰⍰s vital interests.Job Title: Cyber Defense Analyst (Junior)Location: Must be local to the Washington D.C., USA. Role is performed remotely, but candidate maybe called onsite as neededClearance Level: Active – Public TrustRequired Certification(s): Â· An industry technical certification such as Security + and aboveSUMMARY: Agile Defense Company is currently seeking a talented and ambitious self-starting, Junior Cyber Defense Analyst for a challenging position supporting one of our premier clients who conducts 24/7 operations to secure their enterprise environment. This is a unique opportunity for the right candidate to embed themselves into the next generation of operational environments which is now taking place across the US government and commercial sectors.The existing team is a multi-faceted interdisciplinary set of experts with ever-increasing prowess in this unique atmosphere. Our security operations project is aimed at establishing innovative techniques for a comprehensive, cloud-first network enclave defense, identifying the emerging threats, and detecting malicious activity using advanced toolsets provided in the Microsoft cloud security ecosystem. The ideal candidate will have hands-on experience as a Cyber Defense analyst performing Incident Response and Intrusion Detection on a large operational network, specifically, utilizing the Microsoft Sentinel SIEM and related security portals. Schedule: Shift Schedule:Â· Shift Schedule: 6:30 PM â⍰⍰ 4:30 AM ET (Sunday â⍰⍰ Wednesday) Â· Shift Schedule: 6:30 PM â⍰⍰ 4:30 AM ET (Wednesday â⍰⍰ Saturday) Â· Shift Schedule: 5 AM â⍰⍰ 3 PM ET (Saturday â⍰⍰ Tuesday) Location:Â· Must be local to the Washington D.C., USA. Role is performed remotely, but candidate maybe called onsite as needed.JOB DUTIES AND RESPONSIBILITIES:Â· The candidate will monitor and analyze network traffic utilizing traditional network security toolsets, sign-ins, application endpoints and data lakes for security events, reporting any findings to Level II analysts and the Cyber Defense Leads. The candidate will perform incident response to investigate and resolve security incidents which present themselves as alarms and those incidents which are a product of proactive sensor strategies and investigations. Â· The candidate will be able to determine between false and true positives events, prioritizing them appropriately and ferrying them through the approved process from beginning to end. Â· Additionally, the candidate will perform, or review, root cause analysis efforts following incident recovery. The candidate will compose security alert notifications and other communications on behalf of the Cyber Fusion Center.Â· In addition, the candidate will remain up to date with current vulnerabilities, attacks, and countermeasures and develop follow-up action plans to resolve reportable issues and communicate with the other technologists to address security threats and incidents. Â· Also, the candidate will continually develop new use cases for automation and tuning of security tools, define and create privacy and security reportable issues metrics and reports. Â· The candidate will need to contribute to security strategy and security posture by identifying security gaps, evaluating and implementing enhancements. Â· The ideal candidate will possess a strong technical understanding of log and monitoring management systems, security event monitoring systems, network-based and host-based intrusion detection systems, security system technologies, malware detection and enterprise-level antivirus solutions/systems, VPN technologies and encryptions standards.QUALIFICATIONS:Required Certifications:Â· An industry technical certification such as Security + and above.Education, Background, and Years of Experience:Â· Bachelor’s degree preferred but not required.ADDITIONAL SKILLS & QUALIFICATIONS:Required Skills:Â· One to two (1-4) years of experience in network defense environmentsÂ· An industry technical certification such as Security + and above.Â· 1 – 3 years of experience with tools such as Active Directory, Azure Active Directory, AD Connect, SAML, Kerberos, Cisco IOS, MS Server, Azure cloud environments, Incident Handling, Threat hunting experience, fundamental knowledge of IEEE 7 layersÂ· Experience with deployment and documentation of enterprise project management and change management processesÂ· Ability to identify solutions to potential network issues/embrace network simplification and strengthened securityÂ· Ability to conduct event triage and analysis and incident investigationÂ· Write threat reports and incident reportsÂ· Read and ingest various govt. regulations for application to agency environmentPreferred Skills:Â· Understanding of command line scripting and implementation (e.g., Python, PowerShell)Â· Ability to write latest content/searches/scripts (e.g., Create dashboards, Sentinel alerts, Python scripts, PowerShell scripts)Â· Familiarity with differences in on-prem OPSEC in relation to cloud-based securityÂ· Strong understanding of networking (TCP Flags, TCP Handshake, IP addressing, Firewalls, Proxy, IDS, IPS)Â· Ability to perform NetFlow / packet capture (PCAP) analysisÂ· Experience with cyber threat huntingWORKING CONDITIONS:Strength Demands:Â· Sedentary â⍰⍰ 10 lbs. Maximum lifting, occasional lift/carry of small articles. Some occasional walking or standing may be required. Jobs are sedentary if walking and standing are required only occasionally, and all other sedentary criteria are met.Physical Requirements:Â· Stand or Sit; Walk; Repetitive Motion; Use Hands / Fingers to Handle or Feel; See nnEmployees of Agile Defense are our number one priority, and the importance we place on our culture here is fundamental. Our culture is alive and evolving, but it always stays true to its roots. Here, you are valued as a family member, and we believe that we can accomplish great things together. Agile Defense has been highly successful in the past few years due to our employees and the culture we create together. What makes us Agile? We call it the 6Hs, the values that define our culture and guide everything we do. Together, these values infuse vibrancy, integrity, and a tireless work ethic into advancing the most important national security and critical civilian missions. It’s how we show up every day. It’s who we are.Happy – Be Infectious.Happiness multiplies and creates a positive and connected environment where motivation and satisfaction have an outsized effect on everything we do.Helpful – Be Supportive.Being helpful is the foundation of teamwork, resulting in a supportive atmosphere where collaboration flourishes, and collective success is celebrated.Honest – Be Trustworthy.Honesty serves as our compass, ensuring transparent communication and ethical conduct, essential to who we are and the complex domains we support.Humble – Be Grounded.Success is not achieved alone, humility ensures a culture of mutual respect, encouraging open communication, and a willingness to learn from one another and take on any task.Hungry – Be Eager.Our hunger for excellence drives an insatiable appetite for innovation and continuous improvement, propelling us forward in the face of new and unprecedented challenges.Hustle – Be Driven.Hustle is reflected in our relentless work ethic, where we are each committed to going above and beyond to advance the mission and achieve success.Equal Opportunity Employer/Protected Veterans/Individuals with DisabilitiesThe contractor will not discharge or in any other manner discriminate against employees or applicants because they have inquired about, discussed, or disclosed their own pay or the pay of another employee or applicant. However, employees who have access to the compensation information of other employees or applicants as a part of their essential job functions cannot disclose the pay of other employees or applicants to individuals who do not otherwise have access to compensation information, unless the disclosure is (a) in response to a formal complaint or charge, (b) in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or (c) consistent with the contractorâ⍰⍰s legal duty to furnish information. 41 CFR 60-1.35(c)Please mention the word **SUPERBLY** and tag RNDQuMjQyLjE3NC4yMDE= when applying to show you read the job post completely (#RNDQuMjQyLjE3NC4yMDE=). This is a beta feature to avoid spam applicants. Companies can search these words to find applicants that read this and see they’re human.

Contacts

Job listing via RemoteOK.com