Senior Detection and Response Engineer

Hiring organization
CoreWeave

Job Location
New York City, New York, United States

Base Salary
$ 60000 - $ 110000

Date posted
June 7, 2024

Apply Now

Description

About the Role: As a Senior Detection and Response Engineer, you will join a 24/7 Security Operations team and play a critical role in safeguarding our organization’s information assets and ensuring the integrity, confidentiality, and availability of our systems and data. You will be responsible for designing, implementing, and maintaining advanced threat detection systems to safeguard our organization’s digital assets against cyber threats. This role requires a proactive mindset, strong analytical skills, and the ability to work collaboratively with cross-functional teams. Key Responsibilities: Write custom detection logic while working with the the Security Operations team Assist in the day-to-day operations of the security operations center (SOC), including monitoring, analysis, and response to security incidents and alerts. Monitor and report the health of all security sensors across CoreWeaveâ??s environment and drive resolution of reported defects. Demonstrate a keen ability to multitask while still making sound decisions in high pressure situations Develop and implement security monitoring and detection strategies to identify and mitigate threats in real-time. Conduct threat hunting activities to proactively identify and address potential security risks and vulnerabilities. Coordinate with internal and external stakeholders to investigate security incidents, conduct root cause analysis, and develop remediation plans. Contribute to security incident response plans and procedures, ensuring timely and effective response to security incidents. Collaborate with cross-functional teams to implement security controls, policies, and procedures to protect against emerging threats and vulnerabilities. Stay on top of the latest security trends, threats, and technologies, and make recommendations for improving our security posture. Participate in security assessments, audits, and compliance initiatives to ensure adherence to regulatory requirements and industry best practices. Required Skills: Ability to deliver small to medium sized projects that span several technical disciplines and teams. Ability to take documented detections misses and leverage available people, technology, processes to deliver effective detections. Strong Experience writing custom alert logic in any major SIEM (eg Splunk, Rapid 7, Sumo Logic, etc.) Intermediate understanding of Kubernetes fundamentals and the willingness and desire to grow their working knowledge of Kubernetes. Experience collaborating as a stakeholder in Purple Team & Red Team engagements. Practical knowledge of modern TTP frameworks. (Cyber Kill Chain, MITRE ATT&CK) Functional knowledge of at least 1 query language. (SQL, Splunk, HiveQL, Humio, FQL) Proficiency in at least 2 programming languages (Ex: Python, Bash, Go, JavaScript) Intermediate knowledge of Linux or macOS internals. Intermediate knowledge of Linux or macOS event sources. (eBPF, Endpoint Security Framework) Hands-on experience applying the Incident Response Lifecycle. Our compensation reflects the cost of labor across several US geographic markets. The base pay for this position ranges from $140,000-$160,000. Pay is based on a number of factors including market location and may vary depending on job-related knowledge, skills, and experience. Hybrid Workplace Successful candidates will be expected to attend onboarding training at our NJ Headquarters within their first several weeks of employment, with subsequent quarterly travel requirements of 1 week duration. If you reside within a 30-mile radius of our New Jersey, New York, or Philadelphia offices, we’re excited for you to join us at the office at least three times a week, recognizing the significance we place on fostering connections, collaboration, and creativity within our office culture. Our commitment to operating as a hybrid workplace underscores our dedication to enabling our employees to tailor their work-life balance to their individual preferences.Please mention the word **RIGHTNESS** and tag RMzQuMTQ1LjE0MS43OA== when applying to show you read the job post completely

(#RMzQuMTQ1LjE0MS43OA==). 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