Principal Security Operations Engineer

Hiring organization
Vimeo

Job Location
New York City, New York, United States

Base Salary
$ 60000 - $ 110000

Date posted
June 6, 2024

Apply Now

Description

As a Principal Security Operations Engineer at Vimeo, you will engage in a variety of activities, either offensive, defensive, or some combination thereof, ultimately aimed at safeguarding our 300+ million users who entrust Vimeo with their content every day. Youâ??ll plan, carry out, and lead security initiatives to monitor and protect sensitive data and systems from infiltration and cyber-attacks. You will likely collaborate frequently with and support developers, as well as members of the infrastructure security team, the compliance team, IT, Product, and other teams throughout the organization. You love to solve puzzles, and are a great team player. This role is remote. What you'll do: Depending on your preferences and the current needs of the team, you may either focus on just some of the following areas, or you may choose to become involved with all of them. As a Principal SecOps Engineer, you will be responsible for ensuring the security of our systems and infrastructure. You will work closely with our development, DevOps teams to identify and remediate vulnerabilities, implement security best practices, and automate security processes. You will also monitor and respond to security incidents and maintain compliance with industry and regulatory standards. Conduct security assessments of our systems and infrastructure to identify vulnerabilities and risks, identify risk owners and implement mitigating controls. Implement and maintain security controls, including access controls, Zero trust network access (ZTNA), network segmentation, and security monitoring tools. Design and operate identity management, lifecycle, governance and SSO. Implement and operate cloud security hardening and cloud security posture management across Google cloud and AWS. Develop and maintain security policies and procedures, and ensure compliance with industry and regulatory standards. Collaborate with SRE, AppSec and Information technology around vulnerability management, endpoint hardening, detection and response. Participate in incident response activities, including investigating security incidents and responding to security alerts. Collaborate with development and DevOps teams to implement security best practices throughout the software development and infrastructure lifecycle. Automate security processes using scripting and other automation tools. Stay up-to-date with the latest security threats, vulnerabilities, and technologies. Collaboration with the compliance and privacy team â?? help ensure that our company complies with industry best practices and standards Process improvements â?? help strengthen our own internal processes and procedures Skills and knowledge you should possess: 6+ years of experience in a security or operations role, preferably in a cloud-based Linux environment. 3+ years experience with container and container orchestration systems Bachelor's degree in Computer Science, Information Technology, or a related field, or equivalent work experience. Strong knowledge of security best practices and industry standards, such as NIST, CIS, and ISO. Relevant certifications such as CISSP, CCSP, or AWS Certified Security Specialty are a plus. Experience with security tools such as IDS/IPS, SIEM, vulnerability scanners, and endpoint protection. Experience with automation tools such as Terraform, Ansible, or Chef. Strong scripting skills using Python, shell, or other scripting languages. Excellent problem-solving skills and the ability to work well under pressure. Good communication and interpersonal skills.Confident working in and across cloud environments like AWS and GCP. Detailed knowledge of at least one cloud environment. Confident with common SDLC components, like git, Jira, Jenkins, etc At least an upper-intermediate level of English Bonus points (nice skills to have, but not needed): Experience implementing zero trust network access such as Z-Scaler, Warp, Google beyondCorp etc. Experience implementing identity lifecycle including provisioning, quarterly access reviews, role management and deprovisioning. Understanding of FIDO2 and machine certificate authentication

flows. Experience with Crowdstrike and OKTA. Experience with system security hardening guidelines and SDLC principles Experience with implementing Fedramp and/or HIPAA. Targeted Base Salary Range: $149,400 to $227,500 The base salary range listed above is for candidates located in the U.S., including the New York City metro area. At Vimeo, we strive to hire and nurture amazing talent across the globe. Actual salaries will vary depending on factors including but not limited to experience, specialized skills, internal alignment and a candidateâ??s home base. Base salary is just one component of Vimeoâ??s total rewards philosophy. We offer a wide range of benefits and perks that appeal to the variety of needs across our diverse employee base! Other rewards may include bonus or commission, Restricted Stock Units (RSUs), paid time off, generous 401k match, wellbeing resources, and more. #LI-MM1Please mention the word **IMPROVES** and tag RMTA3LjE3OC4yMzIuMjQy when applying to show you read the job post completely (#RMTA3LjE3OC4yMzIuMjQy). 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