Senior Security Incident Response Engineer

Indeed
United States
Remote
$136,000 - $190,000 a year - Full-time

Indeed ›
1,063 reviews
Read what people are saying about working here.

Apply now

Job Company

Resume Insights

Here's how your resume aligns with the job description

Experience & Skills

✓ AWS ✓ HTML5 ✓ Encryption

+ show more

Job details

Salary
$136,000 - $190,000 a year

Encouraged to Apply

Fair chance

Job Type

Full-time
Remote

Benefits

Pulled from the full job description

Paid time off **RSU** **Unlimited paid time off**

Full Job Description

Your Job

As a member of the security team, you will present your technical expertise balanced with common sense. While you will always encourage your team, your customers and Indeed's clients to do "the right thing" based on data from the tools and processes you build that support the established policies and standards, you recognize that issues, risks and solutions are colored in shades of grey.

Your team provides just a part of security to the enterprise and depends on tight coordination and constant communication with other parts of the security organization and, most often, with other parts of Indeed.

A Security Engineer is a life-long learner. You may be an expert in one domain, but always seeking clarity in others. You tinker at home in security domains that may have nothing to do with your role, but you share that expertise with your team and your customers.

Responsibilities

- Lead cross-functional teams and time zones to identify and mitigate or facilitate the mitigation of security issues in Indeed's systems and processes
- Apply documented methodology to ensure a consistent response to security incidents to minimize business impact
- Perform and set standards for triage of incoming issues using ticket tracking system.
- Perform analysis of complex transactional data, log files and/or other system outputs to identify malicious or anomalous activity
- Evaluate, architect, build, monitor and support security infrastructure for use by security and others at home, in an office, in a data center and in cloud environments beyond AWS, GCP and Azure
- Act as a point of escalation for investigation of systems and security events monitored by your team
- Provide tuning and reporting recommendations of security tools
- Own, produce and review team metrics in support of security goals
- As a subject matter expert, curate Indeed's knowledge through documentation, procedures, playbooks, runbooks, awareness content, and/or other inter- and intra-team activities
- Predict trends in the information security community including new vulnerabilities, methodologies, and products
- Organize incident responses and participate in on-call rotation as necessary.

- Identify gaps in sensors/platforms/appliances and direct building content for the SIEM to provide actionable contextual data to improve visibility and detection of anomalous events
- Review and select proven and mature framework (Security Controls Framework, CIS20, MITRE ATT&CK & OWASP, CVSS, etc.), methodologies and practices in delivering work products
- Select and deliver updates in Security group meetings routinely
- Select and deliver tech talks to other Indeed groups
- Identify content for Security awareness campaigns
- Lead high severity or complex initiatives that may involve external partners
- Work with several internal teams to identify, resolve, and mitigate security issues
- Lead regular reviews of policies, standards, plans and procedures
- Prepare and deliver internal conference talks, blog posts
- Mentor team members
- Lead technical implementation of one or more projects to achieve team OKRs

Who You Are

Requirements

- Ability to explain Information Security concepts such as defense in depth to non-security practitioners
- At least five (5) years of experience in Information Security
- Expert level knowledge in at least three (3) incident management tools such as SIEM, Log/Packet analysis, IDS/IPS, Netflow analyzers, EDR, vulnerability scanners, web proxies, etc.
- Passion for incident response, cloud, devops and information security
- Experience with at least five (5) security domains such as Incident Response, Application Security, Infrastructure Security, Detection Engineering, Network Security, Cloud Security, Compliance, Governance, Cryptography, IAM, Privacy, Vulnerability Management, Risk Management, Deception technologies, Threat Intelligence or Red Teams
- Experience reading or writing script, regex or code in common languages, such as C#, Go, Java, Python, HTML, or Javascript
- Ability to turn knowledge and experience into effective change inside an organization
- Quickly adapt to changing events and efforts and realigns resources as needed
- Experience with exerting soft skills within daily tasks and exchanges internally and externally

Who we are

We are builders, we are integrators. We create and optimize solutions for a rapidly growing business on a global scale. We work with distributed infrastructure, petabytes of data, and billions of transactions with no limitations on your creativity.

Our Mission

As the world’s number 1 job site*, our mission is to help people get jobs. We strive to cultivate an inclusive and accessible workplace where all people feel comfortable being themselves. We're looking to grow our teams with more people who share our enthusiasm for innovation and creating the best experience for job seekers.

(*comScore Total Visits, September 2021)

Salary Range Disclaimer

The base salary range represents the low and high end of the Indeed salary range for this position. Actual salaries will vary depending on factors including but not limited to location, experience, and performance. The range listed is just one component of Indeed's total compensation package for employees. Other rewards may include quarterly bonuses, Restricted Stock Units (RSUs), an open Paid Time Off policy, and many region-specific benefits.

Salary Range Transparency

US Remote 136,000 - 190,000 USD per year

Austin 136,000 - 190,000 USD per year

Seattle 166,000 - 232,000 USD per year

Equal Opportunities and Accommodations Statement

Indeed is a proud equal opportunity employer. We are deeply committed to building a workplace and global community where inclusion is not only valued, but prioritized. We are committed to creating an environment where all employees feel included and have a strong sense of belonging. All qualified applicants will be considered for employment without regard to race, color, religion, gender, gender identity or expression, family/marital status, refugee or immigration status, sexual orientation, national origin, genetics, neuro-diversity, disability, age, veteran status, or any other non-merit based or legally protected grounds.

We encourage people from all backgrounds to apply and join us in our mission of helping people get jobs.Indeed is committed to providing reasonable accommodations to qualified individuals with disabilities in the employment application process. To request an accommodation, please contact Talent Attraction Help at 1-855-567-7767, or by email at TAhelp@indeed.com at least one week in advance of your interview.

Fair Chance Hiring

We value diverse experiences, including those who have had prior contact with the criminal legal system. We are committed to providing individuals with criminal records, including formerly incarcerated individuals and individuals with arrest or conviction records, a fair chance at employment. We also comply with state and local requirements such as the San Francisco Fair Chance Ordinance.

Our Policies and Benefits

View Indeed's Applicant Privacy and Accessibility Policies - https://www.indeed.com/legal/indeed-jobs
Learn about our global employee perks, programs and benefits - https://benefits.indeed.jobs/

Where legally permitted, Indeed requires all individuals attending or working out of Indeed offices or visiting Indeed clients to be fully vaccinated against COVID-19. For positions that can only be performed at an Indeed office, candidates must be fully vaccinated against COVID-19 and present acceptable proof of vaccination by the date of hire as a condition of employment. For positions that require some in-office work or in-person client meetings, exceptions to these in-office or in-person job requirements may be made at the discretion of the business through June 2022, at which point full vaccination will be required. Indeed will consider requests for reasonable accommodation as required under applicable law. To qualify as being fully vaccinated against COVID-19 there should have been a two week period after receiving the second dose (or any government recommended booster shot) in a 2-dose COVID-19 vaccine series, or a two week period after receiving a single-dose (or any government recommended booster shot) in a single dose COVID-19 vaccine.

Reference ID: 41289

Hiring Insights

Job activity

Posted 30+ days ago

Indeed
30+ days ago
original job

Report job

Security Engineer jobs in United States

Jobs at Indeed in United States

Security Engineer salaries in United States