Identify 3 software or technology companies the interest you.

**Facebook:**

Data Center Production Operations Engineer:

* Perform deep dives and analyze complex technical issues within the data center, ranging from automated tooling to hardware failures and network issues.
* Work as a technical lead with cross functional teams on large scale data center projects and initiatives.
* Provide cross data center support and identify potentially larger issues, displaying effective communication when something is identified.
* Work with internal hardware teams and vendors to help resolve complex technical issues, maintain high hardware quality levels and influence future design to ensure ease of serviceability.
* Understand/analyze issues and be able to update and develop scripts and smaller sets of software.
* Use data to drive maximum server fleet up-time and utilization rates, by understanding hardware failure rates and SLAs to customers. Identify trends and systemic issues in the fleet and drive resolution.
* Graphical user interface, application

  Description automatically generatedMentor team members to evaluate and identify better ways to resolve issues and define updates to tools and processes.
* Provide guidance and mentor technical leads and the go-to technical resource for management.
* Build cross functional relationships and have the ability to influence policies and procedures to improve global data center operations.
* Participate in an on-call rotation.

* BS, BA or BEng in technical field or commensurate experience.
* 5+ years of infrastructure or related experience.
* Knowledge of Linux and hardware systems support in an Internet operations environment.
* Knowledge of the interdependencies of data center functions and technologies.
* Experience managing multiple projects within the same time schedule.
* Knowledge of enterprise level networking and storage equipment installs.
* Knowledge of out-of-band/lights-out server communication methods, such as IPMI and serial console.
* Time and project management experience.
* Experience in modifying and developing in commonly used scripting or programming languages.
* Proven communication skills.

Facebook is primarily built on the three cornerstones of the World-Wide Web which every Programmer should know, which are:

HTML: HyperText Markup Language. Used for developing rich client side webpages using semantic markup elements that is interpreted by the browser. References: HTML.

CSS: The Cascading Style Sheets. Used for defining HTML semantic elements and markup by implementing rules called cascades, which is a determinant factor in the visual effects of a webpage. References: CSS.

JavaScript: is a dynamic programming language, formerly implemented as ECMAScript, is used to implement certain functionalities unavailable in HTML, such as geographical features and cookie sessions. Facebook uses JSON (JavaScript Object Notation) and AJAX (Asynchronous JavaScript and XML) too, References: JavaScript Language (http://en.wikipedia.org/wiki/javascript).

In Summary Facebook’s visuals is determined by the above client-side technologies.

SentinelOne:

Graphical user interface, application, Teams

Description automatically generatedSt. Cloud Security Engineer (remote):

**Responsibilities:**

* Assist in the design and implementation of cloud security architectures for all of SentinelOne’s cloud services and offerings.
* Assist in driving cloud security solution designs for the security architecture framework (e.g., credential management, access provisioning, authentication and authorization, data security, network security, application security, infrastructure security, security monitoring, and operations security).
* Assist in the design and development of general security patterns and guidelines to enable applications to stay compliant - assist in incentivization and integration of the shift-left paradigm by championing IaC with various teams.
* Assist in the design of security controls that reduce risk and allow for risk-based reporting on SentinelOne’s cloud security posture.
* Summarizes cloud security risks to both technical and non-technical audiences to ensure the appropriate solutions and recommendations are identified.
* Be a Security Champion throughout the organization by utilizing incentivization strategies to gain compliance.
* Be a team player and help elevate everyone on the team to understand initiatives and invite peer-reviews.

**Preferred Qualifications:**

* 3+ years of working with one of the 3 main cloud providers in a deeply technical capacity.
* Strong familiarity with Compute, IAM, KMS, VPC and other core cloud concepts.
* Experience designing cloud networks that are highly scalable, highly available over many regions using VPCs, Gateways, Peering and VPNs.
* Proven experience and desire to operate as a self-starter and be comfortable working in a sometimes ambiguous, yet fast-paced, environment.
* Strong technical understanding to be able to validate that an environment meets all security and compliance controls.
* Experience with GRC and Audits - SOC2, SOX and others where you are providing evidence and creating diagrams for auditors and assisting in the GRC process.
* Have experience with SOA Architecture, Application Security Firewalls, XML Firewalls, and IDS technologies.
* Some exposure to containers and microservices such as Docker, Kubernetes and Lambdas.
* Some exposure to SCA tooling (Veracode, Checkmarx) etc.
* Some exposure to IaC (Terraform, Ansible, Pulumi).
* Some high-level exposure to GCP.
* Nice to have: AWS Certified Solutions Architect, AWS Security Specialty,  Azure AZ-500, GCP Profession Cloud Security Engineer, CISSP.
* Bonus: FedRamp experience, CNCF CKA, CNCF CKS.

Google:

Graphical user interface, application

Description automatically generatedSecurity Engineer, Detection:

Minimum qualifications:

* Bachelor's degree or equivalent practical experience.
* Experience analyzing the security of systems (penetration testing, Web Application security testing, vulnerability scanning, threat modeling, etc).
* Experience coding/scripting in one or more general purpose languages including but not limited to: Java, C/C++, C#, Objective C, Python, JavaScript and/or Go.

Preferred qualifications:

* 3 years of relevant work experience, including experience in responding to security problems in target-rich environments, looking at security alerts, front-line analysis and response.
* Expertise with malware analysis, including investigations of botnet and root-kit behavior.
* Expertise in leading the analysis of large data sets and intrusion detection systems.
* Expertise with signals development, threat hunting and threat modeling.