AWS Security Engineer

You will research the latest threats & methods for deploying infrastructure controls in the prevention, detection and reaction to best securing the environment and automate threat identification and defense capabilities.
Your mission will be to ensure that the environment and customer content remain secure.
You will work across many teams including infrastructure, engineering, operations and product development.
You will work across multiple work streams including infrastructure security, security operations, and incident response.
In this role, you will design and develop for the cloud AWS based Infrastructure controls to support the team and platform consumers utilize.

Requirements

- 3+ years of experience working and securing AWS and its services such as EC2, Lambda, ELB, ECS, IAM, S3, RDS, CloudTrail, CloudFront, AWS Config, etc.
- Experience in security automation and tool development to secure the cloud
- Experience and knowledge of building security data analysis pipelines in the cloud using AWS Kinesis Firehose/AWS Lambda/AWS ElasticSearch
- Extensive experience in security operations and threat detection in the cloud before they cause material damage to the business. In the event an alert is identified as a security incident, you will kick off Incident Response.
- Extensive experience in incident response in the cloud. Incident response includes but are not limited to log analysis, memory and disk forensics, reverse engineering, network containment, threat eradication and postmortems. You will also develop and refine processes, plans and procedures and partner closely with other stakeholders across the business.
- Experience in developing infrastructure-as-a-code using AWS CloudFormation, AWS CodePipeline, AWS CodeBuild, GitHub.
- Experience in working with various AWS logs such VPC Flowlog, CloudTrail, S3, Route53, Elb, CloudFront, WAF, etc.
- Experience in one or more programming languages (Python, Rubby, Node.js, Go, Elixir) and shell scripting
- Experience in patch management and vulnerability scanning in the cloud.

Responsibilities:

- Create an effective set of controls for all of our AWS infrastructure.
- Security operations: Analyze the threats detected by the threat intelligence system and tools in the cloud before they cause material damage to the business. In the event an alert is identified as a security incident, you will kick off Incident Response.
- Cloud Security incidents: provide technical and security expertise throughout the incident; then, implement any improvements assigned to Cloud Security. Incident response process includes log analysis, memory and disk forensics, reverse

engineering, network containment, threat eradication and postmortems.

- Develop security tools and automate existing workflows to improve cloud security.
- Always be identifying newer and more secure ways to access and protect assets.
- Work closely with engineering teams while developing your controls; then, socialize them.
- Be able to measure and prove the effectiveness of your control to auditors as needed.
- Develop and update relevant documentation, including specifications and diagrams.
- • Provide architecture assurance on Cloud Security initiatives and compliance of existing security standards interfacing with infrastructure and development teams.