Are You Using the Three Pillars of AWS Security?

According to one survey,[1] **96 percent** of decision makers have cloud initiatives underway. If you're one of them, check out these simple steps to a more secure AWS environment.

PROTECT YOUR SECRETS

- All changes to infrastructure are made through a build pipeline. No humans should create EC2 instances or other infrastructure.
- Use IAM policies wisely (least privilege). Use IAM for people and for services.
- Don't expose S3 buckets to the public Internet. Use CloudFront or services to front your S3 buckets.

PROTECT YOUR NETWORKS

- Use CloudWatch and VPC Flow Logs to keep an eye on network traffic in your VPC.
- Use Network Ingress Controls, ACLs, and Security Groups to control who can connect to your VPC.
- Use Network Egress Controls, such as routing tables for private subnets and NAT gateways to control which EC2 instances can access the Internet.

KNOW WHAT'S HAPPENING IN YOUR ENVIRONMENT

- Get familiar with AWS logging capabilities: CloudTrail, CloudWatch, and VPC Flow Logs.
- Use a centralized log management solution:
  1. EC2, VPC Flow Logs, and CloudTrail logs are sent to CloudWatch
  2. A custom Lambda function loads data from CloudWatch into ElasticSearch Service.
  3. ElasticSearch Service provides searching and analysis functions for the log data
  4. The analysis is served through a Kibana dashboard client, with a set of proxy servers in front of ES for basic authentication.

HackerOne is trusted by over 1,300 organizations for improving their application security posture. Partnering with us will mean you can implement proven, best-in-class application security testing now.

Contact us today to learn more about partnering with HackerOne to improve your application security.
hackerone.com/contact

hackerone

1. https://www.channelpartnersonline.com/blog/cloud-migration-2-trends-to-watch-in-2018