
8K Miles
Idols Solutions Inc

About the Client

Idols, Inc. is a provider of state of art solutions and services in the design and development of software systems using latest Technologies. They have an expertise in delivering cutting edge solutions which enable clients to realize their strategic enterprise information objectives in a record time. They are mainly focused in improving the productivity of Client Business by building, re-engineering, enhancing and supporting enterprise applications.

Challenges

For Idols, Inc., compliance and data protection in the cloud have been a major challenge due to the shared responsibility model and automation of public cloud infrastructure. Other major challenge is to continuously monitor the infrastructure for any compliance deviation manually. They had to invest on time and manpower to ensure compliance. Hence to ensure consistent compliance controls across their infrastructure, they required new and automated methodologies.

The following are some of the key areas where client required continuous compliance.

- Ensure all the AWS resources are tagged according to the organization's naming standards.
- Ensure all AWS users have passwords matching the Organization's password policy.
- Log all the user actions in the AWS account.
- Ensure all the instances in the AWS account are launched using the approved AMIs and instance types.
- Identify all the unattached AWS resource such as Volumes, Elastic IPs, etc.
- Enabling Multi Factor Authentication (MFA) for the users.
- Ensure all the instances are launched inside a VPC.
- Ensure CIS hardening is maintained always across all the EC2 instances.
- Restricting public access to S3 buckets in the AWS account.
- Ensure SSH traffic are allowed only from the known IP addresses.
- Identify all the DB instances without backup and maintenance windows.

Our Solution

After doing a deep analysis on client's compliance requirements, 8KMiles suggested the usage of AWS Config and AWS OpsWorks to ensure continuous compliance and Center for Internet Security (CIS) benchmark are maintained across the client infrastructure.

AWS Config provides a detailed view of the resources associated with the AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.

AWS OpsWorks for Chef Automate provides a fully managed Chef server and suite of automation tools to automate testing for compliance and security and a user interface to give visibility into the nodes. The Chef server gives a full stack automation by handling operational tasks such as software and operating system configurations, package installations, database setups, and more.

8KMiles helped Idols, Inc to reduce the investment on time and manpower to ensure continuous compliance by configuring AWS Config rules and AWS OpsWorks for Chef Automate. Following are the config rules that ensures continuous compliance in the environment

- **Untagged EC2 resources** – Checks whether the resources have at least one tag attached to it.
- **IAM password policy enabled** – Checks whether the account password policy for IAM users meets the specified requirements
- **Cloud Trail enabled** – Checks whether AWS CloudTrail is enabled in the AWS account
- **Approved AMIs by Ids** – Checks whether running instances are using specified AMIs
- **Unattached Volumes** – Checks whether EBS volumes are attached to EC2 instances
- **Unattached EIPs** – Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.
- **Unattached ENIs** – Checks whether all ENIs created within the VPC are attached to EC2 instances.
- **MFA for IAM Users** – Checks whether the IAM users in the AWS account requires multi-factor authentication for console sign-in.
- **EC2 instances within a VPC** – Checks whether the EC2 instances belong to a virtual private cloud (VPC).
- **S3 Bucket Public Read/Write restricted** – Checks that all the S3 buckets in the AWS account do not allow public read/write access.
- **Disallow unrestricted incoming SSH traffic** – Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.
- **DB instance Backup enabled** – Checks whether RDS DB instances have backups enabled.
- **Instances launched with approved Instance types** – Checks whether all the EC2 instances in the AWS account are of the approved instance types.
- **IAM User Policy Check** – Checks that none of the IAM users have policies attached.

Results & Benefits

Continuous Monitoring: With AWS Config Idols, Inc could continuously monitor and record configuration changes of their AWS resources over a given period of time.

Continuous Assessment: AWS Config allowed Idols, Inc to achieve continuous auditing and assessment of overall compliance of their AWS resource configurations with the organization policies and guidelines.