Case Study

Native-Security Controls Enablement in AWS

Customer: Fox Rent-A-Car

Objective: Increase Security for Rapidly Growing AWS Environment

Solution: Implement Lightstream Phase I AWS Native-Security Control Solution Set

Services: Security Planning, Architecture and Design, Automation and Implementation

Industry: Transportation

Business Challenge

Fox Rent-A-Car is a benchmark for low-cost leisure car rental in the United States and around the world. With a diverse fleet of 20,000 vehicles, the company offers its consumers an attractive and fun selection of foreign and domestic vehicles.

Fox Rent-A-Car's application portfolio runs on AWS. It consumes several different services within the platform and continues to scale with higher demands each day. Recently acquired by Europcar Mobility Group, the parent company wished to ensure that the rapid expansion of Fox Rent-A-Car's AWS environment would not result in security vulnerabilities. To address these concerns, Lightstream recommended implementation of its Phase I AWS native-security control solution set that aligns with the Security Perspective of the AWS Cloud Adoption Framework (CAF).

Solution

The AWF CAF Security Perspective organizes four principles that help drive the transformation of an organization's security culture. These include:

- Directive controls that establish the governance, risk and compliance models that the environment will operate within.
- Preventative controls that protect workloads and mitigate threats and vulnerabilities.
- Detective controls that provide full visibility and transparency over the operation of deployments in AWS.
- Responsive controls that drive remediation of potential deviation from security baselines.

To achieve this, Lightstream put Fox Rent-A-Car's AWS environment through a 30-day Palo Alto Prisma Cloud Redlock security assessment to uncover potential security gaps. The team then aligned those findings to directives within the AWS CAF Security Perspective and recommended Lightstream's phase I native-security solutions for each area.

Directive Component

The Directive component of the AWS Security Perspective provides guidance on planning an organization's security approach as it migrates to AWS. This includes establishing an industry-standard control framework for expected security levels.

To support this component, Lightstream enabled and configured Amazon GuardDuty to continually monitor for malicious activity and unauthorized behavior on Fox-Rent-A-Car's AWS account and workloads. Services and features implemented include:

- **Created Service-Linked Role permissions**
- **Created CFN StackSet Admin role with service role in each sub-account**
- **GuardDuty configured and enabled**
- **Created S3 bucket**
- **Created trusted IP list and activate**
- **Adjusted CloudWatch frequency to 15 minutes**
- **Deployed GuardDuty CloudFormation StackSet, adding sub-accounts ID**
- **Created CloudWatch Events rule and target, subscribed Admin Email DL to SN topic - GuardDuty announcements**

Amazon GuardDuty helps address data from VPC flow logs, CloudTrail event logs and DNS logs to support automatic network and account monitoring at scale.

Preventative Component

The Preventative component of the AWS Security Perspective provides guidance for implementing security infrastructure with AWS and within an organization. This component includes identity and access for the sources of authentication and authorization to reduce human access to production systems and data.

To support this component, Lightstream enabled AWS Single Sign-On service to allow for a single entry point to all current and future AWS accounts. The enablement of this service allowed Fox-Rent-A-Car to centralize its users and implement fine-grained access controls through the use of custom policies and permission sets. Services and features implemented include:

- **AWS Single Sign-On (SSO user database)**
- **Multi-factor authentication (MFA) - SSO solution and Root user**
- **IAM password policy**
- **Custom sign-in URL**
- **Permission sets - based on defined roles and responsibilities**
- **Custom IAM policies**
- **Local user deletion**
- **SSO users created and assigned appropriate permission set andaccount(s)**

AWS SSO helps ensure better security by connecting all AWS accounts to a single source of truth (SSOT) where users are centrally administered and managed. This provides administrators clean access to AWS accounts.

Detective Component

The Detective component of the AWS CAF Security Perspective provides guidance for gaining visibility into an organization's security posture. This component includes logging and monitoring to provide greater visibility near to real time for occurrences in the AWS environment.

To support this component, Lightstream enabled and configured CloudTrail with trails logs sending all log data to S3 to gain visibility into API log data. CloudTrail Insights was enabled to raise, store and trigger events based on abnormal activities. Amazon Macie was also enabled and configured to continuously monitor and alert on S3 buckets for ongoing sensitive data being accessed and/or moved. Services and features implemented include:

- **CloudTrail and CloudTrail Insights enabled and configured with multiple S3 bucket targets**
- **S3 buckets configured with least privileged access bucket policies**
- **Amazon Macie enabled and configured**

AWS Cloudtrail tracks user activity and API usage. It provides an events history of AWS account activity. CloudTrail Insights detects unusual activities in these logs. Together, they ensure governance, compliance and operational risk auditing of AWS accounts.

Amazon Macie uses machine learning to automatically discover, classify and protect sensitive data in AWS. This makes it easy for security administrators to have management visibility into data storage environments.

Responsive Component

The Responsive component of the AWS CAF Security Perspective provides guidance for the responsive portion of an organization's security posture by preparing and simulating actions that require response to prepare organizations to respond to incidents as they occur. Automation plays a large role in the component.

To support this, Lightstream configured and enabled AWS Config, Config rules and an aggregator to support a single-pane-of-glass dashboard for all accounts.

The config rules are backed by Lambda functions that push SNS notifications to specific DL's and self-healing remediation when compliance issues arise. Services and features implemented include:

- **Config and Config Aggregator enabled and configured**
- **Config rules enabled and configured - CloudWatch events, Lambda functions (custom based on rule) and SNS topics**
- **Config rules implemented include:**
    - **IAM-no-policy-no-statement-with-admin-access**
    - **IAM-password-policy**
    - **IAM-root-access-key-check**
    - **MFA-enabled-for-IAM-console-access**
    - **Root-account-MFA-enabled**
    - **VPC-flow-logs-enabled**
    - **VPC-default-security-group-closed**
    - **CloudTrail enabled**
    - **Amazon S3 public read and write (removing public access)**
    - **Insecure security group rules (any SG w/0.0.0.0./0 remove rule)**

AWS Config is a service that enables organizations to assess, audit and evaluate the configurations of their AWS resources. Config continuously monitors and records AWS resource configurations against desired configurations.

Business Outcomes

The Palo Alto Prisma Cloud Redlock security assessment provided visibility on security gaps that Lightstream could then address through AWS native-security controls aligned with best practices from the AWS CAF Security Perspective.

This phase I approach puts Fox-Rent-A-Car on a path to transforming its security culture in order to better support secure, stable and efficient systems. Automation will keep the Fox-Rent-A-Car's security team focused on root cause analysis and forensics versus response, and administrators will have better visibility and control..

The company will experience dramatically better security and scalable workloads that will support future business growth.

Why Lightstream

As an AWS Advanced Consulting Partner, Lightstream helps organizations address, design and manage AWS cloud migration and security plans. Our team of experts provide a full portfolio of services ranging from AWS Analytics to AWS Cloud Optimization and Containment Services, AWS Consolidated Billing Services, AWS Chatbot Services, AWS Direct Connect and AWS CloudFront.

Contact Us At
877) 95-LIGHT

208 N 2100 W #200
Salt Lake City, UT 84116

"Lightstream helped us create a security-first motion with their phase I approach and corresponding AWS native-security controls solution sets."

Kevin Golchin, vice president of IT operations, Fox-Rent-A-Car