SOCi, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, Processing Integrity, and Confidentiality categories for the period of April 1, 2022, through March 31, 2023.

KirkpatrickPrice

KirkpatrickPrice.   innovation. integrity. delivered.

TABLE OF CONTENTS

ASSERTION OF SOCI, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within SOCi, Inc.'s social media marketing and management services system (system) throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that SOCi, Inc.'s service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that SOCi, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). SOCi, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that SOCi, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

Afif Khoury
Chief Executive Officer
SOCi, Inc.
225 Broadway #600
San Diego, CA 92101

Scope

We have examined SOCi, Inc.'s accompanying assertion titled "Assertion of SOCi, Inc. Management" (assertion) that the controls within SOCi, Inc.'s social media marketing and management services system (system) were effective throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that SOCi, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

SOCi, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that SOCi, Inc.'s service commitments and system requirements were achieved. SOCi, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, SOCi, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:
- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve SOCi, Inc.'s service commitments and system requirements based on the applicable trust services criteria

KirkpatrickPrice

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve SOCi, Inc.'s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Inherent Limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion
In our opinion, management's assertion that the controls within SOCi, Inc.'s social media marketing and management services system were effective throughout the period April 1, 2022, to March 31, 2023, to provide reasonable assurance that SOCi, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

July 3, 2023

SOCI, INC.'S DESCRIPTION OF ITS SOCIAL MEDIA MARKETING AND MANAGEMENT SERVICES SYSTEM

Services Provided

Headquartered in San Diego, California, SOCi, Inc. (SOCi) is a marketing platform built to address the complex workflow and management needs of multi-location businesses. The platform includes several different modules that are available to customers depending on the services the customer selects. The company also provides professional services for customers who want SOCi to manage their online marketing on their behalf, including creating content and posts and replying to comments and messages. SOCi provides a marketing platform that addresses the needs involved in all stages of a successful localized marketing program. With a dual focus on protecting the brand while scaling efforts across local pages, SOCi has developed several marketing tools to help brands reach, engage, and grow their online social communities from corporate to the local business level.

Service Delivery Process

During customer onboarding, sales representatives engage customers and conduct demonstrations of the SOCi suite of tools. Customers sign contracts and staff follow a playbook to complete onboarding. Tickets are created in Freshdesk to initiate the technical requirements for the new customer. The onboarding team walks the new customer through the onboarding process by creating an account to their instance, which generates an email to the customer to create a password. The customer who has the first ID for their company can then create accounts for additional staff within the company as needed. The onboarding team helps customers set up their environment, import each of their locations where applicable, and delegate access to other staff, franchisees, and regional teams. Onboarding also includes training the customer on how to manage their own configurations thereafter.

SOCi provides a central command console through which customers can add their social media accounts, such as Facebook, LinkedIn, Yelp, Google Reviews, and Instagram, and manage them from one command center. Customers can import location information of all of their unique locations into SOCi to ensure they can be delegated appropriately. The platform allows large organizations with many locations to delegate social media responsibilities to local staff based on different criteria, such as region or city, state, or ownership. Franchises are delegated responsibilities over the locations they manage. The platform can also allow the customer headquarters to post content and enable customization using variables. Customers can post content to one or more of their social media pages by posting once in SOCi; schedule posts to their social media pages; create content libraries and create a campaign of social media posts weeks or months in advance to automatically publish on dates chosen by the customer; reply to comments or messages on one or more of their social media pages; and choose the SOCi services group to manage media services on behalf of the client for additional fees. When a customer responds to a social media user, the SOCi tool auto-fills the name of the person with an optional greeting.

The customers gain insights into reviews and comments and can choose to respond to comments or reviews made by social media users depending on the content and the positive, neutral, or negative sentiment as determined by the tool. The tool includes a workflow that can require approvals by a manager or multiple levels of approvals by local management or central corporate management. The reporting module shows customers the number of fans and followers for the different social media services, and the reporting module can identify days that a customer gained or lost a high number of followers so that they can investigate the matter. The reporting module can show post impressions for paid posts and organic posts as well as the number of engaged users.

Most customers have annual contracts and have the option of not renewing SOCi services after a year; however, some customers maintain contracts for shorter periods. Prior to the end of the contract, the Customer Success Team contacts clients to renew. For those customers that decline to renew, a ticket is generated in Freshdesk that initiates the offboarding process. Customer success onboarding, and support teams remove all users and locations.
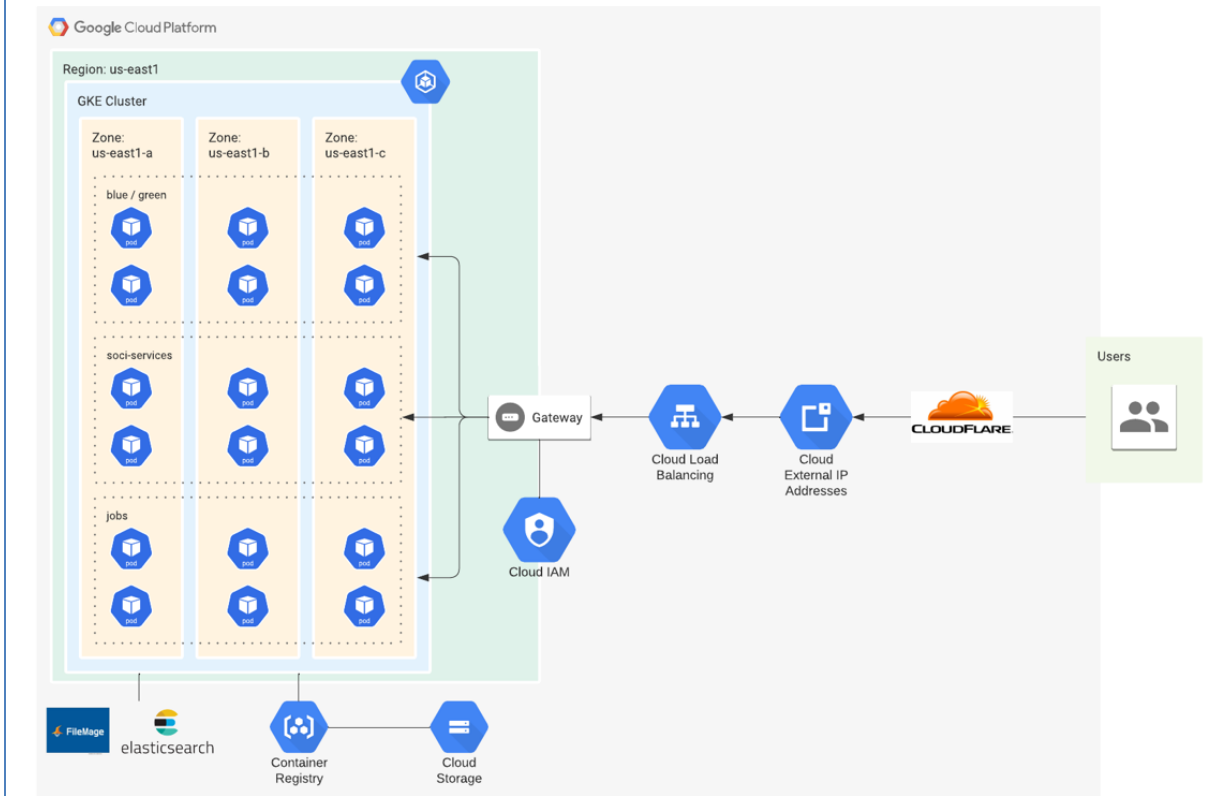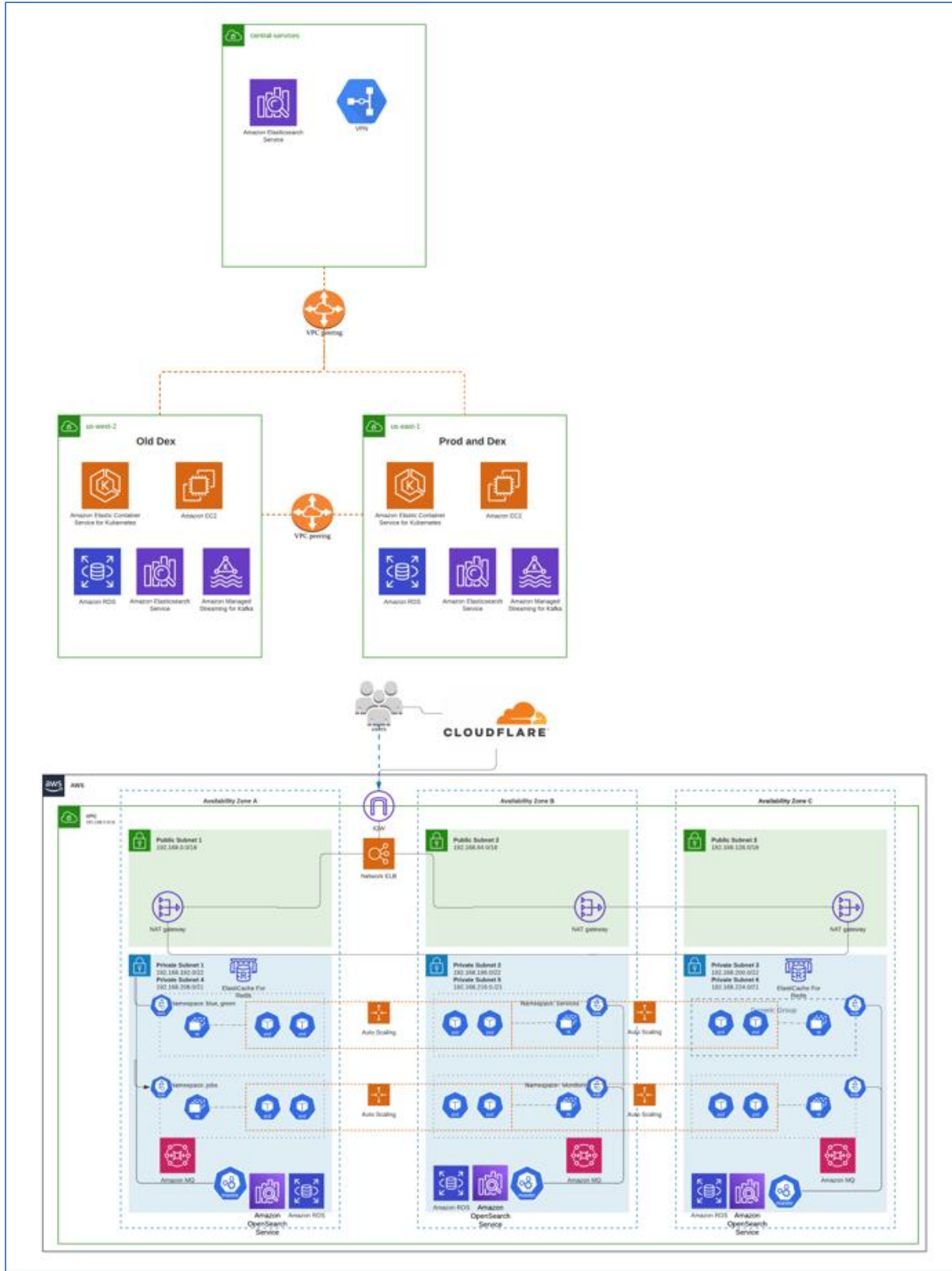
Infrastructure

The organization maintains a network diagram, shown below, to illustrate the topography of its networks.
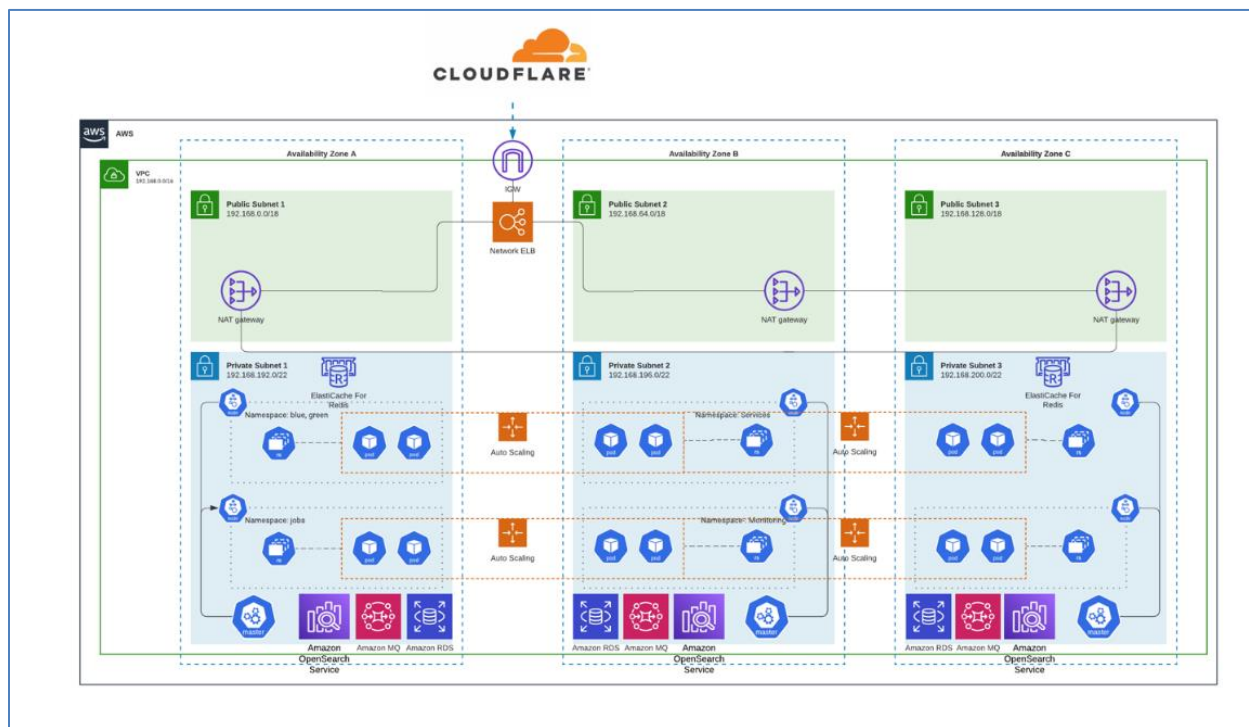
In addition to network diagrams, the organization maintains a system inventory that captures the name, type, vendor, function, OS, and location of all systems in the environment. This inventory includes laptops from the following vendors:

- Apple
- Dell
- HP
- Latitude
- Lenovo
- Surface
- ThinkPad
- Windows
- XPS

Software

The organization maintains an inventory of the critical software it uses. This inventory lists the following:

- Argo CD
- AWS Kubernetes Autoscaler
- AWS Load Balancer Controller
- AWS Node Termination Handler
- ChartMuseum (for Helm)
- Cloudflare
- Docker Registry
- ElastiCache Redis
- Elasticsearch
- Gates
- GitHub
- Grafana
- Jenkins
- Jira
- KEDA
- Logstash
- Loki
- MySQL
- Nginx
- Prometheus
- Promtail
- RabbitMQ
- SonarQube
- Sorry Cypress
- Traefik
- VictoriaMetrics

People

The organization maintains a traditional hierarchy led by the Chief Executive Officer (CEO). This structure and associated reporting lines are illustrated in the organizational chart shown below.
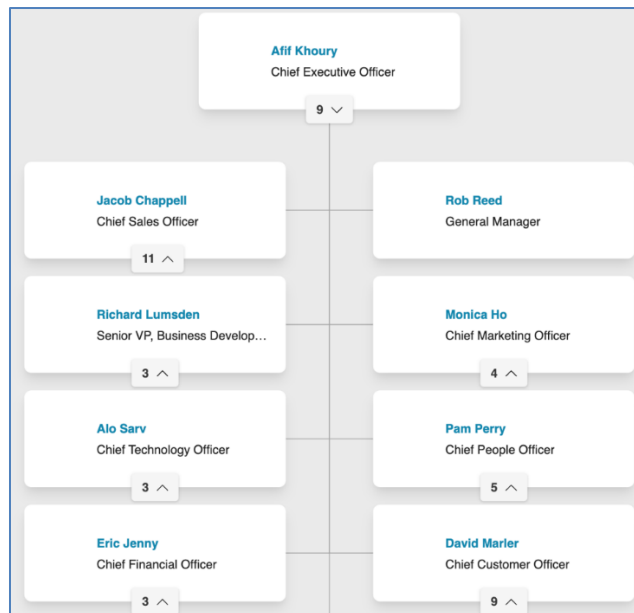
Directors are responsible for leading Finance, Sales, Marketing, Technology, and customer success departments. The executive team consists of the following:

- CEO
- Chief Technology Officer (CTO)
- Chief Marketing Officer (CMO)
- Chief Financial Officer (CFO)
- Chief Commercial Officer (CCO)

To provide organizational oversight, the vCISO meets periodically with the CTO to develop strategies and set objectives for the organization's information security and privacy initiatives. An information security management committee consisting of security staff and senior managers is active and meets in accordance with ISO 27001 guidance. Additionally, a board of directors acts on behalf of shareholders in assessing and guiding the overall direction and strategy of the business. Board meetings are held monthly, and the executive management team also meets with the board regularly. The board is composed of the SOCi CEO and six independent partners.

Data

The organization maintains a data flow diagram, shown below, to illustrate the flow of traffic through its data environments.
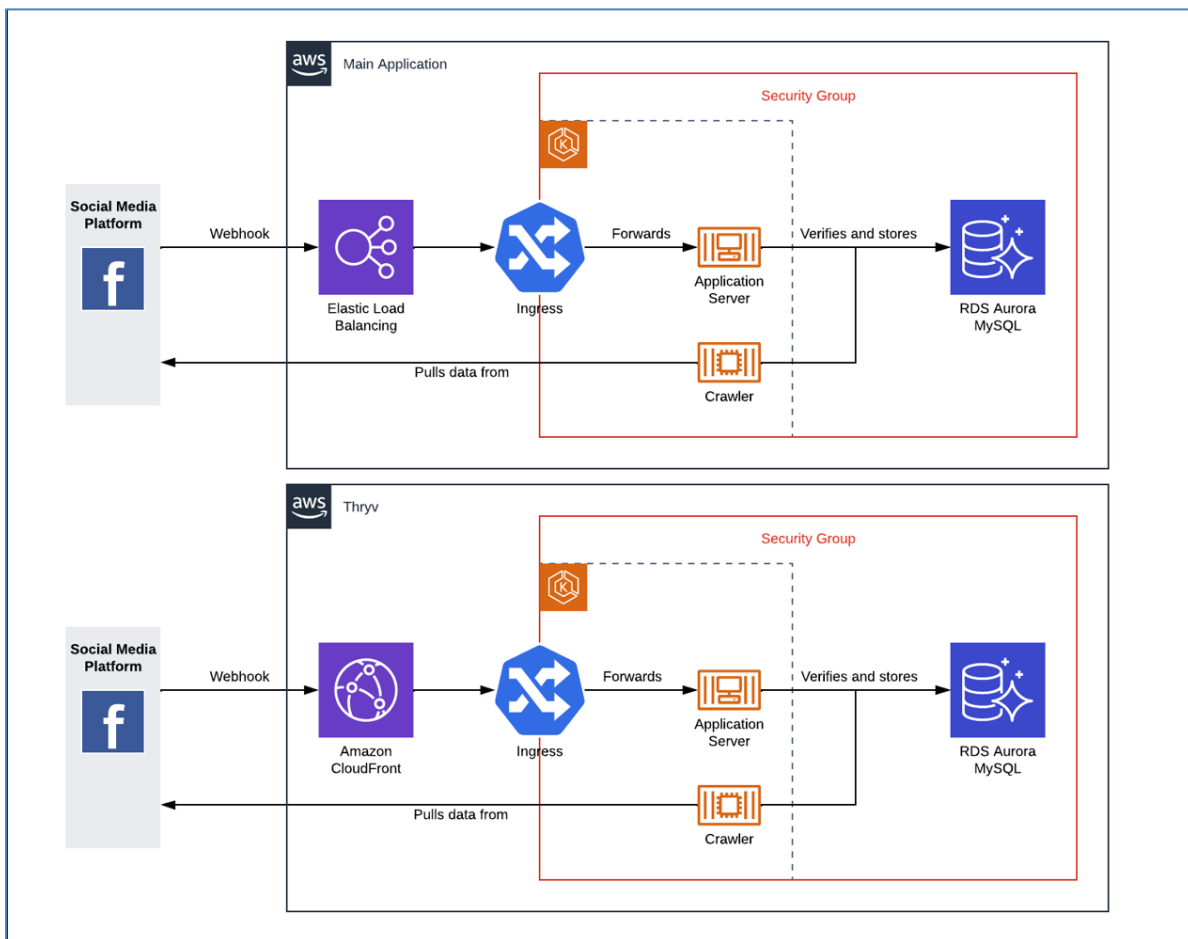
SOCi obtains and stores client data from clients' social media and reputation pages, such as Facebook, Twitter, LinkedIn, Google+, and ApartmentRatings. Social media and reputation pages include metrics such as fan and follower counts of customers' social media pages, social media posts, reviews and comments on those pages, as well as private messages sent to and from the social media pages between the page and the social media user.

The Data Retention Policy defines retention requirements, which are driven by the social media provider and mirrored by the organization. Customer data retention requirements are aligned with SOCi's Terms of Service or as agreed upon within specific customer contracts. All documents stored locally or in the cloud are retained based on the subject matter and all applicable laws and regulations. Emails must be retained based on the subject matter, and employees must not store or transfer SOCi-related emails to non-work-related computers unless necessary.

Data is classified as public, operational, or confidential, and the Data Classification Policy defines the requirements for storing, transmitting, or destroying data based on its classification. Confidential data must be encrypted during storage, must use HTTPS or Secure Shell (SSH) for transmission, and be destroyed completely when needed. Firewalls, access control lists (ACLs), and other security controls are used to separate confidential data from unsecure networks. All company assets stored in AWS or Google Cloud Platform (GCP) are protected by security controls. GCP and AWS Load Balancers are created using standard AWS Kubernetes integration setup and are not manually managed.

Data including personally identifiable information (PII) or protected health information (PHI) is considered confidential and must be treated according to requirements enforced by the Chief Product Officer. Encryption practices are based on AWS and GCP recommended best practices. Specifically, Secrets Manager is used to manage internal SOCi platform credentials, Kubernetes Secrets and Google Secrets Manager are used for GCP, and AWS key management services (KMS) is used to manage encryption keys in Amazon.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:
- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

Contractual Commitments

The organization maintains contractual materials that define the scope of the services provided to clients. The master service agreement (MSA) offers an uptime of 99.5%, excluding defined maintenance periods, customer-caused issues, or internet disruptions outside of SOCi's control. Customers are provided support via a ticketing system to notify personnel at SOCi of service interruptions that interfere with uptime service-level agreements (SLAs). Marketing materials and best practice guidance are also available to customers via the SOCi website. As part of the publicly available information security commitments, the organization defines the following:

- Best practices and industry standards
- Organizational controls
- Technical controls including Amazon Web Services (AWS), Transport Layer Security (TLS), vulnerability assessments, and backups
- Relationship to Health Insurance Portability and Accountability Act (HIPAA) and Financial Industry Regulatory Authority (FINRA) compliance

System Design

SOCi designs its social media marketing and management services system to meet its regulatory and contractual commitments. These commitments are based on the services that SOCi provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that SOCi has established for its services. SOCi establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in SOCi's system policies and procedures, system design documentation, and contracts with clients.