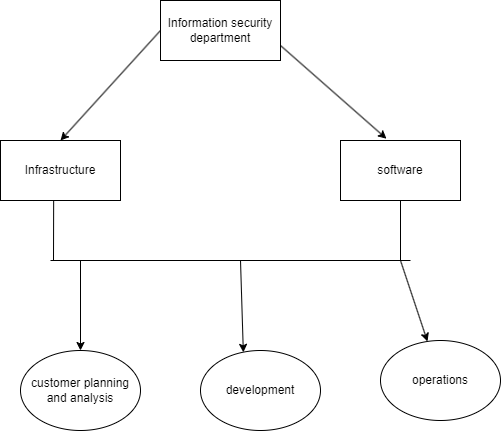
**CASE STUDY**

The use of various information systems in retail shoe stores has a number of aspects. The technologies are used to keep track of supplier stocks and sustain positive customer relations. The services for the shoe stores throughout the department would be built and managed by these teams. The networks, websites, and other crucial functions like accounting and financial transactions would all fall under this category.

A basic idea of information systems in the retail shoe store industry is given below -



The figure provides a basic idea of the basic information security department in the industry of retail shoe store departments. Information systems would also guarantee that neither clients nor staff members of the organization spend a lot of time.

Certain key departments to be involved in the information security departments are -

* **Blue team -**

This team would be in charge of system administration, software development, log management, network security, and other crucial security engineering tasks. This group would be in charge of addressing the performance and functional security issues.

* **Cyber crime team -**

This team would specifically investigate criminal activity against the organization, employees, and customers.

* **Incident Response -**

By doing so, security events and incidents would be specifically detected, analyzed, and handled. targeted personnel, sensitive data, intellectual property, and network infrastructure would also fall under this category.

* **Project management office -**

This team would be responsible for high-level project management and the upkeep of operational information security functions.

* **Security Architecture -**

This team would be specifically in charge of managing, designing and building the

networks.

* **System Administration -**

The management and oversight of network and computer system configuration and operation would fall within the purview of this team. The system's administration would also be in charge of keeping track of the system's flaws and other features.

* **Log Management -**

The log management team would be responsible for handling and monitoring the logs across the complete network.

* **Security and Compliance -**

Keep track of and maintain all necessary reports and actions to comply with security policies, rules, and audits.

* **Red Teams -**

The management and oversight of network and computer system configuration and operation would fall within the purview of this team. The system administration would also be in charge of keeping track of the system's flaws and other features.

**ORGANIZATIONAL CHART**

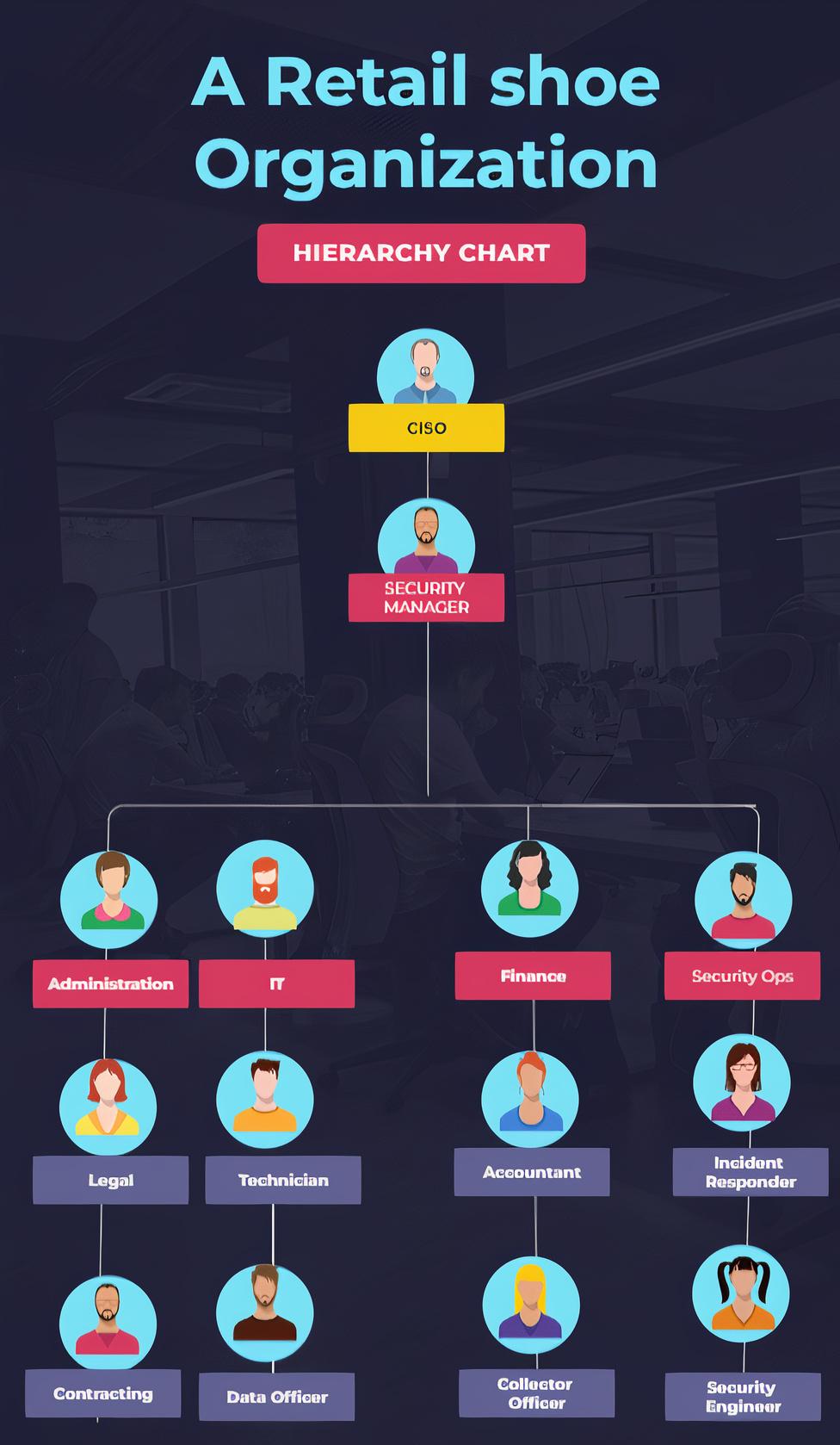
A sample organizational chart of the organization is provided down below.

The general organizational standard chart for the security team with head count is provided below-

| **POSITION** | **HEAD COUNT** |
| --- | --- |
| CISO | 1 |
| Security Manager | 4 |
| Administration | 15 |
| IT | 48 |
| Finance | 34 |
| Security Operations | 55 |

The following drop down menu describes the the following departments are in the respective positions -

* **System architecture - Administration**
* **Red team - IT**
* **Incident response - Security Operations.**



**SECURITY TOOLING BUDGET:**

The budget for the following tools is given below in the table -

| **SOFTWARE** | **HEADCOUNT** | **BUDGET** |
| --- | --- | --- |
| Wireshark | 48 | $0/year |
| Prometheus | 48 | $0/year |
| Atera | 26 | $2028/year \*user |
| Norton 360 | 157 | $2500/year \*user |
| Avast Internet Security | 157 | $3200/year \*user |
| Rapid7 | 55 | $3800/year \*user |
| CrowdStrike Falcon Insight | 40 | $4500/year \*user |
| Cisco Systems Cloudlock | 55 | $5500/year \*user |
|  | **Total** | **$1638920/year** |

**Software -**

software tools used in the organization.

**Headcount -**

Headcount defines the number of employees using an application.

**Budget -**

The budget defines the total amount required for the application to be used in the organization.

**Justification :**

Open source networking monitoring tools include Wireshark and Prometheus. These were created by certain developers and are available for free use through the company. The Norton 360 delivers malware protection in contrast to programs like Altera, an end point analysis tool that also offers IT automation. Additionally, a VPN is offered, enabling safe and anonymous web browsing. Avast Internet Security is a medium-risk tool that can both protect computers against malware and encrypt files. Rapid7 is a high-risk Internet of Things tool that is crucial to the organization's R&D division. Case studies, community resources, and other tools are available through CrowdStrike Falcon Insight to execute and combat end point analysis. In order to manage the risks in your ecosystem of cloud apps, Cisco Systems Cloudlock uses APIs. Combating data breaches and upholding regulatory standards are made simpler by Cloudlock.

This would help the organization to sustain the basic and implement effective ways of security monitoring and systems.