BSDS Assignment 5

Shujian Wen

After all your experience with processing data from FatBot devices gained in this course, Fatbot.com hire you as a consultant. they are negotiating with several organizations such as health insurers to secretly share user data so they can make money. This has to be done very secretly as if users found out, the users would sue. as this data sharing is illegal.

These clients have asked that the data be shared through a cloud service. This means user data needs to be hosted on a cloud and access given to 3rd parties who pay for the data.

Security is of course a major issue. So Fatbot.com ask you to prepare a 2 PAGE (max) report of how a major cloud provider can deliver data confidentiality, integrity and availability. They have specifically requested you choose AWS, Azure or Google Cloud Platform. Your choice.

Here's some specific scenarios to bear in mind:

- FatBot.com will upload new user data daily. this will be both raw readings and aggregated results (eg steps per user/month), as well as new user information including PII data.
- When a new health insurer pays zillions of dollars for access to the data, a set of services need to be securely made accessible to them. Each client will have a different set of services based on how much they pay.
- Hackers will try to access the data either through the services or by getting credentials to see the data on the cloud

Just remember - you have 2 pages to give your boss enough information to make a decision.

Be concise. And convincing so you get paid and requested to do more consulting work! Submit a pdf as usual.

Why choose GCP for cloud service

- Because it's Google (nah...)
- Because Google Cloud Platform (GCP) values cloud security and data integrity in various ways:

Protect

- Phishing: an attempt to obtain sensitive information by sending email from spoofed addresses
    - Google's Gmail system can filter 99.9% of spam and malicious email
    - Even if an employee's security credentials are compromised, Google uses Two-Step Verification to help prevent hackers from accessing the account without a physical security key
    - GCP's Cloud Identity-Aware Proxy (Cloud IAP) limits an attacker's ability to access applications with granular identity-based controls
- Ransomware: malware that encrypts data on a user's computer
    - Chrome Browser displays warnings to deter your employees from visiting sites suspected of hosting malware
    - Chrome Browser prevents malware like ransomware from spreading across a user's system
    - With each reboot, Chrome's Verified Boot makes sure the OS hasn't been compromised. If malware is detected, it will revert back to the most recent version of the operating system
    - Drive's desktop client, Drive File Stream, backs up local files, so "clean" versions of any infected files can be easily restored
    - Google partners with endpoint protection leaders like CrowdStrike and TrendMicro to provide additional layers of protection
- Denial of Service (DoS): an attempt to render your service or application unavailable — for example, by flooding your application with an overwhelming volume of traffic
    - GCP's robust, global load balancing mitigates infrastructure DDoS attacks, such as SYN floods, IP fragment floods, and port exhaustion
    - GCP Armor provides scalable defense against application-aware and multi-vector attacks using IP blacklists and whitelists, geo-based access control, SQL injection and XSS defense, and custom rules
    - In the event of DDoS attacks on cacheable content, requests are sent to POPs all over the globe to help absorb the attack
    - Multi-region application instances increase surface area to absorb attacks. Auto scaling handles traffic spikes seamlessly
    - Partner solutions available on GCP Marketplace integrate seamlessly into deployments and add specialized protection

Control

- Data exfiltration: an unauthorized transfer of sensitive information from your organization by an external attacker or a malicious insider
    - Cloud Data Loss Prevention (DLP) API discovers, classifies and protects sensitive data such as financial records and Personally identifiable information (PII) across your organization
    - Cloud Identity & Access Management (IAM) controls which users can access data and resources
    - VPC Service Controls isolate GCP resources from one another with fine-grained network policies
    - Forseti scans GCP resources to ensure that appropriate access controls are in place. Cloud Security Command Center provides centralized reporting of security events to spot potential threats to your data and applications.
- Smart Access from Anywhere
    - Cloud Identity manages user accounts, authenticates users, enables single-sign on, and manages devices
    - Cloud Identity-Aware Proxy (Cloud IAP) controls access to applications and resources based on user's identity and contextual attributes like location, network, and device status
    - Context Manager creates granular access control policies based on attributes like user location, IP address, and endpoint security status
- Security Monitoring: see vulnerabilities, threats, and incidents in order to assess risks and prioritize corrective action
    - Cloud Security Command Center gathers, integrates, analyzes, and acts on unified security information (e.g., scans, notifications, and third-party feeds) from a single dashboard. Integrate with leading third-party solutions from Cloudflare, CrowdStrike, Redlock, Palo Alto Networks, and Qualys to enhance security assessment and detection.
    - Cloud Security Scanner finds security vulnerabilities in web applications during development before they're deployed
    - G Suite Security Center monitors your G Suite domain for security threats. View security analytics and act on best practice recommendations

Comply

- Google regularly undergoes audits of security, privacy, and compliance controls
    - ISO 27001
    - ISO 27017
    - ISO 27018
    - SOC 2
    - SOC 3
    - PCI DSS