AIG150- Week 9

Data Privacy and Security

Reading Text: Ch 07-08

Data Governance: The definitive guide

Agenda

- Data protection and security
- Monitoring
- Building a culture of data privacy and security

Data Protection

Data protection is one of the key concerns for data governance as it is important to all stakeholders :

- Owners :Potential exposure of sensitive information to individuals and applications without authorization
- Managers: Wary of security breaches or known personnel accessing data for the wrong reasons
- Users: The integrity of the data

Protection At All The Levels

- Physical
- Network
- Operating System
- Application
- Storage

Planning For Protection

- Create a catalog of all data assets
- Which data needs protection from what ?
- Decide the authentication and authorization levels
- Protection of data in transformation
- Protection of raw and aggregated data

Level of Protection

- Calculate the cost and likelihood of security breaches associated with an asset.
- Protecting data stored in a lake versus warehouse.
- CIA (confidentiality, Integrity, Availability) of data should be maintained.
- Data should be always accessed by the authorized users.
- Data should be prevented from unauthorized access.
- Data can be classified as private and personal data, confidential data or intellectual property.

Data Protection In The Cloud

- Multi tenant cloud architecture
- Organizations lose the physical and network security they may have with the on –premise data storage.
- Use cloud identity and access management (IAM) systems instead of Kerberos-based or directory-based authentication.
- Define roles, specify access rights and manage and allocate access keys to ensure authorized and authenticated access by users.

Security Surface Of Public Clouds

- Dedicated, world class security teams.
- Increased security monitoring and auditing.
- Scale and sophistication of tools used on the cloud.
- In short, cloud brings benefits in terms of being able to apply governance practices that may not be possible on premises.

Physical Security

- For authorized access, many safeguards should be in place as such as electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics, and laser beam intrusion detection.
- Regularly patrolled and surveillance
- Uninterrupted power supply
- Reduce the chances of physical damage
- Disaster recovery
- Incident management

You can do the checklist for network and other levels of security as well.

“Security & governance should not be afterthought; they should be baked into the fabric of your organization”

Risks & Consideration For Security

- Data exfiltration specially in public cloud
  - VPC-SC
  - Limit volume and frequency of data transmission
  - Auditing
  - Minimal access
  - Content logging and monitoring system
- Secure code
  - Binary authorization

Virtual Private Cloud Service Controls (VPC-SC)

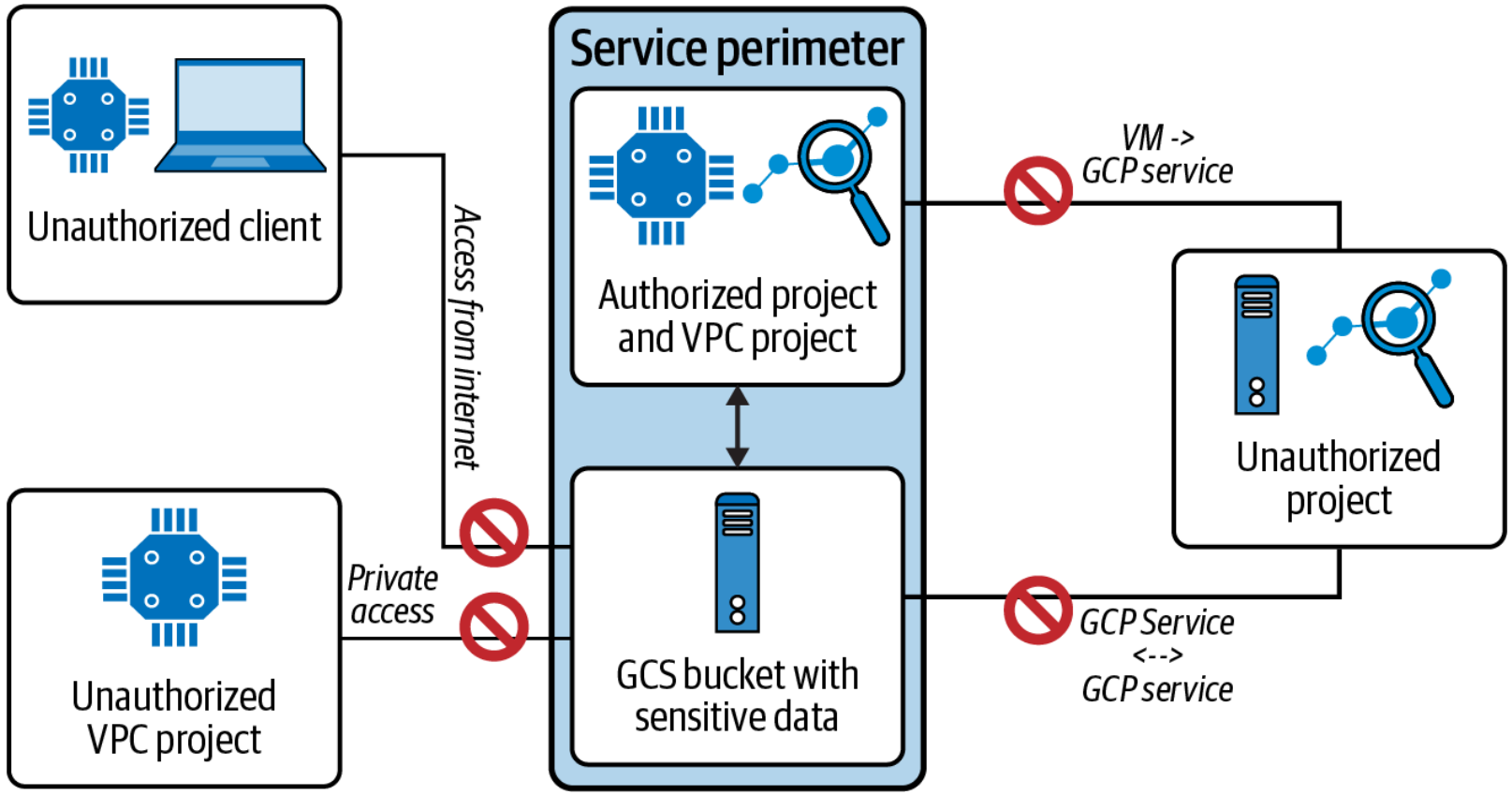


Figure 7-2 from reference text

Zero Trust Model

- Perimeter-based security models are becoming problematic, as when a perimeter is breached, an attacker has relatively easy access to the organization’s privileged intranet.

- Due to mobile and cloud technologies, perimeter is getting difficult to enforce. Zero trust security models allows users to access enterprise application virtually from any location without the need of a traditional VPN.

- All access to enterprise resources is authenticated, authorized, and encrypted based on device state and user credentials.

Identity And Access Management

- Authentication
  - API Keys
  - Access tokens such as OAuth 2.0 client credentials
  - Service account keys
- Authorization
  - Roles
  - Permissions \ privileges
  - Identity-aware proxy (IAP)

Differential Privacy

- Aggregate data while withholding information about the individuals.
- Techniques used to implement differential privacy:
  - K-anonymity
  - Adding statistically insignificant noise to the data set
- Transparent Access

Keeping Data Protection Agile

- Security health analytics
- Data Lineage
- Event threat detection
- Implement data protection best practices

Monitoring

- It is a comprehensive operations, policies and performance management framework.
- The main objective is to detect and alert about possible errors of a program or system in a timely manner and deliver value to the business.
- Organizations use monitoring systems to monitor devices, infrastructure, applications, services, policies, and even business processes.

Why Perform Monitoring ??

- It allows you to review and assess performance for your data assets.
- To introduce policy changes within the organization.
- To identify what is working and what is not, with the goal of creating value for the business.
- Monitoring systems help you with :
  - Alerting
  - Accounting
  - Auditing
  - Compliance

What Should You Monitor ?

- Operating Systems
- Hardware
- Network and connectivity
- Servers
- Processes
- Governance
- ***DATA***

Data Quality Monitoring

- Completeness
- Accuracy
- Duplication
- Conformity
- When setting up the monitoring, consider:
  - Establish a baseline
  - Quality Signals

Data Lineage Monitoring

- Data transformations
- Technical metadata
- Data quality test results
- Reference data values
- Actor

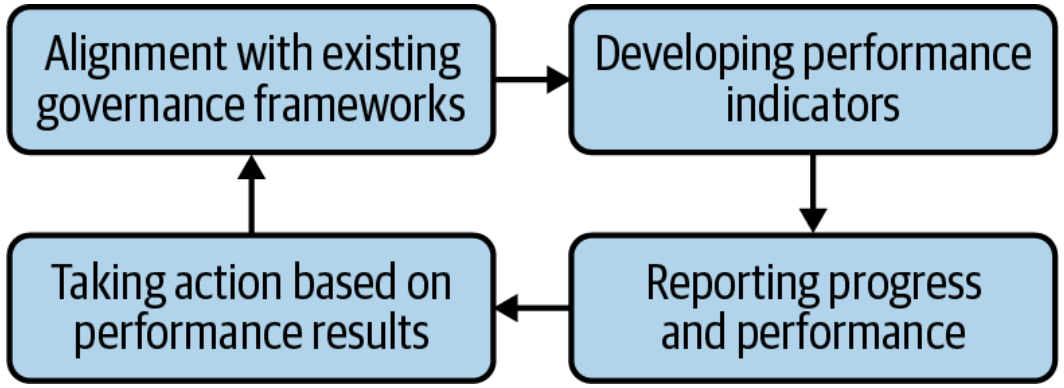
Compliance Monitoring

- Keep an eye on changes in:
  - State and federal regulation
  - Industry standards
  - Governance policies

Program Performance Monitoring

- Monitoring and managing the performance of a governance program is integral to demonstrating program success to business leadership.

- Track progress against the program's aims and objectives, ensuring the governance program delivers the right outcomes for the organization, accounting for efficient and effective use of funding, and identifying improvement opportunities to continue creating impact for the business.



Reference Text, Figure 8-1. Performance management framework

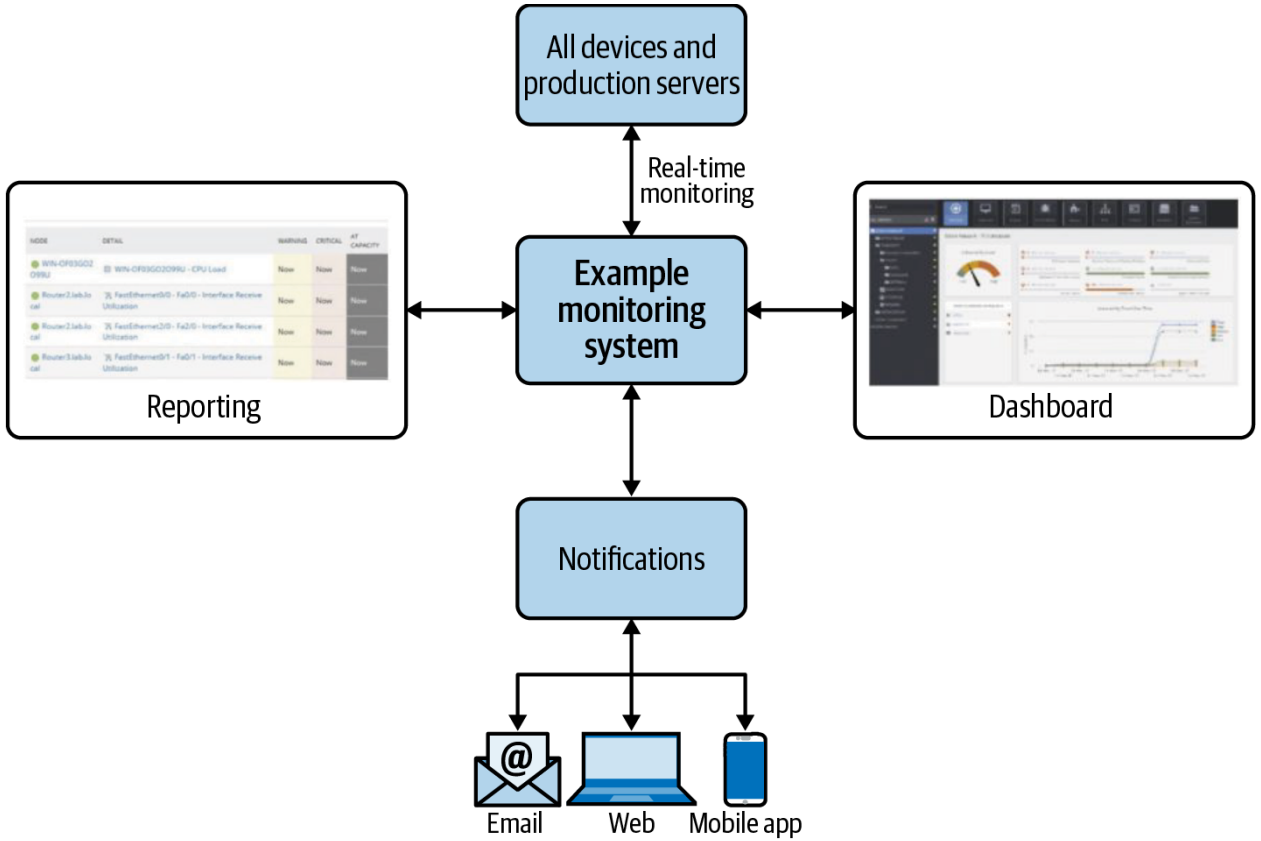
Security Monitoring

- Security alerts and incidents
- Network events
- Server logs
- Application events
- Server patch compliance
- Endpoint events
- Identity access management
- Data loss

Monitoring System: Tools

- System alerts
- Notifications
- Reporting\analytics
- Graphic visualization
- Customization

Sample Monitoring System



Reference Text Figure 8-2. Example monitoring system

Data Culture

- How is data thought about within the company/organization?
  - Is it an asset? Needed to make decisions?
  - The most important part of the company?
  - Just something to be managed?
- How data should be collected and handled?
- Who should be handling data and when?
- Who is responsible for data during its life cycle?
- How much money and/or resources will be committed to serving the company/organization's data goals?

Things You Need to Look

- What's important ?
- Who needs to know what ?
- Communication
- Top-down, bottom-up, and everything in between
- Why ? Motivation and adoption

Transparency

- Building internal trust
- Building external trust