Overall Risk Score

66%

17%
Access Anomalies

57%
Vulnerabilities

43%
Threats

Datiphy Inc

2290 N First Street, Suite 204
San Jose, CA 95134

1.888.343.9938
www.datiphy.com

Security Breakdown

Access anomalies are defined as abnormal behaviors or trends exhibited by users, applications, network traffic, or host environment. A high risk score would indicate that a current snapshot shows a high volume of sensitive data being manipulated by external actors.

Vulnerabilities are defined as weak points in your environment that could potentially pose a risk to the protection of your sensitive data. A high risk score would indicate that a security measure is needed to defend against malicious activities.

Threats are discovered based on abnormal trends or behaviors that are currently detected within your sensitive data environment. A high risk score would indicate that an active threat may be persistent; or a culmination of abnormal behaviors are detected, which may indicate an impending attack.

Categories

- Inside/Outside Threats
- SQL Injection
- Data Security
- Asset Management
- Risk Management
- Privileged Escalation

Inside/Outside Threats

Definition: Inside and outside threats are caused by improper granting of escalated privileges. The threat may be intentional or accidental, due to lack of oversight. Typically, inside threats are due to employees/personnel that have access to highly sensitive data. Outside threats are potentially due to applications or external malware that have immediate access to sensitive data.

Summary:

0 Discovered inside threats

11 Discovered outside threats

0 Escalated privileges threats

Recommendations (Contact Datiphy for detail report):

- Identify the assets in questions and review all users with privileged escalation.

- Scan your network for vulnerabilities or malware that are potentially infecting your hosts, end-points, or applications.

- Investigate your data stores for known weak points.

SQL Injection

Definition: A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Summary:

9 Discovered SQL injection

Recommendations (Contact Datiphy for detailed report):

- Use of prepared statements

- Use of stored procedures

- Escaping all user-supplied inputs

- Least privilege

- White list input validation

Data Security

Definition: Protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption.

Summary:

9 Discovered weak points

4 Types of sensitive data

13 Access control issues

Recommendations (Contact Datiphy for detailed report):

- Encrypt sensitive data.

- Review all exposed sensitive data types.

- Enable database auditing or fine grain auditing.

Asset Management

Definition: A systematic process of deploying, operating, maintaining, upgrading, and disposing of assets cost-effectively.

Summary:

4 Discovered databases with sensitive data

0 Types of assets

0 Unknown access points

Recommendations (Contact Datiphy for detailed report):

- Define an asset inventory.

- Catalog and define a network segmentation to protect the various types of assets.

Risk Management

Definition: The forecasting and evaluation of cyber security risks together with the identification of procedures to avoid or minimize their impact to data loss.

Summary:

10 Risk impact to data loss

2 Areas of high risk profiles

2 Procedures that are high impact to risk

Recommendations (Contact Datiphy for detail report):

- Define an enterprise risk management program.

- Identify assets, data stores, and applications that have the highest risk exposures to data exfiltration.

Privileged Escalation

Definition: Act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

Summary:

0 Instances of privilege users

10 Instances of privilege changes

Recommendations (Contact Datiphy for detailed report):

- Review your user access control list.

- Revoke unnecessary privileges or remove obsolete users to decrease your threat vectors.