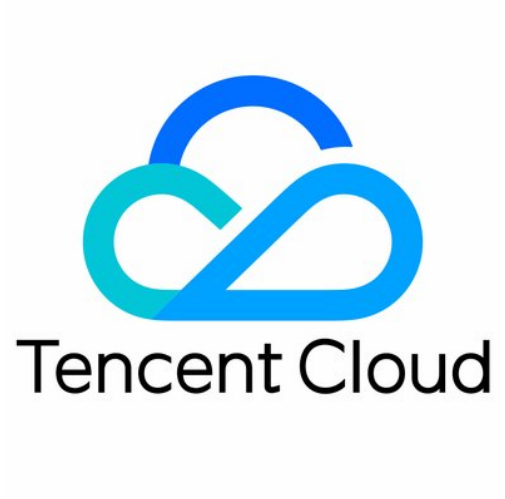
Security Operations Center

Best Practice

Product Documentation



©2013-2022 Tencent Cloud. All rights reserved.

Copyright Notice

©2013-2023 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

Tencent Cloud

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

©2013-2022 Tencent Cloud. All rights reserved.

Best Practice
Data Leakage Detection
Data Leakage Related Explanations

Last updated：2023-08-29 15:59:14

Description

Data leakage refers to the potential viewing, theft, or use of protected or confidential data by unauthorized individuals. Due to the nature of business and development systems, internet companies generally involve numerous version changes. Most internet companies advocate an open-source culture internally. While this openness fosters innovation, it also lays the groundwork for potential data leakage incidents.

Applicable Entities

Developers migrating business to the cloud, operations engineers, and beginners in the field of security.
Enterprises operating in the cloud and showing significant concern for data leakage.

Common Classifications

Taking several significant data leakage incidents from recent years as examples, we can categorize them based on the channels of leakage:

Github Code Type:

Reason for Data Leakage: The intentional or unintentional uploading of code containing sensitive internal corporate information to the Github website, leading to its exploitation by external attackers for intrusion.

Case Study: The backend engineering source code of a large-scale secondary element website was uploaded to Github.

Website Intrusion:

Cause of Data Leakage: Data leakage and loss occur due to vulnerabilities in websites, service platforms, Apps, etc., which are attacked.

Case Study: A large technology community website experienced a leak of 6 million user information.

Network Black Market Transactions:

Cause of Data Leakage: Secondary leakage channels refer to data leakage incidents that occur in underground trading markets where data is sold and traded. The sources of this data can vary widely, for instance, by hiring

©2013-2022 Tencent Cloud. All rights reserved.

hackers to gain access to data servers, or through covert internal operations to obtain internal data. These data leakage incidents are often profit-driven, with the data being published and sold on the network black market.
Case Study: A well-known domestic hotel's guest data leakage incident.

Partner Interface Call Category:

Reason for Data Leakage: The internal data of the partner interface call is not adequately secured or monitored, leading to the leakage of sensitive data through the partner channel. This could be due to technical issues or the illegal use of this data.
Case Study: An analytics company improperly obtained the personal information of 50 million Facebook users.

Origination Cause

The fundamental causes of data leakage can be summarized into the following two categories:
Technical Aspect: Insufficient technical control strategies over data can lead to data leakage. If websites, platforms, applications, or systems have security issues, such as system vulnerabilities or configuration errors, lack of data desensitization methods and data encryption measures, absence of abnormal operation audit methods, or lack of mechanisms to detect sensitive information leakage, these could all potentially be exploited by attackers to gain access to sensitive data.
Management Aspect: The absence of data security management policies or systems can lead to data leakage, as sensitive data may be accessed by unauthorized individuals. Data may be publicly disclosed or illegally misused due to weak security awareness among developers or interns, or due to a lack of constraints or restrictions on the use of data by partners.

Solution

If an enterprise establishes a sensitive information leakage monitoring system, it can swiftly respond to leakage incidents through technical means and actively carry out self-inspection and repair. By rectifying and reinforcing defenses before a hacker intrusion, the enterprise can avoid various unnecessary latent risks and minimize losses.
The aforementioned text discusses four mainstream data leakage event risks. We provide technical methods and management control ideas for the analysis of two typical and more harmful behaviors: Github code leakage and black market data trading.

Technical Control Strategies

Employees are strictly prohibited from setting up code management tools privately. They must use the company's uniformly authorized code management tools (such as Github, SVN) for code management.
Strictly control project code permissions. When personnel changes occur (such as transfers or departures), code permissions must be promptly revoked.

©2013-2022 Tencent Cloud. All rights reserved.

Large-scale projects utilize submodules for division, implementing the principle of minimal permissions for project management.
Avoid storing code on external websites such as Github and Onedrive.
Monitor websites such as GitHub and underground marketplaces for sensitive information leaks. When sensitive information appears, promptly conduct a self-check to confirm and prevent the problem from spreading.

Compliance Management Policies

Establish a "Source Code Open Source Security Management" process. Code open-sourcing must undergo an open-source process evaluation.
Imposing constraints, restrictions, or supervisory audits on the scope of use of partners' interfaces.
Implement legal constraints on internal employee contracts, adopting stringent measures.

Product Application

The advantages of a SaaS-based Security Operations Center for enterprise security operations include:
SaaS-based services eliminate the costs of code maintenance and server upkeep for their own data leakage monitoring systems, allowing enterprise developers, operations personnel, or security administrators to focus more on rule operations.
Integration with the cloud platform enhances development and operations, centralizing event handling to improve efficiency.
In terms of handling false alarm rules, SaaS platforms tend to have more longevity than open-source systems. They optimize based on the collective experience of cloud users. Currently, with the support of the Cloud Ding Lab team for backend strategy maintenance, there are relatively fewer false alarms, resulting in higher quality alerts.

©2013-2022 Tencent Cloud. All rights reserved.