DATA SHEET

Cloud Security Audit

Expertly assessing and fortifying your cloud infrastructure

Overview

A cloud security audit is a comprehensive examination of an organization's cloud-based systems and infrastructure to identify potential security vulnerabilities and compliance issues. The audit typically includes both automated and manual testing, as well as a review of the organization's policies and procedures. The goal of a cloud security audit is to ensure that the organization's cloud-based systems are secure and compliant with industry standards and regulations.

How CyStack Helps

The CyStack Audit Team is a group of highly skilled security testers who use a goal-oriented approach to testing, refined through years of experience and extensive testing. Our team members have a unique blend of app development and security testing expertise, enabling them to conduct comprehensive security evaluations that uncover potential risks for organizations. Members of this team are also regular speakers at world-known cyber security conferences and also talented bug hunters who discovered many critical vulnerabilities in the products and are acknowledged in the Hall of Fame of global tech giants such as IBM, HP, Microsoft, Alibaba, Sea Group, etc.

The team can perform a review of the business's cloud infrastructure, including servers, networks, and storage, as well as the architecture of the systems and how they are configured to identify any vulnerabilities or misconfigurations that could be exploited by attackers. They will also review the security settings and configurations of the business's cloud-based systems and applications to ensure they are properly configured, including checking for proper encryption, access controls, and network security.

Customer Benefits

- Strengthen the security of the cloud-based systems and infrastructure
- Ensure compliance with industry standards and regulations
- Understand and manage security risks more effectively
- Develop a better governance model and make a more robust risk management strategy
- Have an independent third-party validation of the cloud security posture

Methodology

CyStack Cloud Security Audit typically involves:

- **Assessment of cloud infrastructure and architecture**: Our team will review your organization's cloud infrastructure, including servers, networks, and storage, as well as the architecture of the systems and how they are configured. We will identify any vulnerabilities or misconfigurations that could be exploited by attackers.
- **Security configuration review**: We will review the security settings and configurations of your organization's cloud-based systems and applications, looking for any misconfigurations or vulnerabilities that could be exploited. This includes checking for proper encryption, access controls, and network security.
- **Policy and procedure review**: We will review your organization's policies and procedures related to cloud security, including incident response plans, disaster recovery plans, and access controls. We will identify any gaps or inconsistencies in these policies and procedures and provide recommendations for improvement.
- **Compliance assessment**: We will review your organization's cloud-based systems and infrastructure to ensure compliance with industry standards and regulations, such as ISO27001, HIPAA, PCI-DSS, and SOC 2.
- **Penetration testing**: We will perform penetration testing to simulate real-world attack scenarios and identify vulnerabilities allowing an attacker to gain unauthorized access to your organization's cloud-based systems and data.
- **Remediation guidance**: Once vulnerabilities and compliance issues have been identified, we will provide detailed advice and recommendations for remediation, including best practices for securing cloud-based systems and infrastructure.
- **Reporting**: We will provide a detailed report of findings, including a summary of identified vulnerabilities and compliance issues, along with remediation recommendations.

Key Features

- Gain assurance that your infrastructure is secure
- Review comprehensively infrastructure including configurations, architecture, policies, and procedures
- Manage, track, prioritize and remediate the findings in CyStack Vulnerability Management Platform
- Receive actionable recommendations to enhance security
- Reduce your risks and improve operational efficiency

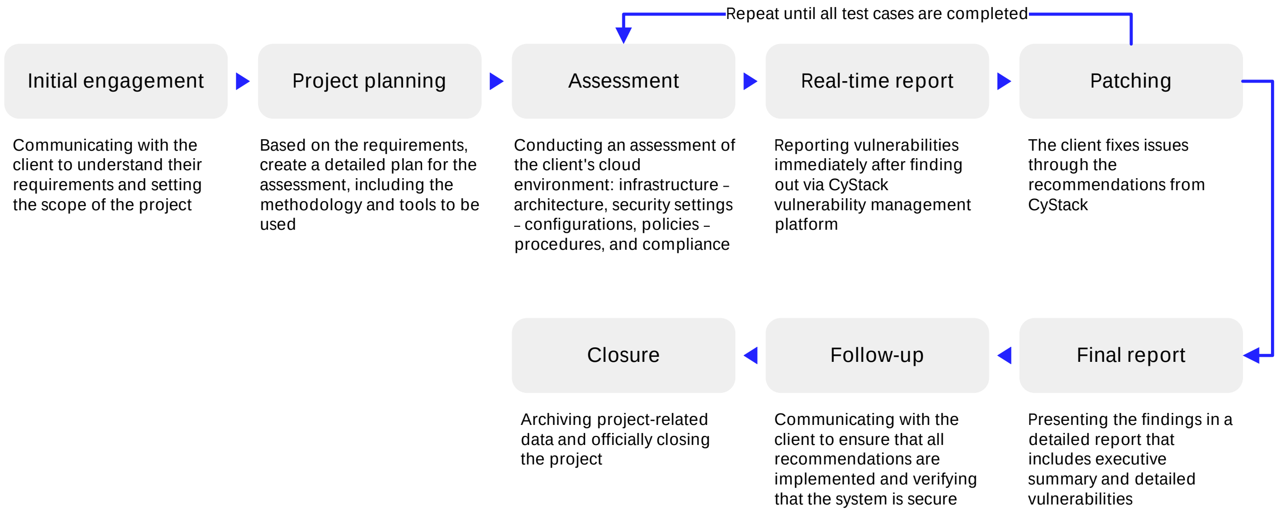
Standards

There are several international guidelines and standards that CyStack uses as a framework for conducting a cloud security audit as follows:

- **ISO/IEC 27001:2013**: This international standard provides a framework for an information security management system (ISMS). It includes guidelines for risk management, incident management, and business continuity management, which can be applied to cloud-based systems and infrastructure.
- **SOC 2**: This standard is developed by the American Institute of Certified Public Accountants (AICPA) and is intended for service organizations such as cloud providers. It focuses on the control activities of service providers related to security, availability, processing integrity, confidentiality, and privacy.
- **PCI DSS**: Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards created to protect cardholders' data. It applies to any organization that stores processes or transmits cardholder data. So it is important to ensure that the cloud infrastructure used to store, process, or transmit cardholder data is PCI compliant.
- **NIST SP 800-53**: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 provides guidelines for the security of federal information systems. It includes control families such as security assessment and authorization, security management, and incident response. This standard can be applied to cloud-based systems and infrastructure, as well as on-premises systems.
- **CSA CCM**: The Cloud Control Matrix (CCM) is a framework developed by the Cloud Security Alliance (CSA) that provides guidelines for cloud security. It includes control domains such as security governance, risk management, and incident management.
- **HIPAA**: Health Insurance Portability and Accountability Act (HIPAA) is a law that requires organizations to protect the privacy and security of individuals' health information. So any organization that stores, processes, or transmits protected health information (PHI) must comply with HIPAA.

We also use the security guidelines of big cloud providers like AWS, GCP, and Azure as well as of Cloud Security Alliance for our audit.

Flow To Work With Clients



Repeat until all test cases are completed

Initial engagement

Communicating with the client to understand their requirements and setting the scope of the project

Project planning

Based on the requirements, create a detailed plan for the assessment, including the methodology and tools to be used

Assessment

Conducting an assessment of the client's cloud environment: infrastructure – architecture, security settings – configurations, policies – procedures, and compliance

Real-time report

Reporting vulnerabilities immediately after finding out via CyStack vulnerability management platform

Patching

The client fixes issues through the recommendations from CyStack

Final report

Presenting the findings in a detailed report that includes executive summary and detailed vulnerabilities

Follow-up

Communicating with the client to ensure that all recommendations are implemented and verifying that the system is secure

Closure

Archiving project-related data and officially closing the project

About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net

CyStack