ZERODAYLAB®

Cloud Security Configuration Review

Many cloud environments are not appropriately configured or use hardened images, and therefore allow unauthorised access. There is an assumption that cloud environments are secure by default; they are not. It is now common to see news stories of cloud environments being compromised by attackers exploiting misconfigurations and vulnerabilities in Containers, WAF's and Web Services run on platforms such as Azure, AWS and GCP, ultimately allowing them to gain unauthorised access to sensitive information.

"Experts agree that by the year 2020, the average cost of a data security breach for a major business would be over $150 million."

Juniper Research Ltd. 2019

Now more than ever, it is important to understand how misconfiguration, weaknesses in hardening of images and insufficient cloud security controls can impact your organisation's reputation and operational efficiency.

To address the aforementioned issues, ZeroDayLab offers a comprehensive Cloud Security Configuration Review that provides an overview of the current security posture of your cloud estate. Examples of assets in scope include AWS, Azure and GCP services and their contents, and Microsoft Office 365. This can however include any cloud assets, ultimately delivering a holistic overview of your current cloud security maturity, and the required remediation actions to reduce your organisation's risk. We deliver this across three domains:

- **Cloud Threat Modelling**
- **Cloud Security Controls Review**
- **Cloud Configuration Review**

ZERODAYLAB®

Cloud Threat Modelling

ZeroDayLab will review the threat landscape in the cloud, undertaking a high level of threat modelling exercise to understand the specific attack vectors facing organisations utlising cloud services. This will include:

- Threat Actor Identification
- Attack Vector Validation
- Target (asset) Mapping
- Attack Scenario Modelling (Apps, Servers, Data Assets)

Cloud Security Controls Review

Using the information gathered during the high-level threat modelling exercise, ZeroDayLab's GRC consultants will undertake a Cloud Security Controls Review. This exercise will address each asset's current control set and policies to understand where potential technical and procedural issues exist.

This will be scoped on a per asset basis, allowing us to address each environment and service with the appropriate tools and knowledge, ultimately allowing for an appropriate, comprehensive and detailed remediation report. The domains to be reviewed include (but are not limited to):

- Cloud Security Architecture
- Cloud Technical Security Controls
- Hardening and Baselining
- Data Security & Information Life Cycle Management
- Access and Identity Management
- Encryption and Key Management
- Threat and Vulnerability Management
- Security Incident Management, E-Discovery & Cloud Forensics
- Application and Interface security
- Governance and Compliance in the Cloud
- Logging and monitoring

ZERODAYLAB®

Cloud Configuration Review

This technical review focuses on ensuring that the cloud account, alongside the resources hosted within the account are configured securely. This review is conducted by our team of expert ethical hackers who have vast experience in issues found within GCP, AWS and Azure.

The service will uncover and demonstrate misconfigurations such as:

- Insecure user authentication
- Improper user management
- Lack of proper encryption
- Insecure update configuration
- Lack of sufficient traffic filtering
- Insufficient monitoring of resources
- Lack of proper key and secret rotation
- Account configurations not in line with best practice standards observed on the internet

In summary, our Cloud Security Configuration Review provides organisations with a 360° approach to understanding how their cloud environments are exposed, where technical and procedural controls are insufficient, and clear technical validation of how attackers can exploit configuration issues and ultimately gain unauthorised access to informational assets. The recommendations from the Cloud Security Configuration Review provide a clear defined roadmap to improve overall maturity and security, and provide peace of mind that your cloud assets pose limited risk to your organisation.

Get in touch today to discuss how we can help you secure your cloud assets.

Europe Headquarters:

ZeroDayLab Ltd
Suite 303, 150 Minories,
London,
EC3N 1LS, UK
Phone: +44 (0)207 979 2067

North America Headquarters:

ZeroDayLab LLC
3524 Silverside Road, Suite 35B
Wilmington, DE
19810-4929, USA
Phone: 1-614-263-9765

Amsterdam I Manchester I Edinburgh I Dublin I Brighton & Hove

www.zerodaylab.com I www.zerodaylab.nl I info@zerodaylab.com