secarma
CYBERSECURITY EXPERTS

SERVICE OVERVIEW

Cloud Configuration Security Review

Secarma's cloud security assessment will test the configuration of the chosen cloud providers management interfaces for security misconfigurations. This should be considered a critical requirement for any businesses that has moved or is looking to move onto cloud infrastructure.

WHO IS IT FOR?

Many organisations these days have at least some workloads hosted within the cloud. Whether it's a simple "lift-and-shift " of moving onsite assets to the cloud, or something more 'cloud native', it's important to make sure that these systems are secure.

We offer security testing appropriate for all levels of complexity, from simple security reviews of cloud hosted virtual machines, to deep-dive assessments of cloud-native applications.

HOW CAN WE HELP?

If you're hosting an application in the cloud and are concerned about application vulnerabilities within the system, then we can perform a traditional application penetration test.

However, if your concern is with how the hosting environment itself is set up then the most efficient way to determine if a cloud setup is secure, is to review the configuration panel itself.

This is an open book approach to security testing that ensures that available security options are configured, that systems are locked down, and that accounts with access are appropriately protected.

WHAT WE TEST

The specifics of the testing depend entirely on the deployment and features in use on the target cloud platform, however some commonly assessed areas include:

- **Identity and Access Management**
  Ensuring account utilise multifactor authentication and adhere to the principle of least privilege.
- **Storage**
  Ensuring that permissions to storage such as AWS S3 Buckets and Azure Storage are locked down and that keys are protected.
- **Network and Instance Security**
  Ensuring that the cloud platform adequately filters traffic and segments services.
- **Transit Security**
  Ensuring that data in transit between systems is encrypted and the configuration is hardened.
- **Logging and Monitoring**
  Ensuring that any actions taken within the cloud platform, and that may impact the systems security, are appropriately logged and that significant issues are highlighted to administrators for review.
- **Remote Access**
  Ensuring that remote access to the cloud platform is hardened against internet-based attacks.
- **Key Management**
  Ensuring that services such as Azure Key Vault and AWS Key Management are appropriately used and hardened, and that logging is enabled.

secarma
CYBERSECURITY EXPERTS

METHODOLOGY OVERVIEW

Cloud Configuration Security Review

Our Cloud Configuration Security Review methodology takes into account the Best Practise guidance released by the cloud vendors themselves, hardening guidance released by organisations such as the Centre for Internet Security and our consultant's broad experience working with a range of security conscious organisations. A list of the major testing categories we will perform, is outlined below:

IDENTITY AND ACCESS MANAGEMENT

The first step is to assess the configuration to ensure that the principle of least privilege is applied. This will ensure that both insider threats and compromised accounts are limited by default.

We will ensure that user accounts use multi-factor authentication which minimises the risk of compromised credentials and attacks such as phishing.

We will review the user password policy for user passwords, including password length, password history, and password complexity.

The account lockout policy is one of the controls in place to prevent online brute-force attacks against user accounts.

STORAGE

Where features such as AWS S3 buckets and Azure Storage are used, we will assess the permissions and storage mechanisms to ensure that access is appropriately restricted .

TRANSIT SECURITY

Ensure that encryption in transit, with Transport Layer Security, is enabled across all services to protect sensitive data.

LOGGING AND MONITORING

Monitoring system usage and logging activity is critical for ensuring that an organisation can effectively respond to security incidents.

The audit policy controls the level of logging and logging should be granular enough to ensure that an incident responder can determine what actions were taken and by whom.

REMOTE ACCESS

Accessing your cloud resources securely is critical to prevent system compromise. There are many options from Bastion Hosts to site-to-site VPNs. These will be assessed to ensure they're inline with best practise guidance and appropriately hardened.

ACCESS CONTROL LISTS

Access between resources such as Virtual Machines is controlled via access control lists, such as Security Groups. These work in a very similar way to traditional Firewalls and therefore should be reviewed to ensure they're as restrictive as possible and don't allow unnecessary traffic to sensitive resources.

Many Cloud Configuration Assessments are best performed in conjunction with security testing of the system itself. For example, if you're hosting a web application or web service within a cloud interface then combining this security assessment with a Web Application/Services Penetration Test will deliver the highest level of assurance.
Alternatively, if you're hosting infrastructure and servers within the cloud, then adding a Host Build Configuration Review will ensure that the servers themselves are hardened from malicious insiders.