Service Definition
Cloud Security Assessment

Introduction

With the ever-increasing use of cloud hosted software, infrastructure or platforms, testing of these deployments provides an independent analysis and information security assurance regarding the governance and controls that are in place to protect services and systems. Such assurance is vital for cloud-based services which possess specific security considerations due to their on-demand, remotely accessible and multi-tenanted attributes.

The service can be tailored to suit individual assurance requirements, focusing on Internet-facing services or applications only, the backend infrastructure that supports these or environments being built or used and are replacing traditional on-premises infrastructure.

Security issues found are detailed in a formal report and recommendations are provided to enable the client to eliminate or mitigate the risk, thus reducing the likelihood of a successful attack and limiting the attack surface of a cloud environment.

Scoping

A scoping conversation will be held prior to delivery to fully understand requirements and expectations, the size of the platform/environment to be tested and the type of systems and/or infrastructure to be assessed. A recommended number of units/days will then be provided to enable requirements to be met.

Cloud Environment Configuration Review

Intertek NTA will assess the security of the cloud environment configuration in accordance with security best practice such as CIS benchmarks, National Cyber Security Centre (NCSC), Microsoft and Amazon Web Services (AWS).

Reviewing configuration and security of Administrator portals; insufficient policies, conditional access policies, RBAC, networking and/or logging from a high level.

Specific components can be reviewed as a part of this review (e.g. S3 buckets, Blob storage, Data Lake, EC2 instances, Lambda, RDS, ECR, ECS, DynamoDB, ElastiCache, API gateways, IAM, GuardDuty, secrets manager, Entra ID, Key Vault).

Intertek NTA will review external interfaces (e.g. services and IP addresses) to ensure resources are restricted and not publicly accessible (where appropriate). Where external interfaces are exposed, typical vulnerabilities will be checked on those services, e.g. SSL configuration, common HTTP/HTTPS vulnerabilities, etc.

Server Build Reviews

The review will involve searching for weakness and misconfiguration in the basic build of the server presented, ensuring it is in accordance with security best practice and NCSC guidance, where appropriate. The review will consist of, but not be limited to, the following:

- Audit the operating system for any setup / configuration weaknesses
- Attempt to gain access to the server first with no privileges and then with an unprivileged account
- Attempt privilege escalation on the server with unprivileged credentials
- Perform authenticated testing of patch levels and software with an administrative account on each server

- Identification of weak passwords e.g., blank, default or common passwords
- Review of services offered
- Review of controls around administrative actions and how they are managed
- Review of SSL/TLS certificate and configuration
- Check for presence of and configuration of anti-virus software/HIDs/NIDs

Intertek NTA will examine the server from an authenticated perspective, having gained access with a set of credentials, which would be provided. This will include examining the anti-virus and device controls and the level of local access to the server including but not limited to local vulnerabilities that can allow privilege escalation.

If in scope, a review of the current device hardening policies applied and whether these can be circumvented or improved will be performed. As a part of this, operating system patch management and checking for version and patch updates in applications, such as MS Office and third-party applications such as Adobe Reader, will also be covered.

A review of the server firewall settings will also be conducted. Internet protection, such as ports allowed outbound to the Internet, proxy-server usage, browser settings and restrictions on Internet content would be examined in line with best practise.

Areas Typically Covered
Areas covered include, but are not limited to, the following:

- Testing of Internet-facing network services for operating system, configuration and software vulnerabilities
- Testing of cloud hosted applications for vulnerabilities using industry standard frameworks, e.g. OWASP Top Ten
- Testing of underlying virtual servers and infrastructure to ensure that it is not possible for an internal attacker (or an external attacker who has gained access to the internal infrastructure) to compromise the environment and gain unauthorised access to system functions, resources or data; or for an authorised user to manipulate or exploit the system to gain unauthorised access to non-permitted system functions or resources. Examples include:
  - Cloud service components and technologies (e.g., Route53, CloudTrail, Lambda, EC2 Instances, S3 buckets, Azure Storage, RDS, etc.)
  - Virtualisation and Containers (e.g., Docker, Kubernetes)
  - Security Groups and Network Access Control Lists (NACLs)
  - Identity and Access Management (IAM) and Microsoft Entra ID (formally Azure Active Directory)
  - CIS benchmarking (e.g., server/database configuration/platform)
- Testing of remote access services (e.g. configuration and security of Administrator portals; insufficient policies, conditional access policies, RBAC, networking and/or logging)
- Review of network topology (e.g. gateways, routes, tenant segregation, etc.)
- Review of Cloud logging solutions (e.g. CloudWatch, Azure Monitor, Platform logs)
- Configuration reviews of VPC's and virtual networks to ensure sensitive information is not publicly exposed, and that the Cloud environment complies with industry best practice standards

Service Definition
Cloud Security Assessment

Due to the variety of environments and depending on the resources in scope to be tested, testing of cloud services and technologies can be performed via the relevant Admin portal, command line interface, from virtual machines deployed into the environment or by allowing access from Intertek NTA's externally facing IP addresses to test the environment directly.

Constraints/Limitations of Testing
Testing of cloud services and environments is restricted in some circumstances due to the rules of engagement put in place by the cloud provider which prohibit certain types of testing and testing of some services and resources.

Examples of Vulnerabilities Found
Intertek NTA frequently identify vulnerabilities related to configuration management issues, such as security patching, unnecessary components being enabled on servers, the availability of additional network services and poor environment configurations. Specific examples of security issues found include Admin passwords on systems being left blank or with guessable passwords, allowing an attacker who connects to the system to run arbitrary commands or read and modify any data held on the system or database. Other examples include misconfigured Conditional Access policies allowing pivoting and compromise of cloud environments and misconfigured S3 buckets/EC2 instances allowing public access to confidential data/systems.

Other commonly occurring weaknesses are poor authentication mechanisms on applications housing sensitive information, poor management of file permissions which lead to data leakage, as well as default user accounts, and poorly configured perimeter devices, such as Web Application Firewalls (WAFs).

Deliverables
The results presented to the client will be categorised by risk and provide clear explanations of vulnerabilities found as well as concise recommendations to fix or mitigate issues. The report will include hyperlinks, both for navigation within the report and to access external references such as patch updates, recommendations and CVE/CVSS references where appropriate.

- An executive overview with business implications
- A summary of risks identified, ordered from high to low severity
- Technical details of each issue found
- Recommendations for closing holes found
- Full listing of test results tables including background information/evidence to support results

The style and format of the report is designed with clarity and ease of use in mind. Features include hyperlinks to relevant sections of the document as well as external sources where applicable.

A technical telephone debrief is available and included as standard following delivery of the report, to explain the areas covered during the testing and the key findings and potential business implication (severity) of the issues found. This will include suggested priorities for the customer to take action against.

Service Definition
Cloud Security Assessment

Service Management
You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

Intertek NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, Intertek NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling the test, ensuring reports are sent out in a timely manner, scheduling follow up tests and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

Ordering and Invoicing Process
Once the scope of work and number of units/days required has been agreed between the customer and Intertek NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

Customer Responsibilities
The customer is responsible for the completion of a Technical Details Form (TDF) prior to delivery. The provision of appropriate information will ensure that delivery meets expectations and requirements.

Technical Requirements
The resources typically required from the customer to ensure the service is performed as efficiently as possible include:

- For Internet-facing Cloud services or applications:
  - Technical contact details for any necessary communication during the testing (e.g. high risk issue notifications)
  - A list of target Internet IP addresses
  - Details of all Fully Qualified Domain Names (FQDNs) and any other unique entryways into applications, remote access or other systems for the entire in-scope infrastructure

- For underlying virtual servers and infrastructure:
  - Technical contact details for any necessary communication during the testing (e.g. high risk issue notifications)
  - Where physical access to the target environment is not possible:
    - Provision of a suitable VPN connection from Intertek NTA's office
    - Pre-configured 'virtual test machines' provided by Intertek NTA installed within the target environment (full support and details for successful implementation available)
    - Provision of relevant documentation for review as appropriate (e.g. network diagram, firewall configurations, etc.)

Service Definition
Cloud Security Assessment