The Cloud is Secure – Cloud Environment is Not

DataArt

Microsoft Gold Partner

Assessment Goals

- Collect detailed information about the environment under review and the related processes by
  - reviewing relevant documentation
  - interviewing the personnel
  - analyzing the system configurations
  - checking the formal processes and policies which affect the environment
- Collect evidence that security controls and policies function as declared
- Collect evidence showing any potential gaps and security flaws

Note: DataArt requires a temporary read-only access to perform the assessment

Assessment Actions

- DataArt **runs** security analysis tools to collect additional reports
- DataArt **reviews** all the gathered artifacts
- DataArt **assesses** the cloud environment architecture and security controls
- DataArt **checks** whether the team follows common cloud security guidelines

We examine:

- Trust boundaries
- User authentication and access control
- Separation of roles and duties
- Data protection measures
  - in transit
  - at rest
- Secure remote and administrative access
- Attack detection and response mechanisms
- Secure backups and disaster recovery plan

Reporting

- DataArt **collaborates** with client's team on disputable items related to the security policy, technical controls and criticality of the findings
- DataArt **provides** the assessment report with the list of identified issues
- DataArt **arranges** a follow-up meeting with the team to discuss the report
- DataArt **provides** the recommendations on how to resolve the identified issues

DataArt

Goals:

- Provide a formal, written description of the assessment findings
- Provide recommendations on how to prioritize the remediation activities

Be safe in the Cloud!

To learn more about Microsoft Azure Security Assessment,
please send an email to sales@dataart.com

www.dataart.com