Cloud Security Maturity Model

Version 2.0

LEVEL 1
Manageably managing policies/procedures, mostly through console.
Architectures tend to resemble traditional infrastructure (e.g. low use of services and high reliance on network security controls).
IAM mostly ad hoc with little to no federation.

Governance
- Overall governance of cloud providers, deployments, applications, and general usage.
  - No formal cloud governance. Either cloud is not allowed, not officially supported, or users completely self-manage cloud usage.

Organization Security
- Single or unconnected deployments with inconsistent core security.
  - Checkpoint for core deployment security on primary cloud platform.
  - Most accounts associated with organization, but manually managed.

Security Monitoring
- No monitoring/alerting on telemetry gathered by the cloud.
  - Multi-account monitoring/alerting with logs aggregated across some accounts.

Network Security
- Cloud network architectures replicating on-premise environments.
  - Networks manually built to define cloud standard and patterns.

Workload Security
- Most workloads are long-running virtual machines leveraging existing datacenter security controls centered directly to cloud.
  - Generally reliant on traditional security tools and practices.

Data Security
- Basic access controls, usually improperly configured.
  - "Checklist" data security encryption/hashing using default keys.

Risk Assessment & Provider Management
- Using existing risk assessment models and provide selection process.
  - Provider driven by business unit, but security assesses the provider and can trigger an escalation. Security inconsistently engaged in early-phase risk assessments (e.g. architecture risk).

Resilience
- No formal resiliency for cloud deployments.
  - Some basic data backup/lifecycles. Some use of autoscaling/automation for workloads, but not single provider/region deployments.

Compliance & Audit
- No reporting or compliance actions taken for cloud-specific resources.
  - No cloud-specific standards. Ad hoc assessment/automation for workloads.

Incident Response
- No cloud-specific response, very inconsistent data collection and escalation.
  - Manual BI response to cloud events.

LEVEL 2
Reusable
Policies/whitepapers, data, and manual or simple tools.
High variability between projects, not coordinated across deployments.
Initial use of infrastructure as code (IaC) for cloud/configurations, but security not consistently engaged in design/audits.
Federation on some accounts, but limited use of IAM due to difficulties supporting teams (especially on the command line).

Governance
- Strong central governance with consistent enforcement.
  - Central cloud team has IaC for all core security policies.
  - Federal Müslüman guard and compliance.
  - Consistent use of advanced conditional authorization and consistent policy.

Organization Security
- Deployments provisioned via IaC including most core security policies.
  - Securities and permissions defined per role.

Security Monitoring
- Fully automated provisioning of IAM. Extensive use of advanced conditional authorizations for enabling/disabling role.

Network Security
- Deployments used extensively to control/blast radius. Deployment automation aligned with cloud infrastructure orchestration.

Workload Security
- Consistency across projects and workloads.
  - Robust security telemetry collected for the management plane, and across workloads.

Data Security
- Extensive use of cloud-native logging and analytics.
  - Initial adoption of the Minimum Viable Cloud Native Network. Legacy security tools/enforcement within automated guardrails.

Risk Assessment & Provider Management
- Extensive use of cloud-native resources and PaaS.
  - Initial use of CSPM or similar for core security.

Resilience
- Initial use of multi-region resiliency.
  - Multi-account monitoring/alerting for each current cloud provider.

Compliance & Audit
- Initial use of cloud-native tools in use.
  - Initial security controls implemented on containers.

Incident Response
- Initial use of customer managed keys.
  - Initial use of IAAS for all data encrypted.

LEVEL 3
Defined
Policies and central coordination in place.
Some initial security automation still executed manually.

Governance
- Cloud team, COE, or equivalent in place to guide usage. Initial policies in use. Basic use of standards and benchmarks (e.g. CIS) for configuration baseline.

Organization Security
- Federated through consistent management with core security policies. Security checkpoints for each current cloud provider.
  - Initial use of CSPM or similar for security visibility.

Security Monitoring
- Management plane logs and core service/workload logs collected across all relevant deployments.
  - Initial alerts triggering for detections for security deviations, but incrementally in place.

Network Security
- Extensive use of cloud-native resources and PaaS.
  - Initial adoption of the Minimum Viable Cloud Native Network. Legacy security tools/enforcement within automated guardrails.

Workload Security
- Initial use of traditional immutability and hybrid networking approaches depending on the application.

Data Security
- Initial use of cloud-native encryption/decryption standards.
  - Initial use of policy-based access controls and data access logs.

Risk Assessment & Provider Management
- Initial use of IaC for all current cloud providers.

Resilience
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Compliance & Audit
- Initial use of CSPM or similar for core security.

Incident Response
- Initial use of horizontal scale.

LEVEL 4
Capable
Strategic centralized management with consistent enforcement.
Automated and guards across multiple deployments.

Governance
- Security driven risk assessment for evaluating providers and deployments.
  - Security provisioned through automated and guards.

Organization Security
- Extensive use of cloud-native resources and PaaS.
  - Initial adoption of the Minimum Viable Cloud Native Network. Legacy security tools/enforcement within automated guardrails.

Security Monitoring
- Extensive use of cloud-native resources and PaaS.
  - Initial use of security controls implemented on containers.

Network Security
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Workload Security
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Data Security
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Risk Assessment & Provider Management
- Initial use of CSPM or similar for core security.

Resilience
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Compliance & Audit
- Initial use of CSPM or similar for core security.

Incident Response
- Initial use of horizontal scale.

LEVEL 5
Perfect
An image shows activity centrally managed, covering all of the CSMF domains.
Integrated into infrastructure as code environment.
Built in to the stack with provisioning automation.
Federation and IaC working correctly across environments (e.g command line support).

Governance
- Security-driven risk assessment for evaluating providers and deployments.
  - Security provisioned through automated and guards.

Organization Security
- Extensive use of cloud-native resources and PaaS.
  - Initial adoption of the Minimum Viable Cloud Native Network. Legacy security tools/enforcement within automated guardrails.

Security Monitoring
- Extensive use of cloud-native resources and PaaS.
  - Initial adoption of the Minimum Viable Cloud Native Network. Legacy security tools/enforcement within automated guardrails.

Network Security
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Workload Security
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Data Security
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Risk Assessment & Provider Management
- Initial use of multi-region resiliency.

Resilience
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Compliance & Audit
- Initial use of multi-region resiliency.
  - Initial use of multi-account resiliency.

Incident Response
- Initial use of multi-region resiliency.

© 2024 IANS. All rights reserved. 617.399.8100 • www.iansresearch.com