REMOTE™
BY DESIGN

Managed Security Services

Cloud Security Assessment

May 2020

<epam>

Cloud Cyber Security Threat Assessment: Agenda

1 PROBLEM STATEMENT

2 BUSINESS IMPACT

3 APPROACH

4 SUMMARY, COMMERCIALS & ASSUMPTIONS

5 RELATED SECURITY OFFERINGS

Top critical issues that lead to security breaches in the cloud:

Unauthorized access

Misconfiguration of the cloud platform/ wrong setup

Insecure interface/ APIs

Is data in the Cloud **Safe**? Are we following **best practices**? Are we **Ready to Release**?

ARE WE SAFE?

- Are our customers and their data safe?
- Are we secure?
  - Secure configuration
  - IAM\CIAM, Network, Kubernetes, Databases etc
  - Data Protection, Secret Management
- Are we compliant with standards and regulations (SOC 2, HIPAA, ISO 27001, GDPR, CCPA, PCI DSS)?

EPAM CLOUD SECURITY ASSESSMENT

Quick and practical way of taking control on cloud security using proven DevTestSecOps approach:

- EPAM Cloud Security Assessment provides a quick way to assess the current cloud security posture, provides analysis and report prioritized and categorized list of issues.
- Cloud Security Assessment informs the Roadmap for highly automated solutions and security programs for the cloud

Cloud Security Breach: Potential Business Impacts

Businesses will even more vigorously look for the new revenue streams to both offset the negative consequences of COVID-19 and seize the opportunity in the rapidly changing environment. The speed of adoption of cloud and digital solutions will be key to survival and competitive advantage.

At the same time, the already overstretched IT and security operations are in a perfect storm with all technical debt created over the years having a suddenly inflated impact on business operations and security risk. With radically more utilization of technology and drastic changes in IT and cloud operations related to work from home, all familiar and brand-new security risks raised disproportionally.

Frankly speaking now is not a good time at all to get a security breach that is normally accompanied with:

LOSS OF CUSTOMERS

Loss of customer and stakeholder trust can be the most harmful impact of cybercrime, since the overwhelming majority of people would not do business with a company that had been breached, especially if it failed to protect its customers' data.

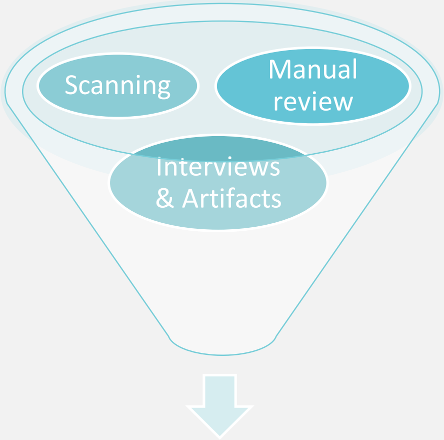
BRAND IMAGE IMPACT

Apart of the direct loss of business, as well as devaluation of the brand you've worked so hard to build. Taking a reputational hit may also affect your ability to attract the best talent, suppliers, and investors.

DIRECT FINANCIAL LOSSES

Direct financial losses as a result of a theft or monetary penalties/fines for businesses that fail to comply with data protection legislation.

Holistic Approach to Cloud Security assessment

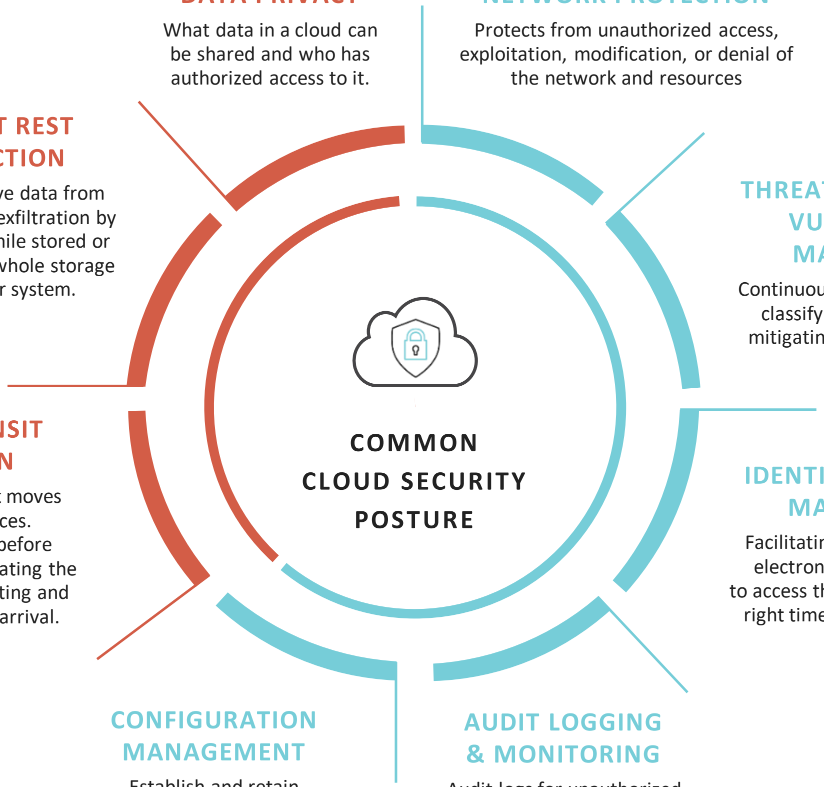


Scanning

Manual review

Interviews & Artifacts

Report: gaps, recommendations, roadmap



COMMON CLOUD SECURITY POSTURE

DATA PRIVACY

What data in a cloud can be shared and who has authorized access to it.

NETWORK PROTECTION

Protects from unauthorized access, exploitation, modification, or denial of the network and resources

DATA AT REST PROTECTION

Protects inactive data from compromise or exfiltration by encrypting it while stored or encrypting the whole storage container or system.

THREAT PROTECTION & VULNERABILITY MANAGEMENT

Continuous identifying, assessing, classifying, remediating, and mitigating security weaknesses.

DATA IN TRANSIT PROTECTION

Protects data while it moves between the services. Encrypting the data before transmission; authenticating the endpoints; and decrypting and verifying the data on arrival.

IDENTITY AND ACCESS MANAGEMENT

Facilitating the management of electronic or digital identities to access the right resources at the right times for the right reasons

CONFIGURATION MANAGEMENT

Establish and retain consistency of a cloud resource's settings throughout its lifecycle.

AUDIT LOGGING & MONITORING

Audit logs for unauthorized security-related activities and monitor the system that contains confidential information.

🟥 Data protection

🟦 Cloud Infrastructure protection

Cloud Infrastructure Assessment

amazon web services · Microsoft Azure · Google Cloud

DESCRIPTION

3-phase engagement includes:

- Discovery of cloud workloads, configurations
- Workshops and interviews with SMEs and Stakeholders
- Architecture assessment of cloud infrastructure against cloud provider security best practices and CIS benchmarks
- Documentation review and cross-check against implementation
- CI\CD Security Review
- Infrastructure security automation assessment

Week 1:
Workshops and interviews

Week 2-6:
Perform scan and a tool-assisted analysis

Week 7-8:
Finalize the report and develop a Roadmap

TEAM COMPOSITION

- Cloud Security Architect
- Cloud Security Engineer

DELIVERABLES

- Assessment report answering the questions:
  - How 'safe'?
  - Conforms to standards and best practices?
  - How efficient is the CI/CD and SDLC automation?
- Mitigation recommendations overview
- Roadmap for fixes

KEY ASSUMPTIONS

- Customer representatives are available as required
- EPAM personnel will be granted a Read-Only access to cloud infrastructure configuration (no access to data or infrastructure is needed)

Healthcare Company

Cloud Security Assessment

A major healthcare provider asked EPAM to assess security controls for a good cloud security posture (HITRUST)

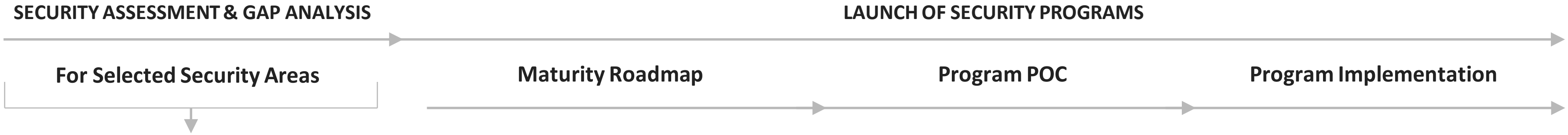
Review current development process and security policies & processes for cloud best practices

• HIGHLIGHTS

- Performed Cloud Security Posture Assessments, provided findings and recommendations
- Performed DevOps assessment and provided Recommendations (Processes, Automation, Provisioning\Configuration management, Deployment, Security Controls, Access etc.)
- Secure control mapping to recommended implementations (the goal is to balance strict security with implementations that are convenient for developers and don’t impede velocity)
- Proposed an automated Security Governance solution:
  - ✓ Automation and security quality gates in CI\CD for proactive security measures and fast feedback
  - ✓ A framework for detection and resolution of deviations from desired security posture
  - ✓ DevOps Transformation roadmap
  - ✓ Model to ensure that agreements between InfoSec\Operations\Development teams is respected and enforced

EPAM Can Support the Full Spectrum of Security Programs End-To-End

HIGH-LEVEL APPROACH



SECURITY ASSESSMENT & GAP ANALYSIS

LAUNCH OF SECURITY PROGRAMS

For Selected Security Areas

Maturity Roadmap

Program POC

Program Implementation

SECURE SDLC

- Application Security and **Secure CI\CD**
- Security Testing
- Security Architecture

SECURE CLOUD

- Continuous Cloud Security Posture Management
- Secure infrastructure provisioning

SECURE DATA & ACCESS

- Data Protection
- Identity Access Management
- Privileged Access Management, Vaults

SECURITY OPERATIONS

- Continuous Vulnerability Management
- Security Operations Center
- Security Analytics & SIEM

Proven Track Record of Successful Projects

TECHNOLOGY COMPANY

- Implemented process of automatic distribution of hardened VM images on regular basis
- Implemented Continuous Cloud Security Monitoring using Evident.io
- Implemented security programs, developed security and networking architecture, prepared for ISO 27001 audit and FedRAMP

HEALTHCARE TECHNOLOGY COMPANY

Helped developing Roadmap for Azure Security Program:

- Performed assessment and provided gap analysis and recommendations for Azure Cloud workloads, Azure DevOps automation, including security best practices for highly secure HITRUST environment
- Provided implementation roadmap to build modern highly automated cloud security program and Azure DevOps automation to allow efficient and secure development and operation in the cloud

MORTGAGE INSURANCE COMPANY

Implemented following Security Programs:

- Full cycle implementation, rollout and operations of Privilege access management solution across an enterprise for Interactive, Windows, Unix, Network, Application Service accounts, etc.
- Data Protection solution based on Protegrity
- Security Data Analytics Solution
- Application Security Program

GLOBAL TRAVEL TECHNOLOGY COMPANY

On a large-scale cloud deployment helped with following:

- Established continuous automated scanning and automation remediation processes for configuration rules
- Automatic remediation of violations of predefined rules
- Implemented access review application and review process

THANK YOU