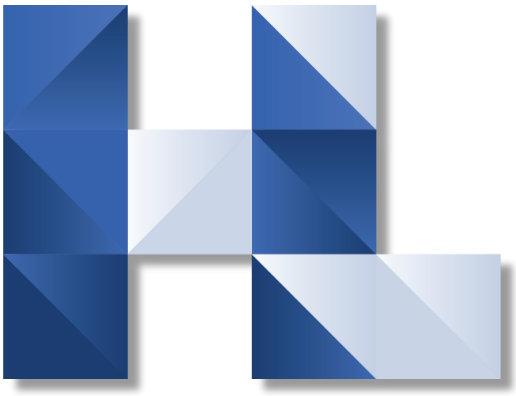
Hidden Lake Technology

Amazon Web Services Security Practice



HIDDEN LAKE
TECHNOLOGY

Abstract: HLT Professional Services may be engaged to conduct AWS Security Services on a project or managed basis to update and maintain the customer's security posture. These services may include overall system analysis and documentation, auditing for compliance, identification of vulnerabilities, penetration testing, reconfiguration and/or rearchitecting. All investigations and recommendations are based on successful past performances, industry best practices and our professional services team guidelines.

OVERVIEW

BIG IDEA

Hidden Lake Technology's AWS Cloud Security Professional Services can be deployed to update and maintain a customer's security posture

CAN BE DEPLOYED FOR

Security Analysis

Documentation and Architecture

Penetration Testing

Maintaining Industry Best Practices

Reconfiguration

Reaching Compliance

Keeping Compliance

WHO NEEDS THIS

All AWS environments need to be secured against bad actors

PROJECT SUMMARY

An initial consultation with HLT sales will establish a scope of work, project timeline and estimate custom to your environment and particular needs. After the contract is in place, HLT professional services will conduct a kickoff meeting with customer stakeholders to review the scope of work, estimated timeline, customer questions and establish a project start date.

Engagements may be either on a project or full time/managed basis, depending on customer needs and what is most appropriate to accomplishing the objectives. Pricing may be either time and materials or firm fixed price with clearly defined project milestones. HLT encourages customers to utilize remote access for ease of project delivery and scheduling, but also offers on-site services as well.

SAMPLE PERFORMANCE

PAST PERFORMANCE- STATE UNIVERSITY HIPAA COMPLIANCE ANALYSIS

Hidden Lake Technology deployed our professional services engineers in support of this state university's cloud security efforts. We conducted an AWS Cloud Security Analysis on their existing security posture with respect to HIPAA compliance and provided recommendations both from that compliance matrix and industry best practices. As agreed the customer then had a period of time to enact those changes, after which we returned to review and document their compliance for both their internal records and as material for their customers/users.

This successful engagement resulted in the customer having an intimate understanding of their security strengths and vulnerabilities, as well as documentation to evidence their compliance status.

CUSTOMER

State University

DELIVERY METHOD

Remote via AWS console

DELIVERY TIMELINE

Initial extensive review with recommendations, followup one month later

OUTCOME

Success- customer has been advised of security posture and remediation needs

DELIVERABLES

Interim report with security/compliance status and recommended remediation

Final report with security/compliance status, overall grade and recommended best practices

SCOPE OF WORK AND PROPOSAL INFORMATION

Following page(s)- redacted, example only

SERVICES PROPOSAL INFORMATION

Scope of Work & Project Timeline

SCOPE OF WORK

Hidden Lake Technology will deploy their Professional Services engineers to perform the following work remotely in support of the customer's IT environment. The overall goal of this project is an AWS Cloud Security Analysis. In addition to the services provided, the professional services team will include detailed documentation of all the work completed during the project timeline. The documentation can include: manuals, knowledge transfer and training information, step-by-step configuration details and ongoing best practices according to HLT and Amazon Web Services.

The Scope of Work (SoW) will include:

- Analysis
  - External network/firewall vulnerability assessment
    - Perform network-based security scans to identify security weaknesses of components supporting the critical IT infrastructure
  - External penetration test to web applications
    - Conduct penetration tests to identify security holes of web applications
  - Application and infrastructure security review
    - Review the security settings of applications and the underlying infrastructure. The review aims to identify vulnerabilities, misconfigurations, and weak security processes
  - Backup validation
    - Review the security setting of the AWS S3 storage solution for backups. Verify the backup is encrypted.
  - Other
    - Conduct other testing as HLT engineer and customer deem necessary and appropriate and as time allows
- Security documentation
  - Review the security policies and procedures that have been developed for the

customer to determine whether customer has the appropriate security controls in place and that they are operative effectively. This documentation is limited to the IT environment and does not apply to customer administrative functions.

- Recommendations
  - Assemble report with comments
    - Security strengths
    - Security vulnerabilities
    - Recommended remediation tasks
- Deliverables
  - HLT will produce a report detailing the findings including the corrective, preventive and detective measures
  - HLT will provide a remote briefing session to the customer management which summarizes the findings as well as the resolutions, recommendations and best practices
  - HLT will create an executive summary of findings that may be shared with clients
  - If applicable, HLT will provide a remediation estimate
- Minimizing impact to production environment
  - Any assessments and penetration tests performed against a production environment shall be non-destructive, non-intrusive and the influence on availability and performance of the production system are strictly minimized.