SISA

CUSTOMER SUCCESS STORY

SISA's two-phased assessment helps a global provider of laboratory-specific software solutions achieve defence-in-depth security for cloud environment

ABOUT THE CUSTOMER

The client is a global provider of laboratory-specific, cloud-based software solutions for the life sciences and other science-based industries. Their solutions help power the digital transformation of scientific laboratories by enabling them with real-time lab data connectivity, infrastructure, and tools to accelerate time-to-market. Headquartered in the US, the client offers vendor-agnostic, lab-specific software that enables science-based industries to integrate new and legacy instruments, applications, and web services into a common, cloud-based platform.

THE CHALLENGE

One of the key challenges the client faced was misconfiguration of cloud, which exposed sensitive resources to various security issues related to confidentiality, integrity, availability, and accountability. This also resulted in challenges in compliance management, arising from multiple factors that included:

- Sensitive data exposure to the public internet
- Granting of public access to storage buckets
- Misconfigured policy
- Disablement of spam and virus scanning/detection
- Storing encryption passwords and keys in open repositories

Secondly, the client was also facing difficulty in distribution and storage of different types of keys and resources. Because virtual machines don't have a fixed hardware infrastructure, and cloud-based content is often geographically distributed, it is more difficult to apply standard controls such as hardware security module (HSM) storage to the keys on cloud infrastructures. This created challenges in implementing standard security metrics and resulted in higher cost and difficulty in running security assessments and audits.

SOLUTION OFFERED BY SISA

SISA adopted a 3-phased approach consisting of Gap assessment, Remediation and Reporting to help address the client's cloud security challenges. SISA kicked off the engagement with a two-stage security assessment, wherein the first part involved gap assessment and the second included AWS assessment. The cloud security assessment was performed using a combination of manual and automated tools.

The findings from the assessment revealed several loopholes in the cloud configuration, that included IAM Principals Privilege Escalation, overly permissive policy, disablement of MFA, disablement of monitoring for EC2 instances, IAM user creation with Administrator access and use of outdated Kubernetes version among others. SISA then educated the client on the severity of the vulnerabilities and their impact on the infrastructure, offered detailed guidance on remediation and shared a final report to enable tracking of actions.

BUSINESS IMPACT

SISA's cloud assessment followed by remediation consulting support helped the client close the gaps and improve the overall security posture of AWS environment. Further, its consultative approach involving multiple rounds of discussions helped the client mitigate the vulnerabilities without hampering the business functionalities. By enforcing SISA's recommended granular policies and various other security measures, the client was able to achieve defence-in-depth security – thereby fool proofing the infrastructure against single-layer compromise.

SISA

A forensics driven cybersecurity company, trusted by organizations across the globe for securing their businesses with robust preventive, detective, and corrective security services and solutions.

Compliance

PCI Compliance

- PCI DSS
- PCI PIN
- PCI 3DS
- PCI P2PE
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- Facilitated PCI SAQ

PCI Compliance

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Swift
- Cloud Security
- Risk Assessment
- Quarterly Security Audits

Security Testing

Application Security

- Application
- Penetration Testing
- CREST/CERT-in Approved
- Security Testing
- API Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- ASV Scan

IoT Security Testing

Managed Security Services

Phishing Simulation

Cyber Resilience

Managed Detection and Response Solution

SISA ProACT

Incident Response and Forensics

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation

Advanced Threat Hunting

Data Protection

Data Discovery and Classification Tool - SISA Radar

- Card Data Discovery
- PII (Privacy) Data Discovery
- Data Classification

Data Discovery as a Service

Training

Payment Data Security Implementation Programs

- CPISI
- CPISI Advanced
- CPISI-D

Security Incident Detection and Response Programs

- CIDR

Forensic Learning Sessions for Senior Management

For more Information visit us at www.sisainfosec.com
OR
write to us at *contact@sisainfosec.com*

Follow us