

CASE STUDY:



COST EFFECTIVE INFORMATION SECURITY INSIGHTS

About the Customer

Capitis Solutions develops, implements and hosts a cloud analytics platform that serves global UV light manufacturing operations. In addition, Capitis Solutions performs development activities for a security compliance solution that is offered as a product to our customers in government and regulated sectors.

The Challenge

Capitis cloud analytics platform development and production hosting activities are performed on AWS accounts organized under a single AWS organization that controls ten AWS accounts. The Capitis team sought to centralize its information security operations activities in a central AWS account that monitors the other nine Capitis AWS accounts. The Capitis team wanted to monitor, analyze and generate alerts for any suspicious activity in a cost-effective way while following AWS well architected principles.

The Solution

The solution included enabling AWS CloudTrail events in all accounts and redirecting them to a central S3 bucket. The CloudTrail event data is stored continuously in JSON format at a frequency of 10-15 minutes. The data from S3 is queried using Athena for analysis. A set of dashboards that provide insights into any suspicious security activities are created in one central AWS account using AWS QuickSight. The dashboards directly source data from Athena so the data is refreshed with the latest data whenever dashboards are accessed.

The technologies used for this solution are:

- AWS Organizations
- AWS CloudTrail
- AWS CloudWatch
- AWS S3
- AWS Athena
- AWS QuickSight

The Benefits

- A central security operations dashboard that gathers data across all account serves as a single pane of glass for the Capitis information security operations team.
- The monthly billing charges for the all the components included in this solution is less than \$25 per month.
- Athena charges are on per query basis. This gives us a huge savings compared to any other database solution.
- S3 storage is cheap and our expenses related to this solution are negligible. In addition, S3 lifecycle storage policy provided further cost optimization by moving the old data to cheaper storage.

We were able to keep our development and hosting costs down without compromising on security controls by using AWS QuickSight & AWS Athena.

www.capitissolutions.com



Advanced
Consulting
Partner



Advanced
Consulting
Partner

Public Sector Partner