Advanced Security with Azure Sentinel



Integration of Azure Sentinel strengthens the security framework of one of the large Government Organizations in Qatar housing applications with sensitive data and equips it with better defense and an even better offense.

## Intelligent and optimized security environment

A completely customized security environment where all future workloads can be secured through the power of artificial intelligence, automated incident response, and investigative toolsets. This state of the state-of-the-art SIEM and SOAR solutions powered by Azure Sentinel and hybrid security operations powered by Azure Security Center are setting a new standard in incident detection, response and remediation for fellow Government organizations .

## The client is a competent of the development of the overall vision for the state, in

About the Client

2.8 Mn + Citizens

Monitoring Data of

cooperation with the concerned authorities; preparation of national development strategies; follow-up of their implementation, in coordination with the concerned authorities; preparation of studies and population policies related to such strategies; supporting the planning process in government agencies; working on linking development priorities to the state budget; monitoring the progress of implementation of plans. It is also mandated to establish an integrated statistical system; conduct, organize

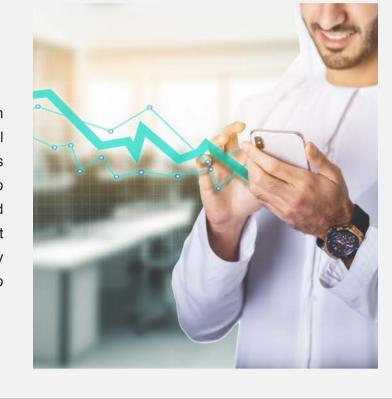
and supervise formal statistical operations; implement various censuses and surveys; and disseminate statistical data and products.

## **Need for Stringent Security Measures**

The Challenge

### The client was dealing with huge amounts of data on

a daily basis. With Qatar now being at a pivotal moment in its history, the organization has ever-increasing responsibilities and burden to monitor and disseminate statistical data and products. The client's vision was to do this in the most efficient yet secure manner used advanced security and monitoring frameworks that are not only easy to deploy but also easy to use.



**The Solution** 

A customized Azure Sentinel environment for enhanced protection and incident management.

### The Client leveraged Cloud4C's Azure cloud architects to provide an accelerated

**Acclerated Implementation** 

implementation of Azure Sentinel for protection of sensitive assets. Cloud4C team worked closely with Microsoft throughout the project, which enabled us to deploy the latest SIEM and SOAR technology. We performed a full investigation of the client's IT landscape, Process and Data flows, including customizations and alerts. By understanding the client's requirements and the elements they wanted to stay consistent with improved capabilities, introducing Azure Sentinel was seamless and cost-effective as possible.

### generate a daily report of security issues has been greatly reduced, since Azure

Targeted and meaningful alerts

abnormalities and accelerate incident response. The time it takes the client to

Targeted alerts were created to help identify

Sentinel is able to reproduce alerts that would have been otherwise been generated in other Azure security products. This inititiative helped the client to dedicate sources for incident management rather than infrastructure monitoring. Their overall security posture and awareness of their IT environment have instantly given them competitive advantage over their peers. **Key Accelerators** 

### Sentinel, one of the world's first cloud-native SIEM and SOAR systems. The solution

Cloud4C chose to deploy Microsoft Azure

to Incidents

**Accelerated Investigation & Response** 

delivered included not just Microsoft recommended best practices but evolved versions of various security policies, aligned to stringent government security guidelines. Even while the full deployment was in progress, the client team was impressed with how fast we got the system got it up and running. Today, the client's IT organization has a better understanding of their data and unusual activity with custom reports (i.e., workbooks) in Azure Sentinel. Security data generated anywhere in their IT environment is aggregated in one centralized location for optimal visibility and

### Sentinel, the client will now be paying only for the data ingested for monitoring.

All-inclusive Features in a

Pay-as-you-go Model

With the client's decreased dependency on

traditional security tools and measures and

increased security portfolio on Azure

### Cloud4C's optimized delivery model, supported by robust processes such as ITIL, ITSM, CoBIT and our proprietary service delivery processes are tuned to deliver a Single SLA up to Application layer.



### **Azure Native Security Tools** We adopt multiple standards, policies and processes to be delivered as a single

real-time. Our competencies include,

Robust Cloud Adoption Framework

Ability Creating Use cases specific to Infrastructure.

with actionable intelligence to improvise security posture.

overall manpower cost and reduces incident response SLA.

Developing custom parsers even for unstructured logs.

**Azure Expert MSP** 

contextual services and offerings to achieve continual improvements. With a home grown IP and research, Cloud4C's MITRE ATT&CK framework adoption comprises of 12 categories, 174 techniques, 15 tactics and 41 migration approaches. **Cloud4C expertise in Azure Sentinel Deployment and Management** Cloud4C has security expertise in Azure Sentinel that can write the custom alert rules and automated playbooks to help you detect threats in your environment in

framework fueled with optimized processes and tools as we build and operate the

Equipped with 600+ Azure certified resources, Cloud4C is an Azure Expert MSP offering Enterprise Grade Managed services to augment complex technology environments.



### • Fine-tuning complete ATT&CK based rules specific to Infrastructure and compliance policies.

 Dedicated Technical account manager from SOC with a complete understanding of client infrastructure.

• Incident Auto remediation in minutes without human intervention that saves

 Perform Incident management with detailed Root cause analysis and Mitigation. Provide weekly and monthly walkthrough on Security posture and developments

 Detailed forensics offered on-demand Team of Threat intelligence experts performing threat hunting.

• Threat modeling based recommendations with a complete understanding of

- infrastructure. Custom data collection even for the applications which cannot forward logs.

**SCALABLE** 

Results



cloud-based

security

# **ZERO**



security lapses with advance intrusion detection



**INCREASED** visibility via a single

pane of

glass



security

capabilities



SIGNIFICANT cost

over time

**FEWER TO NO** 

manual

processes for incident

response

threats

intrusion

and



### INTELLIGENT threat detection



and hunting powered by Microsoft Threat Intelligence as well as Cloud4C experts

