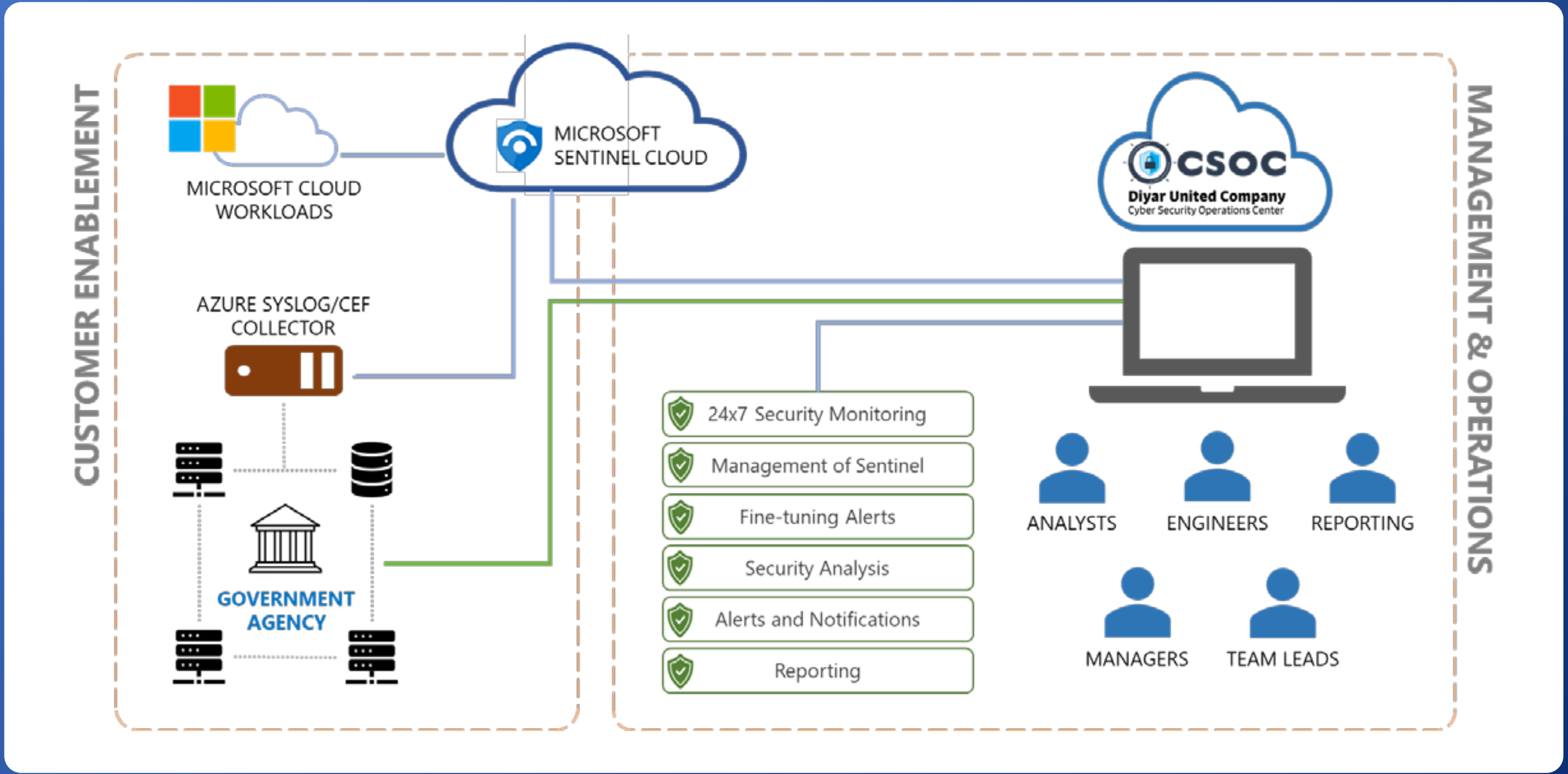
CSOC Services for Microsoft Sentinel

A service package designed to work with Microsoft Sentinel, which gives visibility over your organization's security infrastructure.

Leverage Microsoft's technology, see and stop threats before they cause harm, with SIEM reinvented for a modern world. Microsoft Sentinel is your birds-eye view across the enterprise. Put the cloud and large-scale intelligence from decades of Microsoft security experience to work.

Coupled with Diyar CSOC services, complement the technology with eyes from the experienced and skilled security engineers and analysts to ensure you're at the helm of control of security in real-time.

Services Architecture



Enablement

- Activation of Microsoft Sentinel Platform
- Configuration of Sentinel
- Setup and configure Azure Syslog/CEF Collector
- Onboarding of On-Premise and Cloud workloads
- Fine tuning alerts and notifications

Management & Operations

- Sentinel Management and Operations
- Fine-tuning Policies / Rules
- 24x7 Security Monitoring
- Security Analysis
- Threat Intelligence
- Threat Hunting
- SOAR Automation Playbooks
- Weekly, Monthly, Quarterly Reporting
- Reports Customization
- Incident Response Service
- Vulnerability Assessment (Internal)

24x7 Security Monitoring

Diyar CSOC security team actively monitors cyber activity on onboarded workloads. Provide notification and alerts, as well as escalations based on the agreed escalation matrix.

Microsoft Sentinel Management

Manage and maintain policies and alerts to ensure critical events are detected in a timely fashion. Fine-tuning of rules and SOAR playbook automation.

Security Analysis

To maintain situational awareness of current activity and risks to you, CSOC will detect, monitor, analyze, and mitigate targeted, highly organized, or sophisticated threats. CSOC will analyze the alerts based on various intelligence sources to provide indication and warnings against your systems

Threat Intelligence

A dedicated Cyber Threat Intelligence (CTI) team that monitors the external World Wide Web, deep and dark web to provide customized and highly directed threat intelligence to its clients within the region. Threat intelligence advisory notification is essential for keeping you updated about latest threats and having incident correlated against threat information provides broader visibility over the threats.

Threat Hunting

CSOC team proactively performs threat hunting activity looking for potential compromise that reside on your network. The generally accepted method is to leverage a security information and event management solution that centrally collects log data from disparate sources including endpoints, servers, firewalls, security solutions, antivirus (AV), etc. providing visibility into network, endpoint, and application activity that might indicate an attack.

Reporting

As a primary function, regular reports will be generated and provided to the relevant stakeholders. CSOC shall review all incident records regularly to ensure they were resolved within the parameters defined in the SLA. CSOC would also audit incident records that have exceeded standard resolution times to validate that the incident records were handled appropriately.

Incident Response Services

Diyar IR services provide remote and on-site investigation to help mitigate cyber security incidents and quickly restore business as usual. Our incident response team is well trained and can be available for critical breaches in a matter of hours.

Vulnerability Management

The CSOC will perform vulnerability scanning to discover vulnerabilities and provide recommended actions to system owners for remediation based on threat risk level and impact for all assets. The process includes vulnerability analysis to evaluate severity and determine applicability.

Service Plans Pricing

Services/Features	BASIC	SILVER	GOLD
GB Logs Ingested / Day	10 GB / Day	30 GB / Day	50 GB / Day
Customer Enablement	Included	Included	Included
CSOC Services	Included	Included	Included
Incident Response Services	40 Hours / Year	40 Hours / Year	40 Hours / Year
Vulnerability Management	4 Times / Year	4 Times / Year	4 Times / Year
Penetration Testing	1 Time / Year	2 Times / Year	2 Times / Year
Price (KWD)	**28,000**	**53,000**	**74,400**

Terms & Conditions

- The pricing scheme may change without notice
- Any price change will not be applicable for any ongoing contracts
- EA and/or Microsoft Sentinel licenses are not included in the pricing
- Consumption cost of Microsoft Sentinel is not included in the pricing

CSOC

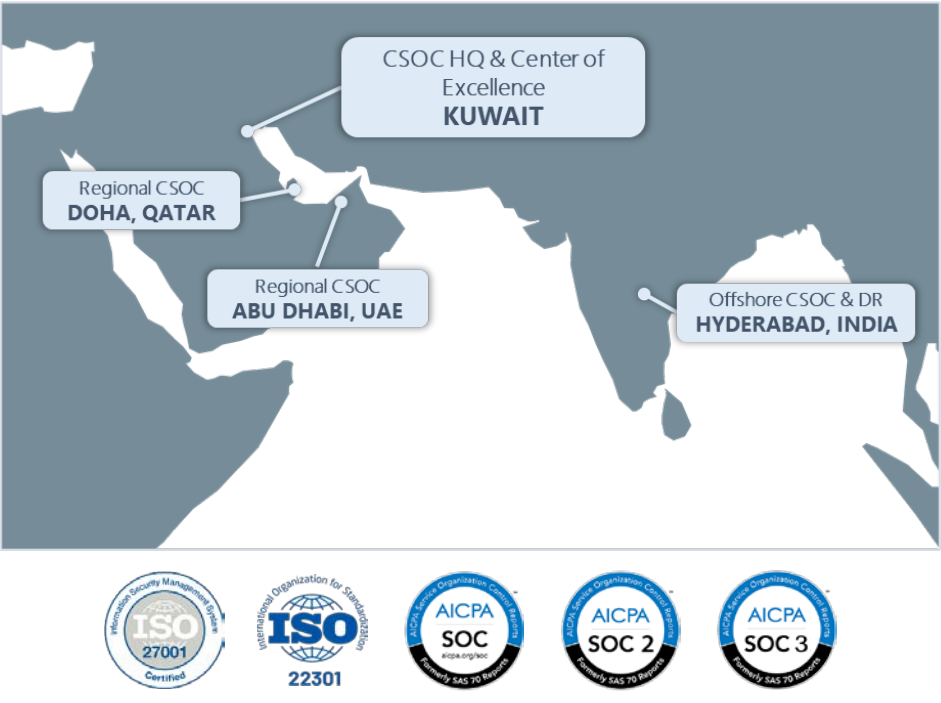
Diyar United Company

Cyber Security Operations Center

Diyar is proud to offer Kuwait government agencies, a comprehensive 24-hour cybersecurity monitoring and surveillance service, provided by our state-of-the-art Cyber Security Operation Center (CSOC).

Our Cyber Security Operations Center (CSOC) is manned by a strong team of skilled and experienced security specialists in various cyber security niches, that continuously "watch" the activity of your organization’s infrastructure to ensure visibility, detection, and appropriate response to vulnerabilities and threats in real time.

REGIONAL COVERAGE



Diyar Highlights

12+

Years of experience in providing CSOC services to our customers

75+

Dedicated, experienced and highly skilled security analysts in our CSOC

1000+

Experienced and certified engineers in industry leading security technologies

- Cyber Security Operations Center (CSOC) Head Quarter and the Center of Excellence in **KUWAIT**.
- Regional CSOCs around the **GCC** in Abu Dhabi (UAE), Doha (Qatar) with new CSOCs in Saudi Arabia and Oman.
- Offshore CSOC and Disaster Recovery in Hyderabad, **India** to support the centers in the region.