

# BDO Managed SOC-as-a-Service

## The BDO Managed SOC-as-a Service Advantage

The BDO Managed SOC-as-a-Service provides comprehensive, managed cybersecurity for modern organisations. It combines a unified security platform with 24/7 SOC operations, delivering rapid threat detection, reduced business disruption, and enhanced team efficiency. Designed for organisations with compliance needs and hybrid/multi-cloud environments, we offers centralised visibility and hassle-free security without vendor lock-in.

- ▶ Supports any log source - Endpoints, network devices, cloud, Servers, apps and security tools.
- ▶ Vendor-agnostic architecture - Works with leading and legacy system alike.
- ▶ Integrates with Endpoint Detection Response (EDR), firewall, Web Application Firewalls (WAFs), Software as-a-Service (SaaS), Cloud platform, and Operational Technology (OT) systems.
- ▶ Enables centralised visibility across hybrid and multi-cloud environments.
- ▶ No vendor Lock-in - flexibility to adapt as your stack evolves.
- ▶ Designed for complete telemetry coverage - no blind spots.

## Key Highlights

- ▶ 24/7 SOC Operations - Continuous monitoring with expert security analysts.
- ▶ Integrated Platform - Unified stack with Security Information and Event Management (SIEM), Extended Detection and Response (XDR), Threat Intelligence, Vulnerability Assessment (VA) and Active Response.
- ▶ AI-Powered Engineering - Advanced threat detection and response.
- ▶ Active Response -Immediate quarantine capabilities.
- ▶ Compliance Reporting -Reduced regulatory risk, simplified compliance audits.

## The BDO Managed SOC-as-Service Platform

### MITRE ATT&CK

Comprehensive mapping of threats to the industry -standard matrix for enhanced detection and response strategies.

### SIEM+ XDR

Real-time correlation and noise reduction to identify genuine threats amidst the alert storm.

### Threat Intelligence

Comprehensive global and proprietary feeds providing actionable insights on emerging threats.

### EDR Ingestion

Seamless integration with leading EDR platforms, enabling rich endpoint telemetry for enhanced detection, correlation, and automated response.



### Anomaly Detection

Behaviour-based monitoring that establishes baselines and identifies deviations in user, device, and system activity.

### Active Response

Immediate quarantine capabilities and sophisticated kill chain disruption to neutralise threats.

### Vulnerability Analytics

Continuous scanning combined with intelligent patch mapping to eliminate security gaps.

### Compliance Reporting

Structured approach to meeting regulatory requirements while maintaining robust security.

## Security - Ready from Day One

*The BDO Managed SOC as-a-Service comes pre-built to deliver value immediately — no waiting, no building from scratch.*



### 500+ Pre-Built Use Cases & Playbooks

Covers ransomware, insider threats, privilege abuse, phishing, cloud misconfiguration, and more.

Ready-made responses aligned to real-world scenarios.



### Decoders Across Assets & Logs

Automatically understands your network, endpoints, cloud, firewalls, and apps.

Speeds up onboarding and detection.



### AI-Powered Engineering

Automates detection engineering by generating rules, decoders, and playbooks from threat intel.



### Built-In Active Response

Automatically blocks threats, kills malicious processes, or isolates hosts.

## About BDO Singapore

BDO Singapore, established in 1972, is a full-service professional firm catering to a diverse clientele that ranges from small and medium-sized enterprises (SMEs) to multinational corporations. With a team of over 600 professionals, BDO delivers a comprehensive suite of services, including audit, tax, advisory, and business services outsourcing. As an independent member of BDO International, the world's fifth-largest professional services network, the firm combines deep local expertise with global insights. In today's digitally driven landscape,

**BDO's Digital Advisory** practice helps organisations to reshape their value delivery and growth strategies by leveraging advanced technologies such as Robotic Process Automation (RPA), Artificial Intelligence/Machine Learning, and smart enterprise applications like ERP and WMS. Their key offerings encompass the development of tailored digital strategies and transformation roadmaps, optimisation of intelligent business applications, and unlocking the value of data through effective analytics and AI integration. Additional services include automation technologies, cloud deployment, ERP implementation, and project management.

**BDO's Cybersecurity** practice provides a comprehensive, turnkey solution for managing IT risks and digital threats. Their core services include cyber risk assessments, security testing, and developing cybersecurity frameworks aligned with enterprise risk management. Additionally, we offers digital forensics and investigation services, as well as compliance and controls reviews against established regulations. Notably, BDO holds prestigious credentials such as a CREST membership, along with accreditations for cybersecurity assessments, reinforcing its commitment to safeguarding client interests in the digital realm.

## Contact Our BDO Team:



**Gerard Seng**  
Executive Director  
gerardseng@bdo.com.sg  
+65 6990 2645



**Cecil Su**  
Director  
cecilsu@bdo.com.sg  
+65 6990 2846