Republic of the Philippines
Iloilo Science and Technology University
Burgos St., La Paz, Iloilo City, 5000 Philippines
Trunkline: (+6333) 320-7190 | Telefax: (+6333) 329-4274
https://www.isatu.edu.ph/
mail@isatu.edu.ph

TERMS OF REFERENCE

Central Managed Detection and Response

- 24/7 Threat Monitoring and Response - Detect and respond to threats before they can compromise the data or cause downtime.
- Can integrate telemetry from third-party endpoint, firewall, network, identity, email, backup and recovery, and other technologies.
- Weekly and Monthly Reporting that can provide insights into security investigations, cyberthreats, and your security posture.
- Monthly briefing that provides insights into the latest threat intelligence and security best practices.
- Account Health Check - Continuously review settings and configurations for endpoints managed by the MDR and make sure they are running at peak levels.
- Expert-Led Threat Hunting - Proactive threat hunts performed by highly-trained analysts uncover and rapidly eliminate more threats than security products can detect on their own.
- Threat Containment - MDR operations team execute threat containment actions, interrupting the threat and preventing spread.
- Direct Call-in Support - Direct call-in access to Security Operations Center (SOC) to review potential threats and active incidents. The MDR operations team is available 24/7/365 and backed by support teams across different locations worldwide.
- Compatible with existing Sophos UTM and Endpoints
- Reseller should be a Platinum partner of the product offered
- Reseller should have a Certified Engineer/Architect of the product offered
- With After Sales Support / Knowledge Transfer

Republic of the Philippines
Iloilo Science and Technology University
Burgos St., La Paz, Iloilo City, 5000 Philippines
Trunkline: (+6333) 320-7190 | Telefax: (+6333) 329-4274
https://www.isatu.edu.ph/
mail@isatu.edu.ph

MDR Guided Onboarding

Provides hands-on support for a smooth and efficient deployment, ensures best practice configurations, and delivers training to maximize the value of MDR service. A Dedicated contact from the MDR for the first 90 days to make sure implementation is successful.

Day 1 – Implementation	**Day 30 – MDR Training**	**Day 90 Security Posture Assessment**
• Project kickoff • Configure Central and review of features • Build and test deployment process • Configure MDR integrations • Configure NDR sensor(s) • Enterprise-wide deployment	• Learn to think and act like a SOC • Understand how to hunt for indicators of compromise • Gain an understanding of using our MDR platform for administrative tasks • Learn to construct queries for future investigations	• Review current policies for best practice recommendations • Discuss features that are not in use that could provide additional protection • Security assessment following NIST framework • Receive summary report with recommendations from our review

Prepared by:

REYNARD Y. CHU
Director, MIS/EDP

Recommending Approval:

RUSS ALLEN B. NAPUD, DIT
Vice President for Administration and Finance

Approved:

GABRIEL M. SALISTRE, JR., PEE, DIT
SUC President III