

B|U|I INNOVATION™
DELIVERY
RESULTS

CyberSOC

TIERED OFFERINGS – AUGUST 2020



	Bronze (Notification Service)	Silver	Gold	Platinum
PURPOSE OF THIS OFFERING	Basic entry level notification-based service for SME and small customer. Could also be used as a POC for one of the larger offerings	Primary SOC offering- For large customers who require intense security monitoring		Very focused SOC service for highly secured environments
* Consulting Support	Not included - but paid-for consulting will be available or customers can opt to use existing SLA (L2-L3 support)	4 hours of SLA security consulting support per month	Total of 8 hours of SLA security consulting support per month	Up to 24 hours of incident support per month. Security consultants to assist with incident response
Hours of Operation - Active Monitoring	Office hours - 08h00-17h00 (Mon - Fri)	Extended office hours (GMT+2) *** (Mon - Fri)	24x7x365	24x7x365
Notification Methods	Automated email from Sentinel	Automated email from Sentinel & SMS notifications	Automated email from Sentinel & Teams or SMS notifications	Automated email from Sentinel & Teams or SMS notifications
			Flow-based automated notifications	Flow-based automated notifications
			Team site for reports and collaboration	Team site for reports and collaboration
Hunting	1 hour hunting per week / systems maintenance	2 hours total hunting per week / sys maintenance	8 hours total hunting per week / sys maintenance	12 hours total hunting per week / sys maintenance
Meetings	Monthly Teams meeting (Exec overview - limited reporting)	Monthly Teams meeting & system generated reports	Onsite monthly meeting with reports	Onsite monthly meeting with reports
Log Ingestion per day	No minimum	Minimum 20 GB per day	Minimum 40 GB per day	Minimum 60 GB per day
Licensing	CSP-BUI (Min PAL) **	CSP-BUI (Min PAL) **	BUI CSP or EA	BUI CSP or EA
Additional Services			Guidance in handling breaches with security incident management	Assistance and guidance with security incident management
Advisory Services			Vulnerability assessment - yearly	Vulnerability assessment - quarterly One external penetration test per year
Incident Management	Not included but can be provided via consulting contract or existing SLA (if available)	Not included but can be provided via consulting contract or existing SLA (if available)	Assistance to remediate breaches *	Assistance to perform root cause analysis and remediation of breaches
Microsoft Secure Score	Reporting on	Reporting on	Advisory services to improve Secure Score	Advisory services to improve Secure Score as well as consulting assistance to implement Secure Score
Management Assistance			Account manager managed	Account manager managed
Forensic Services	Not included	Not included	Not included	Guidance and advice given to conclude Forensic analysis

LET'S TALK

—

WWW.BUI.CO.ZA

+27 (0)87 740 2400
info@bui.co.za

JOBURG Head Office

Second Floor,
Microsoft
Corporate Hill,
3012 William
Nicol Drive,
Bryanston
+27 (0)87 740
2400
info@bui.co.za

CAPE TOWN

Harbour Bridge,
Roggebaai Canal,
Lower Long St,
Cape Town City
Centre, Cape
Town, 8000

DURBAN

Unit 13, Braehead
Office Park, 1 Old
Main Road, Kloof,
Kwazulu-Natal

EUROPE

London BUI LTD
71-75 Shelton
Street Covent
Garden London
WC2H 9JQ

AMERICA

530 Technology
Dr., Suite 100 &
200
Irvine, California,
92618, United
States of America
info@bui.co.za
+1 9493569904
info@bui.co.za

KENYA

Lang'ata Link
Karen,
Nairobi

