BUI

INNOVATION
DELIVERY
RESULTS

Cyber Security SoC

MICROSOFT AZURE EXPERT MSP + GOLD SECURITY PARTNER

BUI

INNOVATION
DELIVERY
RESULTS

OUR STORY

20 yrs

20 years proven **Cloud + Security** capabilities

Long-standing + award-winning **Microsoft Gold Partner.**

Enterprise + Mid-market customers across various industries

Offices in Johannesburg, Cape Town + Durban

LISTEN OUT FOR... KEYWORDS

- Security Posture
- Firewall Services
- Cyber Security Assessment
- Penetration Testing
- Ransomware
- Vulnerability Service
- Cloud Migrations
- Adoption + Change Management
- Network Environment
- Secure Score
- Windows Virtual Desktop
- Data Center Migrations

CASE STUDY

We've used the full spectrum of **Microsoft Solutions** to enable our customers to **stay online, connected + secure** during COVID-19

Assisted customers hardest hit by COVID-19, such as the **travel industry**

OUR PRODUCTS + SERVICES

Cloud, Secure Cloud, Azure Consulting, Data Center Migrations + Hybrid Cloud

Azure Expert Managed Service Provider

BUI CyberSoC

Cyber Security, Identity Security, Vulnerability Scanning

Advanced Adoption + Change Management

Advanced Specialization

Networking + Network Security

Primary focus areas:

- Cloud Infrastructure
- Cyber Security
- Modern Workplace

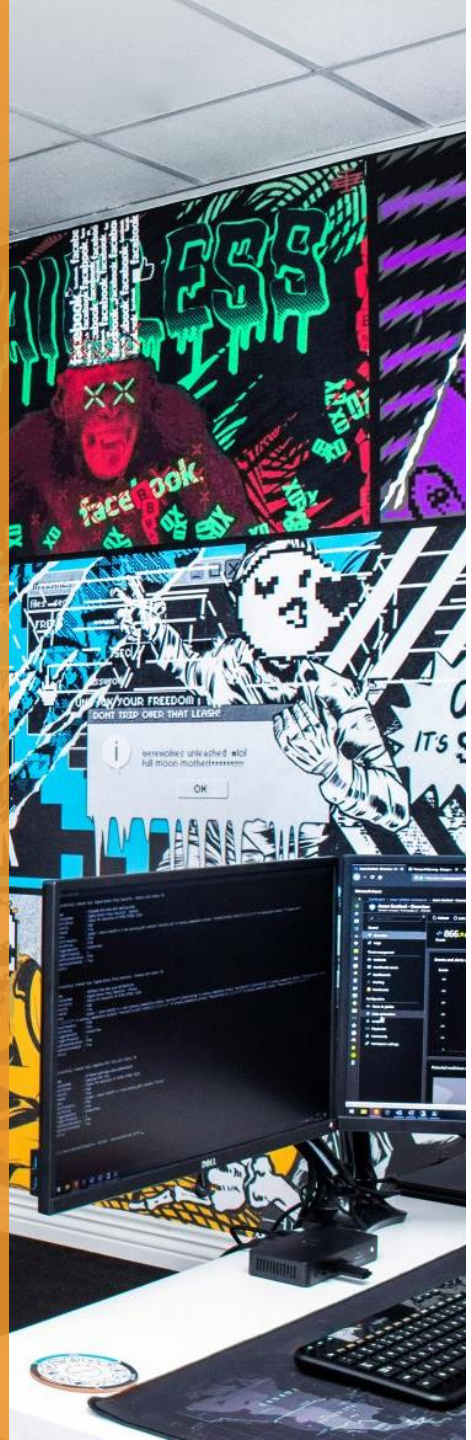
NOTEWORTHY ACHIEVEMENTS

- First + only Microsoft **Azure Expert MSP** in Africa
- **Top performing** FastTrack Ready Partner in South Africa
- **Microsoft Gold Partner** with **16** competencies
- **MCS** Partner
- Direct **CSP** Partner
- Security + Manageability **Elite Partner**
- First CyberSoC powered by **Sentinel**
- Highest **Azure** consumption partner in **Africa**
- **Microsoft 365** Partner Community

What We Offer

At BUI, we use digital technology in new and powerful ways to create customized IT solutions that enable performance and productivity in a changing world.

As a long-standing and award-winning Microsoft Gold Partner, we're proud to provide specialist guidance and industry-leading support to organizations utilizing the Microsoft suite.



1

CLOUD

Our capabilities include Virtualization, Private Cloud, Microsoft Azure, Microsoft Office 365 & Microsoft's Enterprise Mobility and more.

2

MANAGED SERVICES

BUI Managed Services from cloud adoption to managed infrastructure, operations, monitoring and support.

3

SECURITY

BUI is the first Microsoft Partner to hold a Microsoft Gold competency for identity and security in Africa. We take Security very seriously and launched our Cyber SoC early 2020.

4

ISV

From on-premise to the cloud, BUI delivers on technology investments encompassing all aspects of modern datacenters.

BUI INNOVATION™ DELIVERY RESULTS

Microsoft Alignment

www.bui.co.za

BUI as your Azure & Security Partner

Accreditation

Gold Microsoft Partner | Azure Expert MSP

Microsoft Partner
2020 Partner of the Year Winner
South Africa

Microsoft Partner
Gold Cloud Platform
Gold Cloud Productivity
Gold Enterprise Mobility Management
Gold Windows and Devices
Gold Security

Microsoft Partner
Gold Small and Midmarket Cloud Solutions
Gold Data Analytics
Gold Application Development
Gold Collaboration and Content
Gold Messaging

Microsoft Partner
Silver Project and Portfolio Management
Surface Hub Authorized Reseller
Gold Datacenter

- Microsoft Gold Partner
- Microsoft Azure Expert MSP
- Adoption and Change Management Advanced Specialization
- Highest Azure Consumption Partner in Africa
- Regional partner in MCC for Africa
- Direct (Tier 1) CSP Partner
- Microsoft community/program involvement
  - Security & Manageability Elite Partners
  - Microsoft 365 Security, Compliance & Identity Partners
  - FastTrack Ready Partners
  - Participated in Microsoft Sentinel Preview Program
- Microsoft Consulting Services (MCS) Partner – South Africa
- Global OCP Partner with 11 + Co-Sell Ready Offerings
- Published Azure Marketplace Offers

BUI INNOVATION DELIVERY RESULTS

Introduction

BUI's Cyber Security Operations Center (SoC) offers dedicated skills, focusing on real-time analysis of security alerts.

Providing a birds-eye view across your enterprise

Watch our 60 second video on YouTube to get an overview

The BUI Cyber SoC monitors your entire IT security landscape, including On-premise, Cloud, Devices, Applications, Networks, Infrastructure and Users.

The BUI CyberSOC provides a comprehensive and specialized Managed SOC service which runs on Microsoft Security technology, powered by modern Artificial Intelligence (AI) based infrastructure, which provides full security services around Compliance Reporting, Database, Infrastructure, Access Monitoring, Real-time Threat Monitoring and much more.

Managed and monitored by highly skilled cyber security professionals provided to you, as a service with near to no infrastructure requirements.

For a full range of services visit our website.

BUI INNOVATION DELIVERY RESULTS

Overview

BUI Cyber SoC is ideal for any organization that is looking to reduce security breaches and improve threat detection.

Invest in security, not infrastructure

The BUI Cyber SoC provides a proactive 24/7 managed security service backed up by powerful AI based Cloud Technology with dedicated skills focusing on real-time analysis security alerts.

With committed resources and highly scalable AI detection pattern matching to reduce noise and enhanced analysis for your unique security landscape.

Never again let a storage limit or a query limit prevent you from protecting your enterprise. The nature of our service allows your organization to eliminate infrastructure costs by automatically scaling your resources in a for-use consumption model, allowing you to scale as required.

BUI INNOVATION DELIVERY RESULTS

Features

Reduce infrastructure costs by automatically scaling resources and only paying for what you use.

Simplified SecOps for faster threat response

Our consultants are dedicated to the management of the BUI Cyber SoC by providing highly skilled cybersecurity resources to manage our world class infrastructure, the BUI Cyber SoC is backed-up and protected by globally available Microsoft Security Technology in your region.

Detection
Threat detection is smarter and faster

Reducing Noise
The focus is on finding real threats, daily, and minimizing false positives

Custom
Pre-built queries based on years of security experience

Patterns
Previously uncovered threats can be detected

Technology
Built-in machine learning backed by world-class Microsoft Technology

Analysis
BUI's SoC provides monitoring and alerting and, if enough data is collected, an analysis of the attack.

BUI INNOVATION™ DELIVERY RESULTS

Simplified SecOps for faster threat response

Features

Reduce infrastructure costs by automatically scaling resources and only paying for what you use.

Incident Response

Identify Threat and Contain

- Identify all threat activity and attribution
- Minimise impact through (automated) containment run books

Vulnerability Mgmt

Scan and Report

- Identify infrastructure vulnerabilities
- Prioritise remediation and report

Detection

Investigate and Triage

- Swift analysis of surfaced security events
- Triage and escalate potential threat activity or close false positives
- Tune detections to focus on real threats

Security Baselines

Monitor for Deviations

- Implement security configuration baselines on infrastructure
- Detect and respond to configuration deviations

Configuration

Implement and Maintain

- Service design based on Use Cases
- Core platform implementation and integration
- Continual improvement driven from SOC activities and Threat landscape

Threat Hunting

Proactive Threat Detection

- Researching threat attack methods and resulting indicators
- Proactively hunting for threat activity across disparate data sources

BUI INNOVATION™ DELIVERY RESULTS

Solution Architecture

Cloud based architecture using Microsoft Sentinel, enriched with BUI playbooks & analytics, custom dashboards, integrations and supported by the BUI SecOps team.

Cloud based architecture for quick enablement

Collect

Microsoft Services

Apps, Users, Infrastructure, ATP

Public Clouds

Security Solutions

paloalto NETWORKS · FORTINET · Check Point SOFTWARE TECHNOLOGIES LTD.

Data Collectors (cloud and on-premises)

Analyse & Detect Threats

UEBA, SOAR, Custom Analytics

Investigate & Hunt Suspicious Activities

Interactive Attack Visualisation Azure Notebooks

Automate & Orchestrate Response

Standard & Bespoke Playbooks

Enriched with Intelligence

Data Ingestion

Data Repository

Data Search

Azure Monitor (Log Analytics)

BUI Custom Dashboards

BUI CyberSoC

Administration & Support

Integrate

JIRA BUI Service Desk

Azure Lighthouse

Community

BUI Panic Key

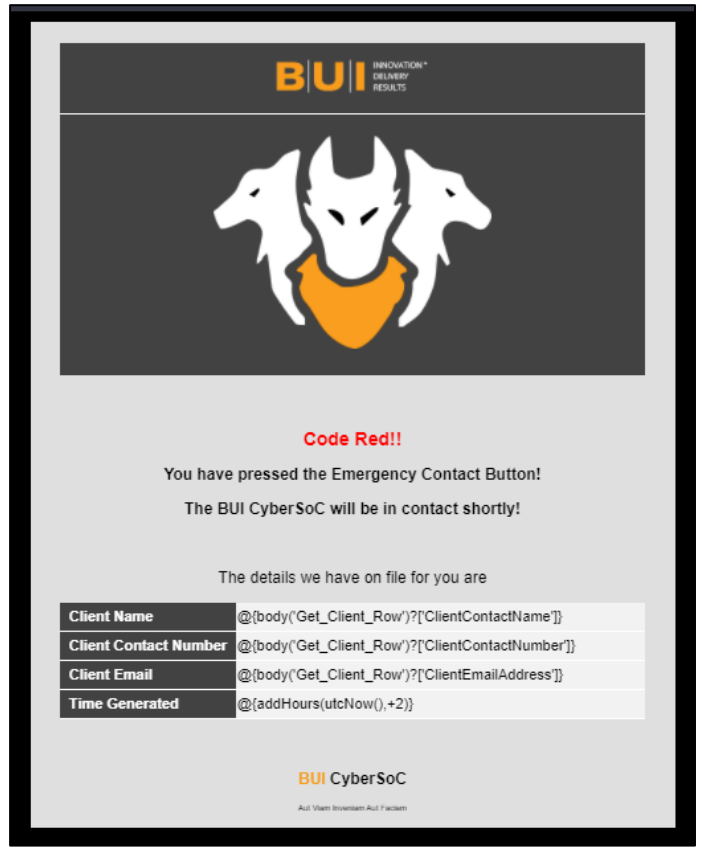
API Custom

BUI INNOVATION™ DELIVERY RESULTS

Solution Architecture

Cloud based architecture using Microsoft Sentinel, enriched with BUI playbooks & analytics, custom dashboards, integrations and supported by the BUI SecOps team.

BUI Panic Button



The BUI Panic Button is a Value-Added Service for our managed customers, which launches a contact request with our CyberSoC. The solution is delivered via API and Logic Apps functionality.

BUI INNOVATION™ DELIVERY RESULTS

How is this billed

The BUI Cyber SoC is billed based on the service tier you select. Service tiers provide basic to premier managed cybersecurity services and is based on cloud technology, providing virtually unlimited capacity.

Our Pricing Model

We offer the BUI CyberSOC Service in four packages which are billed monthly as a fixed service fee

All Subscriptions benefit from these features :

- No Software costs
- Dashboard Access
- Custom detection & automation
- Programmatic remediation
- Infinitely scalable
- AI based analytics
- Up to 90 days data storage included
- Proactive real-time alerting
- Custom and policy-based detections
- Correlated analysis of billions of security events
- Flexible 8/5 or 24/7 monitoring (*Package dependent)
- Location independent
- Highly secured physical facilities

Bronze

Business hours

Free 90 Day storage
8/5 monitoring

Excludes Azure costs
Fixed Monthly Service Fee
Fixed Enablement Fee

Silver

Extended Business Hours

Free 90 Day Storage
12/5 monitoring
Remote Monthly Review

Excludes Azure costs
Fixed Monthly Service Fee
Fixed Enablement Fee

Gold

24/7/365

Free 90 Day Storage
24/7 monitoring
In person Monthly Review

Excludes Azure costs
Fixed Monthly Service Fee
Fixed Enablement Fee

Platinum

24/7/365

Free 90 Day Storage
24/7 monitoring
In person Monthly Review
Additional Services

Excludes Azure costs
Fixed Monthly Service Fee
Fixed Enablement Fee

BUI INNOVATION · DELIVERY · RESULTS	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 Flow-based automated notifications Team site for reports and collaboration	Automated email from Sentinel & Teams or SMS notifications Flow-based automated notifications Team site for reports and collaboration
Hunting	1 hours 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

Visit bui.co.za/soc for updated Terms and Conditions

* Consulting support for security-related SOC incidents or any customization relating to Sentinel. Any additional hours used will be charged for at preferential SLA rates

** Customers using EA licensing incur additional 5% monthly management fee

*** Extended office hours 06h00 until 19h00

Note : Minimum requirement is a new subscription for Sentinel (Silver, Gold and Platinum tiers)

BUI INNOVATION™ DELIVERY RESULTS

BUI Microsoft Partner Awards

www.bui.co.za

2020	Microsoft Country Partner of the Year – South Africa
	Microsoft Azure Expert MSP
	Microsoft Modern Workplace Partner of the Year
	Microsoft Azure Infrastructure Partner of the Year
	Microsoft Security Partner of the Year
2019	Microsoft Cloud Partner of the Year
	Microsoft Security Partner of the Year
	Microsoft Services Partner of the Year
	Microsoft Azure Consumed Partner of the Year
2018	Microsoft Cloud Partner of the Year
2017	Microsoft Partner of the Year South Africa
	Microsoft Cloud Partner of the Year
	Microsoft EMS Partner of the Year
	Microsoft Data Centre Partner of the Year
	Palo Alto Account Manager of the Year
2016	Microsoft Managing Director Partner of the Year
	Microsoft Enterprise Mobility Partner of the Year
	Microsoft Cloud Platform Partner of the Year
	Microsoft Data Center Partner of the Year
	Palo Alto Deal of the Year

LET'S TALK

WWW.BUI.CO.ZA

sales@bui.co.za

BUI INNOVATION™ DELIVERY RESULTS

JOHANNESBURG
Head Office
Second Floor, Microsoft Corporate Hill
3012 William Nicol Drive
Bryanston

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

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

UNITED STATES OF AMERICA
530 Technology Dr.
Irvine
California

UNITED KINGDOM
71-75 Shelton Street
Covent Garden
London