BUI

INNOVATION ™
DELIVERY
RESULTS

Cyber MDR

Managed cybersecurity breach
Detection, Investigation and
Response service

Microsoft Partner
- Gold Cloud Productivity
- Gold Security
- Gold Windows and Devices
- Gold Messaging
- Gold Application Development

■ Microsoft

Microsoft Partner
- Gold Enterprise Mobility Management
- Gold Datacenter
- Gold Cloud Platform
- Gold Data Analytics
- Gold Small and Midmarket Cloud Solutions

■ Microsoft

Microsoft Partner
- Surface Hub Authorized Reseller
- Gold Collaboration and Content
- Silver Communications
- Silver Project and Portfolio Management

■ Microsoft

Member of
Microsoft Intelligent Security Association

■ Microsoft

Struggling to respond timeously and efficiently against everchanging cyber threats?

The BUI Cyber Managed Detection and Response service utilizes Microsoft cloud-based security solutions to deliver preventative protection, post-breach detection, investigation services and automated response.

Our specialized and highly qualified Security Operations team will continuously monitor and manage your environment, reacting to breaches as it occurs in a professional and non-intrusive manner.
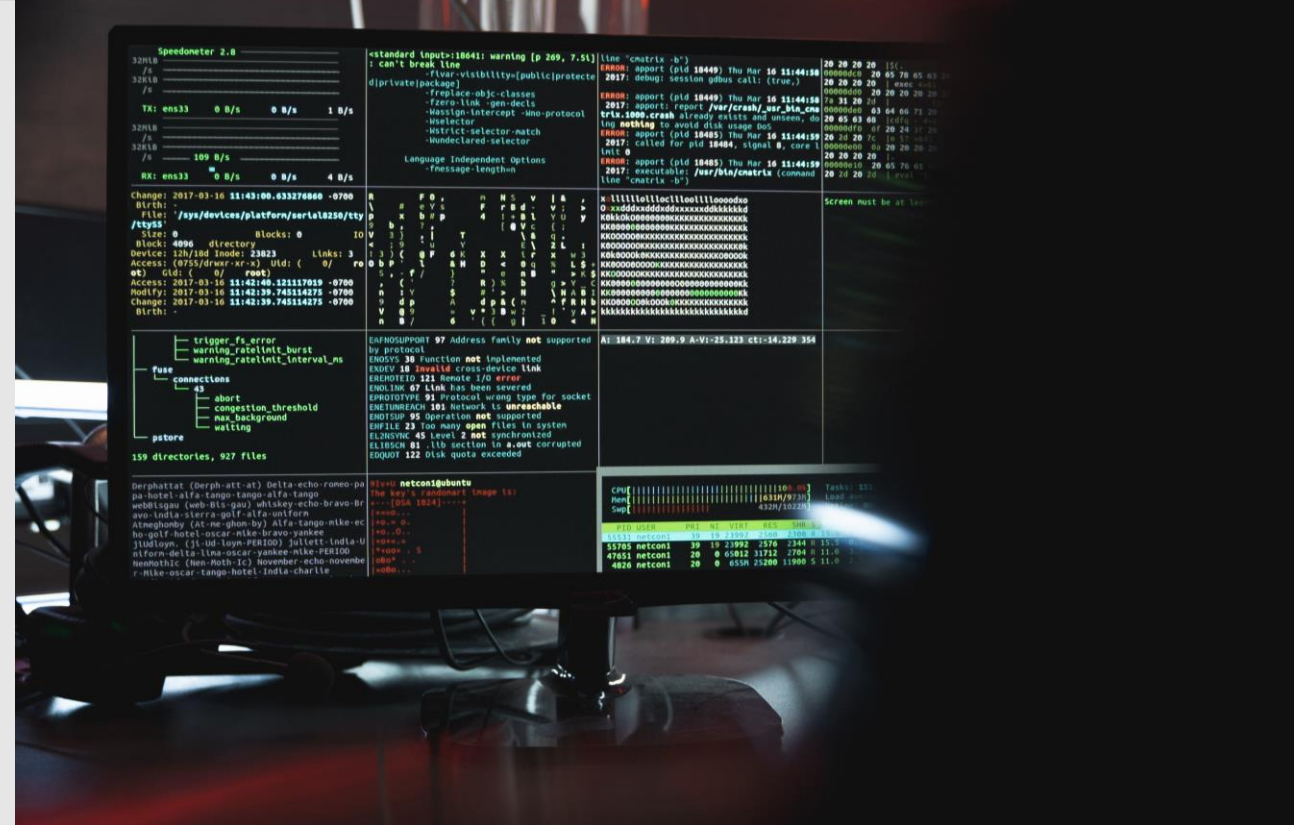
CHALLENGES

Cybersecurity attacks are not industry specific and with the increased numbers and sophistication of cyber-attacks, all businesses are at risk.

Cybersecurity prevention, detection and remediation is required in every IT Strategy.

The lack of cybersecurity skills results in preventable risks not being addressed.

IDEAL SOLUTION

Have full and continuous visibility of your cybersecurity posture, risks and the potential attack plane.

Outsource cyber risks management to a cybersecurity partner, knowing your IT environment is continuously monitored for potential breaches.

Compliment your in-house cybersecurity team with skilled security professionals.

DESIRED OUTCOMES

BUI's Cyber MDR service addresses key cybersecurity pillars – Detect, Investigate and Respond.

Continuously improve your cybersecurity posture through an affordable managed security service.

Automated investigation and response at scale.

BUI – Cyber MDR

An affordable and scalable enterprise grade, cloud monitored and managed cybersecurity breach detection, investigation and response service.

BUI's cybersecurity experts continuously monitors your managed assets for potential and existing vulnerabilities, threats and breaches and have the expertise and tools to respond in minutes.

Discover

- Discovery Call to assess licensing and service requirement
- 12-month Service Agreement
- Choose from two tiers – Silver and Gold
- Monthly invoicing
- Excludes product fees

Detect

- Active monitoring during specified hours
- Automated and feedback notification
- Unconstrained hunting for both known and potential threats

Investigate

- Incident prioritization and triaging
- Impact Analysis and response recommendation
- On-demand Health Check
- Incident feedback

Respond

- Incident management
- Access to the BUI MDR Analyst
- Advisory services
- Threat response
- Monthly Executive reports
- Regular feedback sessions

12-month Managed Cybersecurity Management, Detection & Response service

BUI leverages Microsoft Defender for Endpoint and deliver managed cybersecurity services to all sized businesses.

Using Microsoft Defender for Endpoint, a cloud-based security monitoring and management solution, integrated with your existing security solutions, enables the BUI Security Operations team with the insights to easily monitor, detect and respond to vulnerabilities, threats and breaches in minutes. BUI monitors your cybersecurity environment 24/7, providing continuous risk detection, investigation and response by expert security staff.

1 Fully Managed Cyber MDR

BUI monitors your environment integrating Microsoft cloud security tools with our BUI SecOps services, providing 24/7 monitoring and response.

2 Tiered Cyber MDR Service Options

Affordable per asset pricing with tiered security services, created to fit your budget.

3 Realtime Vulnerability Discovery and Response

Bring security and IT together with Microsoft Threat & Vulnerability Management to quickly discover, prioritize, and remediate vulnerabilities and misconfigurations.

4 Automated Security

Take your security to a new level by going from alert to remediation in minutes—at scale.

5 Agentless Security Monitoring

No additional deployment or infrastructure. No delays or update compatibility issues. Always up to date.

6 Unparalleled optics

Built on the industry's deepest insight into Windows threats and shared signals across devices, identities, and information.

	Bronze	Silver	Gold
Purpose of Offering	Entry level notification-based service for small customers	Entry level notification-based service for small to medium customers	Primary MDR offering - For customers who require focused security monitoring
DETECTION			
License	Bring your own license	Bring your own license	Bring your own license
Deployment	Not Included Available as a deployment project	Not Included Available as a deployment project	Not Included Available as a deployment project
Users	50 Licensed users	Unlimited users	Unlimited users
Security Product Coverage	Microsoft Defender for Endpoint Only	Microsoft Defender for Endpoint Required; XDR recommended	Microsoft Defender for Endpoint Required; full XDR recommended
System Configuration and Maintenance	Included	Included	Included
Active Monitoring Hours of Operation	Active monitoring not included (Automated notifications only)	Extended office hours 06:00 to 19:00 Time zone coverage: GMT to GMT+2 Business workdays: Mon - Fri	24x7x365
INVESTIGATION			
Real-Time Detection and Automated Response	Included out-of-the-box	Included out-of-the-box	Included out-of-the-box Customisation and configuration of bespoke, customer-specific detection and response capabilities is included.
Entity tagging and Prioritization	Included	Included	Included
Notification Methods	Automated notification (email and/or Teams)	Automated and analyst notification of critical incidents (email and/or Teams)	Automated notification (email and/or Teams) Acknowledged notification for critical incidents (text message with acknowledgement and/or phone call)
RESPONSE			
Threat Hunting	Not Included	Not Included	24 hours per month (Optionally extended via SLA)
Consulting Support Hours	2 hours per month (Optionally extended via SLA)	4 hours per month (Optionally extended via SLA)	24 hours per month (Optionally extended via SLA)
Proactive Threat Response	Automated Responses Only	Automated Response Only	Automated Response Threat Expert Response via Consulting Support Hours
Access to MDR Analyst	Included (Up to 2 hour per month)	Included (Up to 3 hours per month)	Included (Up to 6 hours per month)
BUI threat expert assistance	Included via Consulting Support Hours	Included via Consulting Support Hours	Included via Consulting Support Hours
Strategic Cyber Security Advisory Services	Included via Consulting Support Hours	Included via Consulting Support Hours	Included via Consulting Support Hours
Cyber Security Posture Analysis	Included Quarterly Meeting	Included Quarterly Meeting	Included Monthly Meeting
Executive Monthly Reports	Built in Reporting	Built in Reporting	Executive reporting and detailed monthly reporting
Pricing	**R 9,950.00 per Month**	**R 24,500.00 per Month**	**R 57,750.00 per Month**

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

*** Extended office hours 06h00 until 19h00

		Bronze	Silver	Gold
	Purpose of Offering	**Entry level notification-based service for small customers**	**Entry level notification-based service for small to medium customers**	**Primary MDR offering - For customers who require focused security monitoring**
DETECTION	License	Bring your own license	Bring your own license	Bring your own license
	Deployment	Not Included Available as a deployment project	Not Included Available as a deployment project	Not Included Available as a deployment project
	Users	50 Licensed users	Unlimited users	Unlimited users
	Security Product Coverage	Microsoft Defender for Endpoint Only	Microsoft Defender for Endpoint Required; XDR recommended	Microsoft Defender for Endpoint Required; full XDR recommended
	System Configuration and Maintenance	Included	Included	Included
	Active Monitoring Hours of Operation	Active monitoring not included (Automated notifications only)	Extended office hours 06:00 to 19:00 Time zone coverage: GMT to GMT+2 Business workdays: Mon - Fri	24x7x365
INVESTIGATION	Real-Time Detection and Automated Response	Included out-of-the-box	Included out-of-the-box	Included out-of-the-box Customisation and configuration of bespoke, customer-specific detection and response capabilities is included.
	Entity tagging and Prioritization	Included	Included	Included
	Notification Methods	Automated notification (email and/or Teams)	Automated and analyst notification of critical incidents (email and/or Teams)	Automated notification (email and/or Teams) Acknowledged notification for critical incidents (text message with acknowledgement and/or phone call)
RESPONSE	Threat Hunting	Not Included	Not Included	24 hours per month (Optionally extended via SLA)
	Consulting Support Hours	2 hours per month (Optionally extended via SLA)	4 hours per month (Optionally extended via SLA)	24 hours per month (Optionally extended via SLA)
	Proactive Threat Response	Automated Responses Only	Automated Response Only	Automated Response Threat Expert Response via Consulting Support Hours
	Access to MDR Analyst	Included (Up to 2 hour per month)	Included (Up to 3 hours per month)	Included (Up to 6 hours per month)
	BUI threat expert assistance	Included via Consulting Support Hours	Included via Consulting Support Hours	Included via Consulting Support Hours
	Strategic Cyber Security Advisory Services	Included via Consulting Support Hours	Included via Consulting Support Hours	Included via Consulting Support Hours
	Cyber Security Posture Analysis	Included Quarterly Meeting	Included Quarterly Meeting	Included Monthly Meeting
	Executive Monthly Reports	Built in Reporting	Built in Reporting	Executive reporting and detailed monthly reporting
	Pricing	**US$ 720.00 per Month**	**US$ 1,750.00 per Month**	**US$ 4,125.00 per Month**

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

*** Extended office hours 06h00 until 19h00

BUI thwarts cyber attack while strengthening Omnia's cybersecurity defenses.

Omnia, a diversified chemicals Group that supplies chemicals and specialised services and solutions for the agriculture, mining and chemical application industries, fell victim to a merciless cyberattack.

This prompted the business to act immediately and rethink their cybersecurity defence strategy. With the assistance of BUI, Omnia deployed Microsoft Azure Sentinel and Microsoft Defender for Endpoint to improve detection, prevention, investigation, and response across endpoints, identities, and email. BUI SecOps provided much needed investigative, recovery and stabilisation skills with continuous monitoring and metering.

As a result, Omnia were able to enhance control and visibility across their security landscape, mitigating against potential secondary infection and intrusion attempts.

1 **Attack Surface Visibility**
Infection spread became visible and response immediate and effective.

2 **Holistic Cybersecurity Defense Strategy**
BUI SecOps leverages Microsoft 365 Security services and Sentinel AI to monitor, defend and automate responses, ensuring continuous risk management.

3 **ROV**
Having continuous monitoring and metering across all assets, provides the defense required to ensure Omnia, its affiliates and partners can continue to work and collaborate safely.

4 **No Additional Infrastructure**
Agentless security monitoring and cloud based SIEM aligns with Omnia's cloud strategy. No additional infrastructure was required to deploy security solutions.

5 **BUI SecOps Services**
Knowledgeable security operators and cloud-based security solutions resulted in record time containment of the initial infection, simultaneously providing visibility to new and attempted intrusions.

6 **Management and Support**
Using BUI Cyber MDR services, provides continuous monitoring, metering, detection, investigation and remediation across all managed assets with dedicated support team to address security incidents.

LET'S
TALK

Connect with the BUI Sales Team to enroll your assets and make use of the BUI Cyber MDR service – protecting your assets from malicious exploits.

WWW.BUI.CO.ZA
sales@bui.co.za