# Service Overview

| SERVICE | ESSENTIAL | PREMIUM |
|---|---|---|
| Microsoft Defender for Business or Microsoft 365 Business Premium | ✓ | ✗ |
| Service Onboarding | ✓ | ✓ |
| Deployment Services (Microsoft Defender solutions) | ✗ | ✗ |
| System Configuration and Maintenance | ✓ | ✓ |
| Microsoft 365 E5 or Defender for Endpoint Plan 2 | ✗ | ✓ |
| Critical Asset Labelling | ✓ | ✓ |
| Service Scope – Maximum users 300 | ✓ | ✗ |
| Contract Term 12 – 36 Months | ✓ | ✓ |
| Hours Of Operation 24 x 7 x 365 | ✓ | ✓ |
| Service Delivery Manager | ✓ | ✓ |
| Consult the Experts | ✗ | ✓ |
| System Generated Reports | ✓ | ✓ |
| Executive reports | Quarterly | Monthly |
| Active Monitoring | ✗ | ✓ |
| Threat Intelligence | ✓ | ✓ |
| Continuous Detection | ✓ | ✓ |
| Vulnerability Management | Quarterly | Monthly |
| Threat Hunting | ✗ | ✓ |
| Incident Notification | ✓ | ✓ |
| Incident Response - *Reactive Only 24 x 7 | ✓* | ✓ |
| Near Real-Time Detection and Automated Response | ✓ | ✓ |
| Threat Expert Assistance (2 Hours p/m) | ✗ | ✓ |
| Security Consult (2 Hours p/m) | ✗ | ✓ |
| Consulting Support Hours (8 Hours p/m) | ✗ | ✓ |
| Cyber Security Posture Analysis and Microsoft Secure Score | ✓ | ✓ |
| Digital Forensics and Incident Response (DFIR) | ✗ | ✗ |
| Strategic Security Advisory Services | ✗ | ✗ |
| Penetration Testing | ✗ | ✗ |

### Minimum Technology Requirements

Microsoft 365 E5 or Microsoft Defender for Endpoint Plan 2 Required for the Premium offering.
Microsoft Defender for Business or Microsoft 365 Business Premium is required for the Essentials offering.

### Service Onboarding

Configuration of baseline monitoring and notification metrics, and baseline configuration of the monitoring and detection tools.

**Deployment Services**

The Deployment of XDR technologies and services are available from Service Provider professional services following standard security services deployment services, including Assess, Design, Build, Validate & Test, Operational Handover.

**System Configuration and Maintenance**

BUI MDR analysts will guide and advise Company's regarding system configuration and optimisation.

**Critical Asset Labelling**

The Service Provider's experience and threat knowledge coupled with a deep understanding of the Company's environment (including tagged critical assets and other entities) allows the MDR team to prioritize incidents that might be detected by the system at the same severity level.  The team notifies and escalates incidents as per the agreed incident response plan.

**Service Scope**

CyberMDR is a managed security service, focused on protecting devices, networks, and sensitive data from unauthorised access, theft, damage, and other cyber threats. There is a maximum number of 300 users for the Essential offering.

**Hours Of Operation**

The BUI CyberMDR Managed Service is available 24 x 7 x 365.

**Consult The Experts**

Consult with an MDR security analyst for further details or clarification beyond the alert and/or digested reports. This service can be delivered through the included consulting hours.

**System Generated Reports**

BUI offers standard system generated reports which are delivered through agreed communication platform.

**Executive Reports**

The BUI CyberMDR team provides a standard monthly executive summary outlining the services provided including key metrics that allows the Company to measure and keep track relevant trends and to identify areas for improvement. Review sessions are scheduled to present findings and remediation roadmap.

**Active Monitoring**

The BUI CyberMDR team monitor events for new critical alerts, investigate via automated and manual means, and deliver details on the threat.

**Threat Intelligence**

BUI will provide enhanced threat intelligence and entity behavioural analysis.

**Continuous Detection**

Continuous detection capabilities updated automatically and can be augmented and enhanced by adding custom detection, alert suppression, custom indicators and process memory indicators unique to your environment.

**Vulnerability Management**

Detect endpoint vulnerabilities through vulnerability management. This will be included in the executive report.

**Threat Hunting**

Threat hunting for cyber threats lurking undetected in the network performed by the MDR analysts as required.

**Incident Notification**

Automated notifications from the MDR platform to designated communication channels, with agreed escalation path.

Supported platforms: Microsoft Teams, Email

**Incident Response**

MDR teams proactively analyse and act on threats as they evolve. The MDR team provides detailed remediation recommendations and, as applicable, clean-up tools to assist with recovery.

Included:

- Disable compromised accounts as well as isolate devices.
- Identify the nature of the attack, timeline, attack chain, and the attack's underlying persistence to identify and understand adversaries exploit tactic.

Incident response may include incident investigation, containment, and advise on the recovery process.

### Near Real-Time Detection and Automated Response

Bad actors are continuously evolving new techniques and methods to bypass security controls, and therefore, detection capabilities need to be continuously updated.

BUI augments and enhances this detection and response capabilities by adding custom detections, alert suppression, custom indicators, and process memory indicators often unique to the customer environment.

### Threat Expert Assistance

As per the agreed incident response plan, MDR analysis are available to the Company for assistance and guidance regarding incident response.

### Cybersecurity Consult

Consult with an MDR security analyst for further details or clarification beyond the alert and/or digested reports.

### Consulting Hours Support

Not all Businesses have the capacity or expertise to manage the complexities of Endpoint Management on their own. BUI's MDR offering is backed up by world class security consultants to assist with incidents and ongoing advisory services regarding the maintenance of a customer's endpoint environment.

### Cyber Security Posture Analysis and Microsoft Secure Score

The Contractor applies deep operational knowledge and expertise with endpoint management in order to improve security posture. This goes beyond the initial set up of MDR. The Contractor continuously assesses, advises and assists Company’s to understand and apply the necessary security policies and processes as required over time. It is also crucial to ensure that the environment is kept up to date with the latest patches. Performing a Secure Score assessment and Exposure Score assessment is the foundation of this activity and is practiced regularly. Any meeting cadences and recommendation for improvements can be requested by the Company and can be delivered via the support consulting component.

## Optional Add-on Services

Optional add-on services can significantly enhance the value and effectiveness of core MDR service, catering to specific needs that may vary from one organization to another. Customers can choose from a variety of add-ons such as:

### Digital Forensics and Incident Response (DFIR)

BUI’s DFIR managed service equips organizations with the expert resources and capabilities essential to plan, manage, and effectively respond to and recover from cybersecurity incidents.

### Strategic Security Advisory Services

Provides advice and assistance in the implementation of security strategy, advice on how to improve, protect and transform the IT landscape.  This can extend beyond endpoint management and security.

### Cybersecurity Consulting

Security strategy build workshops, assisting Customer with building a zero-trust cybersecurity strategy including actionable activities roadmap.

### Penetration Testing

Detect vulnerabilities through an external or internal penetration test. BUI offer a wide range of penetration testing types and targets. Please speak with your Account Manager for more details.