Managed Detection and Response (MDR)

SERVICE SPECIFICATION

Jan 2024

brightsolid

ideas. solutions.

Table of Contents

Service Overview

The Managed Detection & Response (MDR) service delivers a continuous security data analytics operation which is managed by Brightsolid SOC analysts and is underpinned with advanced detection logic, dynamic use cases, playbooks, and threat intelligence. The service utilises the Microsoft Sentinel Security Information and Event Management (SIEM) platform as the core component to identify Indicators of Compromise (IOCs) 24 hours a day, 365 days a year.

Service Name	Managed Detection & Response
Hours of Service	24x7
Supported Platforms/Services	Microsoft Sentinel

Definitions

The definitions for all capitalised terms used throughout the Service Specification are set out in the Common Definitions document that forms part of the Brightsolid Contract to which this Service Specification relates.

"Alert" means a response to the correlation of one or more individual Events processed the Brightsolid MDR service, generated by such Brightsolid MDR Service where a potential situation requires analysis and investigation;

"Analytic" means a documented mechanism to produce an Alert based on statistical, mathematical, or algorithmic model;

"Azure Lighthouse" means multi-tenant management and access of customer Azure tenants;

"Azure Monitor" means an Azure service to collect, analyse telemetry data from your Azure and on-premises environments;

"Brightsolid MDR Service" means the Managed Detection & Response service delivered by the Brightsolid SOC;

"Business Hours" means 9am – 5pm (GMT) on any day which is a Working Day excluding UK public holidays;

"CIRT" means Cyber Incident Response Team;

"CSP" means Microsoft Cloud Solution Provider Program which is used by partners to manage customer Microsoft cloud services;

"Customer Data Sources" means a list of infrastructure, applications or data that will be provided by the customer in the Onboarding Form to be ingested into the Microsoft Sentinel SIEM;

"Customer Portal" means the Cherwell customer portal (or any alterative portal) made available for access by the Customer as part of the Brightsolid MDR Service, for the purposes of providing secure communications, information exchange, incident management (ticket and incident data), and real time performance metrics;

"EA" means Microsoft Enterprise Agreement which offers large organisations over 500 users access to the volume licencing program for Microsoft cloud services;

"Event" means an individual item of machine data which is generated as a response to an action, change or series of actions and changes made to an IT system or network providing visibility as to the timing and nature of the action or change;

"False Positive" means an alarm which is generated indicating that a security incident has occurred which subsequent investigation determines is incorrect;

"Go Live Milestone" means in respect of the Brightsolid MDR service, the earlier of (i) 12 weeks from the date of acceptance of the applicable proposal and (ii) the date Brightsolid confirms in writing to the Customer that the Set-up Services have been completed;

"Incident" means an event that may indicate that systems or data have been compromised;

"Indicators of Compromise (IOC)" means forensic evidence of potential intrusions on a host system or network;

"Log Analytics" means a tool in the Azure portal to edit and run log queries from data collected by Azure Monitor Logs to interactively analyse their results.;

"MDR" means Brightsolid Managed Detection and Response service as detailed in this document;

"Measurement Period" means the relevant period in which a Service Level is measured, as specified below in respect of each Service Level;

"Microsoft Defender" means the collection of Microsoft Defender security products, which are used to identify, detect, and respond to security Incidents;

"Microsoft Sentinel SIEM" means the Microsoft Sentinel Security Information and Event Management technology that support threat detection, compliance and security incident management through the collection and analysis of security events, as well as a wide variety of other event and contextual data sources;

"Microsoft Threat Intelligence" means is the collection of data which help identify threats and Indicators of Compromise;

"Onboarding Form" means the applicable onboarding form requesting pre-Service information from the Customer, to be completed by the Customer and returned to Brightsolid within 5 Working Days of receipt from Brightsolid;

"Service Level(s)" means the applicable service level(s) that shall apply to the Brightsolid MDR Service Offering, as contained in the Service Description and/or Proposal;

"Service Level Start Date" means, in respect of each Service Level, the date which is 4 weeks from the applicable Go Live Milestone, or such other date as is specified in the applicable proposal;

"Severity Level" means the level of impact from an Alert determined by the SOC on a scale from P1 to P4;

"SOAR" means Security Orchestration, Automation and Response that acts as the remediation and response engine to Alerts;

"SOC" means the Brightsolid 24-hour security operations centre;

"Triage" means that SOC:
undertakes an initial investigation of an Alert or Incident (as applicable) to determine (at its sole discretion) the classification of the Severity Level of such Alert or Incident; and
notifies the Customer by telephone or via the Customer Portal (in accordance with the agreed escalation procedure set out in the Service Description and/or Statement of Work) of the Alert or Incident and the allocated Severity Level classification.

"Triage Time" means the timescale within which SOC will Triage an Incident or Alert (as applicable);

"TTPs" means the Tactics, Techniques and Procedures are the behaviours, methods, tools, and strategies that cyber threat actors and hackers use to plan and execute cyber-attacks on business networks

"Working Day" means any day other than a Saturday, a Sunday

Service Summary

This document provides an overview of the Brightsolid MDR service to be delivered and outlines the technical service specification, assigned roles and responsibilities between Brightsolid and the Customer, and support and service level agreements.

Brightsolid MDR Service Components

The Brightsolid MDR service components combine to form the continuous cycle of service enhancement necessary to protect, detect and respond to the constantly evolving landscape of cyber threats. The following sub-sections provide the specific details for each of the key features listed below:

- Alert Analysis and Investigation
- Threat Intelligence and Use Case Development
- Threat Hunting
- Incident Containment and Remediation
- Service Management and Reporting

Alert Analysis and Investigation

Brightsolid SOC analysts will triage Alerts received into the Microsoft Sentinel SIEM platform from the detection logic running across the available Customer Data Sources, open an Incident ticket in the Customer Portal and assign an Alert Severity Level. The Severity Level rating will determine the appropriate Triage Times which are detailed in the Service Levels and Response Times section.

Brightsolid SOC analysts will provide remote support where required to advise the Customer on containment/remediation actions and provide guidance to ensure non-recurrence of the Incident. Where the customer has procured other Brightsolid infrastructure services, Brightsolid SOC analysts will notify the relevant service delivery team.

This remote support service is capped at 2 hours per incident (being the Alert Investigation Period), during which the SOC shall provide Alert Analysis and Investigation. Any further investigation after the initial 2-hour remote support period will require the activation of the MDR Retained Incident Response Services.

Threat Intelligence and Use Case Development

Brightsolid will ensure that the Microsoft Sentinel SIEM use cases remain up to date with new threats and supports a continual process of increasing cyber maturity. The detection capability of the Microsoft Sentinel SIEM Software relies on up-to-date and actionable threat intelligence that is delivered as a central component of the service. The Microsoft Sentinel SIEM integrates numerous internal intelligence sources (including incident response findings, malware reverse engineering and Threat Hunting exercises) as well as a selection of external intelligence feeds.

The SOC actively develop new use cases which are aligned to the tactics, techniques, and procedures (TTPs) utilised by threat actors. The MITRE ATT&CK framework underpins the defined use cases to detect security anomalies in the customer's environment. The use cases defined by Brightsolid are queried against the customer's Microsoft Sentinel SIEM instance to detect anomalous behaviour which would trigger an Alert. Throughout this process use cases are tuned in collaboration with the Customer to remove any false positive alerts from the SOC, overall improving the detection efficacy.

Threat Hunting

Threat hunting is the approach of looking beyond defined use cases and signature-based detection in order to uncover advanced threats that would otherwise go undetected. Brightsolid SOC analysts interrogate the available data to conduct Threat Hunting campaigns, employing Analytics to find indicators of compromise (IOCs), suspicious behaviour and other unknown activity.

Threat Hunting campaigns are carried out monthly, using Analytics to find IOCs (Indicators of Compromise), suspicious behaviour and other unknown activity. The Customer may request that any such threat hunt campaign is targeted against a specific scenario that is mutually agreed in advance. A summary of each Threat Hunt's activities and any findings will be documented as a SOC ticket which can be found in the Customer Portal, any questions arising from the content or scope can be discussed with the SOC.

A scheduled, targeted threat hunting exercise can be requested at a maximum of once per month whereby the Brightsolid SOC analysts will run precise queries on all the available customer data to search for any unusual behaviour or anomalies particular to known adversaries or attack profiles relevant to the Customer. Each scheduled request must be submitted with a minimum of 14 days' notice and will typically run for approximately 3 hours with the findings and concerns collated into a SOC ticket.

Scheduled threat hunting exercises are typically requested when there is intelligence regarding adversarial activity against a particular vertical industry or a vendor in the supply chain has been breached, such requests should be arranged through the assigned Brightsolid Service Manager who will liaise with the SOC and facilitate the delivery of the findings.

Incident Containment and Remediation

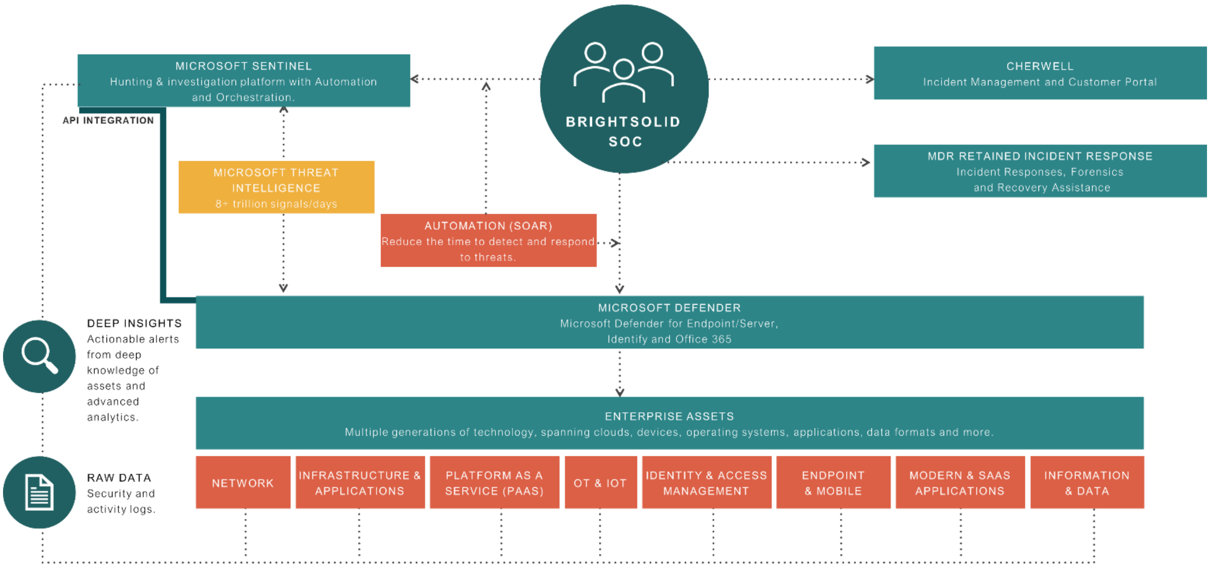
The SOC analyst will work collaboratively with the Customer's nominated point of contact to guide and support the activities necessary to contain and remediate any detected threats arising from the Alert Analysis and Investigation or Threat Hunting activities. Where there is the ability for the SOC to remotely disable, contain and remediate the detected threat, this will be executed following written authorisation from the Customer's point of contact.

If a detected threat cannot be contained or remediated within 2 hours, or where this cannot be executed remotely by the SOC, no further investigation will be undertaken until the MDR Retained Incident Response Services are activated by the Customer. The MDR Retained Incident Response Services ensure the availability of the CIRT team to commence remote and on-site forensic analysis of the incident in accordance with the applicable Service Levels, subject to the receipt of a purchase order for the relevant MDR Retained Incident Response Services.

Service Management and Reporting

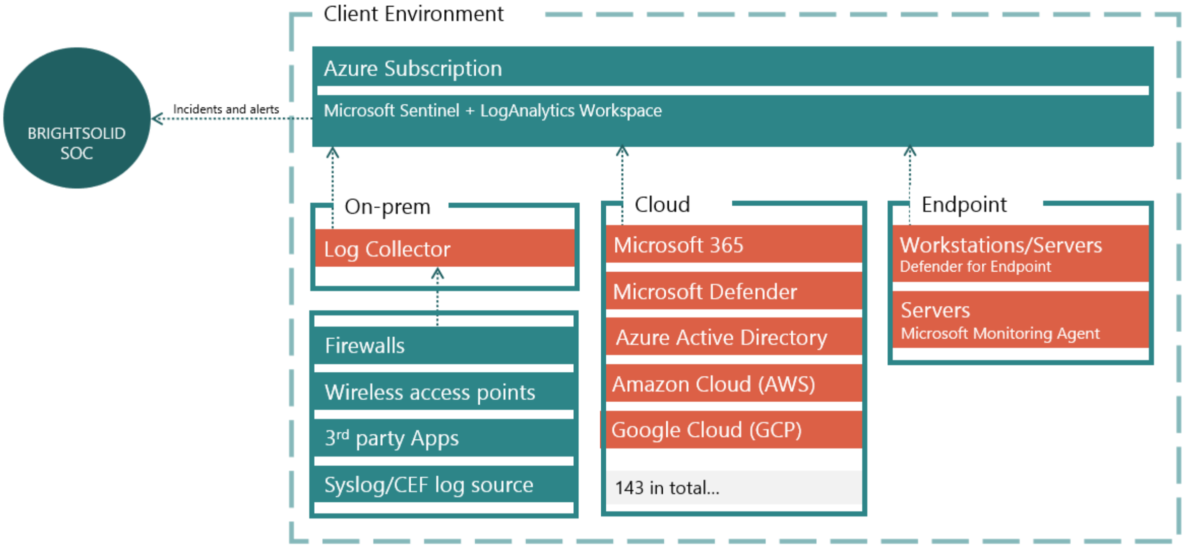
Reporting dashboards are provided on the Cherwell Customer Portal, these are continually developed to provide incident metrics of service performance. The Threat Hunting exercises, and a summary of investigated alerts will also be available on the Customer Portal and can be accessed on demand. Quarterly service review meetings will be scheduled by the assigned Service Manager to discuss performance, improvements, and customer satisfaction.

Brightsolid MDR Service Architecture


MICROSOFT SENTINEL
Hunting & investigation platform with Automation and Orchestration.
API INTEGRATION
BRIGHTSOLID SOC
CHERWELL
Incident Management and Customer Portal
MDR RETAINED INCIDENT RESPONSE
Incident Responses, Forensics and Recovery Assistance
MICROSOFT THREAT INTELLIGENCE
8+ trillion signals/days
AUTOMATION (SOAR)
Reduce the time to detect and respond to threats.
MICROSOFT DEFENDER
Microsoft Defender for Endpoint/Server, Identify and Office 365
DEEP INSIGHTS
Actionable alerts from deep knowledge of assets and advanced analytics.
ENTERPRISE ASSETS
Multiple generations of technology, spanning clouds, devices, operating systems, applications, data formats and more.
RAW DATA
Security and activity logs.
NETWORK
INFRASTRUCTURE & APPLICATIONS
PLATFORM AS A SERVICE (PAAS)
OT & IOT
IDENTITY & ACCESS MANAGEMENT
ENDPOINT & MOBILE
MODERN & SAAS APPLICATIONS
INFORMATION & DATA

The Brightsolid MDR Service leverages the Microsoft Defender suite providing security context and Analytics to detect anomalous behaviour across all data sources. The Microsoft Threat Intelligence feed amongst others identify indicators of compromise (IOCs) from the analysed data sets before presenting IOCs as alerts to the SOC. The Brightsolid SOC provides the use cases developed in the Microsoft Sentinel SIEM platform aligned to the tactics, techniques, and procedures (TTPs) used by threat actors. Finally, the Security Orchestration Automation Response (SOAR) layer is a key component for the SOC to triage known false positives and therefore enhance the detection and response times.

Data Collection



All log data resides within the Microsoft Sentinel SIEM instance in a segregated Customer Azure environment. Only data relevant to incidents and alerts are sent to the Brightsolid SOC. Logs are collected through data connectors, from on-premises log collectors, host-based agents, and cloud native data collectors. The data is transmitted to the Microsoft Sentinel SIEM via secure outbound connections from the on-premises log collectors. Only supported Microsoft Sentinel SIEM Customer Data Sources may be integrated.

Customer Onboarding

The following headline activities are undertaken by the service onboarding team and managed by a Brightsolid project manager. As implementation times vary by size and complexity of service, a detailed project plan will be created with the tasks and timescales to get to the Go Live Milestone.

Log Source Integration

Brightsolid SOC engineers will work closely with the Customer to specify a detailed log collection design. Once the design is signed off by the Customer then the service implementation project plan will be updated and the work to undertake the log sources integration will be scheduled.

Any requirements for the Customer to provide compute infrastructure for the aggregation of logs or for event collection will be specified in the design. The Customer will be responsible for the procurement and deployment of required infrastructure including any associated costs.

Upon successful integration, testing and validation of all the specified log sources into the Microsoft Sentinel SIEM, the Brightsolid SOC engineers will advise on achieving the optimum logging levels during the service-tuning period, the duration of this process is normally 2 weeks unless otherwise stated on the Customer Proposal. This is required to tune out any false positives alerts before transitioning to a live service.

Service Initiation Meeting

Following completion of the initial service setup tasks, the Brightsolid service management team will arrange a service initiation meeting. The aim of this meeting is to provide a smooth transition into live operation of the Brightsolid MDR Service. The meeting will be attended by the Customer and Brightsolid service manager, who will be responsible for ongoing service communications and management.

Following the meeting these documents will be agreed:

- Customer contact and escalation matrix
- Brightsolid contact and escalation matrix
- Incident handling and escalation procedure
- Customer Portal (Cherwell) access credentials

Platform Availability

The Microsoft Sentinel SIEM platform is built on the foundation of Azure Monitor Log Analytics. The availability of Microsoft Sentinel is based on the SLA for Log Analytics which can be found here (Azure LogAnalytics SLA). In addition, the platform is monitored for health, availability, and capacity by the SOC monitoring systems.

The SOC and CIRT operate 24 hours a day, 365 days a year.

Data Retention

The data retention period of the Microsoft Sentinel SIEM platform is set at 90 days by default. (Unless otherwise required by law to be retained for a longer period). However, anything beyond 90 days and up to maximum of 2 years is chargeable. The Onboarding form can be used by the Customer to specify their data retention requirements. If there is a requirement to store data beyond 2 years, Brightsolid can facilitate a solution on request.

Dependencies

Throughout this process, it is important to consider the following factors and dependencies to ensure a seamless transition/implementation of MDR:

Component	Overview	Next Steps/Why?
Azure tenant with an active subscription	The Customer is required to have an Azure tenant with global administrator permissions and an active subscription with owner permissions.	Brightsolid require this to deploy the Microsoft Sentinel solution into the Customer's dedicated Azure environment. If the Customer does not have an existing Azure account Brightsolid can set this up on the Customer's behalf.
Provisioning of log forwarders (syslog/CEF) on servers	The Customer will need to provision 1 dedicated virtual server with Ubuntu Linux v16_04, 2 CPU cores, 4GB vRAM and 40GB disk space to act as the dedicated log collector. This server needs to be accessible remotely by Brightsolid and send log data directly to Microsoft Sentinel.	Brightsolid require a log forwarder to enable logs to be collected from infrastructure resources where a log collection agent cannot be installed (e.g. firewalls, switches, routers, etc.)

Boundaries

The following section outlines features that are not in scope of the standard Brightsolid MDR Service (this list is not exhaustive):

- Provision of any required compute infrastructure to host or aggregate on customer premises (including customer cloud) collection agents
- Configuring customer event sources to enable event collection
- SOC interactions with customer systems not forwarding events to the Microsoft Sentinel SIEM Platform
- On-site remediation for security issues identified by the SOC unless a MDR Retained Incident Response contract has been included with the Customer Proposal
- Site visits, e.g. to install/cable/rack an RMA replacement
- Formal vendor or security training
- Obligation to provide a function or feature not already present or pre-identified.

Roles and Responsibilities

To ensure a successful implementation of the Brightsolid MDR service there are task and actions that need to be completed by key stakeholders within your organisation and by Brightsolid. These are comprised of the following components:

Component	Additional Info	Owner: Customer /Brightsolid	Overview of Responsibilities
Define log sources (Model/Version)	List of sources to be included in the service.	Customer	Brightsolid will provide the Onboarding Form for the Customer to complete.
Brightsolid MDR Azure Marketplace Subscription	This required to provide Brightsolid with access to the Customer environment via delegated permissions in Azure Lighthouse.	Customer	The Customer will be provided with a URL to the Brightsolid MDR Azure Marketplace offer whereby the Customer will need to subscribe to the offer with an Azure account which has Global Admin privileges.
Deployment of Customer Microsoft Sentinel SIEM Instance	This is required to store the collected data for analysis.	Brightsolid	The Customer will be provided with a URL to the Brightsolid MDR Azure Marketplace offer whereby the Customer will need to subscribe to the offer with an Azure account which has Global Administrator / subscription owner privileges.
Provisioning of log forwarders (syslog/CEF) on servers	This is required to collect logs from network devices.	Brightsolid/ Customer	Brightsolid will remotely install the log forwarding software on a physical or virtual server based on a minimum hardware specification provided by the customer.
Patching and maintenance of Log forwarders	This is required to keep the log forwarders secure and up to date with the latest features.	Brightsolid	Brightsolid will remotely install management software on the log forwarders to monitor and patch the operating system and log forwarder application.
Installation of log collection agents on server(s)	Log collection agents are required to send logs directly to the Microsoft Sentinel instance in the Customer Azure Tenant.	Customer	The software will be provided by Brightsolid for the Customer to install on their servers.
Additional log source configuration	Log sources that require configuration to send logs to the log collector or directly to Microsoft Sentinel.	Customer	This may be required for sources which require API configuration to send logs. Brightsolid will provide documented support where possible.
Deployment of Microsoft Defender for Servers	This is required for the SOC to be able to detect and respond to threats on servers.	Customer	The software will be provided by Brightsolid for the customer to install on their servers in passive mode. This will allow it to be run alongside another antivirus product.
Customer access to the Cherwell Customer Portal	A list of staff should be provided to respond to incidents raised by the SOC.	Brightsolid	A template will be provided by Brightsolid for the Customer to complete.

Service Levels and Response Times

Brightsolid maintains a 24x7 SOC which consists of a seamless blend of manned office hours and on-call.

The table below details how the severity of an Alert will be classified, and the associated Triage Time for each Severity Level.

Incident Severity	Description	Triage Time
P1 – High	A major breach of security has occurred, which requires immediate attention as unauthorised access has been obtained, or a denial-of-service attack has been successful	1 hour
P2 – Medium	A medium-risk breach of security may have occurred, which requires prompt attention; OR A protective device has denied legitimate activity and may be preventing critical business activities from occurring	4 hours
P3 – Low	An attempt has been made to breach security, which was unsuccessful either because the attack was not valid, or a protective device denied the activity; OR A low-risk breach of security may have occurred, which requires attention; OR A protective device has denied legitimate activity and may be preventing normal business activities from occurring	24 hours
P4 - Informational	An informational alert may have occurred, which requires attention	48 hours

Any Incidents which are categorised with the severity P1 are triaged 24x7, all other Incident severities are triaged within Business Hours.

The Service Level in respect of Triage Time for Alerts is set out in the table below. For the purposes of this Service Level, the Service Level Start Date shall be 4 weeks from the Relevant Go Live Milestone.

Objective	Service Level	Measurement Period
Alert Analysis and Investigation	90% of Alerts Triaged within the applicable Triage Time	Calendar Month

Additional Charges

The additional charges below are key components required for the Microsoft Sentinel SIEM instance deployed in the customer Azure tenant.

The charges are billed in either one of two ways:

- If the Customer has a CSP agreement with Microsoft, Brightsolid will pass through the cost of each component to the Customer on a monthly basis based on log consumption.
- If the Customer has an EA agreement with Microsoft, each of the components below will be paid by the Customer directly to Microsoft.

Component	Additional Info
Azure LogAnalytics	This is required to store the logs collected from the Customer environments. It is the component in which Microsoft Sentinel is built on.
Microsoft Sentinel	This is required to enable the Microsoft Sentinel SIEM capabilities that is built on top of LogAnalytics.
Microsoft Defender for Servers	This is to provide the Microsoft Sentinel SIEM with additional security analytics required for the SOC to detect and respond to malicious activity. It will be deployed to all server infrastructure in passive mode, which means it can run alongside other antivirus products.

The estimated costs for each component will be determined and provided to the Customer in the proposal.

During the term of the contract the customer can request changes to the scope and configuration of the Brightsolid MDR service which may be subject to an additional charge.