

CYBERHOUND FULLY MANAGED SERVICE



CYBERHOUND'S FULLY MANAGED SERVICE

CyberHound's fully Managed Service provides a comprehensive suite of services to assist schools manage the CyberHound Platforms.

CyberHound will provide full support services and, where necessary, connect to the CyberHound platform, to assist and/or resolve any support requests or to implement any requested changes. CyberHound support will be available during Business Hours (as defined).

The CyberHound Fully Managed Service includes:

- Management and resolution of support requests
- Hardware support incident management (warranty provided by HPE)
- Proactive monitoring of the CyberHound platforms
- Change Request process for CyberHound platform administration
- Management of updates to the CyberHound platform (microcode and major releases).
- Weekly policy backup service and remote restore process
- Reporting
- Annual Review

The proactive CyberHound platform monitoring service provides CyberHound's Managed Service Engineers with real-time alerting and diagnostics on key system components with parameter and threshold-based alerting. This includes memory utilisation, CPU load, HDD IO, RAID performance, HDD utilization and other critical areas.

The school will be responsible for solving any issues that may arise from the connection of third party ancillary infrastructure, software or services that affect the CyberHound platform. Where CyberHound is requested to assist in resolving non- CyberHound related issues, then an hourly charge will be payable.

CyberHound will use its best efforts to meet the service framework targets detailed in the table below.

Authorised school staff are required to provide a Priority / Severity Code on all change and support requests to assist with prioritisation. This helps ensure that Priority One and Two issues are dealt with as a matter of urgency.

The school will provide CyberHound with an up to date list of personnel who may lodge change or support requests with full contact details for each. This assists CyberHound in providing timely support and also ensures only authorised staff members may make change requests.

CyberHound Managed Services Framework

Priority/Severity Code	Description	Response Time* (business hours)	Resolution Time* (business hours)
Priority 1	A total loss of service that cannot be circumvented.	1 hour	4 hours
Priority 2	The service that is partially interrupted or impaired.	4 hours	8 hours
Priority 3	The service is experiencing a minor impact that can be circumvented or is restricted to a limited group of users.	6 hours	1 business day
Priority 4	The problem is circumvented with little or no customer impact. General request for information. Change Requests.	1 business day	1 business day**

Business Hours

Business Hours are defined as Monday to Friday, 8:30 am to 5.30 pm(AEST) excluding national public holidays.

**All response and resolution times are provided on a best endeavors basis and require full information, access to the CyberHound service and full cooperation from the authorised school personnel.*

Hardware warranty is provided by HPE and CyberHound will only take responsibility for incident management.

***For agreed Change Request items.*

CYBERHOUND FULLY MANAGED SERVICE



Definition of Response Time

Response Time is calculated using the associated timestamp (inside service hours only) in which a support or change request ticket is received into the CyberHound Managed Service queue. A response is deemed complete by any of following:

- The issue is resolved independently by the school
- A phone call or subsequent message has been left for the school
- A timestamped email response is sent to the school
- A resolution is provided to the school

Managed Service response times are subject to complete and accurate information being provided by the customer using the agreed support process. If timely feedback to requests from CyberHound are not received then the request will be stalled and placed “on hold” until the information or feedback is provided to enable the request to be progressed by CyberHound managed service engineers.

Definition of Resolution Time

Resolution Time is calculated using the associated timestamp (inside service hours only) in which a support or change request ticket is received into the CyberHound Managed Service queue. A resolution is deemed complete by any of following:

- The issue is resolved independently by the school
- The service has returned to standard working order
- A suitable work-around has been provided, removing or minimising the associated business impact

Disruptions to CyberHound services caused by third party services including fibre, fixed wireless, routers, switches, DNS and directory service faults are not considered in scope and not subject to resolution times. If timely feedback to requests from CyberHound are not received then the request will be stalled and placed “on hold” until the information or feedback is provided to enable the request to be progressed by CyberHound managed service engineers.

Process for Logging Support Requests

School authorised personnel will initiate all technical support requests and use an approved authorization code as a method of authentication. All support requests must follow this process and no support requests logged by third parties or non-authorised staff at the school will be actioned. Technical Support requests must include the following information:

- Authorised staff member logging the request (name, email and phone)
- Sitekey
- Severity level
- Fault description
- Any actions taken to diagnose or resolve the problem
- Phone number (best contact) at school
- Email address (best contact) at school
- Alternative contact at school (phone and email)
- Any additional information that may be relevant

Process for Logging Change Requests

Only authorized school staff will submit change requests Change requests must include the following:

- Authorisation code
- Authorised staff member logging the request (name, email and phone)
- Sitekey
- Change required
- Desired outcome of the change
- Timeframe/change window requested for change
- Priority level (default to be 4 for all change requests)
- Phone number (best contact) at school
- Email address (best contact) at school
- Alternative contact at school (phone and email)
- Any additional information that may be relevant

The school must notify CyberHound in advance (minimum 24 hours) of any planned infrastructure changes that may impact CyberHound platform services and immediately for unplanned interruptions, including:

- Router configuration changes
- Active Directory server changes
- DNS server changes
- Planned power outages
- Internet connectivity of infrastructure changes
- Any other relevant interruption that could affect the CyberHound service