

## MANAGED DEFENSE TERMINOLOGY

The following definitions are specific to the Managed Defense (MD) topics in this documentation portal.

| Term                  | Description   |
|-----------------------|---|
| Supported Technology  | Products or subscriptions supported by MD   |
| Security Event(s)     | An observable occurrence originating from your environment received by MD   |
| Alert(s)              | Security Events that have been reviewed by MD and determined to be evidence of a potential threat to your system or information.  |
| MD Alerts             | A view within the MD Portal which provides real-time prioritization of Security Events, status of the Security Event in the event lifecycle, and additional context as it becomes available.  |
| Investigation Report  | A report detailing MD's findings from an Investigation into a Security Event.   |
| Rapid Response        | A focused Investigation of restricted duration and scope to identify the extent of attacker activity in your environment.   |
| Tech Enabler          | A device which will be managed by Mandiant for the sole purpose of delivering the MD service. MD will have sole access to any Tech Enablers.  |
| Mission Based Hunting | Mission based hunting is defined by having a testable premeditated search criteria to locate malicious activities in an organizational environment. The hunt is conducted proactively and on a regular basis to detect adversaries, which may evade traditional detection or prevention mechanisms. |