Critical Start Managed Detection and Response

Service Comparison for Microsoft Products

	Microsoft Defender for Endpoint	Microsoft Defender for Servers	Microsoft 365 Defender	Microsoft Sentinel
Automatically resolve false positives at scale with the Critical Start Trusted Behavior Registry®	●	●	●	●
Contractual 60-min or less Median Time to Resolution (**MTTR**) service level agreement (**SLA**)	●	●	●	●
Dashboards provides complete and aggregated visibility into every alert with full details on the investigation and each action taken	●	●	●	●
Curate the new and updated detections being released daily by Microsoft	●	●	●	●
Management, curation, and maintenance of out-of-the-box detections and IOCs released by Microsoft	●	●	●	●
Curation of original and 3rd party threat intelligence, combined with real-time threat analysis to create a high-fidelity, actionable view of existing and emerging threats	●	●	●	●
Continuous development and enrichment of new threat detections and Indicators of Compromise (IOCs based on the latest evolving security landscape)	●	●	●	●
Threat detection content mapped to **MITRE ATT&CK® Framework**	●	●	●	●
Cyber Operations Risk and Response™ platform supports organizations with multiple tenants using parent/child hierarchy	●	●	●	●
Enhanced and optimized API ingestion	●	●	●	●

Service Specific Capabilities

	Microsoft Defender for Endpoint	Microsoft Defender for Servers	Microsoft 365 Defender	Microsoft Sentinel
Investigate, remediate, and resolve alerts for Defender for Endpoint	●			
Investigate, remediate, and resolve alerts for Defender for Servers		●		
Investigate, remediate, and resolve alerts for Microsoft Defender for Identity			●	
Investigate, remediate, and resolve alerts for Microsoft Entra ID Identity Protection			●	
Investigate, remediate, and resolve alerts for Microsoft Defender for Office 365			●	
Investigate, remediate, and resolve alerts for Microsoft Defender for Cloud Apps			●	
Investigate and respond to suspicious email phishing alerts and email			●	
Optional capability to send an email to the user informing them of the outcome of the investigation of their reported emails, positive or negative			●	
Notification templates used to provide investigation results of reported email are customizable			●	
Delete phishing emails from user's mailbox, confirm user accounts as risky, lock user, reset session, revoke access and force logoff, force password reset			●	
Remediation actions directly from Cyber Operation Risk and Response™ platform and MOBILE**SOC**® app	●	●	●	
Maintain block and allow lists for file hashes, processes, IP addresses	●	●	●	
Enforce Just-in-Time (**JIT**) Virtual Machine (**VM**) Access based on security threats alerts		●		
Investigate and respond to Network-Level Threat Detections		●		
Investigate and monitor multi-source security events (Active Directory, Windows, Linux, Applications, Firewalls)				●