

Microsoft Azure Sentinel

SIEM Advantage

Why MS Sentinel

Datashield was one of the first MDR providers to adopt Microsoft Azure Sentinel as a leading SIEM tool. With considerable operational experience with the platform over two years Datashield has been able to provide premiere white-glove MDR service to customers.

The Datashield Advantage

READY-TO-DEPLOY CONTENT	MATURE THREAT INTELLIGENCE	CUSTOM USE CASE DEVELOPMENT	EXPERIENCED ANALYSTS
<p>Increased coverage on Day 1 with content aligned with the MITRE ATT&CK framework and tested by red-team experts.</p> <p>Examples:</p> <ul style="list-style-type: none">• Data Exfiltration• Lateral Movement• Account Compromise• Command and Control• Execution	<p>Mature, MISP-driven threat intelligence program, curated by Datashield and brought into Azure Sentinel.</p> <p>Dozens of sources curated and pruned for false positives:</p> <ul style="list-style-type: none">• DHS• Infragard• OSINT• Closed/Paid Sources• Datashield-Developed and Researched	<p>Fully prepared to develop custom content based in unique or previously unseen log sources.</p> <p>Tailored to your environment:</p> <p>No two environments are the same, which is why our MDR service includes custom use case development to ensure the right detections are applied to the right log sources.</p>	<p>Datashield's analysts are already experienced with the platform. No spin up time required.</p> <p>Extensive operational experience in large enterprise environments.</p> <p>Datashield already has customers on Sentinel and are effective the day analysts get access to the SIEM.</p>

About Datashield

Datashield is a leading cybersecurity company that protects organizations by providing complex forensic cyber security services. Over the last decade, Datashield has stood out among our competitors as a true Monitoring Detection and Response (MDR) provider that delivers world-class results with white-glove service and a consultative approach.

