

THE DATASHIELD APPROACH / Truly SIEM Agnostic

1

WE WORK WITH WHAT YOU ALREADY HAVE

We manage or co-manage your SIEM infrastructure, regardless of your security products you already have installed. Gone are the days of imposing a proprietary solution, we provide a tool-agnostic approach.

2

WE KEEP COSTS DOWN

On top of the initial expenditure for the SIEM products; you have highly specialized staff to hire, tools to maintain and a security strategy to implement. Not to mention, misconfiguration, poor correlation rules and interface complexity that can slow you down. We take care of all this by stepping in and handling it for you, many times for less than the cost of a senior security analyst.

3

WE KEEP THINGS SIMPLE

We allow your team to only focus on mission critical items. Our goal is to keep you focused on your core competency. Our security experts, housed in our Advanced Security Operations Center (ASOC) filter out the false positives, handle the analysis and only alert you on validated threats. Oh, and by the way we provide context, remediation recommendations and in-depth reporting.

4

WE POSITION YOU TO BE MORE RESILIENT

SIEM tools are not a set it and forget it solution. You have to be diligent and agile with an ongoing approach to cyber-resilience. We actively hunt and assess threats with not only the scope of your organization in mind, but the context of the entire cyber landscape. With SHIELDVision we can detect threats across our entire customer base simultaneously. Utilizing the latest threat intelligence, we can "travel back in time" to correlate and identify compromises that may be missed by other technologies.



Stop Fighting with Your SIEM –
Eliminate Cyber Threat Uncertainty

PARTNER WITH
DATASHIELD
& STAY DEFENDED

ABOUT DATASHIELD™

- Comprehensive 24x7x365 continuous monitoring
- Full network visibility beyond signatures and logs
- Real-time advanced threat detection using cyber threat intelligence
- Active Hunting
- Deep Forensic Analysis

DATASHIELD's MDR - The DATASHIELD approach allows the customer to focus on validated threats only, which reduces the complexity and cost of threat detection. Working in partnership with your business, DATASHIELD will validate incidents, provide relevant context, investigate to determine scope and severity, and make recommendations for immediate containment and response.