DATASHIELD

Introducing DATASHIELD Managed Detection and Response (MDR) for RSA's Netwitness Technology

Organizations are often confronted with a lack of visibility and knowledge regarding the nature of traffic moving through their environment. The DATASHIELD MDR operates as an extension of the RSA Network Visibility Assessment delivered on RSA's Security Analytics technology.

The inclusion of experienced DATASHIELD Analyst's ensures you gain maximum benefit and showcases how the MDR offering can protect your critical corporate assets from cyber theft or espionage.

RSA's Netwitness captures and enriches network packet data to allow full visibility into your corporate environment. The DATASHIELD MDR uses the technology to detect and search for anomalous activity that may be present. When suspicious indicators are present, an MDR Analyst investigates deeper to determine if a real threat or incident exists. For a validated incident, all critical data is collected to provide you with a granular view of what is happening and how to approach remediation.

How the DATASHIELD MDR benefits you...

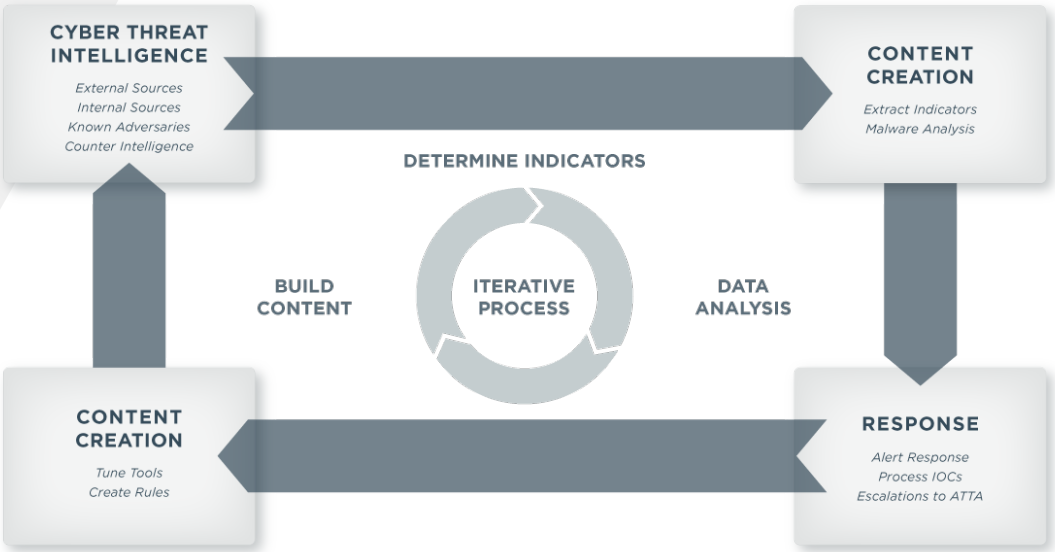
The DATASHIELD Managed Detection Response operates as an extension of your security team, providing the required skills and resource bandwidth to gain visibility into data security anomalies.

Did you know...

The average time from compromise to discovery is 146 days.

Do you have the expertise to reconstruct forensics and understand what was lost?

Dealing with a breach is one thing, effective threat prevention requires staffing, knowledge and resources.



866.428.4567 DATASHIELDprotect.com info@DATASHIELDprotect.com

DATASHIELD

We employ highly experienced Security Analysts who have defended mission critical assets in 24x7x365 National Security environments. We also work with global intelligence groups to actively hunt for bleeding edge threats and malicious conspirators who may be targeting your company's network.

Specifically, DATASHIELD utilizes full packet capture technology to seamlessly monitor ALL traffic on your network, not just those events that triggered an alarm. From this visibility advantage, DATASHIELD can reconstruct the actions leading up to an event to help your team understand how the event occurred as well as any additional activity after the fact. DATASHIELD can then take this knowledge and advise your team on mitigation strategies for any compromised assets as well as future prevention techniques.

Hunting and Critical Prevention with RSA

MDR Analyst Hunting – Also known as Ad Hoc hunting.

DATASHIELD Analysts will spend up to 10 hours during the POC period querying the captured network traffic data looking for abnormal activity that may be an indication of an incident. The MSS MDR Analyst's search criteria is based on years of experience chasing cyber adversaries. They utilize their knowledge of the TTP's employed, as well as, Cyber Threat Intelligence (CTI) indicating current cyber campaigns that may be active during the POC time period. The Hunting Analyst will follow any suspicious indicators to determine if it is a threat or no trouble found (NTF). Based on the results an Incident Notification is generated for all validated incidents.

DATASHIELD specializes in both proactive and postmortem forensics investigations of network activity. We employ highly experienced Security Analysts who have defended mission critical assets in 24x7x365 National Security environments.

SHIELDVision™

In addition to offering real-time forensics analysis Datashield has developed a premier security software called SHIELDVision.

SHIELDVision allows the MDR to quickly scan any customer or group of customer's environment(s) for the existence of threat security indicators. The indicators are gathered from a variety of internal and external sources and classified as breadcrumbs of Tactics, Techniques, and Procedures (TTP). Often these indicators are used by Cyber Criminals in attack campaigns, and in many cases, are not detected by traditional security defenses. A positive indicator from a SHIELDVision scan initiates an Analyst Investigation through RSA Security Analytics to validate an Incident has occurred and gather the specific details to provide context to any malicious activity.

866.428.4567 DATASHIELDprotect.com info@DATASHIELDprotect.com

DATASHIELD

Q & A Spotlight: DATASHIELD's CISO Ben Johnson and CTO Eldon Jenkins

Q: Why do companies need Datashield's MSS MDR?

Ben: Unless you are a company fortunate enough to have a team of 24x7x365 dedicated Information Security professionals monitoring all of your security information and events systems you are at risk of not being able to mitigate threats in a timely manner. DATASHIELD employs security professionals ranging from junior and senior analysts to advanced malware and threat intelligence engineers. Let DATASHIELD's experienced staff of security professionals be an extension to your existing team allowing your existing staff work on critical business projects rather than worrying about threats in your environment.

Eldon: Customers need DATASHIELD MSS because the threat landscape continues to grow every day. The cost and size of breaches continues to grow with the average cost now at $4M. Not all companies have the budget, skill-sets, or desire to build a 24x7x365 advanced security operations center. For most it is not their core competency. It is our core competency and your organization is already a target for cyber criminals. It isn't enough to drop in a tool, you need experienced people to run it. We bring experience, scale, and our own intellectual property. Our analysts hunt in many different environments and bring that experience to yours. Through our own tool, SHIELDVision, we enhance Security Analytics to reduce dwell time.

Q: What is Ad-Hoc Hunting?

Ben: Ad-Hoc hunting is a regular part of DATASHIELD's activities in our customer's environments. Our analysts will regularly search for signs of threats within the environments we protect. Think of this as searching for the 'needle in the haystack.' By using a combination of threat intelligence and data we gather from your environment we find threats that would not otherwise be found through most tools available today.

Eldon: Ad hoc hunting is proactively looking through your network for indicators of compromise, threats not mitigated by your defense in depth, abnormal traffic, and policy violations. We don't just wait for an alert, we hunt threats in your environment.

Q: If you already have the RSA application installed, why do you need DATASHIELD?

Ben: If you already have RSA's Security Analytics platform, DATASHIELD can help you get the most out of the technology. Our team of experts will handle everything from day-to-day management (availability, upgrades, configuration, etc.) to utilizing the platform, to identify and notify you of actual threats within your environment.

Eldon: The tool is not the solution. We run a global 24x7 SOC 2 Type II Advanced Security Operations Center. We bring experienced analysts who have worked in and see diverse environments to monitor and hunt in your environment. We bring threat intel gathered from our global customer base and content created internally. We bring enhancements to security analytics that give you advantages over SA alone and only available through us.

DATASHIELD: Your Managed Detection Response Partner

Contact DATASHIELD to find out how our Managed Detection Response Services can protect your enterprise from costly security breaches.