LevelBlue

WHITEPAPER

10 Opportunities for MSPs and MSSPs to Deliver MDR Services

LevelBlue
PARTNER PROGRAM

LevelBlue

The rise in cybersecurity attacks, coupled with the increasing adoption of cloud applications and services, has shown that traditional prevention-only security approaches are no longer effective. As a result, organizations are shifting toward a detection and response strategy to manage cybersecurity risks. However, keeping up with evolving threats, managing multiple security tools, and sourcing skilled security professionals remain significant challenges. To address these issues, many organizations are turning to Managed Detection and Response (MDR) services offered by service providers, including MSPs and MSSPs.

For service providers, the growing demand for MDR presents an opportunity to stay competitive and enhance value by helping clients defend against and respond to cyber threats. Here are 10 key opportunities to embrace and deliver competitive MDR services:

1	**Provide 24-Hour Monitoring:** Most organizations today operate online and remain continuously connected. However, many lack the resources to monitor their IT security around the clock. Providing 24/7 monitoring alleviates this burden for resource-constrained organizations and helps mitigate cybersecurity risks both during and outside regular business hours.
2	**Monitor Cloud Environments and Applications:** Many organizations are moving toward cloud deployment or have already begun using cloud-based applications for critical workloads such as email, collaboration, CRM, payroll, and identity management. However, traditional security tools and security teams often fall short in effectively monitoring these environments. This gap presents a growing opportunity for service providers to support organizations on their cloud journey.
3	**Identify the Attack Surface with Asset Discovery:** The assets deployed across an organization's environment define its attack surface, making them potential targets for malicious actors. One of the biggest challenges for IT and security teams—both in managing costs and mitigating cybersecurity risks—is maintaining visibility into what assets are deployed and where they reside. This challenge is further amplified by the ease and speed of creating new virtual machines in cloud and virtualized environments, making continuous asset tracking essential. Service providers can address this issue by incorporating asset discovery into their MDR services, ensuring clients have full visibility into their on-premises and cloud assets.
4	**Perform Vulnerability Scanning:** Identifying and addressing vulnerabilities is crucial, as they are often exploited to deliver zero-day threats and ransomware. It's no surprise that regular vulnerability scanning is a compliance requirement for many regulations. Once all assets in an environment are identified, the next step is assessing them for vulnerabilities—a necessary process given that an average of 14 new vulnerabilities are discovered each month. While some organizations may prefer to handle patching themselves, service providers can enhance their offerings by providing vulnerability remediation, including the application of available patches, as an additional service.
5	**Provide Log Management:** Identifying risks and detecting attacks requires analyzing events and logs, often across multiple systems. Determining the root cause of an attack involves piecing together these events, which can be challenging. Manually collecting logs from individual systems is resource-intensive—and that's assuming the logs are still available for the needed timeframe. Service providers can streamline this process with log management, automating event and log collection into a central repository. By normalizing log data for easier analysis and investigation and ensuring data retention for at least one year, providers help customers meet regulatory requirements (such as PCI DSS) and follow security best practices.

6	**Offer Advanced Intrusion Detection and Security Analysis:** These capabilities enable the rapid detection of threats across customers' on-premises and cloud environments, as well as their applications. Host-based IDS, file integrity monitoring (FIM), network IDS, and cloud IDS provide early warnings of attacks and unauthorized activities. Additionally, advanced correlation techniques—such as machine learning and behavioral monitoring—can identify threats that traditional defenses might overlook.
7	**Provide Threat Intelligence and Context:** To stay ahead of cyber threats, some organizations conduct their own research and analyze threat intelligence in-house, while others rely on third-party providers. However, both approaches can be costly—both in terms of upfront investment and the time required—especially when multiple commercial threat intelligence feeds are needed. Service providers that integrate threat intelligence into their offerings gain a significant advantage. By proactively identifying new threats and providing valuable context, they can enhance protection, improve response efforts, and demonstrate their expertise. This allows them to quickly answer key questions about cyber threats—who, what, why, and when—giving customers confidence in their security strategy.
8	**Deliver Incident Validation and Response:** When an incident is detected, the first step is determining whether it is a real threat or just noise— a process that requires advanced expertise. Next, organizations need detailed insights into the threat, including its nature, tactics, origin, target, threat actor, and recommended response. While some organizations prefer to handle response efforts themselves, there is a growing trend for service providers to take a more active role by containing or fully remediating incidents. Additionally, many providers conduct post-incident forensics to identify the root cause and strengthen future defenses.
9	**Deliver Backup and Recovery Capabilities:** Backup and recovery is the most fundamental aspect of business continuity, yet it is often poorly implemented across many organizations. This creates an opportunity for service providers to offer verified backup solutions, along with options for full or partial system and data recovery in the event of an outage or loss, such as a ransomware attack. To further differentiate their services, providers can also offer additional business continuity solutions, such as warm and hot site provisioning, ensuring organizations can quickly resume operations when disruptions occur.
10	**Provide Security Consultation:** Many organizations invest in disparate security tools that don't always integrate well, require expertise they lack, or fail to provide adequate protection for their environments. This challenge is further compounded by the shortage of skilled cybersecurity professionals and the increasing complexity of securing cloud and mobile assets. Service providers can bridge this gap by offering consulting services to help customers assess their environments, identify risks, and develop a comprehensive cybersecurity management plan. Additionally, they can provide training programs on key security topics, such as recognizing phishing attacks and responding effectively when they occur.

LevelBlue

About LevelBlue

At LevelBlue, we simplify cybersecurity through award-winning managed services, experienced strategic consulting, threat intelligence and renowned research. Our team is a seamless extension of yours, providing transparency and visibility into security posture and continuously working to strengthen it.

We harness security data from numerous sources and enrich it with artificial intelligence to deliver real-time threat intelligence, which enables more accurate and precise decision making. With a large, always-on global presence, LevelBlue sets the standard for cybersecurity today and tomorrow. We easily and effectively manage risk, so you can focus on your business.

Cybersecurity. Simplified.

Contact us to learn more, or speak with your LevelBlue sales representative.

LevelBlue
PARTNER PROGRAM