



SOLUTION BRIEF / MAY 2024

Reduce the Cost and Complexity of Threat Detection and Response



Help protect your business and your brand with LevelBlue Managed Threat Detection and Response—an intelligent managed detection and response (MDR) service that provides robust threat management in a single turnkey solution

Threat detection is one of the fastest-growing areas in cybersecurity, but talent is in short supply, leaving organizations to do more with less resources. As cybercriminals get smarter, more sophisticated, and constantly change their tactics, the burden falls to businesses to counter threats to critical networks and devices on premises, the cloud, and remote locations.

As businesses adopt digital transformation technologies, they are searching for better ways of protecting new hybrid and cloud assets. Rather than rely on purely preventative security measures, they're seeking early warning and response solutions to complete their security stack. Security information and event management (SIEM) tools can deliver massive amounts of data, but businesses may struggle to determine how to act on those insights. Facing a shortage of qualified cybersecurity professionals, and with the cost and complexity of mounting an effective detection and response program increasing, many organizations are choosing to outsource MDR services.

Benefits

- 24 x 7 security monitoring and incident response from our world-class Security Operation Centers (SOC)
- Integrate with your security and IT tools through BlueApps to extend the security monitoring and orchestration capabilities
- Built on our award-winning unified security management (LevelBlue USM) platform, MTDR combines multiple essential security capabilities into one unified console
- Fueled by continuously updated threat intelligence from LevelBlue Labs and the LevelBlue Open Threat Exchange
- Goal of getting your MTDR service fully operational within 30 days of signing your contract
- Personalized onboarding, including threat modeling exercises and building a custom incident response plan
- Utilize the security orchestration and automation capabilities of the LevelBlue USM platform to help streamline incident investigation and response activities and to help accelerate time to response
- Help your security team to respond quickly and effectively when an incident occurs, conducting incident investigations on actionable alarms and escalating based on severity
- Built in correlation rules, allowing users to immediately identify anomalous behavior, triggering alarms for the analysts

MDR is a complex and costly process, and cyber professionals are feeling the pressure to improve threat detection and response. Businesses are looking for reliable, trusted advisors to help protect their assets.

MDR: An integrated solution

LevelBlue Managed Threat Detection and Response is a sophisticated service that helps you detect and respond to advanced threats before they impact your business. It builds on decades of expertise in managed security services, our award-winning LevelBlue USM platform for threat detection and response, and LevelBlue Labs threat intelligence. With advanced features like 24x7 proactive security monitoring, security orchestration, and automation in one turnkey solution, you can quickly establish or scale your security program without the cost and complexity of building it yourself.

LevelBlue Labs, the threat intelligence unit of LevelBlue, produces timely threat intelligence that is integrated directly into the LevelBlue USM platform in the form of correlation rules and other higher-order detections to automate threat detection. LevelBlue Managed Threat Detection and Response is fueled with continuously updated threat intelligence from LevelBlue Labs, which has visibility into the LevelBlue Open Threat Exchange and other threat data sources.

With LevelBlue Managed Threat Detection and Response, your critical IT assets are being monitored 24x7 by an advanced SOC, freeing up your existing resources and allowing them to focus on more strategic initiatives. At the same time, we manage triaging and tier 1 and tier 2 support. LevelBlue has experience in delivering managed security services to some of the world's largest and most high-profile companies. Built on that legacy, the LevelBlue Managed Threat Detection and Response SOC has a dedicated team of security analysts who are focused on helping you to protect your business by identifying and disrupting advanced threats around the clock.

LevelBlue offers comprehensive MDR services through our world-class SOCs and Global Network Operations Center. These resources help to enable communication and collaboration and provide research, situational awareness and insight into cybersecurity threat activities on the Internet.

Features

- Continuous monitoring
- Compatible with other security tools
- Built on unified security management
- LevelBlue Labs Threat Intelligence
- Faster time to detect and respond
- Personalized onboarding workshop
- Orchestration and automation
- Incident response
- Built-in correlation rules

About LevelBlue

We simplify cybersecurity through award-winning managed security 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. This 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.

For more information, contact a LevelBlue Representative to request a quote or visit our [LevelBlue Managed Threat Detection and Response](#) page.