LevelBlue

Managed Detection and Response Services

Defend with confidence. Respond with precision.

LevelBlue Managed Detection and Response (MDR) is an industry-leading threat detection and response service. Our experts identify, investigate, and eliminate cyber threats while leveraging your existing security tools to reduce risk and maximize ROI.

Improve your threat visibility

It starts with improving your threat visibility. LevelBlue's cloud-native extended detection and response (XDR) security operations platform, LevelBlue Fusion, leverages your existing security tools and infrastructure to ingest high-value telemetry, expanding visibility into potential threats across your hybrid multi-cloud operations. We connect your high-value security tools to provide you and our security engineers with the context needed to eliminate active threats and prevent lateral movement.

Detect and respond faster

Armed with greater visibility, enriched by LevelBlue threat intelligence and context from your security infrastructure, LevelBlue detects and responds faster than anyone else. The telemetry we ingest, analyze, and contextualize through the Fusion platform enables real-time threat monitoring while significantly reducing unwanted noise.

When a threat or anomalous behavior is detected, our team immediately triages, contains, and investigates. We eliminate false positives so only confirmed threats requiring action remain – improving productivity and reducing time spent investigating alert noise and false positives across your security tools, effectively eliminating alert fatigue. *(case study: "12 million events per day... into 12 priority incidents")*

Most providers leave response up to you. At LevelBlue, response actions can be executed by your team or ours using your predefined response protocols, fully integrated into our SOC workflows. In the event of a breach, every second counts – which is why LevelBlue SpiderLabs Remote Incident Response experts are available to deploy immediately. *(case study: "We weren't expecting... to discover that a member of our own team was spreading malware")*

Boost your security posture

LevelBlue becomes a valuable extension of your team, helping boost your security posture. In addition to 24×7 detection and response, our elite SpiderLabs cyber experts continuously track sophisticated threats and threat groups, analyzing their tactics, techniques, and procedures (TTPs) to help fortify your defenses.

Connect your hybrid multi-cloud operations for greater visibility of threats across your distributed workforce and extract more value from your existing security infrastructure.

Eliminate active threats with speed and precision. Monitor for threats in real-time, detect and respond to incidents within minutes. Augment your security team and focus on what matters.

Future proof your security. Stay ahead of the most sophisticated attackers with an elite team of cyber experts working for you every day to fight cyberthreats.

Benefits

- Eliminate active threats with 24×7 global coverage
- Augment your team with industry-leading cyber experts
- Increase ROI from your existing tools

The cumulative knowledge gained from ongoing threat research, global client engagements, and curated threat intelligence is seamlessly integrated into the LevelBlue MDR service to protect your organization from the latest cyber threats – whether they originate inside or outside your environment. *(case study: "We weren't expecting... to discover that a member of our own team was spreading malware")*

Unlike many other MDR providers, LevelBlue offers a comprehensive portfolio of cyber experts and services designed to take your cybersecurity program to the next level.

LevelBlue MDR Service

Service Features	MDR	MDR Elite
24×7 Threat Detection, Prioritization, and Investigation	•	•
Threat Response	•	•
Threat Hunting and Malware Reverse Engineering	•	•
Unlimited EDR Security Telemetry	•	•
Client Success Manager	•	•
Security Colony Subscription	•	•
Named SpiderLabs Threat Expert		•
SpiderLabs Remote Incident Response		•
Service Levels for MTTA and MTTR		•
LevelBlue Fusion Platform	•	•
LevelBlue Fusion Mobile App	•	•

LevelBlue Fusion platform

The LevelBlue Fusion platform is a cloud-native threat detection and response platform augmented by security orchestration, automation, and response (SOAR). Its primary mission is to ingest high-value telemetry and enrich it with context and threat intelligence to detect threats in near real time. The platform also serves as a security operations workflow engine, supporting investigation and response activities. Through the web portal or mobile app, users can monitor activity in real time, participate in investigations, collaborate with experts, create tickets, and access custom reports – enabling incident response from anywhere.

LevelBlue SpiderLabs

LevelBlue SpiderLabs is a world-renowned team of security researchers, ethical hackers, forensic investigators, and incident responders. Our cyber threat analysts specialize in tracking nation-state and professional criminal threat actors and analyzing their offensive campaigns.

Security Colony

Many of the challenges you face have already been encountered and addressed by others. LevelBlue Security Colony (included) provides access to a library of knowledge and on-demand resources drawn from years of consulting experience across thousands of real-world client engagements. This helps reduce the time and cost required to solve common cybersecurity problems.

Rapid Time-to-Value

- No one in industry is faster to value
- Seconds to ingest data, outcomes produced in 10 min or less
- Onboard in less than 10 days, the right way

Faster Response Times

- No one in the industry responds faster*
- Personalized MTTR of less than 30 minutes
- Client defined response protocol fully integrated into SOC workflows and platform

*based on review of competitors' publicly stated MTTR specifications

Unrivaled Threat Intelligence

- Billions of records in global threat intelligence database
- Only provider with 6 Global Cyber Threat Research Centers
- Decades of threat intelligence leadership and a team prolific in finding threats and vulnerabilities

Dedicated Cyber Success Team

- A dedicated named resource with you for the life of the service
- We detect what others can't with intimate knowledge of your environment for better tuning, faster and more efficient response

Best-of-Breed Partnerships

We're committed to connecting your hybrid multi-cloud operations to help you realize greater value from your existing security investments, together with our partners. No one in industry is faster to value

- LevelBlue MDR for Microsoft Defender
- LevelBlue MDR for Palo Alto Networks Cortex XDR
- 70+ API integrations, bi-directional
- And much more...