IBM Threat Detection and Response Services

Fighting cyberthreats 24x7 with generative AI

Highlights

Unify threat detection and response

Reduce risks with proactive cybersecurity

Prioritize alerts with generative AI

Improve security operations effectively

Cyberattacks have become more pervasive, innovative and faster. The average cost of a data breach has increased to USD 4.88 million. More than half of organizations are being alerted about a breach by a third party or an attacker.[1] Taking these alarming factors into account, it's essential that you build a robust cybersecurity program to protect your organization from cyberattacks. Over 50% of organizations hit by a breach last year plan to increase their cybersecurity investments, focusing on incident response planning and threat detection and response.[1]

IBM® Threat Detection and Response (TDR) Services provide 24x7 monitoring, analysis and remediation of security alerts across hybrid cloud environments. TDR is delivered through the IBM® X-Force® Protection Platform and applies AI and contextual threat intelligence to automate detection and response. It offers consulting and advisory support to strengthen security operations and X-Force services to improve an organization's resilience, risk profile and security posture.

TDR reduces false positives by 90% and helps you prioritize high-value alerts and vulnerabilities, using AI trained on 150 billion telemetry pooints daily.

Benefits

Unify threat detection and response
Our X-Force Protection Platform integrates with your existing security technologies so you can avoid “rip and replace.” You can unify your enterprise-wide security assets and workflows—whether on-premises or in the cloud—using our open API. This approach allows your team to continue using the existing tools while we collaborate through an integrated workflow.

Reduce risks with proactive cybersecurity
TDR helps you prevent vulnerabilities, understand detection effectiveness, and get personalized recommendations to improve your security posture and organizational resilience. To stay ahead of ransomware and other cyberattacks, you can see how your environment aligns with MITRE ATT&CK framework’s tactics, techniques and procedures (TTPs). In addition, TDR uses AI to consolidate your detection tools and policies. It delivers a comprehensive view of how to detect threats and close gaps using the ATT&CK framework.

With TDR, you can practice proactive security and reduce the risk through adjacent services such as exposure and posture management. Also, our X-Force Red Offensive Security Services and X-Force Incident Response Services help you tackle the latest threats.

Prioritize alerts with generative AI
TDR reduces false positives by 90% and helps you prioritize high-value alerts and vulnerabilities, using AI trained on 150 billion telemetry points daily. It allows you to focus on critical threats by decreasing low-value SIEM alerts by 47% and increasing high-value alerts by 28%.

You can accelerate threat detection and response with our generative AI-powered capabilities, built on IBM watsonx™. The IBM Consulting® Cybersecurity Assistant within TDR provides intelligence on operational questions ranging from threats to cases and augments SOC analyst research. It explains complex security events and commands, including providing potential recommendations.

TDR can automatically disposition or remediate up to 85% of alerts, and our new generative AI capabilities can empower analysts to investigate the remaining 15% of alerts faster. The IBM Consulting Cybersecurity Assistant recommends actions based on activity patterns to reduce attackers’ dwell time. With the automation of routine tasks and enhancement of analyst capabilities, we reduce the investigation time by up to 48%, resulting in faster and more accurate threat response.

Improve security operations effectively
Threat management is an ongoing process that demands a strategic approach. We can enhance your security operations by using automated and systematic methods. TDR can help you quantify cyber risk to ensure alignment with business risk, expand operational automation and increase business resilience. You can use our governance model to continuously improve your threat management program. We can benchmark your performance and provide a monthly maturity readout on your progress toward your improvement goals. We can also help you enhance the maturity and effectiveness of your SOC to better address specific areas of concern.

With TDR, you can shift from a reactive threat management strategy to a proactive, AI-infused approach. It can help you guard existing investments, strengthen defenses, improve security operations and protect the hybrid cloud.

Why IBM
We create solutions unique to your organization's cybersecurity needs. We offer world-class consultants, X-Force threat intelligence, generative AI-powered managed security services, and flexible, hybrid delivery models. Entrust your organization's cybersecurity to us and focus on what matters the most—the impact your business is making worldwide.

To learn more about IBM Threat Detection and Response services, please contact your IBM representative or IBM Business Partner. You can also visit the web page.

If you're ready to dive in and start improving your security program today, schedule a no-cost half-day threat management workshop.

If you're experiencing cybersecurity issues or an incident, contact X-Force to help.

US hotline: 1-888-241-9812
Global hotline: (+001) 312-212-8034

1. Cost of a Data Breach Report 2024, IBM, August 2024.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
August 2024