IBM Threat Detection and Response Services

Your partner against cyber threats with 24x7 prevention and faster, AI-powered detection and response

Cyberattacks are more pervasive, innovative, and faster than ever. With the average cost of a data breach reaching an all-time high of $4.45M USD[1], and 2/3 of organizations being alerted about a breach by a third party or attacker[1], you need a security program in place that can speed up threat detection and response and uncover your blind spots. However, an expanding attack surface, disconnected security tools and a rampant cybersecurity skills shortage affecting 57% of organizations[2] present challenges to overcome.

Improve security with automation, AI and proactive defenses

More than half of organizations that have been hit by a breach in the last year plan to increase their security investments[1]. The top areas of expenditure include incident response planning and threat detection and response. Why are these such critical components of a successful security program? The average savings for organizations that use security AI and automation extensively versus those that don't is $1.76M USD and 108 days in saved breach response times[1]. Similarly, organizations investing in incident response see a savings of $1.5M USD in breach costs[1]. These investments produce results, both in cost savings and in reducing business disruption.

Highlights

- Stop attacks 24/7 with faster detection, investigation, and response built on intelligence and AI-powered automation
- Gain comprehensive visibility into your attack surface and programmatically lower your risk profile
- Use your existing security technologies
- Continuously improve security operations
- Proactively hunt for malicious TTPs with IBM's proprietary threat hunt library
- Global scale, local delivery

IBM Threat Detection & Response Services

With IBM’s Threat Detection and Response (TDR) Service, our global team of security analysts provide 24x7 monitoring, analysis, and response of security alerts from all relevant technologies across our client’s hybrid cloud environments. This service is delivered via IBM’s state-of-the-art security services platform, the X-Force Protection Platform, which applies multiple layers of AI and contextual threat intelligence from IBM’s vast global security network - helping automate away the noise while quickly responding to the threats that matter most.

We can help your organization reduce cyber risk with a global, end-to-end, vendor-agnostic threat solution that can manage any alert at any time and give you the visibility and integration necessary to better manage threats.

IBM Threat Detection and Response (TDR) services helps your organization:

Unify threat detection and response with AI

Our X-Force Protection Platform provides a method for integrating all of your security technologies cohesively so you can avoid “rip and replace”. Integrate your enterprise-wide security assets and workflows, whether on-premise or in the cloud, with our open API so your teams can work within your tools while we collaborate.

Practice proactive security to reduce risk

Prevent vulnerabilities before they occur, understand your detection effectiveness, and get personalized recommendations for how to improve your security posture.

To stay ahead of ransomware and wipe-out attacks, organizations can see how their environment aligns to MITRE ATT&CK framework tactics, techniques & procedures (TTPs). By applying AI, TDR reconciles the multiple detection tools and policies currently in place at an organization to provide an enterprise view into how to best detect threats and close gaps using the ATT&CK framework.

Our TDR service also seeks to help you practice proactive security to reduce your risk through adjacent services such as exposure and posture management. Our X-Force Red offensive security services and X-Force Incident Response teams will help you prepare to respond to the latest threats.

Continuously improve security operations: Threat management is a journey and we can help you programmatically mature operations. TDR services can help you quantify cyber risk to ensure alignment with business risk, expand your operational automation and increase business resilience. We also help you drive continuous improvement for your threat management program through our governance model. We benchmark your performance and provide a monthly maturity readout against your continuous improvement goals along with security operations center (SOC) maturity acceleration if you want help targeting specific problematic areas.

IBM TDR helps drive speed and agility

Reduce false positives

Reduce false positives by 90% and prioritize high value alerts and vulnerabilities, with our AI trained on 150 billion points of telemetry daily, to enable faster detection and response.

Increase high-value alerts

Spend time on the threats that matter by reducing low-value SIEM alerts by 47% and increasing high-value alerts by 28%.

Improve investigation time

Experience a 48% reduction in investigation time based on grouping of similar alerts instead of individual alert analysis.

Accelerate response and active threat blocking

IBM's AI-powered automation, integrated SOAR capabilities, and on-going playbook lifecycle management enable automated and human response actions to proactively block threats, resulting in automation of up to 85% of alerts.

Enhanced visibility and detailed investigations

IBM's world-class X-Force threat intelligence and incident response teams combine organic threat intel with analytics to help protect organizations from advanced threats 24/7

Proactive human-led threat hunting to extend beyond traditional prevention

Proactive threat hunting augments traditional security solutions to uncover anomalous activity. IBM's proactive threat hunters work with organizations to help identify their crown jewel assets and critical concerns. This input enables the threat hunting team to create fully tailored threat hunt reports and customized detections.

Powering protection across the enterprise with global threat intelligence + AI-powered automation

Early detection depends on intelligence. IBM TDR's around-the-clock high-fidelity detection integrated with IBM X-Force's advanced threat intelligence feeds and detailed analytics provide IBM security experts with additional context, custom detections, and insights into emerging TTPs for continuous threat hunt development and skilled threat analysis to help organizations proactively detect threats faster.

Our AI machine learning (ML) capabilities filter alerts based on activity observed across our entire global footprint of security operations centers for the past two years, reducing false positives and accelerating detection so teams can focus on high priority threats, including rare event detection. IBM further integrates SOAR capabilities for operational transparency, collaboration, and on-going playbook lifecycle management. We integrate our outcomes to you. Integrate our team with your workflow via SOAR-to-SOAR integration or use our API to integrate our outcomes.

IBM TDR = Powerful Threat Defense

Your organization faces complex challenges and we bring together everything needed to create solutions unique to your business in a way no other organization can. With world-class consultants, X-Force threat intelligence, market-leading managed security services and hybrid delivery models to meet clients anywhere in the world, we can help you maximize your current investments while building for the future. Leave the security of your organization in our hands so you can focus on what matters most - the impact your business is making in the world.

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Threat Detection and Response services, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/services/threat-detection-response

1. IBM Cost of a Data Breach 2023
2. ESG: The Life and Times of Cybersecurity Professionals 2021, Volume V