IBM Security Managed Detection and Response Services

Faster threat defense starts with 24/7 managed prevention, detection and response — powered by AI

With a growing number of laptops, desktops and remote workers, sophisticated cybercriminals have even more open doors to your organization. From these entry points, they can often proceed deep and unnoticed. Compounding the problem is the shortage of in-house security staff to protect organizations against these advanced attacks.

It's essential for organizations to defend this expanding attack surface by shifting from reactive, signature-based threat management solutions to a proactive, intelligence-based approach that utilizes a highly skilled, dedicated security team who delivers continuous monitoring, analysis and rapid response to sophisticated attacks. Technology alone will not ward off advanced attacks. For organizations to successfully defend against attacks, they need a trusted partner to continuously monitor their network and endpoints, provide visibility, automate response actions, hunt threats for malicious activity and apply the latest threat intelligence cultivated from incident response (IR) experience.

Highlights

- IBM Security MDR is a component of IBM Security X-Force Threat Management, the industry's broadest portfolio of solutions that manage the full threat management lifecycle.
- Defend against attacks with AI-powered detection, threat hunting, and response built on threat intelligence.
- Vendor agnostic to preserve existing security technology investments.
- Proactively hunt for malicious TTPs with IBM's proprietary threat hunt library

IBM Security MDR Services

IBM Security Managed Detection and Response Services (MDR) delivers a 24/7 threat detection and fast response capability, fueled by threat intelligence and proactive threat hunting to reveal undetected threats faster while improving SOC productivity. IBM's AI-powered automation coupled with human-led analysis speed threat response across networks and endpoints in hybrid multicloud environments.

IBM Security MDR includes Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) tools to conduct detailed investigations, including IBM's proprietary Tactics, Techniques and Procedures (TTP) threat hunt library and next-generation antivirus for behavior-based blocking and continuous policy management. This comprehensive threat management service utilizes IBM's Global Security Operations Centers (SOC) network, integrated infrastructure, deep expertise and threat intelligence to deliver improved visibility and actionable insights for effective threat defense, including protection from zero-day threats.

IBM Security MDR highlights and benefits include:

Enhanced visibility and detailed investigations

IBM's world-class X-Force threat intelligence and incident response teams combine organic threat intel with analytics to provide muti-vector visibility and context to stop threats across networks and endpoints 24/7.

Consistent outcomes for future threat protection

With a focus on IBM's proprietary TTP threat hunt library, IBM Security MDR finds threats more consistently than static indicators of compromise (IOC) and delivers outcomes regardless of the changing threat landscape.

Comprehensive security without complexity

IBM Security MDR's turnkey capabilities support organizations' existing endpoint and network security technologies, eliminating the need to rip and replace or risk vendor lock-in.

Rapid response and active blocking

IBM Security MDR's AI-powered automation, integrated SOAR capabilities, and on-going playbook lifecycle management enable automated and human response actions to proactively block threats.

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

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

IBM Security MDR's AI capabilities go beyond traditional systems of defense. IBM's AI stack automatically filters alerts across networks and endpoints, reducing false positive noise so teams can focus on high priority threats. Additionally, IBM Security MDR includes proprietary rare event detection algorithms to identify zero-day vulnerabilities in the organization's environment. IBM further integrates SOAR capabilities for operational transparency, collaboration and on-going playbook lifecycle management.

Trained IBM Security specialists combined with IBM's threat intelligence and AI advanced capabilities makes the IBM Security MDR threat management solution a powerful differentiator of enterprise protection. Analysts and incident responders working across IBM's global SOCs in a follow-the-sun model, apply IBM Security X-Force threat intelligence and the experience of working with thousands of IR investigations across all industries to help accelerate the detection, prioritization and response to the most critical alerts. With this deep IR knowledge, IBM Security MDR experts also deliver reports on investigations, IR recommendations and consulting including risk assessments and compliance reviews to help improve security postures.

Proactive human-led threat hunting to extend beyond traditional prevention

Proactive threat hunting is an integral component of IBM Security MDR and augments traditional security solutions to uncover anomalous activity within an organization's environments. 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.

IBM's team of expert hunters further uses the MITRE ATT&CK framework and proprietary TTP threat hunt library, consisting of hundreds threat hunts for telemetry collection automation that enable IBM threat hunters to focus on the analysis required for improved visibility, to reveal dormant threats as well as the most sophisticated attackers. IBM's human-led and automated threat hunting intelligence further feeds into our global threat intelligence, data and capabilities to enable more decisive and accelerated response to attacks.

IBM Security MDR + X-Force Incident Response + Threat Intelligence = Powerful Threat Defense

IBM Security Managed Detection and Response Services deliver a unified threat management strategy, incorporating multiple endpoint and network security technologies, threat intelligence and the expertise of thousands of global analysts to provide the visibility to better protect, detect and respond to threats across the enterprise.

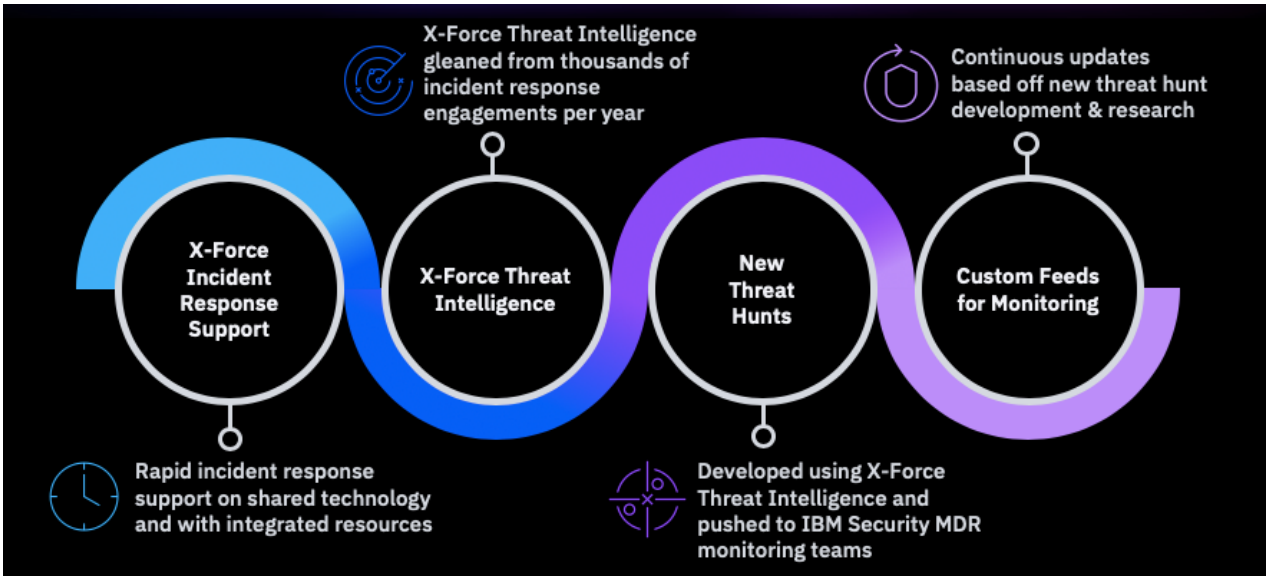

Figure 1: Integrated teams: Incident Response, Threat Intelligence, Managed Detection and Response

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 Security 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.

For more information

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