Managed Detection and Response for AWS Endpoints

Effective threat defense for AWS environments begins with 24/7 prevention, detection and fast response fueled by intelligence and proactive threat hunting

The IBM Security Managed Detection and Response (MDR) Services team is comprised of industry-leading, highly skilled incident response professionals and threat hunters experienced in investigating compromises of AWS environments.

IBM Security MDR leverages AWS-native tools, automation, an intelligence-driven approach, and industry-leading skills to respond to AWS compromises and helps organizations monitor, detect, investigate and respond to security incidents more efficiently and effectively.

Highlights

- Help to minimize time, costs and exposure associated with breaches in your AWS environments
- Defend against attacks with endpoint and network detection, threat hunting, and response built on intelligence
- Decrease dwell time of attacks and accelerate time to investigate
- Proactively hunt for malicious TTPs with proprietary threat hunt library

IBM Security MDR for AWS

IBM Security Managed Detection and Response (MDR) Services delivers a turnkey 24/7 threat prevention, detection and fast response to help secure the hybrid or multicloud environments, including AWS. Fueled by threat intelligence and proactive threat hunting, IBM Security MDR includes Endpoint Detection and Response (EDR) and network telemetry tools to conduct detailed investigations across the enterprise. 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

A global team of cybersecurity experts, powered by world-class intelligence, uses endpoint visibility to help protect organizations from advanced threats 24/7.

Consistent outcomes for future threat protection

With a focus on TTPs, 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

There is no need for integration of new log sources or use cases. IBM Security MDR continuously collects data across multiple endpoint and network security technologies and next-generation antivirus solutions and provides accelerated threat management.

Rapid response and active blocking

Automated threat mitigation and live chats with IBM threat experts help respond to and proactively block threats.

Powering protection with global threat intelligence

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 into emerging TTPs for continuous threat hunt development and skilled threat analysis to help organizations proactively detect threats faster.

Trained IBM Security specialists combined with IBM's threat intelligence and advanced technology makes 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 EDR detections.

IBM's team of expert hunters further uses the MITRE ATT&CK framework and proprietary TTP threat hunt library, consisting of hundreds of 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 technologies, intelligence and the expertise of thousands of global analysts to provide the visibility to better protect, detect and respond to threats across the enterprise. Sold separately, the X-Force Incident Response Retainer service is a subscription that provides 24/7 support to manage major incidents and is recommended as a natural escalation workflow by IBM Security Services. Please see the X-Force Incident Response for AWS solution brief for more information on how the service uses AWS native tools to conduct cloud-native forensic investigations.

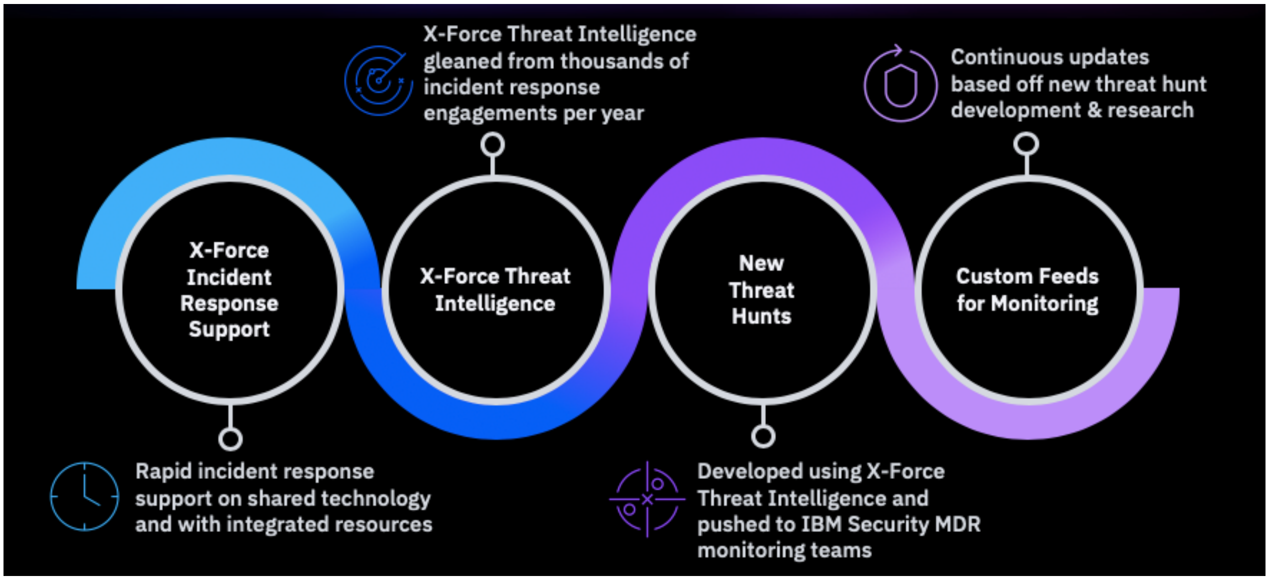
X-Force Threat Intelligence gleaned from thousands of incident response engagements per year
Continuous updates based off new threat hunt development & research
X-Force Incident Response Support
X-Force Threat Intelligence
New Threat Hunts
Custom Feeds for Monitoring
Rapid incident response support on shared technology and with integrated resources
Developed using X-Force Threat Intelligence and pushed to IBM Security MDR monitoring teams

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.

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 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