

IBM Security X-Force Incident Response Retainer

Highlights

- Fast response from an expert team as soon as a breach is suspected
 - Reduced risk and exposure through threat intelligence and analytics
 - In-depth training offered for internal teams to better combat incidents
-

Strengthen your incident readiness with intelligent threat detection and faster response times

A security breach can cause operational disruptions, data leaks, reputation damage and regulatory complications. But, a threat prevention and response strategy can speed recovery from unexpected security breaches and help prevent future incidents.

The IBM Security X-Force® Incident Response Retainer is a subscription-based service that provides access to a team of trusted experts trained to help you effectively respond to threats. This service can give greater visibility into threats, significantly reduce response and recovery times and reduce the impact of a breach. The X-Force Incident Response Retainer offers the flexibility to meet your organization's needs with a number of proactive offerings from its tiered response plans.

Respond to incidents quickly while reducing risk and costs

Featuring 24x7 support through a global emergency hotline, the X-Force Incident Response Retainer is available when you need it the most. Support teams are always available and ready to swiftly respond to any reported incidents. The availability and responsiveness of these teams help reduce the impact of an incident on your brand, reputation and finances.

Once connected to the hotline, security professionals will work to diagnose the incident within one hour. Following the diagnosis, IBM experts will be dispatched and can be on site in 24 - 48 hours.

Once onsite, they take priority actions by:

- Identifying the source of the attack
- Finding the root cause
- Connecting the incident to any known threat actors
- Managing and reducing the impact

All options will be explored to prevent the spread of malware and quickly restore systems and networks. They'll also take steps to reduce the risk of future incidents. This rapid and complete response helps you stop attacks in progress, limit their impact and recover faster. Finally, they'll perform an in-depth forensic analysis to uncover every detail of an incident.

For even more insight, the X-Force team can connect global threat intelligence information with specific events and incidents to deliver complete visibility into any incident. And, using data collected from IBM Managed Security Services operations, X-Force can give you deeper insights into current threats and security events.

Prepare your teams to prevent or quickly respond to future attacks

The X-Force Incident Response Retainer has a menu of proactive services that let clients choose the services that meet their most pressing needs, including:

- Incident response program assessment
 - IBM will review your existing incident response program, interview key stakeholders to better understand personnel, processes and technology, and deliver a roadmap containing priorities for improvement.
- Threat intelligence program assessment
 - IBM will review your threat intelligence services and determine priority intelligence requirements based on industry best practices.
- Strategic threat assessment
 - IBM will review your key assets to associate threat events to typical attackers, likely infection methods and the techniques and procedures that attackers use.

- Incident response playbook customization
 - IBM will analyze your existing playbook or create a new playbook that will address the most likely, high-priority incidents that may occur within your environment.
- Dark web analysis
 - IBM will search the dark web for specific areas of interest using key words. Then, they will analyze the results and provide key findings and recommendations.
- Incident response plan review or creation
 - IBM will perform a high-level assessment of the client's existing incident response plan and outline areas of improvement. If no plan exists, they'll develop a new one.
- First responder training
 - IBM will organize workshops to help improve your IT department's incident preparedness, response and analysis
- Active threat assessment
 - IBM will find current and historical threats across the enterprise using intelligence generated from IBM and indicator of compromise (IOC) or indicator of attack (IOA) detection methods.
- Tabletop exercises with cyber range capabilities
 - IBM will prepare security teams to act against real cyber attacks in a simulated, state-of-the-art environment that tests skills, processes and leadership competence. Through tabletop exercises, organizations can test their incident response plan against multiple scenarios.

Why IBM?

Choosing IBM can give you the confidence of working with an industry leader in cyber security. IBM Security is supported by expert professionals with decades of experience in incident management, security intelligence and corrective actions. These experts have supported the handling of hundreds of the world's largest breach investigations across 17 industries in the public and private sector.

For more information

To learn more about the IBM Security X-Force Incident Response Retainer, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security/services/ibm-x-force-incident-response-and-intelligence.

© Copyright IBM Corporation 2020.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at <https://www.ibm.com/legal/us/en/copytrade.shtml>, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:

X-Force®



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