IBM Security X-Force Incident Response Retainer

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

Highlights

- Fast response from an expert team as soon as a breach is suspected
- Immediate deployment of cloud-based CrowdStrike Falcon® lightweight sensors to detect threats and prevent further impact
- CrowdStrike can detect malware-based, malware free attacks and even attacks leveraging zero-day vulnerabilities
- Reduced risk and exposure through threat intelligence and analytics
- In-depth training offered for internal teams to better combat incidents

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 with CrowdStrike is a subscription-based service that provides access to a team of trusted experts trained to help you effectively respond to threats within your Amazon Web Services (AWS) Cloud or hybrid cloud deployment. 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. These teams leverage CrowdStrike's Falcon Platform to scan and detect your endpoints for possible compromise of endpoints, cloud workloads, containers and data. CrowdStrike's Falcon Platform allows IBM Incident Responders to complete advanced threat hunting in your environments to detect the stealthiest adversaries. The availability and responsiveness of these teams help reduce the impact of an incident on your brand, reputation and finances.

Once connected to the X-Force IR 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, IBM Incident Responders take priority actions by:

- Identifying the source of the attack
- Ensuring complete coverage by CrowdStrike Falcon's single light-weight agent across all assets in the environment
- Finding the root cause
- Connecting the incident to any known threat actors
- Leveraging CrowdStrike Real Time Response (RTR) to manage and reduce the impact
- Provide guidance across all security domains including AWS Cloud or hybrid cloud environments

All options will be explored to prevent the spread of malware and quickly restore systems and networks. IBM Incident Responders also take steps to reduce the risk of future incidents. This rapid 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:

- IR cloud services
    - Incident response support affecting on-prem, cloud-based and hybrid-cloud environments. Services also include maturity assessment, development of IR plans/playbooks, training and simulation exercises for cloud environments.
- 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 will 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 cyberattacks 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.
- Ransomware readiness assessment
  - IBM will review your readiness to respond to and recover from attacks, including delivering an assessment, maturing rating, recommendations, assessment report, and executive debrief.
- Cyber crisis management
  - IBM will provide a "whole-of-business" framework to help all business functions to act in unison during a crisis. It includes a program assessment, plan and playbook development, and tabletop simulation exercises.

Better together CrowdStrike and IBM Security partner together to provide a collaborative response to an incident and assist to secure your environment and people to manage future attacks. IBM Security offers best in class expertise coupled with CrowdStrike's best in class technology.

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 on AWS, please contact your IBM representative or IBM Business Partner, or visit IBM Incident Response Retainer in the AWS Marketplace.

Why CrowdStrike?

CrowdStrike is a global cybersecurity leader that has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk -- endpoints, cloud workloads, identity, and data. Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® Platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

For more information

To learn more about CrowdStrike Falcon® Platform end-to-end protection on AWS, please visit Falcon for AWS.

Why AWS?

Amazon Web Services (AWS) provides a global infrastructure with highly durable and available storage services, making it well-suited for securely scaling your enterprise.

On-demand provisioning enables you to rapidly scale cloud infrastructure resources, so your security services can maintain pace with that or your business growth.

AWS regularly achieves third-party validation for thousands of global compliance requirements and continuously monitors its infrastructure to help ensure it is up-to-part across industry verticals.

AWS infrastructure is highly automatable, making it easier for you to integrate custom and third-party security solutions to your cloud platform.

For more information

To learn more about AWS secure cloud infrastructure, please visit security and compliance in the overview of Amazon Web Services.

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