24/7 Incident Alerting and Response: IBM Security X-Force Threat Management for AWS

Enhance your security in AWS with a combination of IBM Security QRadar and X-Force Threat Management

A powerful combination of IBM Security QRadar and IBM Security X-Force Threat Management provide 24/7/365 visibility, detection, analysis and recommended response actions for your AWS environment.

To add a 24/7/365 operational response capability, where IBM Security will actively contain, disrupt or neutralize threats, consider adding IBM Security Managed Detection and Response (MDR) Services for AWS or an IBM Security X-Force Incident Response Retainer service for critical incident management and forensics.

Highlights

- Gain visibility and detection of threats in your AWS environment using IBM Security QRadar
- Monitor, enrich and investigate alerts 24/7/365 with X-Force Threat Management
- Disrupt, contain and or neutralize threats with the addition of IBM Security Managed Detection and Response
- Leverage X-Force specialists to better prepare for a critical incident or manage incident response

IBM Security QRadar for AWS

IBM Security QRadar offers capabilities built around AWS-native tools and automation, combined with an intelligence-driven approach. IBM Security QRadar can be fully deployed and extended in multiple AWS environments. Additionally, IBM Security QRadar supports hybrid visibility, giving you a combined view of your AWS environment and your on-premise or multicloud environments.

IBM Security QRadar seamlessly ingests and correlates multiple AWS cloud native services, including, but not limited to AWS Security Hub, Guard Duty, CloudWatch and CloudTrail. IBM Security QRadar has free downloadable AWS content extensions that deliver catered security rules, reports, and reference sets to provide context and visibility into your AWS environment.

IBM Security X-Force Threat Management for AWS

The X-Force Threat Management (XFTM) service provides 24/7/365 monitoring, detection, analysis and recommended response actions for your AWS environment. Using a NIST-aligned, programmatic approach, XFTM processes alerts in the IBM Security Services X-Force Protection Platform, powered by IBM Watson® and IBM Security SOAR. The X-Force Threat Management service also manages and monitors the health of your environment as well as configures your IBM Security QRadar for optimal performance.

With IBM Security XFTM, your organization has access to thousands of global researchers, developers, analysts and SOC personnel for market-leading protection of your most critical assets. The XFTM service is fully transparent, allowing you access to IBM Security Services workflow anytime, anywhere via the IBM Security Services mobile application or via integration with IBM Security SOAR.

X-Force Threat Management supports a wide range of security analytics capabilities, including most major SIEM technologies.

IBM Security Managed Detection and Response (MDR) Services for AWS

While it's not necessary to secure your AWS environment with IBM Security QRadar and IBM Security X-Force Threat Management, IBM Security MDR for AWS gives IBM Security an endpoint detection and response capability that adds another powerful 24/7/365 security operations capability to disrupt, contain or neutralize threats. IBM Security MDR can support your existing EDR/MDR capability or IBM Security can provide both software and service.

IBM Security X-Force Incident Response for AWS

IBM Security X-Force Incident Response Retainer services provide AWS customers access to a team of trusted experts trained to help your organization effectively respond to threats. This subscription service, which is a recommended addition to IBM Security X-Force Threat Management, can give greater visibility into threats, significantly reduce response and recovery times, and reduce the impact of a breach. Featuring 24/7 support through a global emergency hotline, the X-Force Incident Response team is available when you need them the most.

X-Force Incident Response Retainer also offers the flexibility to meet your organization's incident response needs with a number of proactive offerings from its tiered response plans.

For even more insight, X-Force leverages its global threat intelligence capabilities to augment the incident response process, helping to contextualize investigative findings, reconstruct attacker activity, and effectively contain the incident.

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 X-Force Incident Response Retainer, please contact your IBM representative or IBM Business Partner, or visit the following website:

https://www.ibm.com/security/services/incident-response-services