IBM Security: Master threat hunting

IBM

Highlights

Master the art *and* science of threat hunting
The science of threat hunting
The art of the hunt

Master the art *and* science of threat hunting

Cybercriminals represent a billion-dollar industry with an almost fanatic interest in innovation. You can't stop all of them with off-the-shelf security tools alone. To find the most dangerous threats — the ones that slip past your front-line defenses to put your data and even your entire brand at risk — it requires a mix of human intuition, deep analytics and artificial intelligence known collectively as *threat hunting*.

Threat hunting isn't something you can trust people or machines to do alone. It's a balance of talented people and advanced technology working together to uncover the hidden cyberthreats that are lurking in your organization's network, applications and endpoints. IBM Security solutions bring best-in-class technology and people together to make your threat hunting efforts faster and more effective.

The science of threat hunting

Internal data and systems

Expand the hunt to include internal systems data that goes beyond what standard Security Incident and Event Management (SIEM) solutions can see.

IBM QRadar Security Intelligence Platform uncovers hidden threats using advanced detection and analysis tools, then presents that intelligence in a single view so security analysts can focus their efforts on the most serious threats. With IBM QRadar, threat hunters discover cyberthreats sooner and mitigate them before they do damage. IBM QRadar can also augment these discoveries with artificial intelligence to help threat hunters accelerate the detection of advanced cyberattacks by sifting through massive volumes of unstructured data.

→ **Learn more**

Case study: Excellium Services

Discover how managed security services provider Excellium doubles its time-to-value with the highly accurate incident detection of IBM's QRadar Security Intelligence Platform.

→ **Read the full case study**

External data and intelligence

Bring in threat intelligence from the wild, including unstructured data sources, for richer context and hidden correlations.

IBM QRadar Advisor with Watson adds the power of artificial intelligence and cognitive reasoning to threat hunting. It can automatically detect indicators of compromise, uncover hidden relationships across millions of different data points and even provide remediation recommendations.

It combines internal and external data analysis to present threat hunters with reliable, real-time global threat intelligence. Its cognitive capabilities uncover relationships in the data that might otherwise go undetected.

QRadar Advisor with Watson also provides future-proof protection against zero-day cyberattacks by ensuring that newly discovered threat indicators are automatically added to your cyberattack watch lists. This provides protection against cyberattacks that may use similar patterns but different signatures — a common tactic among cybercriminals.

→ **Learn more**

Case study: Cargills Bank Ltd.
Read how Cargills Bank preempts cyberthreats and mitigates risks with the cognitive capabilities of IBM QRadar Advisor with Watson.

→ **Read the full case study**

Statistical analysis tools

Compose user behavior patterns, expose abnormalities and anomalies, and find hidden clues that can lead to faster threat detection.

IBM QRadar User Behavior Analytics (UBA) provides contextual analysis that allows threat hunters to model normal and abnormal behavior for each user, then apply those models to detect potential threat activity. It also calculates real-time risk scores that focus additional attention on at-risk users.

QRadar UBA delivers deep drill-down capabilities that allow security analysts to dig deeper into high-risk user profiles, including the factors and log flows behind those risk scores. The QRadar UBA tool can be downloaded and installed in minutes on a laptop or mobile device through IBM's Security App Exchange.

→ **Learn more**

Watch the science of threat hunting

Intelligence analysis

Spot links and patterns in your data that lead to camouflaged threats and flush out bad actors.

IBM i2 Enterprise Insight Analysis combines human analysis with machine-based analytics to quickly assess the threat landscape for hidden risks and vulnerabilities. It uses advanced visualization tools to help threat hunters quickly identify patterns and potential threats from massive amounts of internal and external data.

It integrates seamlessly with third-party applications and external data sources to expand your security efforts and distribute threat intelligence throughout your organization. i2 Enterprise Insight Analysis helps ensure that up-to-the-minute threat intelligence is never a minute too late to stop an attack.

→ **Learn more**

The art of the hunt

IBM Security services

IBM Security services provide the human intelligence needed to help your organization master threat hunting. In a world where security resources can be hard to find, IBM Security services are your source for deep skills and insights into the latest cyberthreats and security best practices.

IBM X-Force Incident Response and Intelligence Services (IRIS) offer world-class security expertise and intelligence to protect your organization against data breaches, ransomware and other high-profile risks. When bad things happen, it's good to have IBM X-Force IRIS on your side.

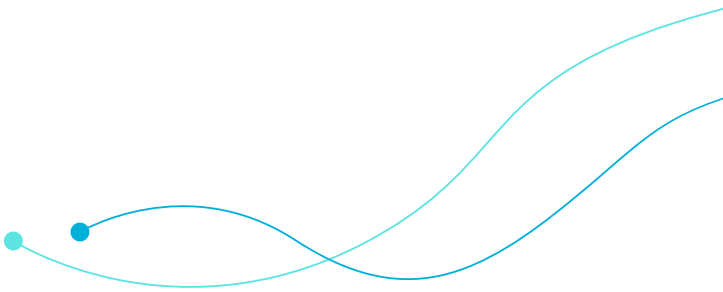
→ **Learn more**

IBM Managed Detection and Response (MDR) Services go straight to the source to stop cyberattacks: the endpoints that are the entry points to your network, applications and data. IBM MDR Services are powered by IBM X-Force Command Centers to enforce endpoint security and block cyberattacks from nesting in your network.

→ **Learn more**

IBM Managed SIEM Services deliver trusted support to your Security Operations Center (SOC) with global, around-the-clock monitoring, reporting and real-time expertise. IBM SIEM Services offer added assurance that someone is always watching out for your safety, with flexible service plans that scale to meet your needs.

→ **Learn more**



Meet an IBM Threat Hunter

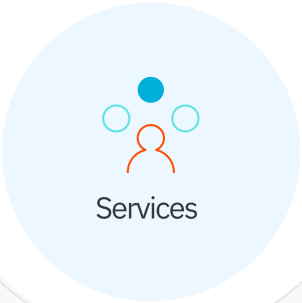
Master threat hunting with these solutions from IBM Security

IBM QRadar Security Intelligence Platform

IBM QRadar Advisor with Watson

IBM QRadar User Behavior Analytics

IBM i2 Enterprise Insight Analysis



IBM X-Force Incident Response and Intelligence Services (IRIS)

IBM Managed SIEM Services

IBM Managed Detection and Response Services

Discover how IBM Security solutions can help your organization master the art and science of threat hunting, dramatically increase security response times and neutralize cyberattacks before they strike.

→ **Learn more**

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
November 2018