IBM Security: Orchestrate incident response

Six steps to outsmart cyberthreats with security orchestration and automation.

Highlights

Before an attack
During an attack
After an attack

Sharpen and accelerate your response to cyberattacks by:

Defining incident response processes proactively based on best practices and your organization's standard operating procedures.

Integrating security tools including Security Information and Event Management (SIEM), ticketing, endpoint detection and response, and threat intelligence.

Automating repetitive and time-consuming tasks to free security operations center (SOC) staff to focus on more strategic priorities.

Leveraging human and cyberintelligence to better investigate threats, guide response processes and eliminate false positives.

Continuously measuring, assessing and refining resilient incident response processes and procedures.

Before an attack

Prepare for progressively sophisticated security incidents

Cybercriminals continue to evolve increasingly complex attacks. SOCs can barely keep ahead of the deluge of alerts they face or the ever-changing regulatory landscape. Analysts and managers spend time preparing executive reports instead of protecting against and addressing threats.

Prepare your defenses by defining incident response processes, integrating security tools and automating time-consuming tasks. Orchestration can help identify threats and anomalies early in the attack cycle, streamline incident response and free security teams to focus on more strategic business priorities.

IBM Resilient blends human and machine intelligence with orchestration and automation to sharpen your organization's response to cyberattacks. Build dynamic playbooks and orchestrate escalation, investigation and remediation tasks with customizable, automated workflows that accelerate response times.

→ **Learn more**

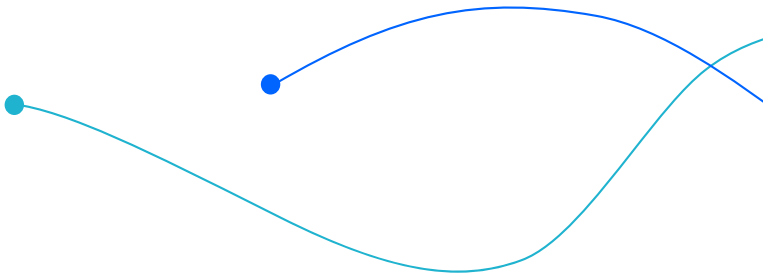
IBM QRadar Security Intelligence Platform gives your security teams the baseline visibility they need to protect your cloud assets, including applications. Detect misconfigurations that could unintentionally expose data and identify unsanctioned tools.

→ **Learn more**

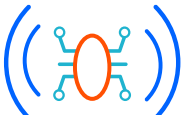
IBM X-Force Incident Response Intelligence Services (IRIS) on-demand incident response experts augment your team to deliver a wealth of skills, expertise and insights. The team is comprised of highly skilled industry professionals who help you prepare for and respond to threats. Ready to jump in when the inevitable happens, these seasoned experts assist in developing incident management processes as well as strategic breach solutions.

→ **Learn more**

See intelligent orchestration in action



During an attack



Detect, analyze and respond to threats faster with intelligent orchestration

It's no secret that cybersecurity incidents and breaches will happen. How will your organization manage the virtual battle? When you're prepared with threat intelligence, operational training and incident management processes, you're ready for the inevitable.

IBM QRadar Security Intelligence Platform accurately detects threats by receiving data from anywhere and applying advanced analytics that improve threat investigation, guide response processes and eliminate false positives. It improves the speed and effectiveness of threat detection and incident response times. Its integration with third-party apps increase productivity with visibility into the entire environment in a single system.

→ **Learn more**

While an attack is happening, **IBM Resilient** guides your security analysts through a fast and complete response with automated incident investigation and remediation. Unlock intelligence from all over your organization, from SOC analysts to marketing, HR and legal. Accelerate the response process with IBM Resilient as the system of record for all incident management activity. Its robust, enterprise-grade integrations with your SIEM, endpoint detection and response, threat intelligence and other tools simplify metrics for team and tool effectiveness.

→ **Learn more**

IBM QRadar: The intelligent SIEM

Leverage human and cyberintelligence in real time

Overburdened and inexperienced SOC analysts are already occupied with their full-time roles. When an attack occurs, the torrent of emergency actions begins. You need security expertise to help you take control of the incident.

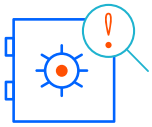
IBM QRadar Advisor with Watson uses artificial intelligence to accelerate the investigation of indicators of compromise. Using cognitive reasoning, it provides critical insights that can help manage the deluge of incident alerts security analysts receive every day. With actionable information, your analysts can make informed remediation decisions.

→ **Learn more**

IBM Managed Detection and Response Services detect and respond to threats with complete root-cause and kill chain visibility to deliver more effective security, delivered from our global network of X-Force Command Centers. Our security experts will help reduce the dwell time of attacks, accelerate investigations, deliver fast responses and prevent similar incidents from causing future damage.

→ **Learn more**

After an attack



Continuously measure, assess and refine to keep improving

Reduce the impact of threats and gain intelligent insights. It's one thing to learn from an incident, and another to successfully translate the lessons into policies and procedures. Is your team able to protect your cloud assets, including applications? Can you detect misconfigurations that could unintentionally expose data and identify unsanctioned tools?

Incidents don't emerge fully formed. Most effective incident response platforms (IRPs) centralize control over your existing security technologies. They extract intelligence from appropriate data sources and automatically adjust your playbooks while you isolate, investigate and remediate.

Outsmart, outpace and outmaneuver cyberattacks in a single response hub. **IBM Resilient** extends your security tools by automating repetitive, time-consuming triage and enrichment tasks. Its agile playbooks adapt in real time to incident specifics and guides analysts through the right response with the right tools. It helps streamline privacy response management with a knowledge base of global regulations and response plans that keeps your reaction timely, efficient and up to date.

→ **Learn more**

When the inevitable happens, **IBM X-Force Incident Response Intelligence Services (IRIS)** help you develop agile incident management processes and conduct strategic breach remediation and implementation solutions.

→ **Learn more**

IBM X-Force IRIS: Proactive, faster incident response

See how IBM Security solutions help you orchestrate incident response and secure your environment from today's complex threats.

→ **Learn more**

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

Produced in the United States of America
November 2018

Please Recycle

700-21870-USEN