Active threat assessment services

Examining your cyber defenses to help identify active and potential threats

Today’s security leaders abide by a common-sense rule of thumb: Yesterday’s strategies and practices may not be adequate against today’s cyber threats, even if the organization meets industry and government compliance requirements.

In the wake of high-profile cyber attacks against some of the world’s best-known brands and organizations, executives need to know whether their defenses measure up against attackers…

In the wake of high-profile cyber attacks against some of the world’s best-known brands and organizations, executives need to know whether their defenses measure up against attackers who probe for weaknesses and hope to cause mischief, damage or outright theft of business assets. As important, security leaders must discover whether undetected threats exist within their infrastructures.
Examine your environment to uncover current and previously unidentified adversaries

Active threat assessment services from IBM are designed to identify hidden but active cyber threats in your enterprise environment. IBM consultants and analysts deploy network and host-based inspection technology to assess your environment, looking for anomalies and signs of compromise based on IBM’s knowledge of attack groups. Are there indications that your organization might be under attack right now, but you are not aware of it? And what recommendations can be made to reduce the likelihood of a future cyber attack?

The IBM approach to active threat assessment includes:

Robust intelligence-driven threat hunting
This proactive service is designed to detect current and historical threats across the enterprise using intelligence generated by IBM, indicators of compromise (IOC) and indicators of attack (IOA) detection methodologies.

Real-time endpoint analysis and alerting
Endpoint detection and response (EDR) tools are deployed to discover currently active attacks in near real time.

Endpoint metadata collection and analysis
Collections of historical metadata are analyzed to discover undetected signs of historical compromise.

Real-time network traffic analysis
Appliance-based analysis, backed by intelligence, helps discover active attacks traversing and egressing the network.

Enterprise log analysis
Logs from firewalls, intrusion detection system (IDS) and intrusion protection system (IPS) devices, network antivirus servers, domain name systems and other enterprise sources help reveal signs of an active or historical attack.

Findings and recommendations
At the conclusion of the active threat assessment, IBM provides a detailed report that summarizes the steps taken during the assessment, the major findings and recommendations for next steps—if appropriate.
Develop an overall cybersecurity doctrine for your enterprise

Active threat assessment services from IBM can provide your organization’s risk and security leaders with critical insights into your cybersecurity posture. These insights include:

- Determining the feasibility of a particular set of attack vectors
- Assessing the magnitude of potential business and operational impacts of successful attacks
- Prioritizing and outlining any identified IOCs, and recommending corrective actions
- Providing evidence to support increased investments in security personnel and technology

Most important, with active threat assessment services from IBM, you can identify known security exposures before potential attackers do — and discover whether your infrastructure has already been compromised.

Why IBM?

IBM offers a wealth of insights and capabilities to help companies take control of and transform their security operations. While the majority of the incident response industry is focused on providing capabilities that are relevant only once an organization has been compromised, IBM® X-Force® IRIS is committed to providing proactive, agnostic incident response and intelligence services, delivered by world-class IBM X-Force experts who can help you make the most of your security investments.

For more information

To learn more about this service, please contact your IBM representative or IBM Business Partner, or visit ibm.com/security/services/cyber-security-consulting-for-active-threats/index.html.

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. IBM partners with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: ibm.com/financing