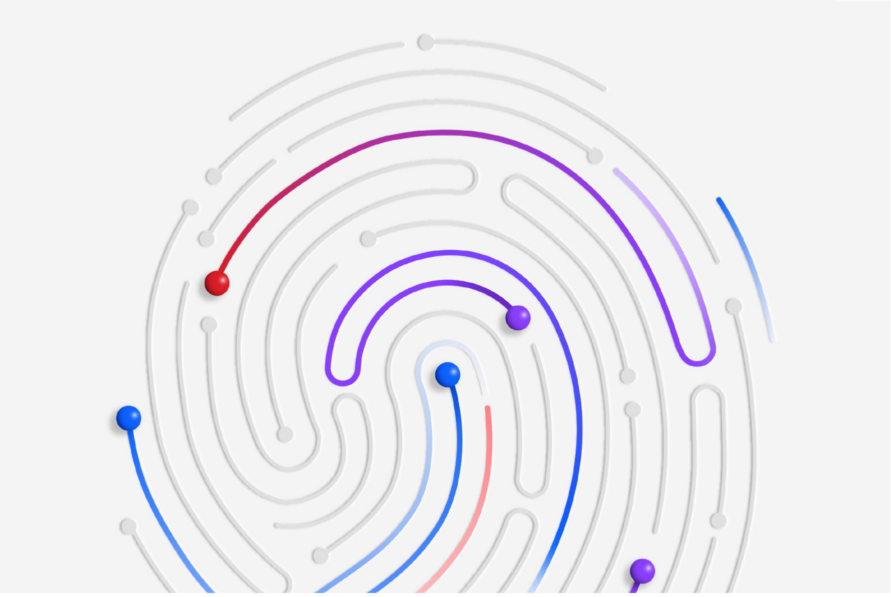
X-Force

Hacker-driven offense.
Research-driven defense.
Intel-driven protection.

- Adopt the mindset of threat actors to identify vulnerabilities
- Collect and translate threat data into actionable information
- Stop attacks faster through incident response
- Improve cyberattack readiness

For some time, cybersecurity leaders have predicted that when it comes to attacks, the question is one of “when” and not “if.” They aren’t wrong. In fact, attacks have evolved and are now a persistent cross-business problem that can lead to real-world consequences, such as inflation and chronic supply chain shortages. But if you know how adversaries attack, whom they target and how they operate, this intelligence can be of significant advantage.

Combatting these growing threats requires a mindset shift—one in which security is viewed as a journey, not a destination. This strategic viewpoint considers security as a continuous cycle of preparedness, remediation and recovery. IBM® X-Force® is a collection of carefully chosen hackers, responders, researchers and analysts, all of whom bring a unique perspective on threats to help you build, manage and refine your security programs.



X-Force offers the following products and services, underpinned by threat intelligence and research.

X-Force Red
Through offensive security services, the X-Force Red team adopts the mindset of threat actors to identify vulnerabilities. Capabilities include:

- Penetration testing: Uncover high-risk vulnerabilities that only humans—not tools—can find. Understand how attackers may leverage those flaws in the case of a security compromise.
- Vulnerability management: Prioritize the remediation of vulnerabilities using the scanning tool of your choice and the X-Force hackers’ risk-based automated ranking engine.
- Adversary simulation: Identify gaps in your incident response (IR) tools, people and processes by initiating a simulated attack against your environment.

X-Force Incident Response (IR)
Through incident preparedness, detection and response along with crisis management services, the X-Force IR team knows where threat actors hide and how to stop an attack. Capabilities include:

- IR emergency support: Stop attacks in progress, limit their impact, recover quickly and reduce the risk of future incidents with 24x7 global IR support and investigation services.
- IR proactive services: Prepare your security team for worst-case scenarios through active threat assessments, IR playbook and customization, dark web analysis, IR plan review and creation, and first responder training.
- Cyber crisis management services: Prepare your business team for crisis-level attacks through plan and playbook development and tabletop exercises.
- Ransomware readiness assessment services: Identify and fix gaps in your response plans regarding ransomware attacks.

X-Force Threat Intelligence
X-Force analysts collect and translate threat data into actionable information. Capabilities include:

- X-Force premier threat intelligence and advanced threat protection: Receive early warning indicators of malware, threat groups, threat activities and industry reports to improve your detection and mitigation capabilities.
- Strategic threat and cyberthreat intelligence assessments: Enable cost-saving and effective security decision-making by understanding threat actors and their techniques.
- Dark web analysis and malware reverse engineering: Identify potential threat actors who may target your company. Gain insight into the malware they may use to build protections against it.

X-Force Cyber Range
The X-Force team trains your business leaders to improve cyberattack readiness. Capabilities include

- Cyber range experiences: Understand if your business, security and IT teams and processes can respond to an attack through customized, simulated breach experiences inside the X-Force Cyber Range.
- Cyber range workshops and executive briefings: Assess your security strategies, identify gaps and educate your IT, security and business teams about crisis best practices that help define response strategies and solutions.

We recognize all aspects of a threat. X-Force hackers adopt the mindset of threat actors, X-Force incident responders help detect and counter threats, and X-Force analysts research and examine threats.

X-Force is an industry leader in cybersecurity, supported by expert professionals with decades of experience in incident management, vulnerability management and threat intelligence. The X-Force team has assisted many of the world's largest breach investigations across 17 industries in the public and private sector.

To learn more about IBM X-Force, schedule a briefing at https://ibm.biz/x-forcebriefing or visit ibm.com/x-force.

Inquire about a cyber range experience at: https://ibm.biz/cyberrange2024.

If you are experiencing cybersecurity issues or an incident, contact X-Force® to help:

US Hotline 1-888-241-9812
Global hotline (+001) 312-212-8034

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
August 2024

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.