X-Force Red

IBM **Security**

Adversary simulation: Put your incident response programs to the test

Understand gaps in defensive strategies by simulating advanced attack techniques favored by criminals

Contents

Introduction

Challenges

Types of security testing

Penetration testing versus red teaming

Types of adversary simulation services

Red teaming overview

Purple teaming overview

Control testing

Threat intelligence testing

IBM X-Force Red Adversary Simulation services

Choosing the right type of test

Choosing objectives

Testing approach

Helping answer the unknowns

The X-Force Red team impact

X-Force Red approach

Success rate of X-Force Red teams

Capabilities

Other IBM X-Force Red services

Next steps

Introduction

Even organizations that have strong security controls and processes in place may not be able to detect and contain a breach quickly. If organizations' incident response teams, also known as "blue teams," don't practice their detection and response capabilities, the likelihood of effectively executing them in a real breach scenario is greatly reduced. Blue teams must be ready to detect and defend against increasingly sophisticated attackers.

Incident response preparedness shows the greatest potential for cost savings

With the average total cost of a data breach in 2020 being USD 3.86M, enterprises are seeking opportunities for cost savings. Incident response preparedness that includes testing incident response plans, may average up to USD 2M in savings with data breach costs.[1]

As a result, organizations are looking to third-party adversary simulation services, which incorporate the same tactics, techniques, and procedures as advanced attackers, to evaluate how well their security teams can detect and respond to an attack.

Adversary simulation exercises can enhance the effectiveness of blue teams and incident response controls by uncovering attack paths and techniques they might miss and help identify gaps in their detection and response capabilities.

Explore this ebook to learn how adversary simulation services can help test, measure, and improve detection and response capabilities.

USD 3.86M

This is the average total cost of a data breach in 2020[1]

USD 2M

Savings in average total cost of a data breach in organizations with an incident response (IR) team that tested their IR plans versus those with no IR team or testing[1]

Challenges

Companies have invested millions in security products and people but lack awareness of gaps in their detection and response capabilities

Adversary simulation exercises offer enterprises the opportunity to evaluate their blue team's detection and response processes by **simulating an advanced, unstructured and opportunistic attack**. This testing can involve assessing the effectiveness of controls in an organization's network or the testing can align with business-specific goals. The latter approach informs the enterprise and its blue teams how attackers can gain access to data with the least privileges possible. The exercises can simulate threats that can be difficult to detect because they incorporate stealthy "low and slow" attack techniques.

Adversary simulation exercises can show organizations where to focus their remediation, detection and response priorities with their internal blue teams over the short and long term. The exercises can also uncover and help fix gaps in incident response programs so that if a breach were to occur, the damage could be minimized.

Types of security testing

Penetration testing and adversary simulation play important roles in your security strategy

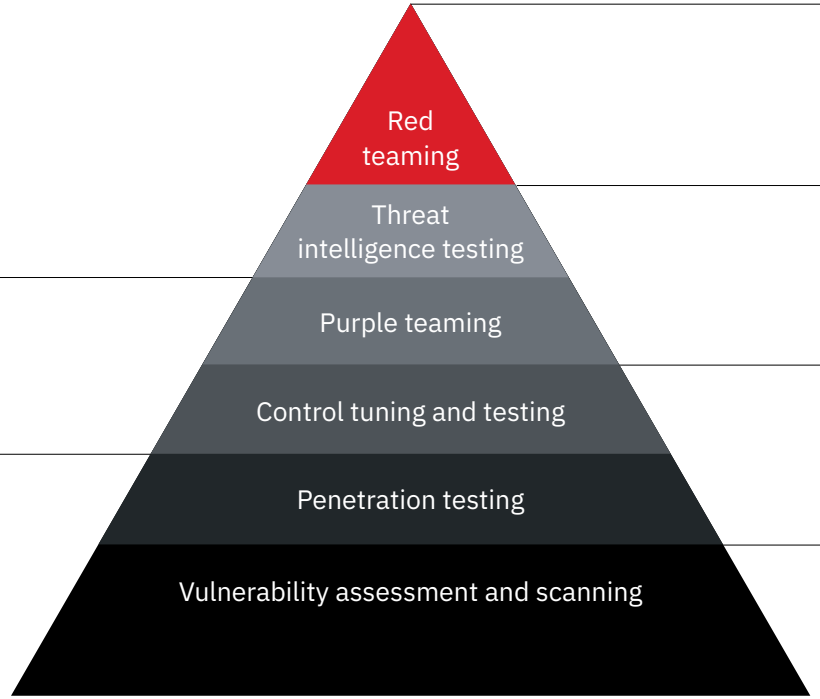
Across the cybersecurity industry, the terms “adversary simulation” and “penetration testing” are often used interchangeably. They are, however, two different approaches with two different objectives. Adversary simulation also encompasses various types of testing, such as red teaming, purple teaming, threat intelligence (intel) testing, and control tuning and testing.

Penetration testing, red teaming, purple teaming and control testing play important roles in an organization’s overall security testing program. The key is to properly understand the difference between the approaches and knowing where in your overall strategy to use them.

Testing types

Purple teaming
- Focused on automated and manual detection and not response
- Goal-based
- Collaborative and blue aware

Penetration testing
- Not focused on detection and response
- Assurance based
- Defined scope
- Network, application, hardware, social engineering and operations testing
- Blue aware



Red teaming
- Focused on detection and response
- Goal-based and threat intel driven
- Best mirrors opportunistic advanced attacker
- Blue unaware

Threat intelligence testing
- Focused on detection and response
- Follows external threat with the intelligence provider’s targeted threat intelligence (TTI) report scenarios
- Blue unaware

Control tuning and testing
- Focused on automated detections
- Technique based
- Blue and red collaboration

Vulnerability assessment and scanning
- Automated scanning of missing patches or insecure configurations
- Internal, external, or application scanning with manual result review

Penetration testing versus adversary simulation

Red team engagements can help organizations improve their “mean time to detection” (MTTD) and “mean time to response” (MTTR)

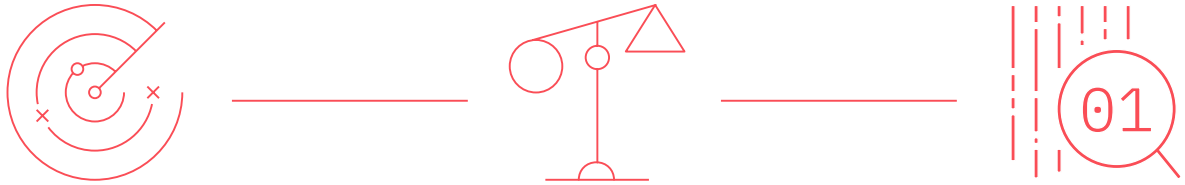
Similar to scenario-based penetration tests, red team engagements are designed to achieve specific goals, such as gaining access to a sensitive server or business-critical application.

Whereas a standard penetration test is focused on identifying and demonstrating the exploitability of vulnerabilities in your network, hardware, and applications, red teaming exercises evaluate the effectiveness of your security controls and the security team’s ability to identify and contain an actual breach.

To achieve this goal, adversary simulation assessments are focused on emulating an advanced threat actor using stealth, subverting established defensive controls and identifying gaps in a client’s defensive strategy.

Like advanced adversaries, red team engagements are focused on understanding your organization and its key business units, applications, groups and processes to support achieving your end objectives.

The value of this type of engagement can be derived from a better understanding of how an organization detects and responds to real-world attacks. Although, most penetration tests last 2–3 weeks, red team engagements average 8–10 weeks.



Types of adversary simulation services

IBM X-Force® Red is an autonomous team of veteran hackers within IBM Security™. The X-Force Red team is comprised of offensive security experts that simulate attacks against clients' environments to test, measure, and improve their detection and response capabilities.

Put your security teams to the test

X-Force Red Adversary Simulation services include the following four categories:

Red teaming
Evaluation of security operation blue team's detection, response, and defense capabilities, while focusing on major business impact-driven scenarios

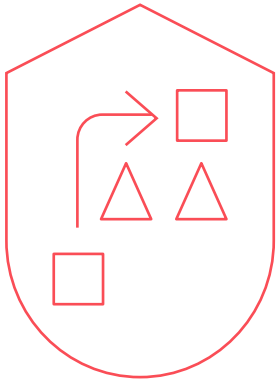
Threat intelligence-based testing
Threat scenarios based on external threat intelligence provider's targeted threat intelligence (TTI) reports with a narrow focus on specific threat actors and tactics, techniques, and procedures (TTPs)

Purple teaming
Objective-focused testing in collaboration with blue teams to validate manual and automated detections, but not response

Control tuning and testing
Verification of automated detections in your security controls against MITRE ATT&CK and TTPs

Red teaming

Red teams help to better detect and respond to future incidents



Red teaming is carried out without a company's blue team knowing in advance that it's being conducted, and with oversight from select project stakeholders. If during an engagement, a targeted company detects a red team's malicious activity, it responds as if it were a real attack.

For example, if a red team's activity is detected on a compromised system that's being used to access the target's internal network, the blue team will likely respond and remove that access, pushing the red team back a step in its progression.

Red team exercises typically focus on living off the land, relying on existing tools that are already built into the operating system. Adversaries will typically only use tooling when they are confident it can evade or bypass endpoint detection and response solutions or avoid common threat hunting queries by dedicated teams focused on finding nefarious activities through PowerShell or Sysmon event logs. During a red team engagement, the team is more focused on targeting DevOps and end users and using the least obvious ways to gain the minimum elevated privileges required to achieve its objectives.

At the end of a red team engagement, the blue team provides the red team any indicators of compromise (IoCs) that were detected during the engagement. This data can then be compared to other data collected during the course of the engagement and incorporated into a report timeline.

Threat intelligence-based testing

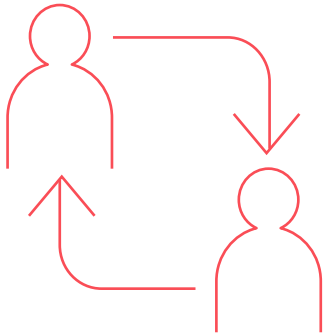
Threat intelligence-based testing focuses on executing attack scenarios tailored to specific threat intelligence reports

The service involves using intelligence collected by IBM Security and external sources to build and execute TTPs that mirror the same TTPs attackers are using in the chosen attack.

The objective is to identify and help fix gaps in the targeted organization's blue team and security operations center so that they are prepared to detect, respond, and contain the attack if it occurs. Examples can include building attack scenarios that mimic specific ransomware or other malware attacks.

Purple teaming

Purple teams work collaboratively with blue teams



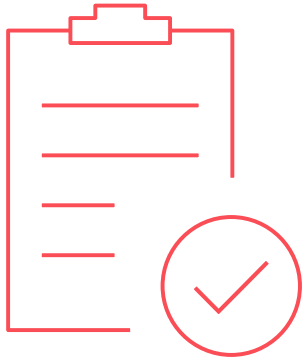
Purple teaming differs from red teaming in that it's collaborative, carried out with a company's blue team knowing in advance that it's being conducted. If during an engagement, a targeted company detects a red team's malicious activity, the security team confirms with the red team and the attack continues, while recording key data points along the way.

Oftentimes, the blue team will get access to logs of the red team in near real-time so they can review and evaluate the performance of security controls throughout the duration of the test as it happens.

To help draw value from the exercise, the red team works closely with the blue team throughout the engagement to explain its TTPs and how to better detect and respond to such offensive methods in future incidents.

Control tuning and testing

Control tuning and testing entails performing testing against controls such as email security sandboxes, egress firewall filtering, endpoint detection and response (EDR) and antivirus to determine effectiveness against common and advanced TTPs. Once the baseline is established, clients can better understand where to focus their efforts for addressing detection and prevention gaps in their security controls



X-Force Red control tuning and testing services can cover ad hoc or program-based testing including the following activities:

Assessment
X-Force Red works with clients to identify which controls are deployed, and maps those controls to the respective MITRE ATT&CK techniques to identify gaps in prevention and detection.

Automated control testing
Using an automated platform, the X-Force Red team launches the various attack techniques to identify which sub-techniques are detected and scores the controls' detection maturity levels.

Using automation, the platform can be used to simulate known advanced persistent threat (APT) campaigns or emulate specific malware samples and IoCs.

Automated control testing can be conducted quarterly to track how clients' detection capabilities are improving over time using repeatable metrics as part of a wider program.

Advanced control testing
While automated attack platforms are effective in mapping to a broad range of MITRE ATT&CK TTPs, it's important to take a deeper dive into the most advanced sub-techniques and variants designed to evade detection.

Control tuning
The X-Force Red team provides tool-agnostic detection guidance from an attacker's perspective for internal blue teams to use to improve detection accuracy and coverage.

IBM Security services teams like X-Force incident response and intelligence services, security intelligence and operations consulting, managed security services, and infrastructure and endpoint security are available to help implement any control-specific rules that clients may require further assistance implementing and tuning.

X-Force Red Adversary Simulation services

Simulating advanced threat actors takes industry leading offensive research and tooling

Using the same TTPs as advanced attackers, X-Force Red Adversary Simulation hackers perform exercises that closely simulate an advanced attack.

The goal is to measure and improve the capabilities of enterprises' blue teams in detecting, responding to and defending against various attack techniques. X-Force Red Adversary Simulation can include red and purple teaming, threat intel testing and control tuning and testing.

X-Force Red Adversary Simulation hackers can customize their attack scenarios and tools based on each client's environment. The team understands the overall business landscape and where detection and response weaknesses typically exist for specific industries.

Delivers insights and highlights vulnerabilities

Adversary simulation exercises can help mature organizations' incident response programs by uncovering gaps and providing a better perspective on how to respond to the latest threats.

Insights from adversary simulation exercises conducted by the X-Force Red team, can give security and business leaders a better understanding of their security stack coverage. They can also learn how to mature their logging, detection, and response capabilities in case a real-world attack occurs.

Choosing the right type of test

The approach can differ based on the maturity of the blue team, and the goals of the security organization

- Goal-based, advanced threat emulation focuses on stealth and evasion of both blue team and goals of the security organization—red teaming
- Collaboratively working alongside the blue team, focused on detection capabilities—purple teaming
- Largely automated control tuning and testing designed to provide a baseline against a larger set of MITRE ATT&CK TTPs—control tuning and testing
- Attack scenarios mapped to specific types of APTs, based on external threat intel to uncover if incident response programs can detect them—threat intel testing
- Testing not focused on specific TTPs, used to verify vulnerabilities in applications, networks, hardware, and personnel—penetration testing

Choosing objectives

As part of the engagement, X-Force Red Adversary Simulation hackers identify objectives aligned to the client's business unit. Working with your team, we'd first look to establish some initial scenarios or objectives specific to key business concerns.

Here are several scenarios for which we have tested, all while evaluating the organization's ability to detect and respond to a real-world attack and evasion techniques:

- Demonstrate general long-term persistence into the environment.
- Demonstrate access to key applications, files, or systems.
- Demonstrate mass access to customer financial information.
- Target healthcare data.
- Target access to unreleased media.
- Access banking front-end and back-end applications.
- Target business groups, such as marketing with excess access to customer financial records.
- Gain network access to isolated trading terminals.
- Demonstrate access to monitor capital markets and trade order information disclosure.
- Target any bank fraud surveillance platforms in place.
- Gain elevated privileges as required to facilitate the above objectives.

Testing approach

For red teaming, the X-Force Red team works with the client to gather information and plan attack scenarios. The execution includes progress reports that show each stage of an attack, the length of time the team tried to compromise the organization, and the findings.

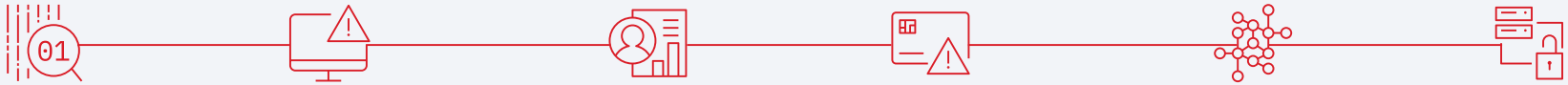
Organizations may choose to include external exploitation and phishing in an engagement or start from the perspective of an assumed breach with an initial foothold on the network provided to focus on evaluating the organization's post-breach detection and response capabilities.

Red teaming approach

External reconnaissance
- Review threat intel
- Passive information gathering
- Active information gathering
- Port scanning
- Service enumeration
- Network and app vulnerability testing

Host reconnaissance
- Host controls and logging reconnaissance
- Host controls bypass
- Tools transfer
- Short-term persistence
- Host privilege escalation
- Credential theft

Lateral movement
- Evade network security controls
- Lateral movement
- Network exploitation
- Elevate network privileges



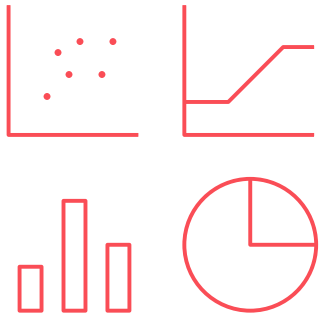
Gain a foothold
- Exploit vulnerabilities in exposed applications and services
- Spear phishing
- Social engineering
- Wireless
- Physical
- Or assume breach

Internal reconnaissance
- Network reconnaissance
- Domain reconnaissance
- Asset reconnaissance
- Admin reconnaissance
- Network security reconnaissance

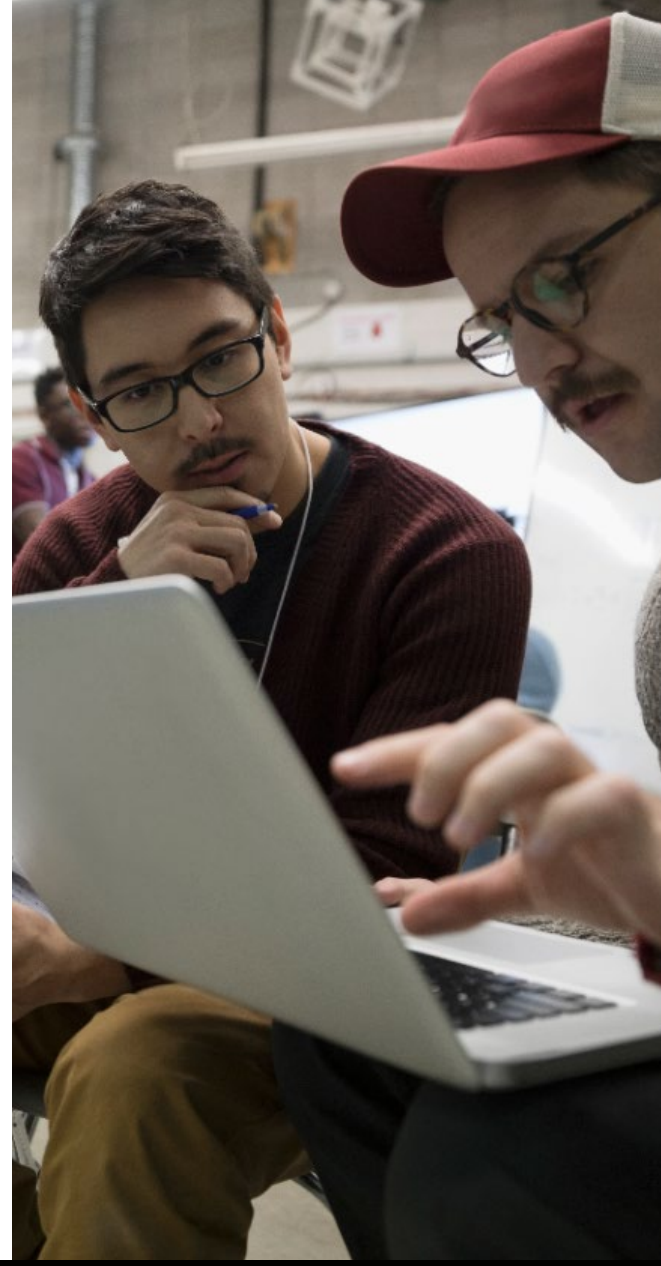
Achieving goals
- Complete primary exercise goals
- Successfully access sensitive data
- Perform privileged actions
- Sensitive asset access
- Exfiltrate sensitive data
- Long-term persistence

Helping answer the unknowns

The real value comes from the data points created during testing



- What techniques were fully detected, partially detected, or not detected at all?
- What monitoring and incident response processes and procedures were effective versus need improvement?
- Which controls in the security stack are effective versus need tuning or investment?
- What long-standing assumptions can be challenged?
- What actionable recommendations can be made to improve an organization's defense and detection capabilities with the tools already available?
- What improvements can be recommended based on experience testing other industry leaders?



The X-Force Red team impact

When working with in-house red teams, X-Force Red provides an external attacker viewpoint and tooling and can knowledge share with internal teams to help bring their incident response program to the next level

Complementing in-house red teams

X-Force Red works with some of the largest organizations in the world, some of which have mature in-house red teams. Oftentimes, those teams gain significant value from working with X-Force Red because the team of hackers:

- Brings unique tooling and experience from testing industry peers
- Uses experience to bring a new perspective and different testing skills to augment the internal team's capabilities
- Performs knowledge sharing with internal teams
- Brings a third-party perspective that doesn't have background knowledge of the environment and has no assumptions about staff and technologies
- Provides perspective on how an advanced external adversary would perform intelligence gathering and different post-exploitation TTPs against the environment, separate from the knowledge the internal team has already gained

Sizing and pricing

All adversary simulation testing can be conducted as an ad-hoc exercise or as part of a larger testing program with multiple exercises per year. Pricing is based on easy to select SKUs on a fixed cost basis.

X-Force Red approach

Your defenders need an effective sparring partner

What makes IBM's approach different?

Attacker mindset
X-Force Red hackers think like attackers and use the same TTPs to compromise organizations. We help defenders better understand the gaps in their prevention, detection, and response strategies using industry-leading attack techniques, and provide detailed report recommendations to address gaps mapped to frameworks like MITRE ATT&CK.

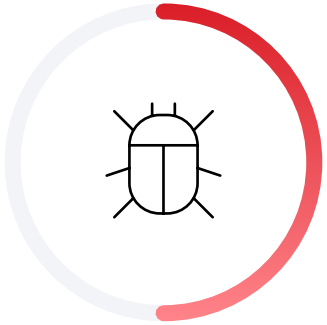
Expertise
X-Force Red hackers have decades of experience breaking into global organizations using red teaming techniques, evading security teams, and building custom payloads and command and control (C2) frameworks to achieve their goals. We've spoken at dozens of security conferences on bypassing, evading, and disabling security controls, helping defenders up their game.

Industry knowledge
The X-Force Red team focuses on business processes unique to industry verticals and business units and understands where detection and response weaknesses typically exist. We take the time to understand core business applications from an attacker's perspective.

Success rate of X-Force Red teams

99%

X-Force Red team's success rate for physical compromises

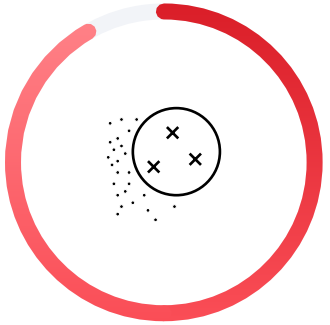


50%

Percentage of USB drives that are opened after an X-Force Red team USB drop

30%

Percentage of employees who click on links crafted by the X-Force Red team



90%

Percentage of successful phishing exercises conducted by the X-Force Red team

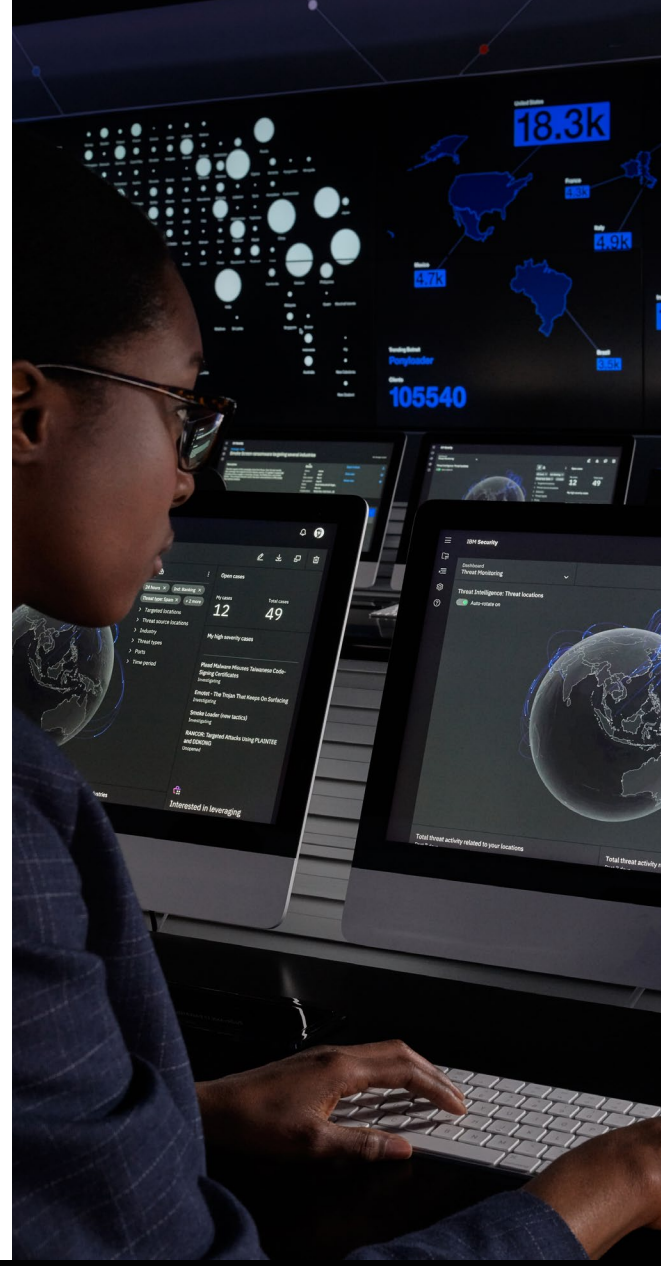
Capabilities

Testing the effectiveness of an incident response program shouldn't first happen during a real compromise

Testing the effectiveness of an incident response program shouldn't first happen during a real compromise. With its extensive experience emulating advanced attacks against some of the largest organizations in the world, the X-Force Red team fills a red teaming gap or augments existing in-house red team capabilities to help improve detection and response processes. That way, if an actual compromise occurs, the client's blue teams and controls are equipped to detect and respond quickly, which minimizes the potential damage.

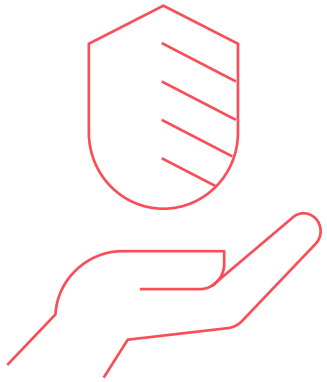
X-Force Red Adversary Simulation services enable organizations to effectively manage risk and defend against emerging threats with the following capabilities:

- Engages in real-world scenarios, using the experience of the X-Force Red team, emulating advanced threats against the world's largest companies
- Evaluates your fraud or security operation blue team's prevention, detection, and response capabilities
- Helps internal red teams mature internal red team programs and augment TTPs
- Simulates advanced threats designed to evade detection, establish persistence, and steal or modify key information
- Works closely with staff post-exercise to explain the attacks conducted and educate them on how to better detect and respond to an incident
- Performs ongoing engagements designed to emulate consumer and advanced threat actors, educate your team, identify gaps, and mature your cybersecurity capabilities



Other IBM X-Force Red services

In addition to its adversary simulation services, the X-Force Red team offers penetration testing services, application testing (penetration testing, DAST, SAST, code reviews and threat modeling), vulnerability management services and vulnerability assessments.



Differentiating IBM X-Force Red services

Skills

- Hack anything criminals can hack
- Decades of hacking experience professionally and personally
- Manual penetration testing virtually and physically, no questionnaires
- Engineers and developers who also have security expertise

Scale

- Automated vulnerability prioritization based on weaponization and asset value
- Output from any scanning tool can be inputted into the automated ranking engine to enrich and prioritize the highest-risk findings
- Fixed price with subscription testing program; can change what to test without re-signing contracts

Scope

- Four secure, global “X-Force Red Labs” for IoT, IIoT, IoMT, and OT testing
- Specialized testing services (ATM, automotive, mainframe, blockchain)
- Red teaming service separate from penetration testing
- Cloud testing—private, public, hybrid, multicloud

Technology

- The X-Force Red Portal is a hacker-built collaboration and communication platform
- It provides an enriched view of clients' vulnerability scan data
- Shows highest-risk vulnerabilities, associated exploits, remediation recommendations and risk reduction progress over time
- Clients can also schedule or change tests, share information with testers, and view findings

Next steps

For more information
To schedule a meeting with an X-Force Red team member, fill out the contact us form.

Learn more about IBM X-Force Red Adversary Simulation services by visiting ibm.com/security/services/adversary-simulation-services.

To understand more about the differences between penetration testing, red teaming and purple teaming, read the blog.

About IBM Security
IBM Security works with you to help protect your business with an advanced and integrated portfolio of enterprise security products and services, infused with AI, that modernize your security strategy according to zero trust principles, helping you thrive in the face of uncertainty. By aligning your security strategy to your business; integrating solutions designed to protect your digital users, assets, and data; and deploying technology to manage your defenses, we help you to manage and govern risk and grow with a modern open approach that supports today's hybrid cloud environments.

To learn more, visit ibm.com/security.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
February 2021

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 performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. 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.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. 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 systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. 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.

1 Cost of a Data Breach Report 2020, *IBM Security and Ponemon Institute*

GWB3E8ZV