A picture containing object

Description automatically generated

# *Who is X-Force Red?*

# *What value does X-Force Red provide?*

# *What makes X-Force Red different?*

# Overview

X-Force Red is an autonomous team of veteran hackers hired to break into organizations and uncover risky vulnerabilities that criminal attackers may use for personal gain. X-Force Red offers offensive security services which includes penetration testing, vulnerability management services, adversary simulation, code review, static analysis and vulnerability assessments. Our goal is to help security leaders identify and remediate security flaws that could expose their digital and physical ecosystem to an attacker.

X-Force Red is an autonomous team inside IBM Security.

As part of X-Force Red’s penetration testing services, the team performs manual tests against applications, networks, hardware, devices and personnel. Through the X-Force Red Portal, security leaders can see testing results as X-Force Red uncovers each vulnerability, so that remediation can begin immediately.

Using X-Force Red’s Vulnerability Management Services (VMS), security leaders know which vulnerabilities need immediate attention. X-Force Red ranks vulnerabilities by correlating threat intelligence that shows if a vulnerability can be exploited by attackers, along with the criticality of the asset at risk.

For its Adversary Simulation (also known as red teaming) offering, X-Force Red simulates an advanced attack to measure how well organizations’ security teams (a.k.a. blue team) and controls detect and respond.

To help developers build products and applications securely, X-Force Red is hired to manually review code - during design and once products are on the market - to identify vulnerabilities. The team also can identify malicious code.

X-Force Red also offers static analysis of code, which is a tool-based code review to identify vulnerabilities.

Finally, X-Force Red offers vulnerability assessments which involves scanning the client’s environment to uncover known vulnerabilities that an attacker could leverage in an automated attack. The team also manually pokes and prods a vulnerability to validate it’s real (not a false positive) and see if there are any others associated with it. This is a good door opener services since it’s less costly.

X-Force Red can do whatever attackers can do, but with the goal of helping security leaders harden their defenses and protect their most important assets.

Here’s a deeper dive into X-Force Red’s core services…

# Penetration Testing Services

X-Force Red’s hackers, also known as penetration testers, are hired by private companies and government agencies worldwide to manually test hardware, networks, applications, devices (IoT, IIoT and OT), personnel and other systems and technologies to find security vulnerabilities before criminal attackers find them.

The team uses the same tools, techniques and practices attackers use and have a “think like a criminal” mentality. For many X-Force Red testers, hacking is in their blood. They have been figuring out ways to break into things since they were kids and made a career out of it. X-Force Red testers hack for the “good.” They aim to help organizations uncover and fix security vulnerabilities before criminal attackers can exploit them.

X-Force Red penetration testing services range from raw, automated testing to hands on manual testing. For manual testing, the team tests across the four pillars – network, application, hardware and personnel. They perform social engineering exercises such as phishing campaigns to uncover weaknesses among employees (i.e. those who repeatedly click on suspicious links), and virtual and physical tests against networks, applications, hardware, and more.

The team can manually test hardware and embedded devices, such as ATMs and internet-connected devices, to discover security flaws that would enable an attacker to gain access to sensitive data and assets. Testing can be done on site, virtually or in X-Force Red Labs, four global secure testing facilities.

As part of our vulnerability assessments, X-Force Red can run any scanning tool (we are vendor agnostic) to uncover known vulnerabilities that an attacker may leverage in an automated attack. The team also “pokes” and “prods” to validate the findings are actual vulnerabilities (not false positives) and sends the findings to the client for remediation.

A big differentiator for X-Force Red’s penetration testing services is that all of the test information – from scheduling to testing progress to findings – is available for clients to review via the X-Force Red Portal. The portal is a centralized, collaboration platform that gives a real-time view into customers’ testing programs. Security leaders can see vulnerabilities as they are discovered and begin remediation immediately. The portal enables security leaders to cut down exposure time, giving criminal attackers a smaller window to compromise an asset. Clients can also schedule and change the testing scope through the portal, eliminating the back and forth passing of emails and spreadsheets.

# X-Force Red Vulnerability Management Services

# X-Force Red Vulnerability Management Services (VMS) identifies, prioritizes and helps remediate vulnerabilities exposing clients’ most important assets. Prioritization is based on several factors, including whether the vulnerability is being weaponized by attackers in the wild, and the importance of the exposed asset to the organization.

# X-Force Red VMS is a consulting service, combining patent-pending tools with hacker expertise. Using data science to perform correlation across potentially millions of records, the purpose-built automation enables security leaders to prioritize the remediation of critical vulnerabilities using a true risk-based approach.

# X-Force Red Vulnerability Management Services enable organizations to identify, prioritize and remediate vulnerabilities based on asset importance and exploitability. Here’s what the service includes:

* **Self-Service or Managed Scanning:** Using whichever best-of-breed scanning solution the customer prefers, X-Force Red provides deployment, support and premium services to help secure our customer’s most critical assets
* **Scan Fundamentals**: Helps customer understand which systems and applications are the most important, and configure the scan tool to identify vulnerabilities at the right depth and frequency
* **Ad-hoc Scan Requests**: At the customer’s request, conduct out of schedule scanning or scan profile updates
* **Prioritization**: After a scan, X-Force Red’s automated ranking algorithm ranks vulnerabilities within minutes based on asset criticality and if the vulnerability can be exploited by attackers.
* **False Positive Reduction:** X-Force Red validates identified vulnerabilities, delivering only legitimate vulnerabilities to the client.
* **Remediation Management**: Remediation oversight & subject matter expertise for remediation efforts, including tracking to completion. X-Force Red facilitates the process making sure the most critical vulnerabilities are sent to the right remediators and ensuring they are patched.

# X-Force Adversary Simulation Services (Red Teaming)

Red teaming is NOT penetration testing. Whereas penetration testing entails uncovering security vulnerabilities, red teaming is an attack simulation to measure how well organizations’ security controls and teams (a.k.a. blue team) detect and respond to attacks. The goal of this service is to help clients improve their detection and response capabilities.

While X-Force Red’s Adversary Simulation Services include:

* **External Recon –** Information gathering about your business from outside view
* **Intrusion –** Various options used to gain an initial foothold, such as external network compromise, spear phishing, physical onsite social engineering, or assume breach
* **Host Recon –** Logging recon, identifying security software, establishing command and control without being detected, escalating privileges, etc.
* **Internal Recon –** Active directory recon, asset recon, behavior analytics tools, network security controls, etc.
* **Lateral Movement –** Evading security controls, remote code execution, elevating network privileges, long term persistence established
* **Privilege Elevation –** Gain elevated access required to accomplish goals
* **Scenario Completion –** Demonstrating ability to achieve stated objectives
* **Post Engagement –** Comparing Indicators of Compromise (IoC) with blue team findings, detailed narrative and timeline, findings mapped to MITRE ATT&CK™, actionable recommendations

**X-Force Red can also perform “purple teaming” or “control tuning.”**

* **Purple teaming** – Spot-testing specific prevention and detection capabilities of clients’ security stack against techniques within the MITRE ATT&CK™ framework. Testing is conducted live in conjunction with the blue team.

The exercise is often automated. Open-source tools, such as MITRE Caldera, Uber Metta, Atomic Red, or Endgame RTA, are used to automate portions of a purple team / control tuning exercise, allowing organizations to easily benchmark their improvement against repeatable metrics.

# Target Audience

**Target company size:** Fortune 1000

I**deal accounts:** 1-5,000 employees; 10,000+ employees

**Target verticals:** All industries

**Target departments:** IT & Security, Risk Management, Vulnerability Management, Compliance

**Target contacts:** CISO/CIO, Chief Risk Officer, Chief Compliance Officers, IT and Security Managers, IT Administrators, Vulnerability Managers, VP of Application Development

**Common compliance drivers:** GDPR, PCI DSS, functional safety (companies are being fined millions because they are not making sure products are secure. Cars, planes, trains, all examples), upcoming IoT security standard, GCHQ mandates, TIBER

**Other attributes:**

* **VMS:** If they use a scanner already, that’s best. We have a partnership with Qualys so if they have a Qualys scanner that’s good to look for. We are vendor agnostic, so we can use any scanner as part of the service.

Also, some clients may want to refresh their scanner license with IBM to unify providers and cut costs. IBM’s Qualys discount can be very advantageous in competitive situations.

VMS is a sore spot for most C-level security executives. This fresh approach is often a good conversation starter because the current methods are not working, and board-level scrutiny of VMS programs is not uncommon.

We also offer a flat rate for our VMS service. Clients do not need to worry about overtime charges. They receive a fixed, predictable rate for the duration of the contract.

* **Penetration Testing:** Customers can sign up for a subscription program which includes multiple tests during a set period of time for one, flat rate. Or, they can request ad-hoc testing, if they want a specific application, network, hardware etc. tested at a specific point in time (i.e. some customers wanted X-Force Red to test their applications to see if they were vulnerable to the WannaCry ransomware. Others wanted their technologies tested to make sure security controls met compliance mandates).

**Make Sure You Are Speaking with Key Decision Makers:**

Who is interested and why?

* General: Organizations that need to address:
  + Penetration testing
  + Understanding if their applications and systems are vulnerable to specific malware (i.e. WannaCry, EternalBlue)
  + Ensuring their applications and devices (internet-connected devices) are designed securely.
  + Ensuring their technologies and processes are enabling compliance with mandates such as the GDPR, PCI DSS and others.
  + Identifying and fixing vulnerabilities across their applications, networks, hardware and personnel
  + Identifying security weaknesses related to physical security of an office building and which assets can be accessed by a potential attacker on site.
  + Vulnerability Management
  + Vulnerability Prioritization
  + Adding Manpower for Vulnerability Management
  + Expertise shortage for Vulnerability Management & Remediation
  + Identifying if a vulnerability is being actively exploited
  + Vulnerability reporting
  + Too many false positives
* Chief Information Security Officer (CISO): “Are you concerned that your company is vulnerable to WannaCry? (or any other recently released malware strain)
* CISO: According to the National Institute of Standards and Technology (NIST), it costs companies thirty times more to fix vulnerabilities after they release a product than it would if those fixes were performed during the design phase. Are you interested in testing your products while they are being built?
* CISO for bank: From 2017 to 2018, X-Force Red saw a 300% percent increase from banks requesting ATM testing. Have you identified security vulnerabilities on your ATMs?
* CRO: Do you know which vulnerabilities are posing the greatest risk to your organization? How do you know you are fixing the most critical weaknesses first?
* CISO: Do you have a penetration testing program in place? If not, how do you know which vulnerabilities could expose your most important information to criminal attackers?
* CISO: If you have a penetration testing program in place, is there a centralized place where you can see your test results as vulnerabilities are discovered?
* CISO: “Many organizations we speak with are trying to improve how they are prioritizing vulnerabilities after a scan. Is this a priority for your organization?”
* CISO/CIO: “How do you know your vulnerability management team is addressing the most critical vulnerabilities first, those that if exploited, elevate risk the most?”
* CISO/CIO: “Do you have any way of knowing if an attacker is actively exploiting a vulnerability that’s in your environment?”
* CISO/CRO: “Are you looking to transition your vulnerability management program, so it enables a more risk-based approach?”
* CRO: “How do you know you are prioritizing the vulnerabilities that impact your most important systems and applications?”
* CISO/Vulnerability Managers: “Is your team spread thin on manpower and expertise? Are you manually connecting the dots figuring out who owns which asset and who is accountable for patching vulnerabilities on those assets?”

Confirm the following benefits:

* Pricing – X-Force Red charges a flat rate for subscription testing services, in a “gift card” format so that customers can use the allotted dollar amount on a SKU for whatever they want to test. They can also add or change what they test whenever they choose, at no additional cost. Because the fee is flat, there is no additional cost for overtime.
* For one large bank, in three months, X-Force Red’s VMS reduced the bank’s high/critical vulnerabilities by 55% (eliminated more than a million high/critical vulnerabilities).
* We also offer a flat rate for our X-Force Red VMS. Customers pay the same fixed rate for the duration of the contract – no overtime charges nor staff augmentation applied.
* Testing anything – X-Force Red performs manual tests against any application, network, hardware, physical, human, technology, product, anything and everything.
* Using the X-Force Red Portal, customers get real-time views of their testing progress including identified vulnerabilities, so they can begin remediation immediately – no lag time.
* Global expertise. X-Force Red has more than 200 hackers worldwide.
* Subscription-based or ad-hoc testing as needed.
* “Think like a hacker” mentality. X-Force Red’s veteran hackers have decades of experience breaking into everything and anything. Hacking is in their blood.
* Automation. X-Force Red automates the vulnerability ranking process so that manual labor is not needed to prioritize the most critical vulnerabilities.
* Identify if a vulnerability is being weaponized in the wild.
* Prioritize vulnerabilities based on weaponization and importance of the system/application at risk. Our vulnerability ranking algorithm was built by our hackers so we understand which vulnerabilities can be exploited by attackers.
* Work with customer on a risk-based remediation plan. We facilitate the remediation process to ensure vulnerabilities are patched.
* Identify most important systems/applications, who owns them, who’s responsible for patching vulnerabilities on them, and keep up-to-speed with patching progress.
* Customers can use whatever scanner they want. The service is vendor agnostic (significant discounts offered for Qualys customers)
* If the customer is short on skillsets and manpower, X-Force Red can manage the vulnerability management program for them.
* X-Force Red reduces false positives by validating which vulnerabilities are real
* Right-fit, right-price as compared to staff augmentation approaches; price is optimized for VMS use case and can be as much at 90% less than staff augmentation.
* The X-Force Red staff involved are VMS experts, not general consulting.

# Discovery Questions

* Do you have a penetration testing program in place? If so, do you pay by the hour including paying extra if testers work overtime?
* Are you identifying security vulnerabilities in your IoT, IIoT and OT products during the design phase or afterwards?
* Are you interested in identifying all the security vulnerabilities across your applications, networks, hardware, personnel and technologies that criminal attackers may be able to exploit?
* Do you want to know if your company is susceptible to “X” malware? (i.e. WannaCry or whichever highly publicized malware is announced)
* Do you know if your applications, networks, hardware, personnel and processes are in compliance with industry security mandates?
* Are you tired of manual processes? Do you lack the resources to manually identify, prioritize and remediate security vulnerabilities?
* Do you know which employees repeatedly click on suspicious links or violate security policies?
* Do you have a vulnerability management plan? And if so, how do you know you are prioritizing the right vulnerabilities?
* Is your vulnerability management team buried in vulnerabilities and don’t know where to start?
* Would it help to understand if a threat could actively exploit a vulnerability currently in your environment, so you know which ones to prioritize?
* Are you short on resources and looking for someone to manage your vulnerability management plan for you?
* Do you rely solely on CVSS scores?
* Do you use a Qualys scanner or any other vulnerability scanner?
* Do you have a vulnerability false positive problem?
* Are you spending time remediating vulnerabilities that end up representing minimal risk to the organization?

# Competitive Differentiators

# Flat Rate “gift card” pricing: X-Force Red charges a flat rate for subscription testing services, in a “gift card” format so that customers can use the allotted dollar amount on a SKU for whatever they want to test. They can also add or change what they test whenever they choose, at no additional cost. Because the fee is flat, there is no additional cost for overtime, and to add tests, clients don’t need to go through procurement every time.

# We also offer a flat rate for our X-Force Red VMS. Customers pay the same fixed rate for the duration of the contract – no overtime charges nor staff augmentation applied.

# X-Force Red Portal: Customers get a real-time view into their testing programs including identified vulnerabilities as they are discovered and testing progress. They can also schedule and change the scope of tests through the portal, meaning no hassle with phone calls, emails, and get daily updates on testing. For our X-Force Red VMS, the portal serves a centralized place where clients can see the most critical, exploitable vulnerabilities exposing their environment and drill down to see how many exploits exist against a specific vulnerability, so they understand exactly which ones to fix first.

# Expertise: X-Force Red has decades of experience breaking into everything and anything. They think like criminal attackers and use the same tools, techniques and practices to compromise companies.

# X-Force Red’s testers are engineers and administrators who are also security experts. We speak engineers’ language and understand how products are built including protocols, electrical signals, cost constraints, reliability constraints

# Autonomy: X-Force Red is an independent team within IBM Security, meaning the team’s processes, reporting structure, and services are completely separate from all other IBM teams. In fact, IBM is a client of X-Force Red. The team tests IBM’s applications, systems, and other infrastructure to help IBM remediate security vulnerabilities.

# Storytelling: X-Force Red documents and reports every step testers take to break into a company’s infrastructure. The report builds a story, so the customer can see the entire process from the beginning until the end, which tools were used and how the target was compromised.

# No questionnaires: Whereas many vendors use questionnaires to understand a company’s security posture, X-Force Red actually digs in and manually tests a company’s infrastructure using the same methods and tools criminal attackers use. The team finds vulnerabilities that oftentimes no one saw on the radar.

# Multiple testers: At least two X-Force Red testers are put on each project, and they can tap into the knowledge base of the overall team. Clients are on a first name basis with their tester and can pick up the phone at any time or submit a comment/question to the X-Force Red portal if they have an issue.

# Subject Matter Expertise: X-Force Red has subject matter experts in areas that many other companies don’t such as mainframes, SAP, ATM, IoT, mobile application testing, and more.

# Vulnerability Validation: X-Force Red validates if a vulnerability is real vs. a false positive before it is sent for remediation

# Attacker Mindset: X-Force Red has an “attacker mindset” so the team understands how a criminal would exploit a vulnerability in the customer’s environment.

# Automation: Vulnerability prioritization is performed using purpose-built, patent-pending tools, significantly speeding up remediation time and saving resources typically needed for manual vulnerability management programs.

# Executive Level Consulting: X-Force Red hackers are true subject matter experts in vulnerabilities and remediation.

# Flexibility: Tools can be run inside client networks when privacy regulations require it (very common). Penetration tests and VMS can be run virtually or on prem.

# Platform

X-Force Red offers a portfolio of services. The X-Force Red Portal is a cloud-based collaboration platform for X-Force Red testers and customers.

# Additional Resources

**Experts to contact:**

* Head of X-Force Red: [Charles Henderson](https://w3.ibm.com/bluepages/profile.html?uid=5G9046897)
* Regional Lead NA & LATAM: [Krissy Safi](https://w3.ibm.com/bluepages/profile.html?uid=7A5974897)
* EMEA and APAC: [Thomas Mackenzie](mailto:https://w3.ibm.com/bluepages/profile.html?uid=121780866) and [Colin Sheppard](https://w3.ibm.com/bluepages/profile.html?uid=124865866)
* Solution Design/Client Conversations (global): [Seth Glasgow](https://w3.ibm.com/bluepages/profile.html?uid=2J3057897)
* Marketing and Communications: [Abby Ross](https://w3.ibm.com/bluepages/profile.html?uid=2J7266897)

**Additional Materials:**

* X-Force Red home page: <https://www.ibm.com/security/services/offensive-security-services>
* X-Force Red Wiki: <http://ibm.biz/enable-xfr>
* Slack:

xfr\_solution\_design

#x-force-red-public