IBM Security

3 Strategy Essentials: Preparing for and Responding to Cyberattacks

IBM

Get started →

Strategy essentials: Be on the offensive and defensive

Every organization wants to avoid the loss of millions of dollars[1] that can result from a major security breach—not to mention the potential loss in reputation and market share. However, many companies still place their primary security focus on analyzing an incident long after it has been detected and after it has caused damage. True, a post-attack analysis is always necessary. But with the right tools and processes in place—threat preparation before a major breach occurs can help maintain better business continuity. Both offensive and defensive approaches to security are essential and should work together to help thwart or, when necessary, contain damage.

The shifting threat landscape alongside lack of preparedness in organizations underscore this approach:

- Today's threats often combine extortion tactics with business disruption and data leakage.
- Organizations struggle with slow detection and response times, while threat actors are rapidly gaining speed and moving to the cloud—increasing both their agility and ability to harvest more data.
- Useful threat information is often unavailable as security teams struggle to analyze massive volumes of data and endless alerts from multiple security tools.
- Endless vulnerabilities bury security teams in work that can prioritize the wrong issues while creating more opportunities for attackers to succeed.

As these trends continue to escalate, comprehensive offensive and defensive security programs can cut the overall response time and prevent extensive damage, costs and reputational impact.

IBM Security X-Force® offers a world-class team of hackers, responders, investigators and researchers who help organizations reduce attacker impact through offensive and defensive security services.

$3.86 million

Average cost of a data breach.[1]

[1] "2020 Cost of Data Breach Study: Global Overview," *Ponemon Institute,* June 2020. https://www.ibm.com/security/data-breach

Reduce the impact of a security crisis

Perhaps one of the most startling trends today is attacks in which threat actors target entire supply chains, and then blend their attack with extortion tactics to apply additional pressure to victims. Threat actors can execute highly sophisticated and organized attacks that can completely shut down an organization, including entire data centers and enterprise resource planning (ERP) systems. Recovery from a disruption of this magnitude requires the support of a provider with a global footprint that can act quickly to rebuild and restore business systems from the ground up.

Recent examples of such large-scale attacks include:

- **DarkSide** – In May 2021, cybercriminals who deploy ransomware in targeted attacks managed to infect a large U.S. refined products pipeline system, causing the disruption of its operations. DarkSide blends crypto-locking of data with data exfiltration and extortion, similar to other gangs that operate modern ransomware, such as Sodinokibi and Maze. If not paid by a set deadline, the attackers threaten to publish confidential data stolen from the victim and post it on their dedicated website.
- **SolarWinds** – A major nation-state attack campaign on U.S. government and commercial organizations was exposed in March 2021 as a far-reaching supply chain compromise. Threat actors infected an update patch for a popular network monitoring product. Organizations using the software downloaded the Trojanized update and were infected and exposed, and many were impacted by a subsequent attack.
- **ProxyLogon** – In March 2021, a collection of Microsoft Exchange Server zero-day vulnerabilities were discovered and linked to a nation-state threat group dubbed “Hafnium”. Soon after the initial wave of attacks, additional threat groups were detected using the same vulnerabilities to implant ransomware into compromised networks and extort vulnerable organizations for money.
- **Accellion** – This widespread supply chain attack started in December 2020, and was enabled by a cluster of vulnerabilities in a file transfer appliance product. Threat actors wielding ransomware used a zero day to attack the vendor’s customers and partners with malware.

In these and similar attacks, IBM Security X-Force acted with speed and scale to coordinate efforts among its global teams to help customers triage the compromise, making same-day, next-day and ongoing recommendations to customers. X-Force integrated on-site incident response teams and threat researchers to determine the nature of the threat, the initial compromise point into the network and the remediation measures needed to restore business continuity.

$10.5 trillion

Cybercrime to cost the world $10.5 trillion annually **by 2025.**

Minimize time between detection and response

When an attack occurs, security teams are tempted to add a new security product to combat the threat. This approach, however, can leave your organization with multiple point solutions that lack integration and automation and add complexity to the infrastructure. This lack of integrated tools, coupled with manual processes, can create dangerous delays for your security teams. Bad actors are keenly aware of this reality and the delays it can cause, and use it to their benefit when seeking to cause rapid and large-scale destruction.

IBM Security X-Force can help to reduce delays between detection and response—where even a few minutes can have a substantial impact on how much damage a breach can cause. X-Force teams guide organizations through the process of strengthening their defenses, building in up-front connectedness and automation, and helping to streamline business processes, close security gaps and increase visibility and control. Additionally, the X-Force teams can assist in aligning the right stakeholders to build a response playbook, and can provide ongoing assessments and recommendations for improvement.

When a security breach occurs, X-Force serves as the first-responder, putting teams on-site to work seamlessly in the background with your security teams to rapidly triage damage. They also leverage threat intelligence for insights into why the breach occurred and map the best steps to repair the damage and coordinate with the appropriate IBM organization, such as IBM Managed Security Services, to remediate future threats. This 360-degree process is essential to prepare for or respond to increasingly sophisticated security threats.

Reduce the opportunity for a threat to succeed in the first place

While rapidly detecting and responding to threats is a critical component of any security program, preventing those threats from succeeding in the first place is also key. Scanning tools typically uncover an average of 1.7 million vulnerabilities, with 16% having associated public exploits. How are vulnerability management teams supposed to know which vulnerabilities to fix first? How can they find the 16% of exploitable vulnerabilities before attackers find them? By adopting a vulnerability prioritization and remediation process that can pinpoint the most important vulnerabilities to fix first, organizations can reduce the opportunities for attackers to strike. X-Force Red, IBM Security's team of hackers, leads vulnerability management programs for global companies of all sizes. From running scanners to prioritizing the highest risk vulnerabilities to facilitating the remediation process from tracking to close, X-Force Red can do it all so that the opportunity for threats to succeed is minimal. After all, without a vulnerability, there is no threat.

But what about vulnerabilities that scanning tools alone cannot find? X-Force Red's team of 200+ hackers provides penetration testing services to organizations worldwide. The services include hands-on testing to find vulnerabilities that only humans, not tools, can find, such as logic flaws, sensitive information disclosure, encryption flaws, business workflow issues, username enumeration and password reset issues. Testing can also show how vulnerabilities can be chained together to enable an attacker to move deeper into the environment. Because of its attacker mindset, X-Force Red knows which vulnerabilities are most exploitable and can assist attackers in achieving their goals. The team's insights can help your security teams know which vulnerabilities to remediate first.

A combination of vulnerability scanning and penetration testing can reduce the attack surface by eliminating both publicly known and not-yet-known vulnerabilities that attackers could find and leverage.

211

Average number of days it takes to detect a data breach.[1]

[1] **"2020 Cost of Data Breach Study: Global Overview,"** *Ponemon Institute,* June 2020.

Leverage deep threat intelligence

A key reason why attacks move with such strength and speed is that cybercriminals have become adept at sharing their successes, methods and tools with each other—and quickly. Meanwhile, security teams struggle to analyze massive volumes of data from millions of events in their environments, weeding out false positives while prioritizing real security events.

IBM Security X-Force threat researchers provide forensic analysis, malware reverse engineering, threat modeling and threat assessments. Additionally, the researchers analyze both publicly available data sources, such as malware repositories and IBM telemetry data, which includes intelligence on threat activity occurring in 133 countries across the globe. X-Force communicates and integrates these findings throughout IBM Security products and services. Even a day's notice about a pending threat can dramatically help to reduce the potential breadth of damage.

During a compromise, X-Force threat intelligence teams work together with incident responders to help them understand the threat's tools and attack infrastructure. The team reviews host and network data, enriching threat information based on on-site findings and provides both your organization and IBM Security incident responders with guidance on what to search within the compromised environment. It's an exercise in deep forensics.

IBM Security X-Force Threat Intelligence Services provide end-to-end assistance, working with you before, during and after a compromise to identify:

- The initial compromise point
- The scope and scale of the compromise
- The threat actor's tools
- How the threat actor maintains access
- The possible motive and next moves of the threat actor

X-Force threat information is provided in a usable, actionable format so your senior leadership can make informed business decisions and communicate effectively with internal and external stakeholders.

37 billion

Number of records breached **in 2020.**

Act with force: Real-world accounts

The SolarWinds attack on US government entities in 2021 had far-reaching effects, and it was indicative of one of the directions security breaches have taken: supply chain compromises. Previous attacks on supply chains have been known to cause damage to a large number of companies. In a campaign discovered by IBM Security X-Force in 2020, nation state threat actors **continually targeted** the COVID vaccine supply chain even as vaccines were rolled out in 2021. Subsequent supply chain attacks in early 2021 were marked by the Accellion breach that impacted numerous organizations who were later extorted by the Clop ransomware group. These attacks caused a ripple effect across various industries as massive amounts of data were illegally accessed and compromised. In just one case, the records of **1.3M** patients of Centene subsidiaries (insured healthcare programs) were exfiltrated by the attackers.

In each case, X-Force threat intelligence teams worked closely with incident response teams to identify and confirm the initial method and procedures used to gain entry and discover the malware and tools being used. X-Force used its threat intelligence to provide near real-time support and rebuild the customer environment working in tandem with in-house teams. X-Force executed informed, sustainable remediation to help customers recover and maintain preparedeness over time.

During a cyber espionage campaign X-Force uncovered in 2020, which was intended to compromise organizations that form part of the COVID-19 vaccine's cold chain, attackers impersonated executives from major cold storage suppliers as their method of attack. The campaign targeted 44 companies in 14 countries in Europe, North America, South America, Africa and Asia. Information X-Force teams provided to CERTs and the security community, helped defenders spread awareness and vigilance to prevent potential compromise.

For more information

Learn more about the **COVID supply chain attack** discovered by IBM Security X-Force.

Learn more about the **CISA advisory** released about the campaign by the US-CERT.

IBM Security X-Force hackers, responders, investigators and researchers

IBM Security X-Force services play an integral role in IBM Security's expertise and are part of a larger ecosystem of products and services that can help you strengthen your organization's security posture. The X-Force team's focus is building a security strategy and infrastructure that minimizes attack opportunities while also expecting breach attempts and possible compromise. With this approach, you can combat security threats that aim to cause widespread disruption at scale. You can also tap into the global X-Force threat intelligence to understand events before and after they happen, and to minimize the time between detection and response.

From an offensive standpoint, X-Force Red can find, prioritize and fix the most important vulnerabilities, and can make recommendations to improve your security infrastructure. From a defensive standpoint, while the X-Force team serves as a first responder during a compromise, the team can also engage a wider network of appropriate experts. Together with X-Force and the broader **IBM Security products and services offerings**, IBM can help mitigate compromises through a variety of competency areas and build transformative capabilities that enable your organization to more effectively detect, respond to and prevent security breaches.

For more information

IBM Security Services helps customers accelerate cyber resilience, protect against security incidents and enable automation. We do that by delivering a full range of planning, response and readiness solutions to help transform your security program, build a cognitive security operations center and take control of digital risk.

Learn more about IBM Security X-Force Incident Response and Threat Intelligence Services

Learn more about IBM Security X-Force Red Offensive Security Services

Learn more about **IBM Security.**

Learn how **IBM Cloud Pak for Security** helps you respond faster with automation across hybrid, multicloud environments

Establish your security plan for tomorrow based on where you are today. **Take the assessment now.**

To learn more about IBM Security X-Force® Incident Response and Threat Intelligence Services, please contact your IBM representative or IBM Business Partner, or visit: https://www.ibm.com/security/services/ibm-x-force-incident-response-and-intelligence

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition.
For more information, visit: ibm.com/financing

To learn more about X-Force Red offensive security services visit: https://www.ibm.com/security/services/offensive-security-services

IBM Security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
April 2021

00000000USEN

IBM