IBM Security

You have an incident response plan. But in an attack, does your organization understand what attackers are doing?

The experts at IBM know security.
And now you, too, can use threat intelligence to enhance your security.

IBM Security Thought Leadership White Paper

Threat intelligence moves security to the next level

Your security products send alerts when a cyber attack strikes. Your incident response plan tells you what to do to block the attacker's action and recover normal operations. But do you know how or where the attacker was able to get into your environment? Do you understand the tactics, techniques and procedures the attacker used?

How the attacker maintains a foothold on your network? What information it is targeting? Where in your network it is going? And what kind of damage it is trying to do?

Most importantly, do you know how to use information about this attack to help prevent threats in the future?

In many organizations, gathering and using threat intelligence can be a challenge. Organizations relying only on monitoring and an incident response plan may not know how to take the next step toward using intelligence to enhance security. And if they're already gathering detailed attack data, they can be overwhelmed by the sheer volume of information a security platform generates.

In either case, they're likely to need help moving their organization to a more insightful and effective approach to stopping and reducing the impact of attacks.

The answer is to focus on tactical, operational and strategic cyber threat intelligence. But to get there, organizations need a more efficient approach than deploying dozens of standalone security solutions, each with its own data feed. They need the insight that's possible when massive data volumes are integrated, rather than scattered across solutions. They need the ability to prioritize threats and target a response rather than waste time and money on false positives. And they need relief from the complex workload that burdens the security operations center team when it's managing multiple technology platforms and vendor relationships.

In short, to move to the next level of security, organizations need a way to both understand and manage threat intelligence. Because an organization that can uncover the context of a threat can also better respond to it.

USD3.62 million

Average cost of a data breach.[1]

Learn more about the impact of security threats from the experts at IBM® X-Force®.

[1] Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview," June 2017.

Get help from the experts to understand and act on threats

To catch cybercriminals, IBM has assembled a team of industry-leading security experts who understand not only the needs of the organization requiring protection but also the methods of the bad actors behind attacks. With this team, IBM continues to grow and improve its security services in response to the rapidly evolving nature of security threats.

Now, IBM Security clients can leverage threat intelligence capabilities to better respond to threats and build a more comprehensive security plan.

IBM X-Force Incident Response and Intelligence Services (X-Force IRIS) leverages its team's industry-leading expertise to help business and enterprise security leaders better understand the threat landscape—and leverage intelligence data in products and services across business units. X-Force continuously enriches and updates new and existing data via all-source analysis and research, in order to rapidly discover, identify and characterize threats.

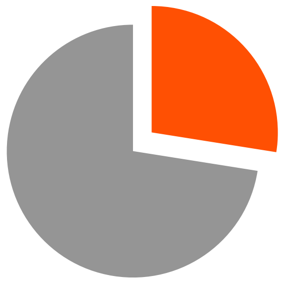
This, in turn, empowers organizations to make better decisions in structuring their cyber defenses.

Read about the industry leadership of X-Force on the web.

Through X-Force, IBM provides expert threat intelligence capabilities including:

- **IBM X-Force Threat Analysis Service**, delivering quality, timely and targeted information on Internet-based threats to help IBM clients take decisive, proactive measures to protect their infrastructure from imminent attack
- **X-Force IRIS impact analysis capabilities** that take a deep look at threat groups, discovering what kind of danger they pose, how they work and how the enterprise can prevent them from happening again following an initial breach
- **X-Force IRIS strategic threat assessment**, using threat intelligence to help an organization understand how threat actors would attack its most vulnerable assets

X-Force IRIS Cyber Threat Intelligence workshop, a two-day workshop designed for cybersecurity analysts across industries, is customized to the needs of individual organizations to help them use threat intelligence to enhance their security posture.



27.7%

Likelihood of a recurring data breach within two years.[1]

[1] Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview," June 2017.

Understanding the landscape: Get timely and reliable threat analysis

Who has the time and resources to research and analyze security intelligence? You almost certainly don't. But X-Force does—in fact, for IBM X-Force Threat Analysis Service, this is the focus. Its service offerings are designed to help you actively anticipate and prevent attacks rather than simply reacting after the fact when you don't have sufficient insight and preparation. Using security intelligence X-Force itself gathers and analyzes, the service is your trusted, reliable source for near-real-time global threat information to help you take decisive, proactive measures.

With its capabilities delivered to clients through a dedicated portal and via email, X-Force Threat Analysis Service provides information that includes:

- Daily summaries and assessments of active vulnerabilities, malware and threats, with links to recommended fixes and security advice
- A graphical representation of the top five affected TCP/UDP ports reported during the previous 24-hour time period
- Customizable notifications based on geography, sector and security product
- Summaries of the top security news stories
- Notification of IBM X-Force Protection Advisories and Alerts

Through X-Force Threat Analysis Service, you can also receive daily and forecast information from IBM X-Force Research and Development AlertCon™ that indicate the current and expected threat state of the Internet. By measuring the current threat level, this service can help you quickly determine the likelihood of an attack against your assets.

X-Force Threat Analysis Service additionally issues priority alerts and advisories that deliver breaking information on threats. These notices include security advisories that contain new vulnerabilities researched by the IBM X-Force Research and Development team, as well as solutions to manage and resolve the threat.

Integrated X-Force threat intelligence provides the capability to rapidly identify and remediate threats.

Learn more about X-Force Threat Analysis Service in the X-Force Threat Intelligence Report.

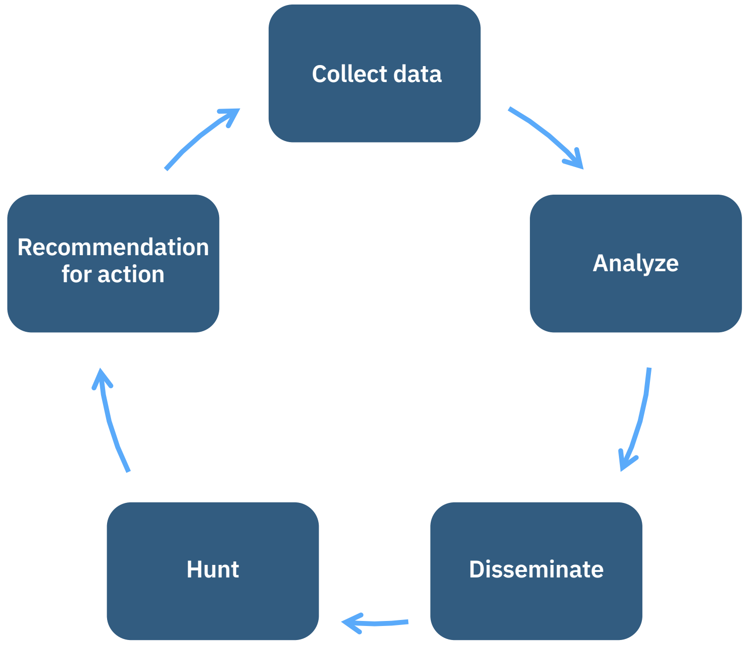
Preparing for an attack: Know where you face the greatest risks

Every organization faces security risks, but the risks aren't the same for everyone. An attacker targeting a retail organization, for example, will likely go after different assets than an attacker targeting a hospital. Within the organization, targets vary, too. An attack on the accounting department might target financial data or employees' personal information, while an attack on the engineering department might target trade secrets and other intellectual property.

As part of a strategic threat assessment, X-Force IRIS can help identify and classify these threats. Based on data IBM gathers for the client, threats are characterized by types of attackers, common points where an infection might occur and the procedures attackers are likely to employ—information an organization can use to protect itself.

For a company facing threats to payment card information, for example, the strategic threat assessment might reveal that attacks arrive through malicious code remotely installed on point-of-sale devices or poorly secured third-party connections. For a company facing threats to intellectual property, the strategic threat assessment might note that cybercriminals often hold data hostage for ransom. For a company facing threats to its internal communications, the assessment might notify the company that it faces potential disruption to its ability to perform business operations or financial damage in the form of contractual breaches or fines from regulatory bodies.

Using incident response investigations and technical observations by IBM experts, plus information on previous attacks at the organization and data from open sources, X-Force IRIS assigns a risk rating for the client. It then provides recommendations for improving security measures, such as utilizing threat intelligence to update risk assessment plans or briefing leaders on key threat intelligence regarding attackers, tools, vectors of infection and methods of exfiltration.



IBM provides a continuous loop of threat investigation and intelligence.

Learn more about X-Force IRIS.

When an attack strikes: Know who is doing what, where and how

When a risk or a threat turns into an actual attack, information and insight become powerful tools for protecting your organization. Whether the attack damages physical systems, network and equipment, or harms your trust relationships with customers, partners or government, threat intelligence can play a major role in helping to quickly and accurately mitigate its effects.

As part of the strategic impact analysis, X-Force IRIS can collect valuable information you can use in stopping an attack or helping prevent others of the same type. A typical scenario provides a description of the attacker, a description of the attacker's capabilities and a collection of indicators that can reveal the attacker's activities.

Threats are categorized into groups, which describe aliases under which the threat actor operates, the mission the attacker hopes to achieve (such as destruction of assets or theft of intellectual property), sponsorship (such as a government or military), previous campaigns by the same attacker, country of origin, targeted countries and targeted industries.

The X-Force IRIS impact analysis identifies the tools, techniques and procedures the attacker is using, including the attacker's working hours and length of time in a target network, as well as actions used against specific files, hosts or networks. In an attack on files, for example, X-Force IRIS can identify programming languages, techniques used to obscure code, techniques used to encrypt content, or malware that may be attached. Investigations can reveal files made to look as if they are from governments, militaries or private companies; malware that is made persistent by the use of legitimate user credentials; or decoy files designed to attract users' clicks with the inclusion of political, security or other hot-button themes, including bogus job announcements.

191 days

Average time required to discover a data breach.[1]

Learn more about the IBM Vision Retainer offering, which includes the X-Force IRIS impact analysis.

[1] Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview," June 2017.

Conclusion: Reduce your security exposure today and tomorrow

X-Force IRIS offers a world-leading team of experts—recruited for their abilities both to address the security needs of enterprises and to understand the attack methods of cybercriminals—who provide threat intelligence and proactive security services.

These IBM experts provide insight into the capabilities of malicious code, why the breach occurred, and steps the organization should take to repair the damage and remediate the incident. Armed with this information, your organization can be better positioned to prepare for the next security breach before it occurs, and to execute rapid and strategic response and remediation after a breach is discovered.

With X-Force IRIS, your organization can respond faster and more effectively to help reduce the impact of an attack. Threat intelligence can help optimize incident response processes to minimize the chance of future breaches. It can help business and technology leaders better understand the threat landscape to better structure their defenses.

What differentiates IBM X-Force IRIS Threat Intelligence?

Timely	Relevant	Accurate
Quicker to action	Actionable	Reliabile
Machine-to-machine	Context from breaches	Elimination of unneeded searches
Scalable	Reduced work cycles	Organizational risk assessment
Prioritized	Delivery to right person and place	Smarter decisions

Learn how X-Force IRIS can help you prepare for and rapidly respond to security threats.

For more information

To learn more about IBM X-Force Incident Response and Intelligence Services, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research, provides security intelligence to help organizations holistically protect their infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors one trillion security events per month in more than 130 countries, and holds more than 3,000 security patents.

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, vist: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
March 2018

IBM, the IBM logo, ibm.com, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

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 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. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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.