



---

### Highlights:

- Helps identify weaknesses and harden your defenses
  - Determines whether compromise has occurred
  - Enables a more rapid response should a cyber incident occur
- 

## IBM APT Survival Kit

*Make sure you are ready for cyber incidents and data breaches*

The cyber threat landscape requires constant vigilance against disgruntled insiders, sophisticated criminals and aggressive nation-states. In fact, in the words of a former FBI director, there are only two types of companies—those that have been hacked and those that will be. Yet even they are converging into one category: companies that have been hacked and will be hacked again. The costs related to a data breach now total more than US\$3.5 million per incident<sup>1</sup> and old security strategies such as defense-in-depth and perimeter security can't keep up with multiple threat surfaces. A security skills shortage only magnifies the key problem—how does an enterprise know if it has already been the victim of an advanced persistent threat (APT) or whether it can detect and respond to a new one?

The IBM APT Survival Kit can help address the challenges of preparing for a cyber attack. Unlike many other service providers, we help you determine whether the response plan you have on paper actually works in the real world of cyber threats. Most important, we can provide an end-to-end cyber readiness package with tools ranging from assessment and incident preparedness, to real-world simulation—all backed by IBM's Global Threat Intelligence.

---

*Costs related to a data breach now total more than US\$3.5 million per incident.*

---



<sup>1</sup> Cost of a Data Breach Study, 2014, Ponemon Institute, <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=SEL03027USEN#loaded>

## Planning for the inevitable cyber attack

The IBM APT Survival Kit includes three components that can build your threat awareness and help plan a more robust response: a **cybersecurity awareness workshop** that goes behind the scenes, using real-world scenarios, illustrative examples and interactive demonstrations to examine the anatomy of modern cyber attacks; **incident response planning**, which outlines appropriate response activities in the event of a security breach; and **threat modeling and mock incident testing**, where IBM security experts conduct and supervise a cyber incident simulation for up to eight hours at your location. This exercise helps determine how well your security team responds to, communicates during and remediates a possible breach.

## Helping to discover security vulnerabilities and possible breaches

The attack surface of your IT infrastructure is the sum of software, network and human vulnerabilities that an attacker can exploit—something you need tested by trusted professionals. Additionally, your infrastructure may already be harboring undetected malware. In fact, 83 percent of compromises take weeks or more to discover, and 59 percent take months or more to contain.<sup>2</sup> The IBM APT Survival Kit addresses these challenges. First, we conduct **penetration testing** of your defenses. IBM experts with the knowledge of the latest threat vectors probe your defenses to identify where you are most vulnerable and can be exploited—a method more extensive than most other kinds of automated or manual penetration testing. Additionally, we perform an **active threat assessment** to answer the question “Am I already infected?” This service looks for malicious software and activity that is already present in your IT and network environments.

---

*83 percent of compromises take weeks or more to discover, and 59 percent take months or more to contain.*

---

## Getting the help to prevent or respond to a cyber attack

**One thing is clear:** the longer a stealthy attacker sits undetected in the enterprise network and its endpoints, the more damage they can do.<sup>3</sup> If you want the peace of mind that comes from having a team of experts who can more quickly respond to a cyber incident, the IBM APT Survival Kit provides IBM's **emergency response services**. You have access to an around-the-clock global hotline that provides an immediate response from our computer security professionals; forensic analysis of your cyber incident; global threat intelligence with IBM X-Force® Service; and expert help in remediating your problem.

<sup>2</sup> 2012 Verizon Data Breach Investigations report, [http://www.verizonenterprise.com/resources/reports/rp\\_data-breach-investigations-report-2012\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)

<sup>3</sup> “Okay, Breaches Are Inevitable: So Now What Do We Do?” Current Analysis, July 20, 2012, <http://itcblogs.currentanalysis.com/2012/07/20/okay-breaches-are-inevitable-so-now-what-do-we-do/>

Based on your needs, we can add additional services to your IBM APT Survival Kit that further enhance your threat readiness and security posture. These include:

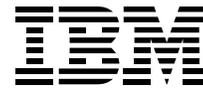
- Distributed-denial-of-service (DDoS) attack simulation—a simulated denial of service attack on your web sites with IBM security specialists who use automated tools to test your defenses
- IBM Managed Web Defense—a service that helps protect you from DDoS attacks and increase your web presence without compromising security
- Security intelligence analyst—an IBM threat professional dedicated to your organization who provides up-to-date information on threat actors and tactics specific to your organization, industry and sector

Take advantage of our proven expertise, techniques and methods to help your organization achieve its security objectives. Benefit from IBM's holistic approach, with critical considerations around people, technology, process and governance.

### Why IBM?

IBM's integrated security intelligence helps protect businesses from cyber threats around the world. Our consultants are certified by many leading security associations in penetration testing, analysis, and incident response and forensics. IBM has 10 security research centers, 10 security operations centers and 14 security development laboratories. We also have more than 1,000 security patents. Additionally, we manage tens of thousands of security devices for thousands of clients world-wide. Our systems monitor 15 billion network events for our clients each day across 133 countries.

IBM APT Survival Kit includes:
Cybersecurity awareness workshop
Incident response planning
Threat attack modeling and mock incident testing
Penetration testing
Active threat assessment
Emergency response services
Optional services include:
Distributed-denial-of-service (DDoS) attack simulation
IBM Managed Web Defense
Security intelligence analyst



© Copyright IBM Corporation 2015

IBM Global Services  
Route 100  
Somers, NY 10589 U.S.A.

Produced in the United States of America  
April 2015  
All Rights Reserved

IBM, the IBM logo, [ibm.com](http://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 [ibm.com/legal/copytrade.shtml](http://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 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.



Please Recycle

## For more information

To learn more about security intelligence and operations consulting from IBM, please contact your IBM marketing representative or visit the following website: [ibm.com/services/security](http://ibm.com/services/security)

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: [ibm.com/financing](http://ibm.com/financing)