Preparing for—and responding to—the inevitable IT breach

Build a strong security posture with IBM X-Force Incident Response and Intelligence Services

IBM Security Thought Leadership White Paper

Security essentials: A proactive and reactive approach

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 *after* it has been detected—and *after* it has caused damage. While a post-attack analysis is necessary, it's important to note that—with the right tools and processes in place—threat preparation *before* a major security breach occurs can help to maintain business continuity and reduce the time to recover an enterprise environment. Immediate and decisive proactive and reactive approaches to security are essential—especially since three alarming trends have emerged:

- Today's threats are intended to cause massive destruction at enterprise scale.
- Organizations are struggling with slow detection and response times, while threat actors are automating many areas of their tactics, techniques and procedures (TTPs).
- Contextual and actionable threat intelligence is significantly lacking as IT security teams struggle to analyze massive volumes of data.

As these trends continue to evolve, a proactive approach that focuses on preparedness before an incident occurs is just as important as having a solid incident response plan for use after. This way, organizations can build a comprehensive security defense—much in the way that an immune system can protect the body from illness.

IBM® X-Force® Incident Response and Intelligence Services (IBM X-Force IRIS) offers an exceptional global team of experts who provide threat intelligence and proactive services that organizations need to prepare for a security breach before it occurs—and to execute rapid and strategic response and remediation after a breach is discovered.

USD3.62 million

Average cost of a data breach.[1]

Learn how IBM X-Force skills and expertise can help you proactively tackle security threats.

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

Addressing the expanse of a security crisis

Perhaps one of the most dramatic trends that has emerged recently is the speed of attacks and the amount of destruction they cause. These threat actors execute highly sophisticated and organized attacks that can shut down a business—including entire data centers and enterprise resource planning (ERP) systems. Destruction of this magnitude requires a provider with a global footprint that can act quickly to rebuild business systems from the ground up.

Recent examples of such large-scale attacks include:

- Shamoon, which disabled tens of thousands of computers in the Middle East region and launched additional attacks in late 2016 and early 2017, causing sweeping damage across the petrochemical and financial industries in the region[1]
- WannaCry, a form of ransomware that shut down computers around the world in 2017, knocking out banks, public transit systems, hospitals and universities[2]
- NotPetya, the 2017 malware-disguised-as-ransomware attack that infected victims in at least 65 countries[3]

In these and similar attacks, X-Force IRIS acted swiftly and comprehensively to coordinate efforts among its global team to help clients triage the compromise, making same-day, next-day and ongoing recommendations about what clients needed to do and when they needed to do it. X-Force IRIS 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 clients needed to restore business continuity.

USD4 billion

Estimated total losses from the WannaCry attack.[4]

Learn how the TrickBot Trojan used the same self-spreading worm module found in WannaCry and NotPetya.

1 Bradley Barth, "Shamoon malware remains destructive force since 2012 Saudi oil attacks," *SC Magazine,* December 6, 2016.

2 Brandon Vigliarolo, "WannaCry: The smart person's guide," *TechRepublic,* June 20, 2017.

3 Danny Palmer, "Petya ransomware attack: What it is, and why it's happening again," *ZDNet,* June 28, 2017.

4 Jonathan Berr, "'WannaCry' ransomware attack losses could reach $4 billion," *CBS News,* May 16, 2017.

Minimize time between detection and response

When an attack threatens—or breaches occur—IT security teams often simply add a new product to combat the threat. This approach, however, leaves the organization with multiple point solutions that lack integration and automation and add complexity to the infrastructure. This lack of integrated tools, as well as manual processes, can create dangerous delays in the security environment, which bad actors are counting on to cause rapid and large-scale destruction.

X-Force IRIS can help to reduce delays between detection and response—where even a few minutes can have a substantial impact on how much damage the breach will cause. They can guide organizations through the process of strengthening their immune system, building in up-front communications and automation, and helping to streamline business processes and close security gaps to increase visibility and control. X-Force IRIS can assist in involving the right stakeholders in building an incident response plan and coordinated playbooks, and can provide ongoing assessments, tabletop exercises and recommendations for improvement.

When a security breach happens, X-Force IRIS serves as the first responder, with our IR experts working seamlessly in the background with client security teams to rapidly triage any damage. They leverage threat intelligence for insight into the capabilities of malicious code, why the breach occurred and the best steps to repair the damage, and remediate and resolve the incident to get clients back to business quickly. X-Force IRIS can coordinate with the appropriate IBM organization, such as IBM Managed Security Services, to remediate future threats.

66

Average days it takes to contain a data breach.[1]

Learn more about X-Force IRIS.

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

Leverage deep threat intelligence

A key reason why attacks move with such strength and speed is that today's threat actors have become adept at sharing their successes, methods and tools with each other—and quickly. Meanwhile, IT 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.

X-Force IRIS threat researchers provide malware reverse engineering, threat modeling and threat assessments. Additionally, they analyze both publicly available data sources such as malware repositories and IBM telemetry data, such as threat activity occurring around the globe in 133 countries. X-Force IRIS communicates 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 IRIS works together with incident responders to help them understand the actor's tools and attack infrastructure. The X-Force IRIS team reviews host and network data, enriching threat information based on findings and providing X-Force IRIS and client incident responders with guidance on what to continue hunting for within the compromised environment.

X-Force IRIS provides end-to-end services, working with clients 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 what the threat actor might do next

At the same time, X-Force IRIS provides threat information a client's senior leadership could use to make informed business decisions and communicate to internal and external stakeholders.

1.5

billion

Records Yahoo reported leaked from breaches that occurred in 2013 and 2014.[1]

Read about the biggest security events that occurred in 2016.

1 Thomas Fox-Brewster, "Yahoo: Hackers Stole Data On Another Billion Accounts," *Forbes,* December 14, 2016.

Acting with force: Real-world accounts

The first Shamoon attack on Saudi Arabian computers at oil company Aramco had far-reaching effects, and it was indicative of one of the directions security breaches have taken: disrupting business. Subsequent attacks occurred in 2016 and 2017 targeting Middle Eastern petrochemical companies and other networks within Gulf Cooperation Council states, destroying hundreds to thousands of file systems. The attack caused a ripple effect across the petrochemical and financial industries as the data in entire data centers and ERP systems was destroyed.

X-Force IRIS 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 IRIS used its threat intelligence to execute informed, sustainable remediation, provide real-time support and rebuild the client environment, working in tandem with the IBM Security regional team. Once it identified the attack lifecycle, X-Force IRIS provided proactive notification to a larger group of IBM clients.

During the NotPetya attacks of 2017, which were intended to cause widespread destruction by acting as a “wiper” to destroy data, X-Force IRIS was able to identify the method of attack—tax software used by global companies doing business in Ukraine. NotPetya has since been identified in 65 countries. Though the malware was disguised as ransomware, the team discovered that the threat actor’s intent was not financial gain—but, as in the case of Shamoon, to shut down businesses. X-Force IRIS uncovered the full anatomy of the attack, including root cause, initial execution, propogation and destructive capabilities. The team then used this information to create a response playbook that has been shared with the broader IBM X-Force Exchange community.

- Learn more about how X-Force IRIS detected and responded to the Shamoon attacks.
- Learn more about the details X-Force IRIS uncovered during the NotPetya attacks.

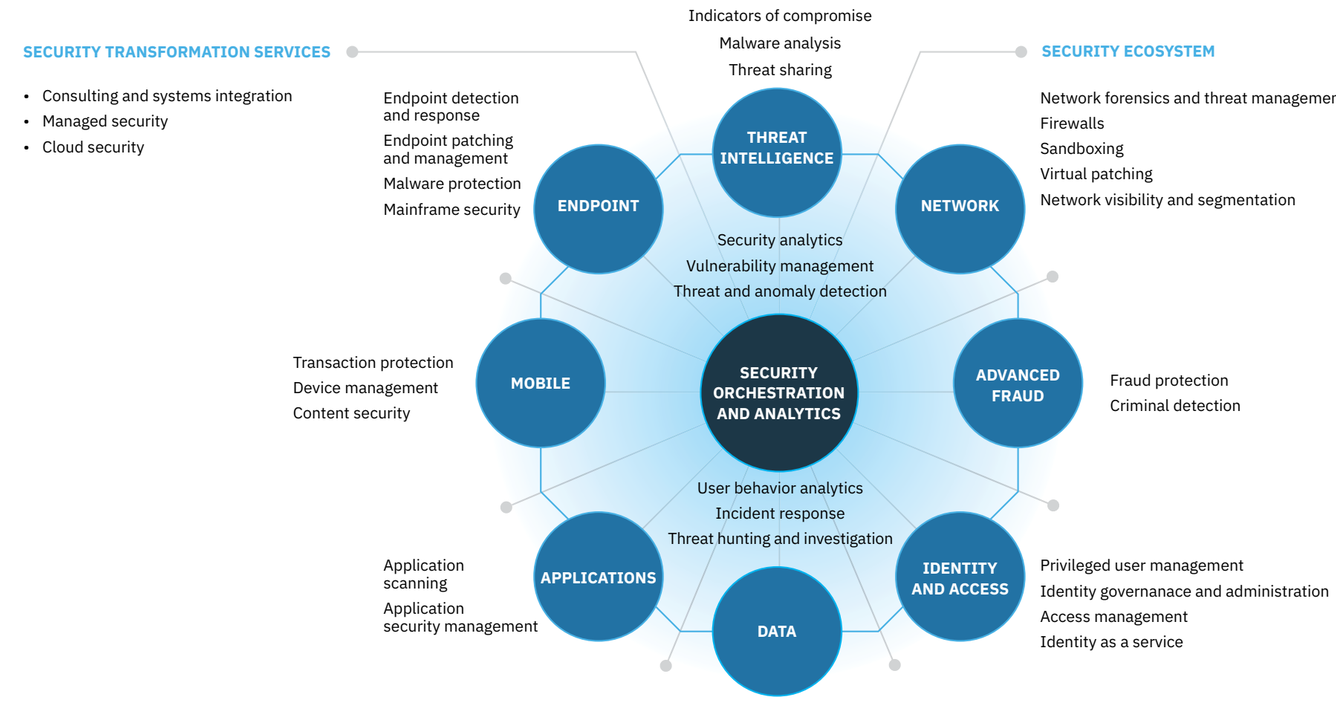
X-Force IRIS is a key part of the IBM Security immune system

X-Force IRIS plays an integral role in the IBM Security immune system, part of a larger ecosystem of products and underlying services that can help clients strengthen the health of their security posture. The X-Force IRIS focus is on building a security strategy and infrastructure that expects to be exposed to threats. With this approach, clients can be both proactive and reactive to security threats that aim to cause widespread damage at rapid scale, tapping into global X-Force IRIS threat intelligence to understand events before and after they happen, and minimize the time between detection and response.

Proactively, X-Force IRIS can provide assessments and recommendations to improve a client's security infrastructure. Reactively, while the X-Force IRIS team serves as a first responder during a compromise, the team can also engage a wider network of appropriate experts. Together with X-Force IRIS and the broader IBM Security network, IBM can help mitigate compromise through a variety of competency areas and build transformative capabilities that enable organizations to more effectively detect, respond to and prevent security breaches.

- Learn more about the IBM Security immune system.
- Watch a video about IBM Security immune system capabilities.
- Learn more about the X-Force IRIS approach to security.

An integrated and intelligent security immune system



The IBM Security immune system delivers 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.

For more information

To learn more about IBM X-Force IRIS, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/services/xforce-incident-response-and-intelligence.html

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
October 2017

WGW03339-USEN-00