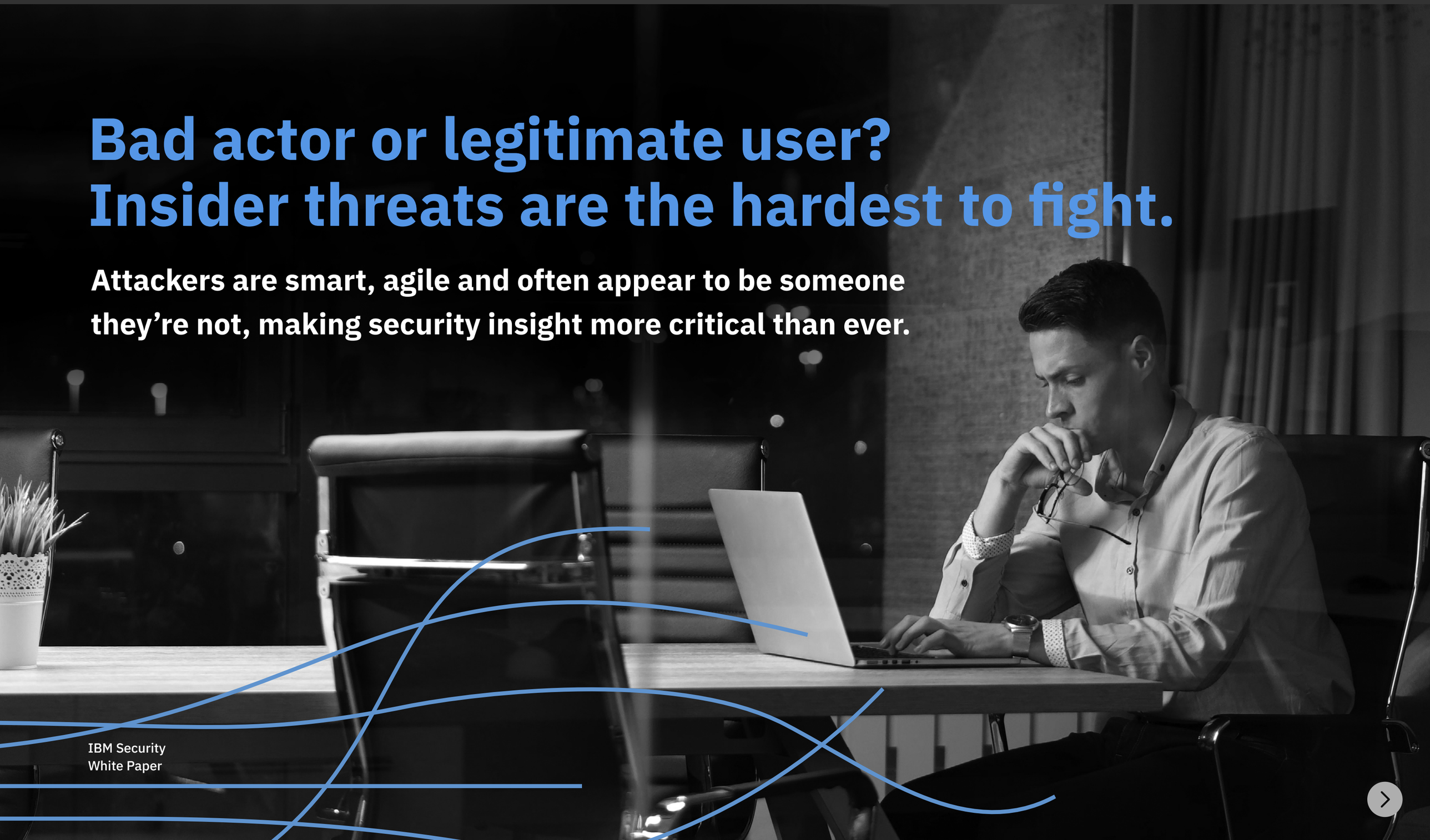
IBM Security

Bad actor or legitimate user? Insider threats are the hardest to fight.

Attackers are smart, agile and often appear to be someone they're not, making security insight more critical than ever.



IBM Security
White Paper

Your insiders: Business requires trust. But security demands caution.

An enterprise has to trust its employees, partners and suppliers. Business simply can't run without them. But when these trusted insiders are accessing your valuable digital resources, you need to know who they are and what they're doing—and you need to know if resources have been compromised. Without those insights, your risk of data theft or application compromise can be unnecessarily high.

Consider: The average cost of an enterprise data breach is USD3.26 million.[1] Up to 60 percent of attacks have been attributed to insiders.[2] The numbers are compelling. But reducing this danger eludes many firms.

That's because the stereotype of a threatening insider—a disgruntled employee intent on revenge or profit—is not necessarily true. People can be careless. They can be easily tricked by well executed social engineering schemes. And as they work to maintain productivity, they may compromise security. In the financial services sector, for example, threats from inadvertent insider actions are 10 times the number of malicious insider actions.[3]

Learn more in the 2017 IBM® X-Force® Threat Intelligence Index.

Your systems administrator's server misconfiguration can create a vulnerability that's easy to exploit. Or more commonly, your accountant's click on a spear phishing email can result in stolen credentials. This can open the door for cybercriminals to freely enter your infrastructure—and remain there for a long time, undetected, because the attackers appear to be legitimate users.

These attacks are the hardest to beat because, on the surface, they don't appear to be attacks at all. They don't stand out as malicious outsiders who have invaded your network. Instead, they're either authorized and simply careless, or disguised and clever. You can fight them only by identifying what they do, by analyzing behavior to discover actions that differ from the norm. Once you have that insight, you can identify these threats, take steps to block further actions and recover from damage they may have caused.

60%

of cyber attacks are attributed to insiders.[2]

1 "2017 Cost of Data Breach Study: Global Overview," *Ponemon Institute*, June 2017.
2 "Reviewing a year of serious data breaches, major attacks and new vulnerabilities," *IBM X-Force Research: 2016 Cyber Security Intelligence Index*, April 2016.
3 "IBM X-Force Threat Intelligence Index 2017," *IBM Corp.*, March 2017.

Danger signs: Beware of these user actions

Internal threats are less about breaking into the infrastructure than about already *being* in. Of course, there has to be a way in—whether as simple as a mistake stemming from a lack of employee training or as sophisticated as a spear phishing campaign that steals credentials. But what makes these threats so hard to discover and deal with is that the actor already has access—and operates unknown.

So what should you look for? There are three tell-tale signs:

Theft and corruption: Insiders are behaving badly

- Access to and downloads of high-value assets that occur more often than normal
- Use of an account for the first time in a long time or from a new location for the first time
- User activity that deviates from normal over a short period or gradually changes over an extended period
- Patterns of activity that are different from a user's peers' activity patterns

Damaging mistakes: Insiders are acting carelessly

- Misconfiguration of the organization's security tools
- Changes to other people's attributes without requesting permission
- Users opening personal accounts on enterprise servers
- Users sharing credentials for virtual private networks
- Contractors checking messages and emails via a third-party provider, especially from abroad
- Users connecting to a cloud server or a personal account on a file-sharing service

Openings for outsiders: The cybercriminals are in

- Increasing numbers of data transfers to and from servers and/or external locations
- Higher-than-expected numbers of logins from machine accounts
- Attempts to change privileges on an existing account or open new accounts

81%

of insider attacks used another person's credentials to bypass controls or gain elevated rights.[1]

Watch the IBM video to learn more about identifying insider threats.

1 "Ponemon Survey Indicates the Growing Threat of Insider Fraud Not a Top Security Priority for Organizations, Proves a Costly Mistake," *Ponemon Institute*, February 28, 2013.

Necessary action: Add powerful tools to your kit

The leakage of sensitive business data by malicious or inadvertent insider actions—compounded by the possibility that these actions can trigger larger-scale theft and application misuse by cybercriminals using malware and bots—is a critical concern for today's enterprises.

The challenge is that without the right analytics tools in place there is no way to differentiate between well-intentioned employees and malicious outsiders who operate in disguise—until it's too late. Short staffing in security operations centers (SOCs) aggravates the issue. And while most organizations deploy security solutions, many of those measures focus on keeping outsiders out.

As a result, in order to deal with threats that are already inside the organization, SOCs need a new approach. They need capabilities that enable them to detect insider threats faster, quickly contain attacks and limit the impact of the incident—all while balancing security against the trust and access privileges they give to legitimate users.

At its core, combating insider threats requires three foundational capabilities:

- **Security analytics**—Tools that bring together a wide variety of security data and threat feeds to automate threat detection and facilitate investigation and response
- **Threat intelligence**—Data feeds from trusted external sources that provide up-to-the-minute, global insights into activities of malicious entities
- **Threat hunting**—Effective investigations that are constantly on the lookout not only for attacks but also for the vulnerabilities that lead to them

With core capabilities in place, SOC analysts can take targeted actions against insider threats—for example, using flow data to detect anomalies in user behavior, establishing thresholds for each user's risk and blocking user access if necessary. The SOC can streamline investigations, improve visibility and respond faster to threats using best practices.

"... insider attacks targeting financial services and healthcare were largely the result of inadvertent actors ... having a greater susceptibility to phishing attacks. Organizations ... should focus on educating employees about phishing and how to avoid becoming a victim..."[1]

Learn more on the web about the integrated IBM approach to combating insider threats.

1 "IBM X-Force Threat Intelligence Index 2017," *IBM Corp.*, March 2017.

Why IBM? An integrated approach helps keep you safe.

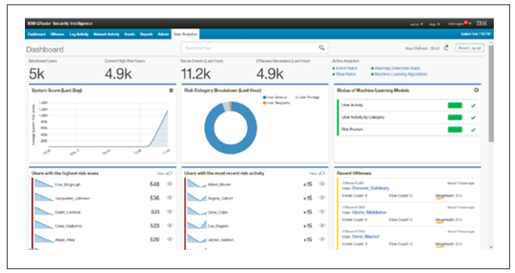
To better detect insider threats, IBM offers an approach designed to enhance the SOC's ability to monitor users and investigate suspicious activity. Based on IBM QRadar® Security Intelligence Platform, an analytics engine that continuously collects security data, this approach creates a baseline of user behavioral patterns and activity profiles, then uses algorithms to detect anomalies and deviations.

To meet the specific demands of combating insider threats, the QRadar platform can be extended with two plug-in solutions, both downloadable from IBM Security App Exchange.

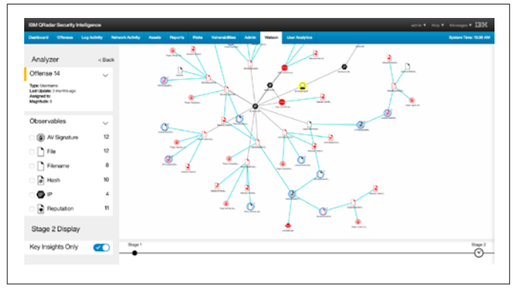
- **IBM QRadar User Behavior Analytics** provides an easy-to-use approach that employs machine learning, individual user behavior analysis and user group behavior analysis to detect anomalous activity and assign risk scores to individuals based on actions. Its dashboard integrates directly into the IBM QRadar SIEM console and allows analysts to view high-risk users at any time and determine necessary security actions.
- **IBM QRadar Advisor with Watson™** utilizes cognitive capabilities to investigate the information it receives from QRadar User Behavior Analytics, qualify the incident and identify the root cause. Operating at 60 times the speed of manual investigations,[1] it draws from structured and unstructured sources to provide context and scope to the attack.

The solution can also be integrated with IBM Security Identity Governance and Intelligence to automatically revoke user access when high-risk activity is detected. And it can be integrated with IBM i2® Analyze to enable security teams to visually map out data relevant to an incident and easily share analysis with team members.

Click image to enlarge. Click again for original size.



IBM QRadar User Behavior Analytics



IBM QRadar Advisor with Watson

- Read more about how IBM QRadar helps organizations detect and investigate insider threats.
- Download the QRadar User Behavior Analytics app from IBM Security App Exchange.
- Download a complimentary 30-day trial of QRadar Advisor with Watson.

1 Results observed by clients who participated in the beta test program of QRadar Advisor with Watson.

For more information

To learn more about QRadar, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/qradar/

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 and development, provides security intelligence to help organizations holistically protect their people, 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 15 billion security events per day 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, visit: **ibm.com**/financing

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2017

WGW03340-USEN-00