Mitigating risks with security intelligence and identity assurance

Gain the visibility to help defend against insider threats, manage access and boost compliance

For organizations around the world, nearly nonstop security threats are simply a way of life. In fact, the average organization experienced more than 91 million security events in 2013—a 12 percent increase over 2012. But security intelligence tools make it possible to reduce these millions of events to a small, manageable list of potentially critical attacks that require further attention. What’s more, these tools can correlate data from across multiple security domains (networks, servers, applications and people) to help organizations understand the context of threats so they know where to focus first.

To provide this valuable context about user activity, security intelligence solutions need to be integrated with the right identity and access management (IAM) tools. Thanks to ever-changing user populations, access points and applications (including mobile, social and cloud), it is increasingly important to know who has access to what at all times for effective security. Reports show that among security events, unauthorized access incidents were more prevalent in 2013—up six percent over the previous year—aligning with a growing use of malware to elevate privilege levels after a network is hacked.1

IBM® Security QRadar® and IBM Security IAM solutions enable organizations to quickly and accurately identify anomalies in user behavior, understand user roles and group memberships, protect against insider fraud and demonstrate compliance with burgeoning security regulations.
And these solutions are integrated out of the box—no costly professional services engagements required. Using the comprehensive analytics and reports provided by these IBM solutions, IT teams can prioritize risk and cost-effectively deploy resources for threat detection, prevention, response and remediation.

**Gain comprehensive security intelligence**

Anchored by powerful security information and event management (SIEM) capabilities, QRadar solutions provide organizations with a unified platform for detecting and defending against network security threats. An intuitive, web-based user interface shared across the QRadar family helps IT personnel quickly identify and remediate network attacks. By applying sophisticated intelligence, QRadar solutions help prioritize thousands of alerts and patterns of anomalous activity, reducing them to a handful of action items for IT teams to address.

QRadar solutions can serve as the linchpin within a small or large organization’s security operations center, helping to collect, normalize and correlate network and security event log data, using years’ worth of contextual insights. QRadar integration with IBM IAM solutions brings additional visibility of user activities and strengthens identification of internal misuse by providing the context of who, and not just what, is accessing critical assets. In particular, QRadar and IBM IAM solutions help organizations monitor the activities of privileged users, enabling easier detection of malicious or inappropriate behavior by these trusted insiders.

IBM IAM solutions centralize and automate the management of users and access activities across the enterprise. They enable organizations to manage user entitlements throughout the user lifecycle with greater accountability and transparency. The solutions close the identity and access loop, providing industry-leading capabilities not only for assigning and enforcing user access rights, but also for monitoring user activity and for detecting and correcting situations that are out of compliance with security policies.

Going beyond identity provisioning and access enforcement, IBM IAM solutions provide identity analytics reporting, role management and recertifications in support of business and security regulations. By simplifying user lifecycle management and providing better visibility into user entitlements and activities, IBM IAM solutions can help maximize IT staff productivity and reduce the cost and complexity of maintaining security and compliance.

Pairing QRadar solutions with IBM IAM solutions enables organizations to:

- Monitor user activity to help prevent targeted attacks
- Detect insider fraud involving privileged users
- Help facilitate compliance with closed-loop analytics

**Monitor user activity**

In response to the ever-evolving threat landscape, security is now focused on systems, applications and the content of information moving across the network. QRadar and IBM IAM integration empowers organizations to get the upper hand on highly targeted attacks that can be multifaceted, difficult to detect and very difficult to eradicate. By correlating data from different security domains—user identities, access attempts and network flows—suspicious activity can be flagged as a potential threat. And the right resources can be deployed for a fast response.

Together, QRadar and IBM IAM solutions support identity-oriented monitoring that ties user activity to other activity across an organization. QRadar leverages identity data for event correlation, enabling security teams to understand how identities relate to threats, policy/compliance violations and access to critical assets. QRadar also maps identities to all log and network activity data for real-time views and reporting on identity activity and behavior.
QRadar can collect identity data from IBM Security Identity Manager, IBM Security Access Manager, human resources (HR) systems and other identity stores. By correlating this data with other network events, it can then detect anomalies in user activity and create and prioritize offenses for action.

In addition, QRadar has significantly expanded its identity monitoring and analysis capabilities through tight integration with third-party IAM products. This integration provides QRadar with access to comprehensive user identity information, enabling deeper security insights for event correlation, forensics and reporting.

For example, employees within the organization may be collecting data from applications and sending it outside the network. (These may be disgruntled employees or, more likely, attackers who are using someone’s compromised credentials to steal confidential data.) Using a centralized asset profile, QRadar can gain full visibility into the user roles and group memberships applied in IBM IAM solutions. If QRadar detects, for example, that a contractor has logged into a database and uploaded a significant amount of data to the Internet—an action not approved for his or her role—it can designate the action as a “potential data loss activity” offense. The database login and network flow events are correlated, and the suspicious activity is prioritized for investigation. IT staff can drill down into the offense within QRadar to learn more about the potential impact and how to proceed with remediation.
Detect insider fraud

Security intelligence is also essential for rapid detection of insider fraud. By integrating QRadar solutions with IBM IAM solutions, organizations can establish a baseline for user behavior and quickly detect when anomalies occur. QRadar solutions are especially useful for tracking and auditing the use of privileged user identities. Extended user identity data is imported into QRadar and mapped to the QRadar user identity and asset model, making it possible for security teams to understand the identity context of incidents, view network and log activity related to identities, and report on user activity, privilege changes and exception events.

To help organizations monitor privileged user activity—as well as inappropriate or abnormal user activity—QRadar analytics can correlate identities with known threats or suspicious IP addresses, generate alerts and prioritize offenses requiring investigation. For example, security analysts have real-time visibility into privileged users accessing an unusual amount of critical or private data. In this case, the system provides the awareness needed to block the attack, helping prevent the loss of intellectual property, customer/patient data or other sensitive information.

IBM Security QRadar Incident Forensics can greatly aid in the rapid investigation of these types of offenses. It can help track the step-by-step actions of the user engaged in suspicious activities and, using full-packet capture capability, reconstruct the content of an email or other communication to see exactly what information was compromised by the user.

In addition, using QRadar reference sets, organizations can write searches, reports and rules based on a specific set of elements, such as a list of IP addresses or user names that may be of interest on the network. By correlating network activity with, say, whether the geographical location of the person trying to access the systems is unusual, QRadar can create an offense.

IT staff can use the QRadar dashboard to inspect the activity at the packet level, review the underlying evidence of sensitive data leaving the network, and prioritize remediation activities.

International paint company governs user access and reduces risk

Supported by 8,500 workers and 25,000 partners and service providers, an international paint company needed a cost-effective way to monitor user access and help ensure regulatory compliance in 17 different countries. By deploying IBM Security QRadar and IBM Security IAM solutions, the company gained visibility into the actions of individuals—both authorized and unauthorized—so they can now identify risky behavior and restrict access that can lead to security breaches. The IBM solutions enabled the firm to enhance governance, reduce help-desk costs, and integrate IAM tasks across diverse applications and IT services.

Help facilitate compliance

Ongoing security breaches have created an environment of ever-tightening government regulations on the handling of sensitive data and user access privileges. Organizations must comply with these regulations or face financial and even criminal penalties. Maintaining compliance with these standards requires organizations not only to govern and enforce user access but also to provide closed-loop processes for auditing and reporting on user access entitlements and activities.

By monitoring broadly across the IT infrastructure—across events, configuration changes, network activity, applications and user activity—QRadar solutions consolidate compliance capabilities into a single product suite. Using more than 1,000 out-of-the-box reports, rules and analytics, security personnel can easily track and monitor critical compliance metrics, user lifecycle management processes and user access details across the organization.
Integration of QRadar and IBM IAM solutions also enables users to quickly create ad-hoc reports to support the unique needs of the business as well. Business-friendly reports provide compliance and audit teams with the ability to monitor and analyze the organization’s performance around key compliance controls for users, including:

- The status of access certifications
- Policy violations
- Remediation activity
- Risk metrics
- IAM server logs
- User identity and access data, such as user logins and access rights
- Group memberships
- Changes in administrative privileges
- Account creation
- Password changes

QRadar and IBM IAM integration brings additional visibility of user activities and internal misuse by identifying exactly who is accessing valuable assets. The integration allows QRadar to augment its asset profiles—which already include network activity data, log data and vulnerability data for assets—and add identity and user attributes for a more comprehensive mapping of identity context. This way, organizations can monitor and report on attempts to access resources for which a user lacks appropriate permissions, as well as attempts to run specific tasks for which the user lacks appropriate rights. QRadar supports security personnel with:

- Out-of-the-box rules and analysis that automatically ties user identity information to specific threats, compliance regulations and policy violations
- Global tracking of user activity with the ability to easily investigate individual user behavior, including resources being accessed, tasks being performed and applications being used
- Reporting of anomalies to help speed the investigation and resolution of security threats

---

Bank in Vietnam helps strengthen security and compliance

Operating 90 branches and employing more than 1,600 people, a bank in Vietnam needed to improve its ability to analyze security logs in a timely and efficient manner to meet government security requirements. By deploying IBM Security QRadar and IBM Security IAM solutions, the bank can now use advanced analytics to help identify and prevent approximately 90 percent of security risks, including insider fraud and other advanced threats. It can quickly and easily support corporate-wide regulatory compliance. Plus, the IBM solutions provide contextual surveillance for reducing millions of security events into a manageable list of actionable offenses.

---

Why IBM?

IBM Security solutions are trusted by organizations worldwide for both identity and access management and security intelligence. These proven technologies enable organizations to protect their most critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. In addition, IBM Security solutions can integrate with third-party environments, including Oracle, Microsoft and SAP, for robust protection. As a strategic partner, IBM empowers organizations to reduce security vulnerabilities and focus more on the success of key business initiatives for many years to come.
For more information
To learn more about IBM security solutions, 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 IBM 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 can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We’ll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: ibm.com/financing

© Copyright IBM Corporation 2014
IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
September 2014

IBM, the IBM logo, ibm.com, QRadar, 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

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

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.

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 or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a 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 systems and products are immune from the malicious or illegal conduct of any party.