IBM Security
Thought Leadership White Paper

June 2015

IT executive guide to security intelligence

Transitioning from log management and SIEM to comprehensive security intelligence

IBM

Contents

Introduction

Security intelligence is the act of gathering every available piece of information passing through an organization's network in order to better understand who's doing what with whom. Similar to business intelligence, it involves the automated processing of large volumes of data in order to develop profiles, seasonality patterns and other network usage insights; but unlike business intelligence, the goal is not to gain a deeper understanding of a market or identify related customer buying patterns. Rather, security intelligence seeks to understand what is normal with respect to user, application, and data-access behaviors so that when abnormal conditions exist, they can be detected. Sounds somewhat easy, right? It's anything but.

Too often, the response to new information security threats is a "finger-in-the-dam" approach with limited funding available for a particular point technology or the reactive construction of new policies or rules. This is in large part because a unified security program—based on automated analyses of unified information from across the IT infrastructure—is costly, complex, difficult to implement and inefficient. As a result, many organizations lack accurate threat detection and informed risk-management capabilities.

This white paper discusses how security intelligence addresses these shortcomings and empowers organizations—from Fortune Five companies to midsized enterprises to government agencies—to maintain comprehensive and cost-effective information security. In particular, it will show how security intelligence addresses critical concerns in six key areas:

- Data silo consolidation
- Threat detection
- Fraud discovery
- Risk assessment and management
- Vulnerability management
- Regulatory compliance

Setting security intelligence goals

High-performance organizations excel at business in large part because they know how to put their information to work. Aided by the automated use of business intelligence technology, they apply analytics to extract maximum value from the massive amounts of data available to them. For example, some organizations use their data insights to better leverage web-based applications and social media technology for making opportunistic offers for goods and services.

Using a similar approach, organizations can secure their proprietary information by implementing a security intelligence program. However, security data can be overwhelming and cryptic. Done poorly, a security intelligence program can drown IT security teams in extraneous data and false positive alerts. They may have to spend hours and hours searching through logs only to find nothing of particular value. The approach is not as prescriptive as business intelligence; security intelligence searches are more event based, requiring the use of established correlation rules to help detect threats and network breaches, identify security risks and areas of noncompliance.

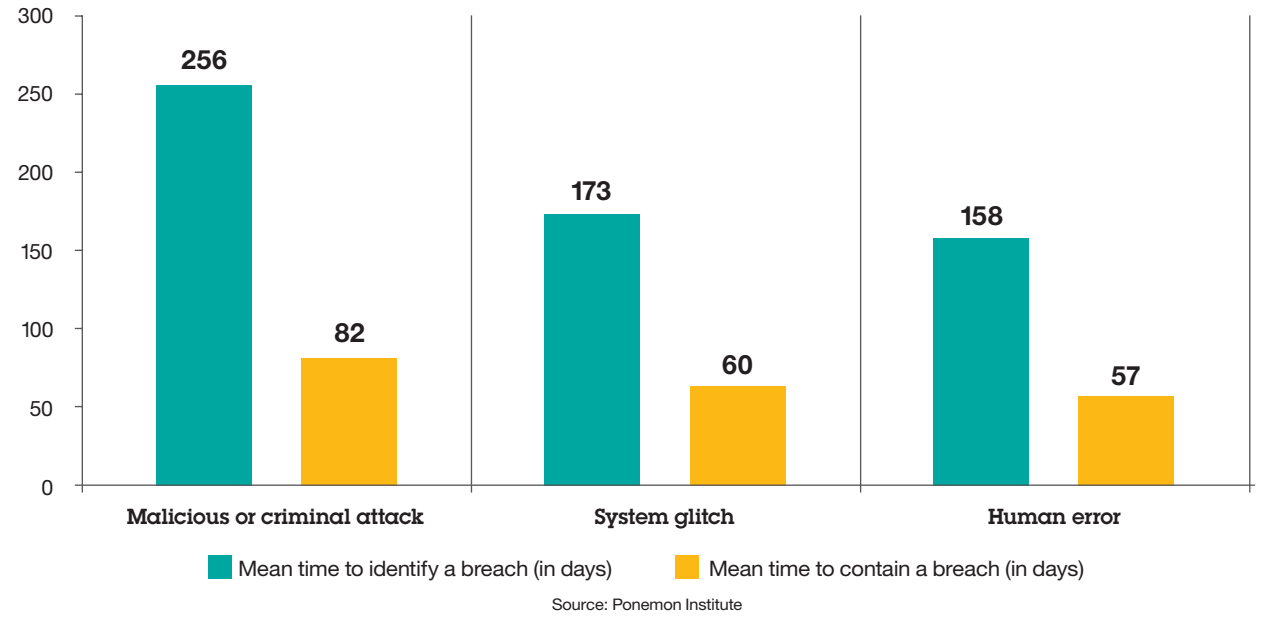
So, if organizations have found the case for business intelligence and analytics valuable, the case for security intelligence is equally, if not more, compelling. Enterprises and government organizations have vast quantities of data that can help detect threats and areas of high risk—if they have the means and the commitment to collect, aggregate and, most importantly, analyze it. This data comes not only from point security products, but also from sources such as network device configurations, servers, network traffic telemetry, applications, and end users and their activities. It's one of the original big-data challenges.

Security intelligence reduces risk, facilitates compliance, shows demonstrable return on investment (ROI) and maximizes investments in existing security technologies by:

- Distilling large amounts of information into an efficient decision-making process, reducing a billion pieces of data to a handful of action items
- Operationalizing data collection and analysis through automation
- Delivering enterprise network visibility and clarity that enable organizations to understand and control risk, detect problems and prioritize remediation
- Validating that the organization has the right policies in place to comply with industry standards and governmental regulations
- Assuring that controls are in place to effectively enforce defined policies

Organizations are seeing dramatic shifts in their IT security environments. In a recent IBM survey of chief information security officers (CISOs), 82 percent of respondents said that the very definition of security had changed in the last three years.[1] Today's security strategies need to account for the expansion of data, devices and user needs—in cloud, mobile and social media initiatives, for example. Plus, they have to protect against a broader array of threats, including advanced persistent threats, criminal enterprises, state-sponsored hackers, hacktivists and other cybercriminals. In fact, close to 60 percent of security leaders said that the sophistication of attackers was outstripping the sophistication of their organization's defenses.[1]

In addition, a Verizon Data Breach Investigations report revealed that attackers are able to compromise an organization within a matter of minutes or days. Their research showed that in 60 percent of cases, attackers were able to compromise an organization in minutes.[2] But the time to identify the compromise—and contain it—can be significantly higher. According to a recent Ponemon Institute study, the mean time to identify a breach was 206 days, while the mean time to contain it was 69 days. What's more, those times can vary based on the root cause of the incident. In their research, the time to identify and time to contain a breach was highest for malicious or criminal attacks and much lower for human-caused breaches.[3]



According to the Ponemon Institute, the average time to identify and contain a breach is the highest for malicious or criminal attacks.

Defining the problem

The security model of five to seven years ago is no longer adequate to meet contemporary challenges, as "Internet hooliganism" has given way to organized criminal activity. The older model is outmoded and does not scale in the face of today's threats and IT environment. Perimeter-based security that focused on protecting all systems using a defined signature approach has evolved into a highly distributed model that assumes a breach has already occurred. The new model focuses protection on high-risk assets using behavioral-based methodologies and continuous monitoring technology.

In an era where employees, partners and customers regularly conduct business on the Internet, cybercriminals are able to exploit new attack vectors and leverage misplaced user trust. Consequently, government and industry mandates have emerged that have stronger penalties for noncompliance—and more diligent enforcement.

The security industry has responded with new and enhanced products to meet each threat. All of these tools add value to overall enterprise security, but they are, in effect, islands of security technology. They are not conducive to a risk-based, enterprise-wide security program that quickly swings into action when a breach occurs.

In many cases, organizations must deal with incomplete data because an isolated security point product may not recognize a threat or risk for what it is without correlation from other data sources. On the other hand, even when data is collected from

disparate sources, analysts are challenged by the sheer volume, making it extremely difficult to distill actionable information. Without the right intelligence, many security products simply deliver information overload.

A true security intelligence solution addresses these problems by centralizing data from disparate silos, normalizing it and running automated correlation analyses using predefined rules. This enables organizations to focus on their most immediate and dangerous threats by finding signals within the noise—helping them to detect, prevent and respond to the most critical situations.

Moving beyond log management and SIEM

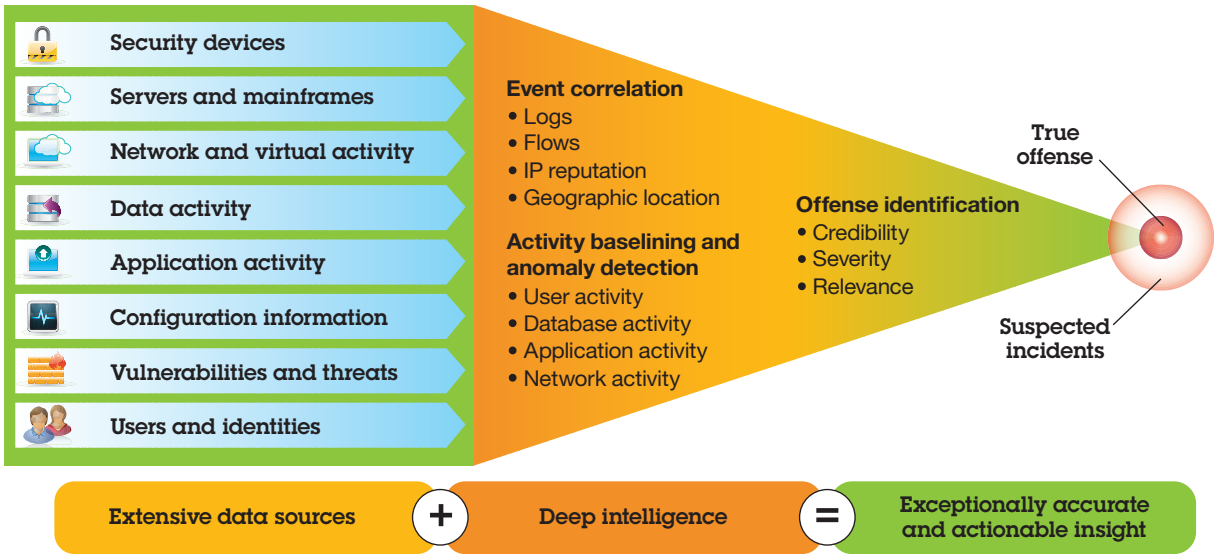
The concept of security intelligence is partially realized in security information and event management (SIEM) tools, which correlate and analyze aggregated and normalized log data. Log management tools centralize and automate the query process, but they lack the flexibility and sophisticated correlation and analysis capabilities of SIEM and, ultimately, security intelligence.

But SIEM should be regarded as a point along the way rather than a destination—the end goal is comprehensive security intelligence. SIEM is very strong from an event-management perspective and plays a particularly important role in threat detection. Comprehensive security intelligence, however, must encompass and analyze a far broader range of information. It requires continuous monitoring of all relevant data sources across the IT infrastructure, as well as evaluating information in contexts that extend beyond typical SIEM capabilities. That context includes, but is not limited to, security and network device logs, vulnerabilities, configuration data, network traffic telemetry, packet captures, application events and activities, user identities, assets, geo-location, and application content.

A key value point for security intelligence beyond SIEM is the ability to apply context from across an extensive range of sources. This can reduce false positives, tell users not only what has been exploited but also what kind of activity is taking place as a result, and provide quicker detection and incident response.

This produces a staggering amount of data. Security intelligence provides great value in leveraging that data to establish very specific context around each potential area of concern and executes sophisticated analytics to accurately detect unusual situations. For example, a potential exploit of a web server reported by an intrusion detection system can be validated by unusual outbound network activity detected by network behavioral anomaly detection (NBAD) capabilities. Anomaly detection works by understanding the standard behavioral profiles of users, applications and data. Then, rules can fire off when unusual behavior occurs, such as someone logging into new resources at odd hours of the day or data transfers that exceed a defined threshold of capacity.

In addition, analysis of events and flows can help IT security teams focus on the highest priority incidents, giving them broad visibility into potential offenses. However, even an automated data reduction capability of 1,000 to 1 can still overwhelm the investigative abilities of most organizations. In a Ponemon Institute study, researchers found that an individual security incident investigation can consume up to 4.4 days.[4] So, even if the typical security team receives only 10 high-priority offenses a day, they're going to rapidly build a backlog of security investigations without specialized network forensics tools. For example, tools that use an alternative source of data—such as full-packet capture (PCAP) data—can help expedite investigations, reducing the time it takes to determine the root cause of a breach down to hours or minutes, rather than weeks or several days.[4]



IBM QRadar Security Intelligence Platform delivers total security intelligence.

Once all the reactive investigations have completed, security teams can spend their remaining hours working on proactive security measures. This will help them reduce their overall attack surface. One of their never-ending tasks is to patch legacy applications developed years before IT security became a boardroom focus. Consider, if a report surfaces indicating a server has a newly disclosed vulnerability, how do security teams evaluate the threat for this particular server? Security intelligence can analyze all available data and outline:

- The presence or absence of the vulnerability
- The value the organization assigns to the asset or data
- The likelihood of an exploit based on attack-path threat models
- Configuration information, which may indicate, for example, that the server is not accessible because a default setting has been changed
- The presence of protective controls, such as an intrusion prevention system

Determining the business value of security intelligence

One of the most compelling arguments for security intelligence is operational efficiency, or better use of people, time and infrastructure. This is the ability to incorporate several security and network technologies into an integrated system rather than operating products independently. A recent Ponemon study showed that companies that adopted integrated security tools

were also able to reduce their staffing costs. In their research, 43 percent of respondents said they had reduced their headcount by one full-time individual, while another 36 percent had reduced their headcount by a half full-time equivalent.[5] With advanced automation, intelligence and integration, organizations don't need as many people to have full visibility and clarity into high-risk situations.

The focus on security intelligence is also particularly relevant, as operational responsibility for security is increasingly being placed in the hands of network operations teams. It makes sense to mirror this consolidation of operational responsibilities with consolidation at the intelligence layer. Think in terms of enabling multiple tasks in single-platform and cross-functional development of skills across the organization, and then deploying access based on roles.

Further, security intelligence adds value in other areas of IT, such as troubleshooting system problems, network issues, and user support and authorization analysis. It enables organizations to use integrated tools across a common framework, and to leverage a unified data set to address problems along the entire security spectrum. This can be illustrated in five of the most prominent use cases in which security intelligence provides high value.

Data silo consolidation

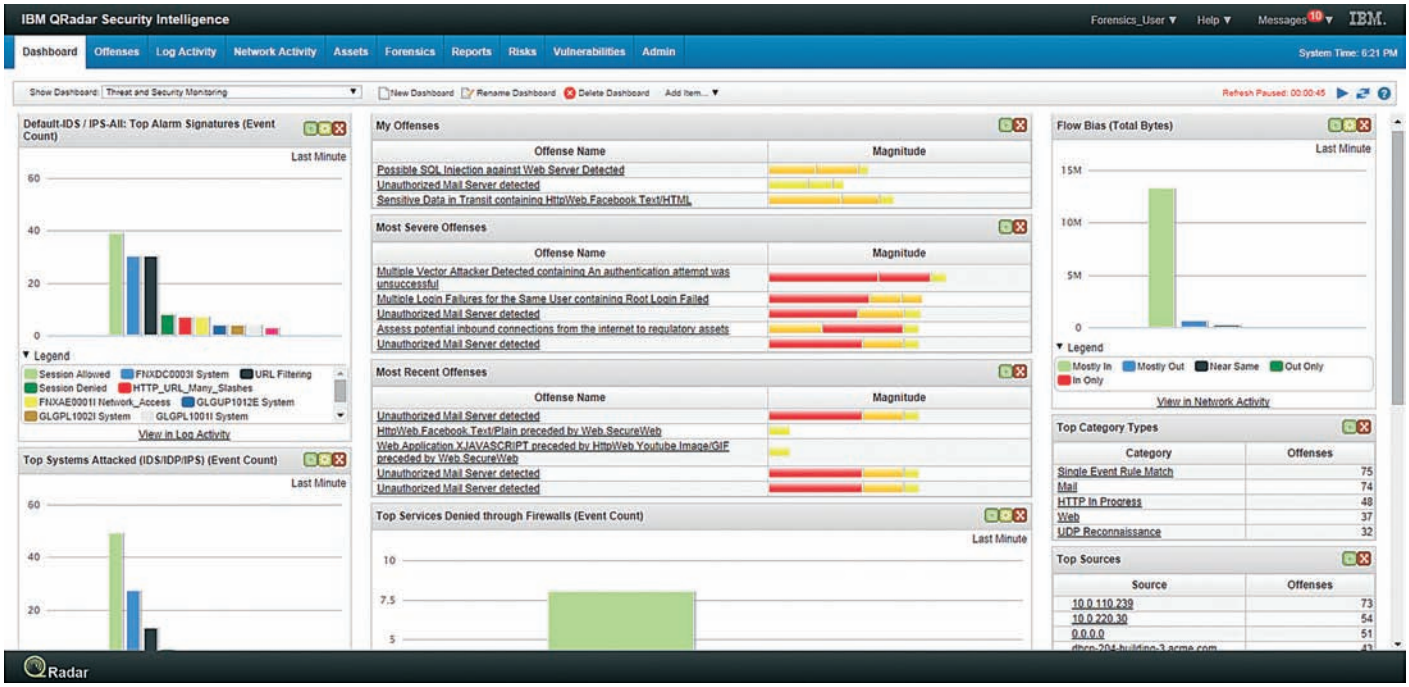
Without automated technology, business intelligence analytics are difficult to execute. The data that would enable users to understand inventory returns, supply chains and more is available, but it is siloed in different applications and databases.

It falls upon the analyst to compile data from all those sources and pour them into spreadsheets or databases to perform manual analyses. Security analysis poses similar problems, and the sheer volume of available information can easily overwhelm IT analysts. A rules-based security intelligence solution provides the means to extract insights from an abundance of seemingly unrelated network activities. From a security perspective, data can exist in three types of silos:

- Log source data locked up in disparate security devices, applications and databases
- Network flow data that identifies IP addresses, ports, protocols and even application or "payload" content crisscrossing through the network
- Full packet capture data that includes everything sent or received by any network user

In the first two cases, security intelligence breaks down the silos by integrating data feeds from disparate products into a common framework for automated analysis rather than simply collecting and reporting events for compliance purposes. This brings in all the enhanced detection and risk assessment capabilities the consolidated telemetry of security intelligence can deliver and, from a CIO perspective, reducing these silos enables the rationalization of security products that would otherwise have to be managed on a point-product basis. The third case requires vast data collection resources and sophisticated parsing and processing to turn packetized network transfers into meaningful insights.

Threat detection



The Threat and Security Monitoring dashboard shows a prioritized view of high-risk offenses.

As enterprises have opened themselves to Internet-based commerce and remote users, security has moved from a perimeter-based model with all policy centered on the firewall and intrusion prevention systems to something that simply assumes a breach has already occurred and tries to quickly detect intruder behaviors. Security is now focused on users, hosts, applications and the content of information moving out of the organization.

Moreover, we're seeing growing incidences of highly targeted attacks, including attacks on high-profile companies. Sophisticated, targeted intrusions are typically multistaged and multifaceted, difficult to detect and very difficult to eradicate; advanced persistent threats are characterized by the tenacity of the attackers and resources at their disposal.

An overarching intelligence should be applied to the diverse security technologies that have been developed in response to the evolving threat landscape. As noted in the discussion of security context, an activity that appears innocuous to one part of an

infrastructure may be revealed as a threat when that data is correlated with other sources. For example, an attacker may disable logging, but can't shut down network activity. Proprietary applications may not produce logs; some parts of the network may be without firewalls. A true security intelligence solution can still identify the applications and services running between that host and the network by analyzing network flows and, subsequently, flagging a potential threat.

Fraud discovery

Security intelligence is absolutely essential for effective fraud detection. Besides network telemetry, data from the switching and routing fabric, and the security-device enforcement layer, the key ingredient is an understanding of normal behaviors for users, applications and data.

Fraud detection requires monitoring everything that goes on across the network: network activity and events, host and application activity, and individual user activity. Security intelligence enables organizations to bind the user to a particular asset. By tying together network, DNS server and application activity with directory information, for example, security intelligence can tie a specific user to a specific IP address for a specific VPN session. Deviations from normal usage patterns are early indicators of insider fraud.

Risk assessment and management

Security intelligence provides the backbone for risk management through network traffic analysis, impact analysis and threat modeling in the form of attack path simulations. It is the difference between reacting to attacks on the network and proactively protecting one's most important assets using a thorough analysis of possible connections.

Impact analysis is based on the value an organization assigns to a particular asset and negative consequences to the business if it is compromised. Security intelligence addresses this by asset and data discovery and classification to identify critical assets.

Further, it answers questions such as, how exposed is the asset? Does it have direct access to the Internet? Does it have known vulnerabilities for which there are known exploits?

Threat modeling takes into account all these factors and more, identifying not only vulnerabilities on the target system, but possible attack paths based on exploiting weaknesses between the target and the Internet—poorly designed firewall rules, badly configured router access control lists and more.

Vulnerability management

Today's security teams need to minimize the chances of a network security breach by finding key security weaknesses and identifying unpatched or out-of-date systems. However, a typical vulnerability scan can reveal up to tens of thousands of potential exposures—depending upon the network size. Security intelligence can help prioritize these endless lists of vulnerabilities, so security teams can focus their efforts on the exposures that pose the greatest risk.

By correlating vulnerability scan data with network flow and log events, security intelligence provides a single, integrated view of an organization's vulnerability posture. It presents vulnerability scanning results within the context of an enterprise SIEM, and produces an actionable plan for addressing the largest risks. It also understands vulnerability patching activities and will downgrade issues on assets and endpoints scheduled to be addressed with the next patch deployment. This way, organizations can make the best use of their often constrained IT staffing resources, while also facilitating compliance with the latest government and industry mandates.

Regulatory compliance

Compliance is a foundational use case for security intelligence. Security intelligence addresses many compliance requirements, particularly all aspects of security monitoring. For example, security intelligence does not meet all Payment Card Industry (PCI) requirements, but it does meet all PCI monitoring

requirements in a way that SIEM and log management alone cannot. Security intelligence provides the data that serves as a foundation to deliver and demonstrate audit requirements for all regulations.

By monitoring broadly across the IT infrastructure—across events, configuration changes, network activity, applications and user activity—security intelligence consolidates compliance capabilities in a single product suite rather than relying on multiple point products, each delivering its own piece of the audit puzzle.

Outsourcing security intelligence

Organizations that understand the business value of security intelligence may still be faced with budget, bandwidth and skills shortages—making them unable to deploy and manage a robust security intelligence solution. But just as organizations have been moving IT workloads to the cloud for years, there are now cloud-based solutions for security intelligence. These solutions offer an alternative to traditional on-premises deployments using a software-as-a-service (SaaS) model. As a result, organizations can simplify their operations and treat network security costs as a series of monthly operating expenses, rather than any capital investments.

With these outsourced solutions, organizations can benefit from a professionally deployed and managed IT security infrastructure. Security experts can help ensure that the underlying software is always updated to the latest releases. The solutions can scale up to meet dynamically changing business needs, remove the need for additional technical resources to monitor and manage the solution infrastructure, and better fit the operating expenditures budget model.

Addressing the bottom line

Security intelligence, like business intelligence, enables organizations to make smarter decisions. It enables organizations to process more information more efficiently across the entire IT infrastructure. Applying security intelligence technology enables organizations to do more with less: Instead of having analysts devote extensive hours manually poring through a fraction of the available data, the technology automates analysis across all available data and delivers role-based information specific to the task.

Information technology is about automating business processing—for purchasing, logistics, enterprise resource planning and more. Security intelligence is about automating security, including understanding risk, monitoring the infrastructure for threats and vulnerabilities, and prioritizing remediation.

By centralizing security tools and data from the IT infrastructure, security intelligence enables consolidated management and more efficient use of resources devoted to security. Organizations can improve their security posture without additional operational and personnel costs or the expense of purchasing, maintaining and integrating multiple point products.

Security intelligence yields key cost and efficiency benefits, enabling organizations to:

- Reduce deployment and operation costs by using existing staff to help make security relevant to the business
- Simplify purchasing by using a single platform, rather than multiple products
- Use one integrated platform, instead of many—thus, lowering skills barriers
- Automate the collection, normalization and analysis of massive amounts of security data from technical and organizational silos
- Enhance threat detection, applying context to detect possible attacks that might go unnoticed by a particular security technology
- Improve incident response through accurate, quick detection and by using search engine technology in the latest forensics tools

Enabling security intelligence

IBM® QRadar® Security Intelligence Platform provides a highly integrated set of solutions designed to help organizations achieve total security intelligence implemented on a unified operating system and managed through a single console.

Anchored by a powerful SIEM, this platform presents a unique security intelligence capability, integrating a set of high-value security and network-monitoring applications into a unified solution that empowers organizations to deploy security and network operations resources based on analysis of a comprehensive set of data sources.

The platform is built on QRadar Security Intelligence Operating System, which enables IBM to deliver a set of common services around data integration, normalization, rule-based correlation and forensics analysis. This unified structure produces uniform workflow, reporting, alerting and dashboarding capabilities. These support organization-wide policies and processes, rapidly identify threats and assess risk, and support executive-level security information and response requirements.

QRadar Security Intelligence Operating System provides a platform on which users can continue to add new security modules to accommodate new use cases around the intelligent securing and intelligent risk assessment of the enterprise infrastructure. The underlying database is infinitely scalable, eliminating the possibility of a rip-and-replace scenario.

Conclusion

Forward-thinking organizations have recognized and embraced the value of business intelligence technology, as their success is predicated on the ability to analyze and act upon the essential information derived from staggering volumes of data. Similarly, security intelligence is essential because information security is integral to doing business in the Internet-driven, 21st century. Powerful, automated analytics for centralized data from sources that cover the entire spectrum of the IT infrastructure make a high level of cost-effective security not only possible, but indispensable.

Companies reap the benefits of security intelligence

- **An international energy company had to wade through billions of security events daily to find the ones that needed to be investigated. By deploying QRadar solutions, the company can now analyze two trillion events per day—correlating data in real time across hundreds of sources—to identify the 20 to 25 potential offenses that pose the greatest risk.**
- **A credit card firm was struggling to manage legacy technology that not only lacked visibility into the latest threats, but was also costly to operate and maintain. Using QRadar threat detection and analysis, the firm can now protect its critical data and infrastructure from advanced threats. Plus, it reduced its deployment, tuning and maintenance costs by 50 percent.**

For more information

For the latest news and insights on security intelligence, visit securityintelligence.com

To learn more about IBM security intelligence offerings, 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 13 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. For credit-qualified clients we can customize a financing solution to suit your business and development requirements, 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

[1] Marc van Zadelhoff, Kristin Lovejoy and David Jarvis, "Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment," *IBM Center for Applied Insights*, December 2014. http://www-935.ibm.com/services/us/en/it-services/security-services/index.html?lnk=sec_home

[2] Verizon RISK Team, "2015 Data Breach Investigations Report," *Verizon*, 2015. http://www.verizonenterprise.com/DBIR/2015/

[3] Ponemon Institute, "2015 Cost of Data Breach Study: Global Analysis," *Ponemon Institute Research Report*, May 2015.

[4] Ponemon Institute, "Network Forensic Investigations Market Study," *Ponemon Institute Research Report*, December 2014. **ibm.com**/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=WGL03070USEN#loaded

[5] Ponemon Institute, "Security Intelligence Client Study," *Ponemon Institute Research Report*, May 2015.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
June 2015

WGW03018-USEN-01