IBM Security
Thought Leadership White Paper

September 2016

IT executive guide to security intelligence

Transitioning from log management and SIEM to state-of-the-art security intelligence with advanced IBM Sense Analytics Engine

IBM

Contents

Introduction

Security intelligence is the act of gathering and analyzing all the security-related data available to your organization to provide greater visibility into what is happening on your network. Similar to business intelligence, security intelligence involves the automated processing and analysis of large volumes of data. However, 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 arise, they can be rapidly detected and investigated. Sounds somewhat easy, right? It's anything but.

Too often, the response to new security threats is a "finger-in-the-dam" approach where the immediate problem is solved by purchasing a new point product, or hurrying to implement new policies or rules. This frequently generates a sub-optimal result because using increasingly more disparate point solutions can be costly, complex and difficult to implement. What's more, this can create a false sense of security because point products do not always share data across the various management, investigation and response modules of the solutions. As a result, many organizations lack accurate threat detection and informed risk-management capabilities.

This white paper discusses how the advanced capabilities of IBM® QRadar® Security Intelligence Platform, powered by IBM Sense Analytics Engine™, address these shortcomings, empower organizations—from Fortune Five companies to midsized enterprises to government agencies—and provide leading-edge, cost-effective information security.

In particular, it shows how QRadar with Sense Analytics addresses critical concerns in key areas including internal and external threat detection, risk assessment and management, vulnerability management, fraud discovery, forensics investigation, incident response and regulatory compliance. Plus, it shows that the platform can be expanded even further through collaboration with peers and the integration of applications and third-party products to help ensure the continued improvement of security intelligence capabilities.

Setting high goals and exceeding them

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 enormous amounts of data available to them. For example, some organizations use their data insights to better leverage web-based applications and social media to making opportunistic offers for goods and services.

Using a similar approach, organizations can secure their proprietary information by implementing a security intelligence and analytics program. Enterprises and government organizations have vast quantities of security data from many sources they can use to detect threats and areas of high risk—if only they have the solutions required to collect, normalize and, most importantly, analyze it.

Security data, however, can be cryptic and overwhelming. Conventional log management solutions can be poorly integrated or lack the necessary capabilities for proper data analysis and reduction. They can also drown IT security teams in extraneous information and false-positive alerts. Using these solutions, administrators may find themselves spending countless hours searching through logs only to find nothing of particular value.

A better approach is to implement a solution that goes beyond what conventional log management offerings provide. Such an advanced security intelligence solution delivers scalable, enterprise-wide network visibility and clarity to support efficient decision-making. It helps reduce risk, facilitate compliance, show demonstrable return on investment (ROI) and maximize investments in existing security technologies by:

- **Using analytics to eliminate threats**—Collaboratively transforming raw security data into visible and meaningful insights that portray adversaries' actions throughout the entire attack chain
- **Deploying a platform to scale with speed**—Allowing the organization to collect and understand security data from every enterprise device, application and user in hours rather than days, weeks or months
- **Enabling automation, remediation and collaboration**—Helping security operations center (SOC) analysts speed through investigations and use integrated threat intelligence, new applications and solution extensions to limit the downside of a breach, and to prevent breaches from happening again

Advanced analytics and flexibility in deployment options are critical in an era when organizations are seeing dramatic shifts in requirements for securing their environments. In a recent IBM survey of chief information security officers (CISOs),

close to 60 percent of security leaders said that the sophistication of attackers was outstripping the sophistication of their organization's defenses.[1] A Verizon Data Breach Investigations report revealed 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 256 days, while the mean time to contain it was 82 days.[3]

Defining the problem

The security model of only two years ago is no longer adequate to meet contemporary challenges, as independent attackers have now banded together into sophisticated criminal organizations. Yesterday's model is outmoded and does not scale in the face of today's readily available exploit kits and self-morphing malware. Sadly, perimeter-based security is easily defeated by phishing scams, SQL injections, watering-hole schemes and other cleverly disguised methods. The forward-leaning organization assumes not only that a breach will, but that it probably already has, occurred.

It's a given; employees, partners and customers regularly conduct business on the Internet, allowing cybercriminals to exploit new attack vectors and leverage misplaced user trust. The security industry has responded with enhanced products to meet each threat. These tools add value to overall enterprise security, but can be, in effect, islands of security technology. They can unnecessarily complicate investigations of suspected malicious activities. By contrast, speed and decisiveness require more integrated, risk-based, enterprise-wide security solutions that scale with the environment and quickly swing into action when a breach occurs.

In many cases, organizations must deal with incomplete data because a point product solution did not recognize a threat or risk. On the other hand, even when data is collected from disparate sources, analysts are challenged by its sheer volume, making it extremely difficult to distill actionable information. Random and ad-hoc searches of log source events are an inefficient method for discovering attacks and breaches.

A comprehensive, effective security intelligence solution addresses these problems by collecting and centralizing data from disparate silos. It then normalizes the data and runs automated correlation analyses using predefined, flexible, easily customizable rules to sense and detect security offenses in near real time. This enables organizations to focus on their most immediate and dangerous threats by finding signals within the noise—helping them to prevent, detect and respond to the most critical situations.

Moving beyond log management and SIEM

The concept of security intelligence is partially realized in 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.

However, 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 and flows, vulnerabilities, configuration data, network traffic telemetry, packet captures, application events and activities, user identities, assets, geo-location, and application content.

To be fully comprehensive, there is also need for solutions that can consume log and service data from cloud applications to provide security visibility across on-premises, hybrid and cloud infrastructures.

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.

Expanding the approach with Sense Analytics

While a necessary start, the ability of SIEM to search, read logs, report on usage, and perform basic event correlation and analysis is only a partial step toward achieving the goal of true security intelligence—to establish real network security. The better approach is to deploy a technology that can go beyond SIEM to prevent, detect and respond to security offenses. It must be able to detect subtle differences in the environment—from advanced threats to internal misuse—and alert security teams when unusual or forbidden behavior occurs.

Powered by the ability to sense change and an engine that can attach context and meaning, QRadar Security Intelligence Platform with Sense Analytics is a scalable, integrated platform managed through a single console that delivers the necessary global enterprise visibility to help uncover malicious behaviors better than other solutions.

QRadar first collects network activity data, then engages its Sense Analytics Engine for real-time analysis of that data to identify indications of advanced threats and internal misuse. It then adds valuable context to deliver critical insights and value in three key areas:

Sense Analytics threat detection
Uncovers abnormal, risky behaviors across users, entities, applicarions and data; discovers low and slow threats in real time; and finds and prioritizes weaknesses before they're exploited

Single platform, unified visibility
Automatically integrates with many IBM and thrid-party sources; collects billions of events per day, whether on-premises or in the cloud; and unifies threat monitoring, vulnerability and risk management, forensics, and incident response

The power to act at scale
Enables security experts to collaboratively take action for intelligent incident prioritization and comprehensive insights; and leverages the power of threat intelligence and collaboration with IBM X-Force® and the IBM security App Exchange

IBM QRadar Security Intelligence Platform delivers security intelligence using advanced Sense Analytics.

Providing context for huge volumes of security data

A key value point for extending and enabling security intelligence beyond SIEM is the ability to apply context from across an extensive range of data sources. This can reduce false positives, give security teams visibility into exploits taking place, and provide quicker detection and incident response.

An un-tuned SIEM produces a staggering amount of data, but security intelligence with Sense Analytics provides great value by leveraging that data to add context around each potential area of concern, and applying sophisticated analytics to accurately detect unusual situations that could be signs of a breach. For example, a potential exploit of a web server reported by an intrusion detection system can be validated by unusual outbound network activity discovered by behavioral anomaly detection capabilities. Anomaly detection works by understanding the standard behavioral profiles of users, applications and data. Rules then can fire off an alert when unusual behavior occurs, such as someone logging in to new resources at odd hours of the day, or large data transfers that exceed a defined threshold of capacity.

In addition, analysis of events and network flows gives IT security teams broader visibility into potential offenses, and allows them to focus on the highest priority incidents first. 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 unless they have specialized network forensics tools. Tools that use alternative sources of data—such as full-packet captures (PCAPs)—can help expedite investigations, and reduce the time it takes to determine the root cause of a breach from weeks or days to hours or even minutes.[4]

Once all the reactive investigations have completed, security teams can spend their time on proactive security measures to address vulnerabilities and risks, and prevent breaches. One of their frequent tasks is to patch applications that contain weaknesses. Consider: If a report surfaces indicating a server has a newly disclosed vulnerability, how do security teams evaluate the threat? Security intelligence with Sense Analytics 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 or absence of protective controls, such as an intrusion prevention system

The business value of Sense Analytics

One of the most compelling arguments for security intelligence with Sense Analytics is greater 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—creating a single platform with unified visibility. A recent Ponemon study showed that companies that adopted integrated security tools were also able to reduce their staffing costs or reallocate existing security personnel. Forty-three percent of respondents 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.

Comprehensive security intelligence also 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 use cases where security intelligence with Sense Analytics provides high value:

Advanced threat detection: IBM QRadar SIEM aggregates security logs and network flows, and uses its Sense Analytics Engine to identify advanced threats. Using behavioral-based analytics, it detects anomalies and suspicious activities, performs event aggregation and correlation, assesses severity, and provides security analysts with a manageable list of prioritized offenses requiring investigation.

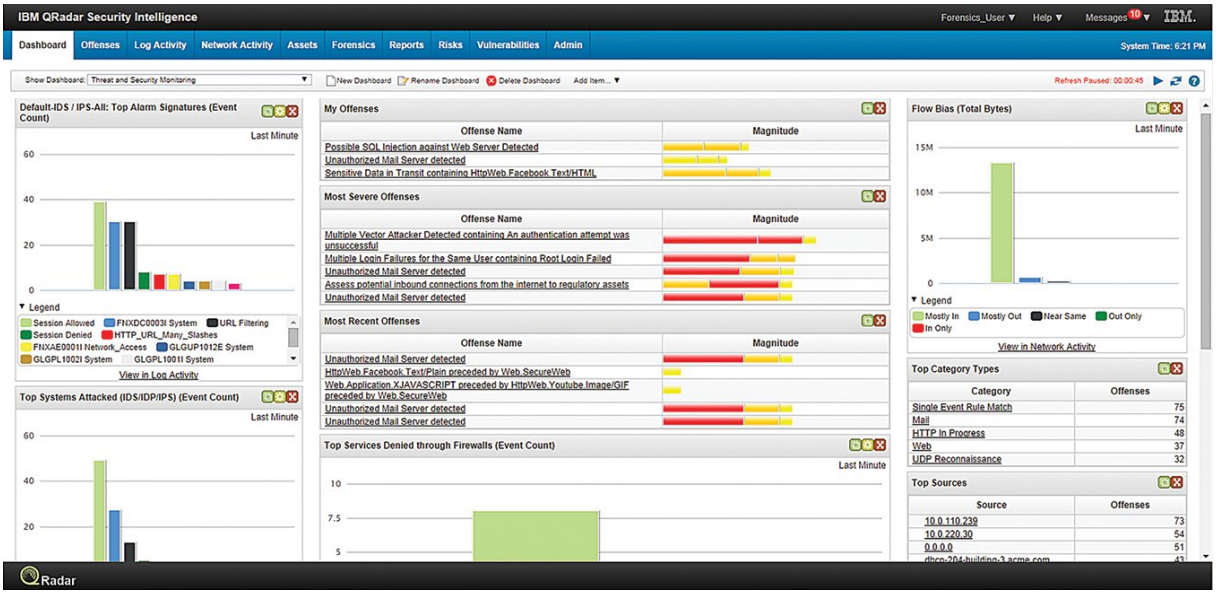
User behavior analysis and insider threat monitoring: IBM Sense Analytics performs automated asset, service and user discovery and profiling. After profiling behavior and determining a baseline, QRadar detects deviations from normal and generates alerts for items to be investigated. It then supports quick and easy forensics analysis and incident response for rapid insider threat resolution.

Compliance reporting: QRadar automatically senses and discovers log sources, network devices and configurations. It analyzes data collected to identify conditions that are noncompliant with internal policies and regulations. It includes customizable reports for best practices, internal policies and regulations including Control Objectives for Information and Related Technology (COBIT), Sarbanes-Oxley (SOX), Gramm–Leach–Bliley Act (GLBA), North American Electric Reliability Corporation (NERC), Federal Information Security Management Act (FISMA), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act of 1996 (HIPAA), UK Government Connect Secure Extranet (GCSx) and more.

Risk and vulnerability management: QRadar senses the addition of new network assets, scans them to detect vulnerabilities, identifies configuration errors and out-of-policy conditions, and generates network topology views that identify potential attack paths. It then prioritizes the vulnerabilities and risks discovered to help organizations develop corrective action plans.

Threat detection

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



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

The IBM approach provides advanced threat detection using behavioral-based Sense Analytics to detect anomalies and suspicious activities, perform event aggregation and correlation, assess severity, and provide analysts with a manageable list of prioritized offenses requiring investigation. For insider threat monitoring, the solution performs automated asset and user discovery and profiling to detect behavioral deviations from normal conditions, and generates alerts for further investigations.

Risk and vulnerability management

Security intelligence with Sense Analytics not only helps you after an attack has occurred, it also proactively protects important assets before they're compromised. QRadar helps security teams manage risks and vulnerabilities by sensing new assets, scanning them to detect vulnerabilities, identifying configuration errors and out-of-policy conditions, and generating network views that identify potential attack paths. It prioritizes vulnerabilities and risks to support the development of actionable remediation plans. For example, if vulnerability exists on an endpoint that is scheduled for the next patch deployment, it may assign a higher priority to a high-risk web server that is accessed via the Internet. This way, organizations can make the best use of their often constrained IT staffing resources, and address risks and vulnerabilities in the proper sequence based on priority.

Fraud discovery

Fraud detection requires monitoring everything that goes on across the network, including network activity and events, host and application activity, and individual user activity. QRadar can sense unauthorized network traffic and detect potential security offenses—such as employees who use their personal devices to access corporate email and personal contacts via social media. In protecting the network, QRadar collects and analyzes log events and network flows, detecting, for example, when Internet chat sessions start connecting through port 80, the port normally reserved for HTTP traffic. It correlates network, DNS server and application activity with directory information to 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.

Forensics investigation

Discovery is critical to knowing what threats have occurred—but a comprehensive security intelligence solution will also tell security teams who did what, when, where, and how. Using QRadar, the team can quickly and easily recover the network packets associated with a security offense, rebuild items such as exfiltrated documents or Voice over Internet Protocol (VoIP) conversations, and reconstruct the step-by-step actions of an attacker to enable rapid problem investigation and remediation, along with prevention of future recurrences.

Incident response

Once an offense has been detected, incident response processes need to be quickly implemented to minimize its impact and take it to closure. QRadar offers a powerful integrated capability for detailed incident response planning, management, mitigation and reporting based on best practices. Incidents can be quickly and easily tracked and managed to ensure that they are captured and followed through to resolution.

Regulatory compliance

Compliance is a key security use case for most organizations, and security intelligence with Sense Analytics addresses many regulatory requirements. For example, QRadar automatically senses and discovers log sources, network devices and configurations. It analyzes data collected to identify conditions that are noncompliant with internal policies and external regulations. It includes customizable reports for COBIT, SOX, GLBA, NERC, FISMA, PCI, HIPAA, UK GCSx and more.

By monitoring broadly across the IT infrastructure—across events, configuration changes, network activity, applications and user activity—QRadar consolidates compliance capabilities in one integrated platform with global visibility rather than relying on multiple point products, each delivering its own piece of the audit puzzle.

Keeping up with evolving threats and risks

Cybercriminals don't stand still and they don't work alone—and neither should the enterprise security team. Security analysts need to collaborate not only to keep their security intelligence and Sense Analytics deployments up to date but also to expand capabilities for detecting threats, managing risks and vulnerabilities, and remediating threats in the future. And they need ways to increase efficiencies and extend the capabilities of their often overworked or understaffed security teams.

Even if their security intelligence needs seem limited today—perhaps requiring only log management and compliance reporting—organizations need to future-proof their capabilities to meet changing conditions going forward. To assist, IBM provides three key programs:

- **IBM X-Force Exchange**—A cloud-based threat intelligence sharing platform where teams can rapidly research the latest global security threats, aggregate actionable intelligence and collaborate with peers. The platform provides timely threat intelligence powered by more than 700 terabytes of machine- and human-generated data, with thousands of malicious indicators classified and updated every hour.
- **IBM Security App Exchange**—A collaborative, web-based ecosystem of IBM security developers, IBM Business Partners and IBM customers sharing security-related information and tools, including extensions to QRadar Security Intelligence Platform capabilities. Assets available on the exchange for download include IBM-approved QRadar applications, with rules, reports, searches, reference sets, custom properties, analytics and dashboards, historical data analysis, and plug-ins for QRadar. New applications are posted on the exchange independent of product release cycles in order to keep up with the latest internal and external threats.
- **IBM X-Force Incident Response Services**—Assistance designed to help IBM clients respond to cyber breaches by tapping the knowledge of 3,000 IBM consultants and security researchers globally. Services include a remote incident-response capability to help clients map how a breach occurred and take action to shut it down.

Conclusion: Addressing the bottom line

Like business intelligence, security intelligence enables organizations to make smarter decisions. It enables organizations to process more information more efficiently across the entire IT infrastructure. Applying security intelligence with Sense Analytics enables organizations to do more with less: Instead of having analysts devote extensive hours manually poring through a fraction of the available security 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 with Sense Analytics

is about automating security, including understanding risk, monitoring the infrastructure for threats and vulnerabilities and risks, monitoring the infrastructure to detect internal and external threats, conducting forensics analysis, prioritizing remediation, and executing incident response plans

By centralizing security tools and data from the IT infrastructure, security intelligence with Sense Analytics 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.

IBM QRadar with Sense Analytics enables organizations to "sense" chains of malicious activities and provides an integrated security platform for eliminating threats by analyzing security data and user behavior.

Companies reap the benefits of analytics

- **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

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 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
Route 100
Somers, NY 10589

Produced in the United States of America
September 2016

Please Recycle

[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.

WGW03018-USEN-02