IBM Software
Thought Leadership White Paper

October 2013

Get actionable insight with security intelligence for mainframe environments

IBM provides integrated solutions to report compliance and combat advanced persistent threats in heterogeneous mainframe environments

Contents

Introduction

When it comes to enterprise security, no news is not necessarily good news. A lack of alerts about attempts to attack your system does not mean they did not happen—because chances are, they did. Many large organizations track multiple attempts a week. A lack of alerts just means that while previous attacks were unsuccessful, you may not have received the information and insight you need from your security system to protect against the next attack. Plus, security event analysis might be siloed within individual departments with no enterprise-wide view of the attacks taking place. The next attack could be successful—and devastating. In today's interconnected business environment, no system is immune to threats, including mainframe environments.

To meet this need, IBM has developed an approach to enterprise security called security intelligence. Using integrated solutions, IBM delivers threat analysis, real-time alerts, audit consolidation and compliance reporting to help you keep pace with today's increasing threats, with a single view into the risks affecting both mainframe and distributed systems. Covering people, data, applications and infrastructure, the IBM security intelligence program includes the automated analysis and reporting capabilities you need to deal with the complexity of event monitoring and compliance reporting without burying your staff with an endless stream of log data that does not record threats. Moreover, security intelligence can increase the depth of insight and real-time anomaly detection, improving the integrity of both mainframe and distributed systems, demonstrating compliance and protecting your mission-critical workloads.

Providing rich context that enables meaningful insights

Security issues are rarely isolated events, but few security solutions are broad and integrated enough to deliver insights that make a difference. Information provided by third-party log management and security information and event management (SIEM) solutions typically includes voluminous data with limited context—and hence, limited value. Identifying who did what and when, recognizing what's normal versus abnormal, and obtaining visibility into subtle connections between millions of data points are the goals—but achieving them requires a great deal of contextual data and the analytical means to make sense of it. Security teams also need to be able to integrate mainframe data with distributed events to gain insights that apply to the entire enterprise. Only a highly integrated series of solutions, such as those found in the IBM security intelligence offering, can

produce the necessary visibility to safeguard the environment. Security intelligence enables the organization to better discover and respond to:

- External threats such as financially-motivated criminals and "hacktivists" seeking sensitive data
- Internal threats such as employee or contractor theft of intellectual property
- Unintentional but exploitable weaknesses such as misconfigured security devices, improperly configured access controls, or unpatched device and application vulnerabilities

To achieve comprehensive and insightful reporting on vulnerabilities and threats, including monitoring privileged and non-privileged users, the organization needs centralized event consolidation, network flow analysis and intelligent normalization, and correlation of security data. To ensure that compliance and security goals align, it needs visibility into network segments where logging may be problematic. To discover unknown, excessive or unauthorized mainframe access, it needs visibility into asset usage patterns.

Overcoming the complexities of mainframe security management

Managing mainframe security requires separation of duties across system management functions, processes for identifying exposures and misconfigurations, and a clear audit trail to establish accountability for actions. Managing security requires maintenance of confidentiality and integrity, controlled access to sensitive information, and monitoring of system and data access by all individuals—internal and external, authorized and unauthorized. In reality, separation of duties may be impractical for small management teams. Technicians often require multiple IDs, including full system security privileges or UNIX superuser privileges that bypass security. The urgency to resolve high-impact problems may result in bypassed policies. And manual procedures can introduce system errors—including those that compromise security.

Security challenges in mainframe environments

- **Complexity:** The mainframe is an integral component of multiple, often large and complex, business services, making it difficult to identify and analyze threats.
- **Visibility:** Mainframe processes, procedures and reports are often siloed, impeding cross-enterprise information sharing to combat threats.
- **Compliance:** Verification of compliance is frequently a manual task—with problem alerts all too often received only after a problem has occurred.
- **Cost:** Mainframe management requires highly skilled administrators, who often are in short supply.
- **Security change control:** Change control procedures for security administration often are not followed or not even in place, threatening availability.

In organizations of any size—but especially in the large, mainframe-based enterprise—it can be impossible for humans to keep up with the complexity and dynamic nature of the infrastructure, with new vulnerabilities and with rapidly evolving threats.

What is the result of such security management challenges? In the security-sensitive healthcare sector, for example, one survey revealed that 43 percent of organizations graded their ability to withstand security threats as poor, failing or in need of improvement.[1] More significantly, 23 percent of organizations overall admitted to security breaches in a 12-month period.[2]

And what can be done about it? Best-practice approaches dictate the deployment of automated monitoring, auditing and reporting solutions that can distinguish between normal or baseline activities and suspicious events to provide a more effective way to identify threats and compliance risks.

A best practices approach to security intelligence, auditing and compliance management

A comprehensive approach based on security best practices can help detect and prevent security and compliance exposures throughout the security lifecycle.

Using best practices to detect and prevent exposures

Security intelligence aligns well with best practices designed to meet internal policies, governmental regulations, and the unique security requirements and practices of specific industries. Regardless of the policy, regulation or need driving security, organizations typically seek three goals:

- **Accountability**: Proving who did what and when comes from the ability to manage security-related information from networks, hosts and applications across the IT infrastructure. Accountability correlates this information with an accurate picture of activity to achieve the forensic granularity necessary to investigate violations.
- **Transparency:** Insight into business and IT assets that must be protected comes from visibility into security controls. Transparency enables the organization to assess its adherence to policies by extending visibility into network and application traffic, and into the sensitive resource-related events governed by security rules.
- **Measurability**: An understanding of the organization's security risk comes from the ability to assess and measure both compliance and threats. Measurability supports real-time awareness and responsiveness through interactive dashboards and reporting.

The security intelligence approach builds on these goals to achieve richer insight and dramatically fewer, more accurate alerts through advanced data collection, normalization and analysis. Heuristic capabilities establish patterns of activity so that any activity outside of normal behavior ranges is flagged for investigation and presented in a context that enriches the organization's understanding of the incident to facilitate timely investigation and effective remediation.

Taking steps to put security intelligence into place

The accountability, transparency and measurability made possible by security intelligence help organizations find the threat needle in the event haystack by correlating massive data volumes in real time. An effective security intelligence implementation delivers actionable insight across the environment, from mainframes and distributed systems to applications and data to network and security devices.

But how do you get there? Typically, organizations follow steps that include:

- Collecting and monitoring data from initial data sources, such as authentication events, operating system logs, anti-malware logs, firewalls, configurations, and file and directory auditing on high-value servers

- Constantly monitoring network flow traffic (using taps or spans) to understand both the sources and destinations of network communications
- Defining targeted use cases by examining key business challenges, which may be industry- or company-specific
- Providing the security team and others with role-based access and customizable views into real-time analysis, incident management and reporting—enabling them to drill down into raw data and summarized security incidents
- Providing management tools to summarize and analyze access control, remove unused access authorizations and simulate the effect of new security rules before they are deployed
- Phasing in additional data sources—such as intrusion detection system/intrusion prevention system (IDS/IPS) data, database and database security logs, application logs and physical security system logs—for added context and intelligence
- Creating activity baselines for key metrics and configuration settings, and monitoring for meaningful anomalies
- Deploying a risk management solution to analyze network and device vulnerabilities—enabling the shift from reactive to proactive management

Leveraging the comprehensive IBM security approach

Security intelligence is an integral part of the IBM Security Framework, a comprehensive approach that addresses key areas of security and compliance risk: people, data, applications and infrastructure. Tied together with common capabilities for security intelligence and analytics, the IBM Security Framework delivers a comprehensive structure for policy management, event handling and reporting on which organizations can build their enterprise security programs.

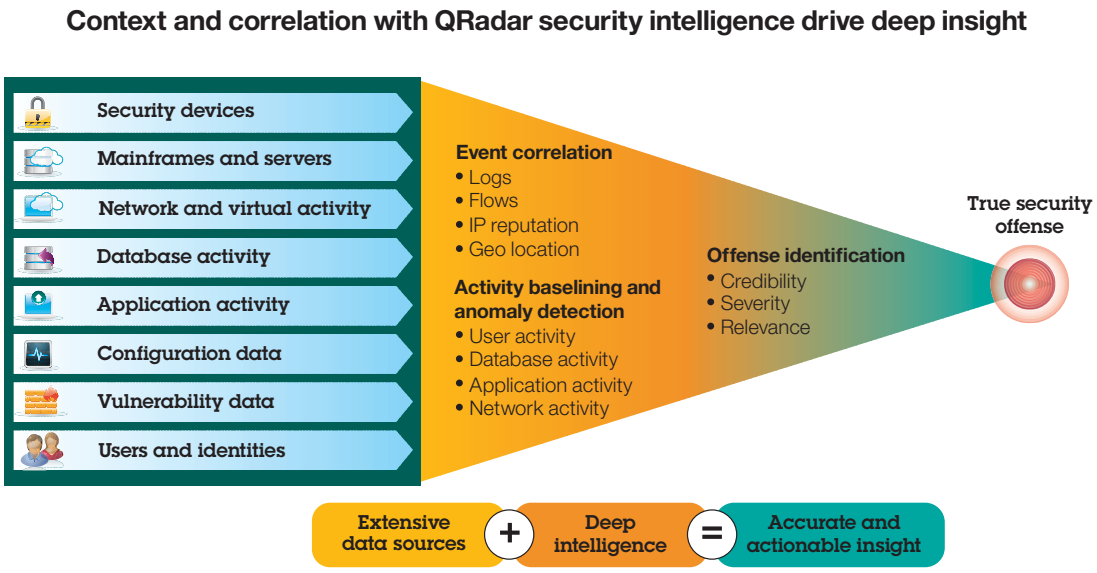
What's more, IBM security intelligence solutions provide integrated capabilities to replace the point solution and "piece parts" approach that many organizations use. IBM solutions build on the mainframe strengths of event analysis and reporting to deliver a broad, enterprise-wide view of security with IBM® QRadar® Security Intelligence Platform.

Integrating IBM solutions for monitoring, analysis and action

Integrated IBM security intelligence capabilities for the mainframe begin with IBM Resource Access Control Facility (IBM RACF®), a component of IBM z/OS® Security Server responsible for administering and defining authorized users according to policy, making access control decisions and creating security log records in IBM System Management Facility. RACF provides integrated application and data security for IBM Information Management System (IMS™), IBM Customer Information Control System (CICS®) and the IBM DB2® database. IBM security solutions also support other enterprise security management products such as CA-Top Secret or CA-ACF2.

Using the security events gathered by RACF, IBM Security zSecure™ solutions provide capabilities such as analysis of and reporting on security events, detection of security exposures, ongoing mainframe threat monitoring and real-time alerts to identify intruders and misconfiguration. IBM Security zSecure Audit provides extensive audit and analysis capabilities beyond z/OS systems, including the ability to audit UNIX security definitions and events on the mainframe, DB2 audit security definitions and events, CICS security definitions and events, IMS security definitions and events, Linux for System z® events, audit security events from IBM Tivoli® Key Lifecycle Manager,[3] IBM WebSphere® Application Server, IBM Tivoli OMEGAMON®, IBM Communications Server network configuration for TCP/IP, and PDS(E) member-level auditing. This provides an integrated view of the health of your system. In fact, mainframe solutions can save up to 70 percent in audit overhead.[4]

IBM InfoSphere® Guardium® and IBM InfoSphere Optim™ solutions discover and classify sensitive data, detect vulnerabilities, and enhance data security with capabilities such as encryption to ensure the privacy and integrity of enterprise data.



QRadar solutions accept data from a wide variety of sources to provide mainframe visibility in the enterprise environment.

IBM Security QRadar SIEM can collect and monitor data from the RACF, DB2, Security zSecure and InfoSphere Guardium solutions for detailed visibility into mainframe operations. Vulnerability data can be gathered for each asset and tracked in a comprehensive asset profile. Event and log data are normalized and enriched with advanced analytical methods such as real-time correlation of network flows and anomaly detection algorithms to identify suspicious actions. IBM solutions also integrate with other SIEM products in the marketplace such as HP ArcSight and NetIQ Security Manager.

Consolidating security intelligence with QRadar SIEM

QRadar SIEM provides enterprise security intelligence with full visibility and actionable insight to protect IT assets from a wide range of advanced internal and external threats. Distinguishing itself from first-generation SIEM solutions, QRadar SIEM collects security events—not only from the mainframe but also from hundreds of other log and flow sources—and correlates log events with network flows and a multitude of other data, presenting all relevant information on a single screen. When used with IBM Security QRadar QFlow Collector appliances, the platform provides Layer 7 application visibility and flow analysis to help you fully understand and respond to activity taking place within your network. Working together, these solutions help you detect threats other solutions might miss, helping ensure policy and regulatory compliance, and minimizing risks to mission-critical services, data and assets.

QRadar SIEM also supports a variety of anomaly detection capabilities to identify changes in behavior affecting applications, hosts, servers and areas of the network. For example, QRadar SIEM can detect off-hours or excessive use of an application or cloud-based service, or network activity patterns that are inconsistent with historical, moving-average profiles and seasonal patterns. QRadar SIEM learns to recognize these daily and weekly usage profiles, helping IT personnel to quickly identify meaningful deviations.

Gaining insights from IBM database security products

Offerings in the IBM Security zSecure suite feed real-time data to QRadar SIEM, IBM InfoSphere Guardium Vulnerability Assessment or other SIEM solutions to strengthen mainframe security and more easily comply with regulations, by simplifying audit and reporting efforts. A consolidated view supports easier identification of and more effective reaction to threats, and a forensically secure database stores event data for use in meeting regulatory mandates. Also integrated into this security intelligence solution, InfoSphere Guardium offerings support continuous, policy-based, real-time monitoring of database activities, including actions by privileged users, by scanning the database infrastructure for missing patches, misconfigured privileges and other vulnerabilities.

The resulting improvements to mainframe security monitoring enable organizations to better detect intruders and malicious employee activity, while identifying misconfigurations that could hamper compliance efforts.

Complying with regulations and standards

Other key aspects of security intelligence include enforcing security policies and site standards as well as demonstrating compliance with industry or governmental regulations and standards. These standards often require protection of sensitive information, segregation of duties, monitoring privileged users, extensive audit reporting and more. As new threats evolve, these standards are constantly changing and becoming more stringent. Noncompliance can result in costly exposures, punitive fines and loss of reputation.

Security zSecure Audit includes the capability to report on Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes Oxley (SOX) regulations and more. Security zSecure Audit can ease the effort and cost required for compliance reporting with a new, flexible interface to automate reporting for external security standards, including:

- Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG), using customizable rule definitions, testing and compliance reporting
- IBM Outsourcing GSD331 (iSeC), which is the primary IBM information security controls documentation for strategic outsourcing customers

Conclusion

It has never been more difficult to protect both your mainframe and distributed environments—and if you are not able to connect the dots between disparate security data in a manageable and insightful way, now is the time to consider a new approach.

Security intelligence offerings from IBM provide organizations with comprehensive and actionable insight into threats and vulnerabilities in mainframe and distributed systems environments. Applying real-time event collection, normalization, and analysis of access information and other security-related data, IBM offerings can reduce both the risk of security breaches and—just as important—the ongoing manual effort of security operations, freeing your team to focus on more serious incidents rather than wading through an endless stream of data without context.

Integral to the IBM Security Framework, IBM security intelligence solutions can strengthen mainframe security operations and enhance availability by consolidating security views to improve identification and remediation of threats. The IBM approach integrates a number of solutions including RACF, DB2, CICS, the Security zSecure suite, InfoSphere Guardium solutions and QRadar SIEM. These products build on the threat intelligence expertise of the IBM X-Force® research and development team to provide a preemptive approach to security. IBM solutions integrate with competitive products for seamless

operations designed to help organizations stay ahead of today's ever-increasing risk of advanced threats, and comply with regulations and standards.

For more information

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

About IBM Security Systems software

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 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

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.

[1] 2011 iSMG Healthcare Information Security Survey. http://www.bankinfosecurity.com/press/ismg-announces-release-healthcare-information-security-today-survey-p-256

[2] 2011 HIMSS Leadership Survey. http://www.himss.org/2011survey/healthcareCIO_final.asp

[3] On October 29, 2013, IBM Tivoli Key Lifecycle Manager will officially be renamed IBM Security Key Lifecycle Manager.

[4] Based on IBM customer experience.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2013

WGW03013-USEN-01