IBM Security zSecure Adapters for SIEM

Extend advanced threat detection and security intelligence for mainframe environments

Highlights

- Help lower the cost of event collection from many products and efficiently handle large numbers of events
- Automate analysis to help identify security weaknesses and minimize the risk of costly breaches
- Integrate IBM® Z® security event analysis with distributed events for real-time enterprise-wide monitoring and reporting

Security is a cornerstone of any organization's IT operations, and in today's cloud, mobile and big-data environments, it is essential to address internal and external threats. Security breaches can result in financial losses, unauthorized access to confidential information, theft of intellectual property, service disruption and damaging publicity.

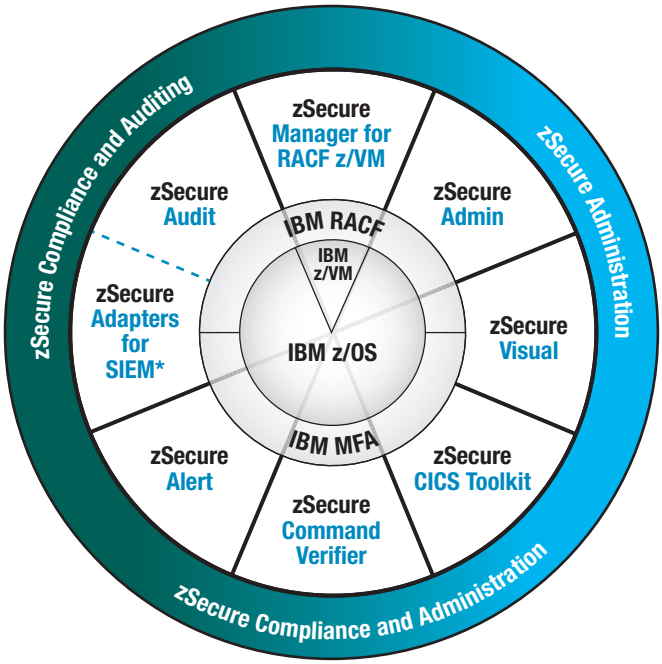
Gathering, collecting, analyzing and integrating the necessary information to help stop security breaches can be a stressful, time-consuming, complex and costly process. It is often a challenge to implement a repeatable, sustainable and automated process for enterprise-wide event analysis, threat detection, auditing, compliance and reporting. Mainframe event information is often omitted from distributed security information and event management (SIEM).

IBM Security zSecure™ Adapters for SIEM is a mainframe solution designed to help security personnel automatically collect, format and send enriched mainframe System Management Facility (SMF) audit records to analytics tools (for example, IBM QRadar® SIEM), to enhance enterprise-wide security intelligence. It is one of eight zSecure products that compose the IBM Security zSecure suite to help reduce cost, simplify compliance reporting, and automate threat analysis and detection.

IBM Security zSecure Adapters for SIEM:

- Collects and formats information from SMF records
- Adds enriched descriptive audit information about the user and the resource

IBM Security zSecure suite



* Product offers a subset of the capabilities provided by zSecure Audit

Collects and formats information from SMF records

zSecure Adapters for SIEM extends coverage to information in more than 40 different Z SMF record types. zSecure Adapters for SIEM generates QRadar Log Event Extended Format (LEEF) files with Z SMF information that can be integrated with enterprise-wide QRadar SIEM, log management, anomaly detection, incident forensics, and configuration, risk and vulnerability management. As new SMF records are introduced for Z security events, including them and reporting on them from the outset is very important in conducting detailed investigations as well as routine security monitoring.

zSecure Adapters for SIEM provides support for:

- IBM Resource Access Control Facility (IBM RACF®)-related events reflected in SMF 30 and 80 records, such as logons, RACF commands, and successful or failed access attempts to resources and data sets (with appropriate logging options).
- CA ACF2-generated SMF records (by default SMF 230).
- CA Top Secret-generated SMF 80 records. (These records are very different from SMF 80 as written by RACF but serve a comparable purpose.)
- IBM DB2®-generated SMF 102 record types. This allows for logging of access violations, administrative commands (GRANT, REVOKE, CREATE, ALTER, DROP), operator commands and options, and access to tables, including SQL commands and connections. To enable this capability, the events must be logged by DB2 to SMF through the audit options for the subsystem or the TRACE AUDIT command.
- IBM Customer Information Control System (CICS®)-generated SMF 110 subtype 1. This allows for logging of CICS transactions. To enable this capability, events must be logged by CICS to SMF through the CICS monitoring facility.

- Additional SMF record types that are generated by IBM z/OS® and its subsystems, such as SMF 14, 15, 18 and 19 for data set access (even when not audited by the security system); SMF 42 for PDS member updates and deletes; SMF 92 for UNIX file activity; SMF 118 or 119 for FTP, Telnet and other TCP/IP activity; and much more. These are essential when trying to build a picture of user behavior, whether this is part of conducting an investigation or performing routine security monitoring. zSecure Adapters for SIEM also provides support for records generated by IBM WebSphere® Application Server (WAS), IBM Security Key Lifecycle Manager, and Linux on z Systems® (SMF 83).
- Additional information fields generated by pervasive encryption and IBM Multi-Factor Authentication for z/OS. This information can be used to help demonstrate compliance associated with privileged user monitoring and sensitive data protection.

Adds enriched descriptive audit information about the user and the resource

In addition to the fields from SMF records, zSecure Adapters for SIEM adds enriched descriptive audit information about the user and the resource, identifying the name, privileges, and other security information for the user, and the function and purpose for system-critical data sets. This information is helpful to build essential audit reports incorporating information such as:

- All RACF commands issued by users with the system special attribute.
- All logons by users with the system operations attribute.
- All logons by users with superuser privilege.
- All updates to authorized program facility (APF) data sets.
- All members updated in parmlib data sets.
- Security events that are not logged by RACF. (This can help a security officer make informed decisions based on the enriched data.)

zSecure Adapters for SIEM sends mainframe security event information to QRadar in near-real time such that it can also be used by IBM QRadar Advisor with Watson™ in cognitive analytics. It can also be configured to send events in batches, once per configurable interval.

zSecure Adapters for SIEM also invokes IBM Common Data Provider for z Systems (CDP) as an option.

Relationship with other zSecure solutions

The functional capabilities found in zSecure Adapters for SIEM are also included in the following products and solution packages:

- IBM Security zSecure Audit
- IBM Security zSecure Compliance and Auditing
- IBM Security zSecure Compliance and Administration

Business benefits

IBM Security zSecure helps meet current and emerging customer needs for integrated industry-leading Z security implementation, providing enhanced integrity, assurance, data protection, security intelligence, identity governance and compliance capabilities. Customer needs are driven by ever-evolving threats, innovative business processes and services, extensions of Z capabilities, and relevant laws and regulations around the globe. zSecure strategy continues on the path of providing integration of auditing and alerting for z/OS,

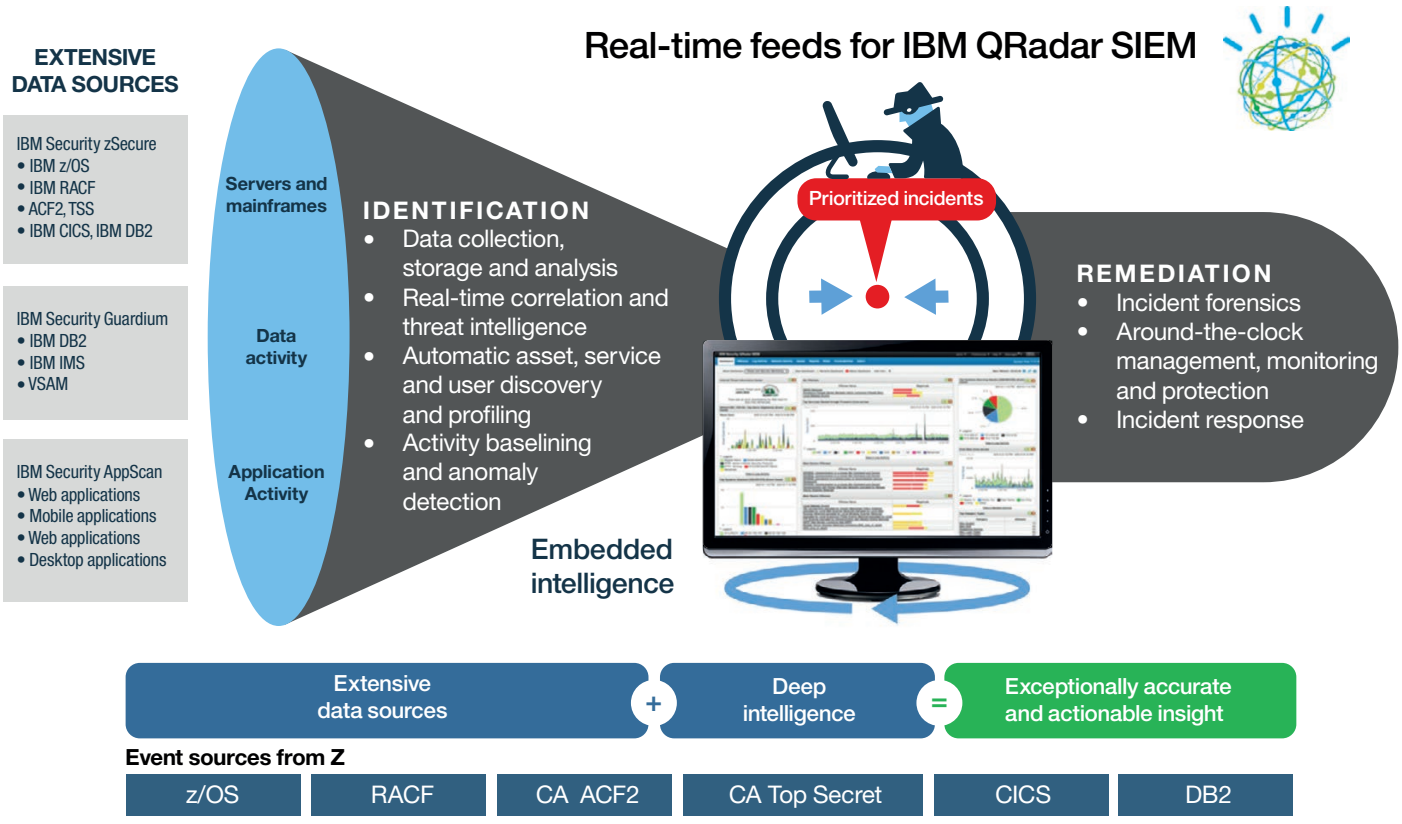
subsystems, products, and applications; delivery of customizable reporting and analysis of audit records; and enhanced threat monitoring with automated remediation.

zSecure solutions help provide comprehensive, end-to-end security across Z platforms that can also interoperate with distributed security solutions to eliminate security silos by providing integration with:

- Mainframe security products: RACF, IBM Multi-Factor Authentication for z/OS and others.
- IBM Z subsystems: DB2, IBM IMS™, CICS, IBM MQ for z/OS, Linux on z Systems and others.
- IBM Security solutions: IBM Security Guardium®, QRadar SIEM, QRadar Advisor with Watson, IBM Security Identity Governance and Intelligence, IBM Security Key Lifecycle Manager and others.
- Other vendors' security governance, risk, security and compliance products.

Integration with analytic solutions such as IBM QRadar SIEM solution can improve security intelligence across an enterprise. It can help automate the analysis of millions of events and simplifies the prioritization of potential threats across mainframe and distributed systems. This helps to effectively identify threats and respond in a timely manner. It can help prevent breaches, reduce outages, protect resources and demonstrate compliance.

IBM Z products enable integration with IBM QRadar



Why IBM?

Security is a journey, not a destination. An IBM zEnterprise® security strategy should align with overall IT security strategy as an extension of the existing IT infrastructure. IBM offers a broad portfolio of security products and services to help build more secure cloud, mobile and big data environments with more intelligent security policies. IBM security solutions are supported by the world-renowned IBM X-Force® team—one of the most respected commercial security research teams in the industry. X-Force helps organizations stay ahead of emerging threats by analyzing and maintaining one of the world's most comprehensive vulnerability databases. X-Force researches and evaluates the latest security threats and trends, and develops countermeasure technologies for IBM security solutions.

zSecure Adapters for SIEM can help extend advanced threat protection and security intelligence for mainframe environments in a distributed environment.

For more information

To learn more about IBM Security zSecure Adapters for SIEM, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/zsecure-adapters-siem

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2017

WGD03050-USEN-01