IBM Security zSecure Alert

Monitor the mainframe for external and internal security threats

Highlights

- Monitor sensitive data for misuse to enhance access controls
- Leverage configurable alerts to analyze events, improve security and reduce costs
- Detect configuration mistakes or changes before others exploit them; audit for compliance reporting

As the core repository for crucial data, the mainframe is increasingly at the center of the interconnected enterprise. Employees, business partners and customers depend on the mainframe for vital information and services, which makes it essential to protect this important resource against external threats, internal abuse and undesired configuration changes. Proactive monitoring and timely alerts enable an organization to establish a consistent security policy, enforce security best practices and avoid potential compliance violations.

Ideally, mainframe monitoring should be part of your overall enterprise threat monitoring solution. As a near-real-time mainframe monitoring solution that allows you to efficiently monitor for internal or external threats and improper configurations, IBM® Security zSecure™ Alert makes this easier to accomplish. Through more responsive incident management and streamlined audit efforts, zSecure Alert can reduce security housekeeping on the mainframe, enhance system availability, supplement access controls and integrate information with enterprise-wide security information event management solutions such as IBM QRadar® SIEM and HPE Security ArcSight.

Monitor critical data to help maintain data integrity

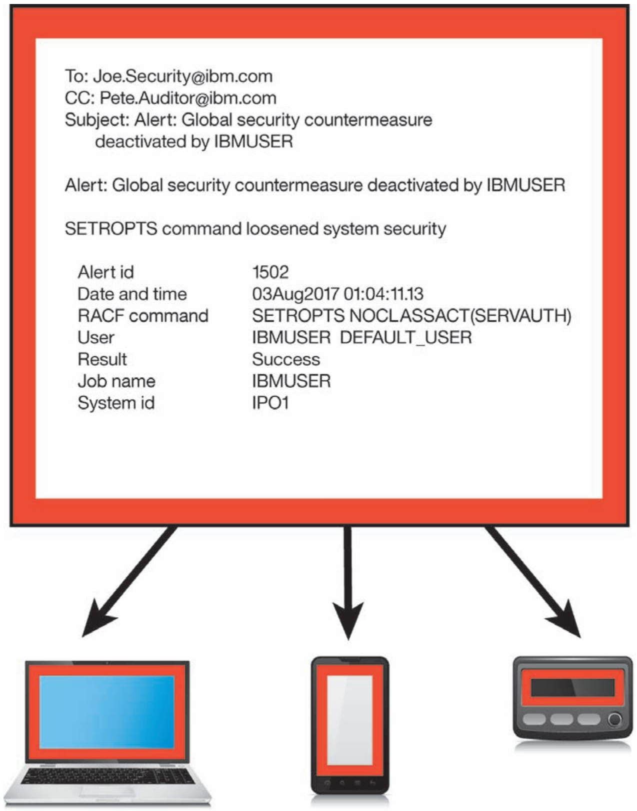
When certain crucial data is touched—even by authorized users—you should know about it. The ability to successfully monitor data access is even more critical when your compliance posture is at stake. zSecure Alert resides on the mainframe, monitoring IBM z/OS®, IBM Resource Access Control Facility (IBM RACF®), IBM Multi-Factor

Authentication for z/OS (IBM MFA) policy, the pervasive encryption feature of IBM Z®, IBM Db2®, CA ACF2, IBM Customer Information Control System (CICS®), IBM Information Management System (IMS™), IBM Communications Server, IBM Workload Scheduler, IBM Health Checker, Linux on IBM z Systems® and UNIX subsystems. By combining a threat knowledge base with parameters from your active configuration, zSecure Alert can help identify resources that need protection and isolate relevant attack patterns.

Unlike other products that only detect breaches from system management facility (SMF) information, zSecure Alert can also detect malicious activity—even if it is not recorded in the event log. By comparing real-time activity with recent access patterns, zSecure Alert can help discover additional threats.

With a broad range of monitoring capabilities, zSecure Alert can also help you detect multiple types of attacks and configuration threats, including:

- Improper or privileged logons and failed logon attempts
  - Logon with emergency user ID
  - UNIX-privileged user logon
  - Logon by unknown users
  - Excessive failed logon attempts
  - Multi-factor policy violations
- Changes that violate security policy
- Addition or removal of system authority
  - Revocation of production user IDs
  - Granting of excessive universal access
  - Disabling of system security options (SETROPTS, GSO)
  - Disabling of audit trail
- Suspicious activity on the UNIX subsystem
  - File access violations
  - Authorized program facility (APF) or controlled program assignment
  - Global write or read specification
- Sensitive data resource information associated with data access or privileged user/group activity or pervasive encryption
- Payment Card Industry (PCI) Primary Account Number (PAN) information associated with sensitive data access or privileged user/group activity
- Communications Server TCP/IP changes
- IBM Workload Scheduler job alerts for jobs not started, jobs that are late or jobs that failed
- IBM Security zSecure events such as Access Monitor not active or IBM Security zSecure Server connection lost



To: Joe.Security@ibm.com
CC: Pete.Auditor@ibm.com
Subject: Alert: Global security countermeasure deactivated by IBMUSER

Alert: Global security countermeasure deactivated by IBMUSER

SETROPTS command loosened system security

Alert id	1502
Date and time	03Aug2017 01:04:11.13
RACF command	SETROPTS NOCLASSACT(SERVAUTH)
User	IBMUSER DEFAULT_USER
Result	Success
Job name	IBMUSER
System id	IPO1

IBM Security zSecure Alert offers timely alerts to help you provide more efficient incident response. Configurable alerts can be sent via email, cell phone and pager, as well as to central security and network management consoles and SIEM solutions.

In addition, zSecure Alert can help determine when your core system resources are at risk through the occurrence of one or more of several events, such as:

- Updates on a system data set
- Dynamic addition of an APF data set
- SMF buffers becoming full, risking data loss
- SMF record flooding, causing denial of service
- Tasks started with unspecified authority
- Access to sensitive data or PCI account numbers

Get fast, flexible alerts to help prevent costly damage

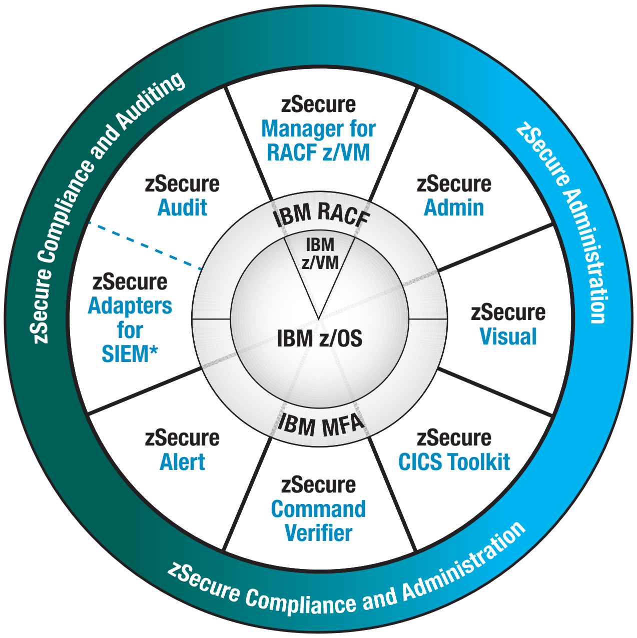
Timely alerts are a critical part of monitoring because they help you respond quickly to prevent further damage. For example, you want to fix detected configuration mistakes before others can exploit them. zSecure Alert delivers robust alerting capabilities across your mainframe estate to quickly notify relevant personnel of changes, improper access events and security vulnerabilities. The alerts are written in the easy-to-use CARLa Auditing and Reporting Language (CARLa) and can be customized for email, cell phone and pager delivery. The selection and layout can be dynamically reconfigured from an IBM Interactive System Productivity Facility (ISPF) application. This allows you to easily configure IBM-supplied alerts and gives you the flexibility to build your own.

zSecure Alert integrates with other tools, enabling you to send relevant alerts to your central security or network management console. For example, you can send Simple Network Management Protocol (SNMP) alerts to IBM Tivoli® NetView.

zSecure Alert can send UNIX syslog messages to the QRadar SIEM dashboard (in Log Event Extended Format), to HPE Security ArcSight (in Common Event Format), and potentially to other security information and event management (SIEM) solutions. Such an integration enhances security intelligence and provides visibility across the entire IT environment including the mainframe, other servers, networking devices, endpoints, databases, applications and more.

Monitoring critical system settings and sending alerts if changes are detected can also demonstrate compliance with regulations including Sarbanes-Oxley (SOX) and Japanese Sarbanes-Oxley (J-SOX), the Health Insurance Portability and Accountability Act (HIPAA), the US Federal Information Security Management Act (FISMA), the Payment Card Industry Data Security Standard (PCI DSS), the European Union General Data Protection Regulation (GDPR) and others.

IBM Security zSecure suite



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

zSecure Alert helps streamline incident management and audit efforts to minimize the risk of breaches. It is part of a family of products designed to provide an optimum interface for managing mainframe security.

Take effective countermeasures

zSecure Alert goes beyond conventional intrusion detection solutions by providing guidance on countermeasures to take when a threat is detected. For example, you can predefine and customize a countermeasure using IBM Security zSecure Admin, such as instantly revoking a user or shutting down an application when a certain security event occurs. In addition, you can send Write To Operator (WTO) messages to trigger automated operations or issue RACF commands autonomously. These countermeasures enable administrators to quickly diagnose and respond to failures or exposures with end-to-end, closed-loop monitoring, intervention and remediation.

Why IBM?

zSecure Alert is the result of decades of experience—gained through tests on mainframe systems—collected into a threat knowledge base that can quickly alert you to suspicious activities. zSecure Alert integrates seamlessly with the complete IBM Security zSecure suite of enterprise-wide security administration and auditing solutions, providing a comprehensive, end-to-end workbench for RACF security management.

For more information

To learn more about IBM Security zSecure Alert, please contact your IBM representative or IBM Business Partner, or visit the following website:
ibm.com/us-en/marketplace/zsecure-alert

For more information on IBM security, please visit:
ibm.com/security

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
September 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Recycle