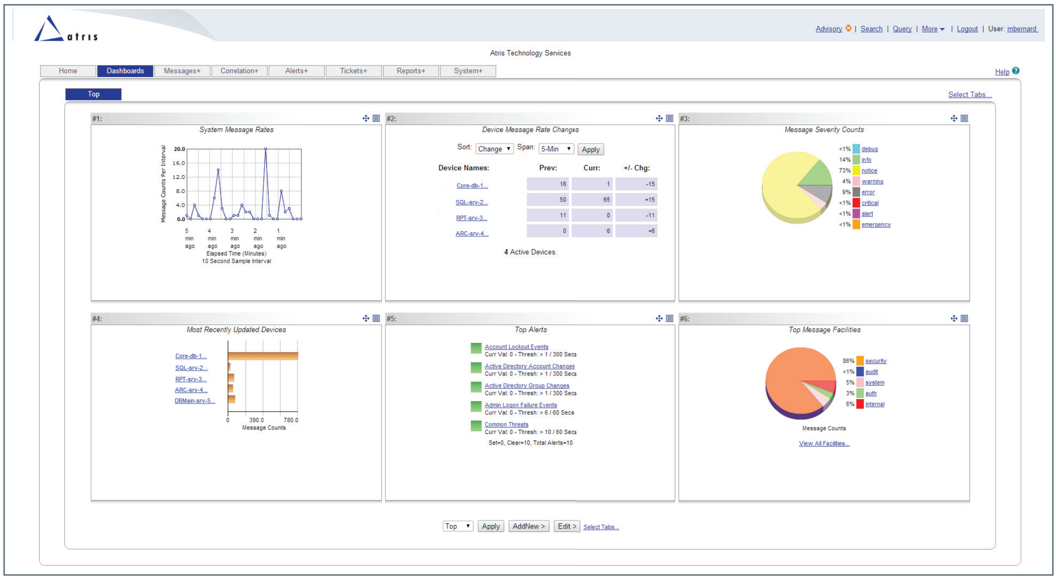
Atris Technology Services

Security Information and Event Management (SIEM)

Atris Security Information & Event Management (SIEM)

An integrated approach to tracking user activity across multiple systems, providing data security, compliance and an audit trail for bank examiners, all from a service deployed from the cloud.

ATRIS TECHNOLOGY SIEM SERVICE is an automation solution designed to quickly provide information technology security and immediately meet key compliance requirements including GLBA and Sarbanes-Oxley. Unlike basic log archival systems, Atris SIEM Service automatically learns your bank security trends to perform real-time analysis and deliver immediate response to potential threats across your network devices. Security officers have comprehensive access to analysis/monitoring tools and rely on a well-defined process to satisfy rigorous bank examinations.



Sort: Change Span: 5-Min Apply

Device Names:	Prev:	Curr:	+/- Chg:
Core-db-1...	16	1	-15
SQL-srv-2...	50	65	+15
RPT-srv-3...	11	0	-11
ARC-srv-4...	0	6	+6

4 Active Devices.

Account Lockout Events
Curr Val: 0 - Thresh: > 1 / 300 Secs

Active Directory Account Changes
Curr Val: 0 - Thresh: > 1 / 300 Secs

Active Directory Group Changes
Curr Val: 0 - Thresh: > 1 / 300 Secs

Admin Logon Failure Events
Curr Val: 0 - Thresh: > 6 / 60 Secs

Common Threats
Curr Val: 0 - Thresh: > 10 / 60 Secs

Set=0, Clear=10, Total Alerts=10

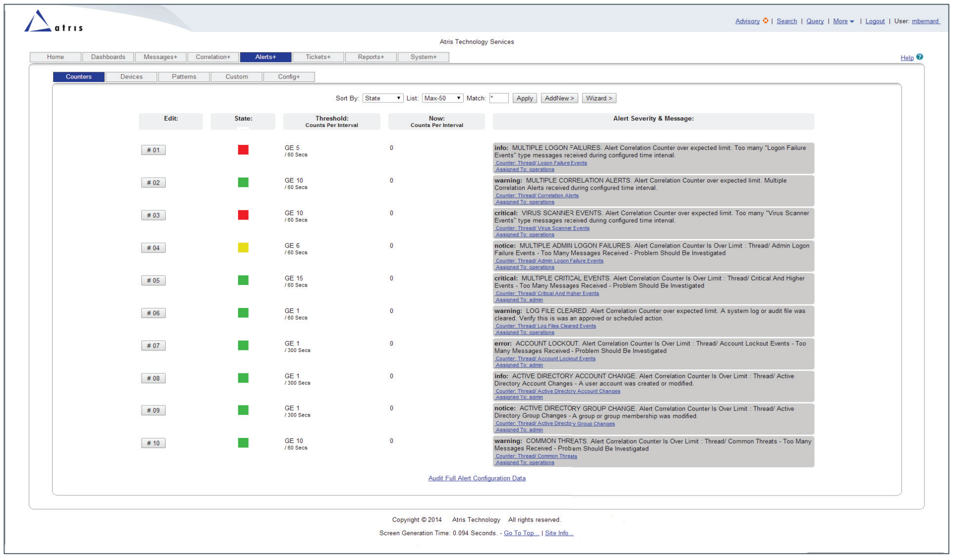
Why Atris SIEM Service?

- Follows FFIEC information technology recommended best practices.
- No hardware deployments - start in days, not months.
- Integrated monitoring of user activity to identify careless or malicious insider behavior.
- Realize big-bank functionality but with the affordability needs of community banks and credit unions.
- A monthly cloud subscription means you can add/remove functionality as needed with no configuration required onsite.
- Leverage our nearly two decades of proven technology automation experience.

GLBA and SOX Compliance

Atris SIEM Service provides real-time monitoring, alerting and reporting of insider threats to financial institution data. This facilitates the GLBA requirement for IT systems and applications that contain confidential customer information. IT administrators and security officers have access to the entire suite of SIEM monitoring tools but confidential customer information remains secure.

For Sarbanes-Oxley compliance, Atris SIEM provides effective oversight of your financial reporting controls by tracking user log activity linked to these controls. Senior management and examiners have access to both summary reporting and comprehensive audit trails. Custom distribution lists can be scheduled to deliver ongoing audit data to key personnel as desired.



Atris Technology Services

Sort By: State List: Max-50 Match: *

Edit:	State:	Threshold: Counts Per Interval	Now: Counts Per Interval	Alert Severity & Message:
# 01	🟥	GE 5 / 60 Secs	0	**info:** MULTIPLE LOGON FAILURES. Alert Correlation Counter over expected limit. Too many "Logon Failure Events" type messages received during configured time interval. Counter: Thread/ Logon Failure Events Assigned To: operations
# 02	🟩	GE 10 / 60 Secs	0	**warning:** MULTIPLE CORRELATION ALERTS. Alert Correlation Counter over expected limit. Multiple Correlation Alerts received during configured time interval. Counter: Thread/ Correlation Alerts Assigned To: operations
# 03	🟥	GE 10 / 60 Secs	0	**critical:** VIRUS SCANNER EVENTS. Alert Correlation Counter over expected limit. Too many "Virus Scanner Events" type messages received during configured time interval. Counter: Thread/ Virus Scanner Events Assigned To: operations
# 04	🟨	GE 6 / 60 Secs	0	**notice:** MULTIPLE ADMIN LOGON FAILURES. Alert Correlation Counter Is Over Limit : Thread/ Admin Logon Failure Events - Too Many Messages Received - Problem Should Be Investigated Counter: Thread/ Admin Logon Failure Events Assigned To: operations
# 05	🟩	GE 15 / 60 Secs	0	**critical:** MULTIPLE CRITICAL EVENTS. Alert Correlation Counter Is Over Limit : Thread/ Critical And Higher Events - Too Many Messages Received - Problem Should Be Investigated Counter: Thread/ Critical And Higher Events Assigned To: admin
# 06	🟩	GE 1 / 60 Secs	0	**warning:** LOG FILE CLEARED. Alert Correlation Counter over expected limit. A system log or audit file was cleared. Verify this is was an approved or scheduled action. Counter: Thread/ Log Files Cleared Events Assigned To: operations
# 07	🟩	GE 1 / 300 Secs	0	**error:** ACCOUNT LOCKOUT. Alert Correlation Counter Is Over Limit : Thread/ Account Lockout Events - Too Many Messages Received - Problem Should Be Investigated Counter: Thread/ Account Lockout Events Assigned To: admin
# 08	🟩	GE 1 / 300 Secs	0	**info:** ACTIVE DIRECTORY ACCOUNT CHANGE. Alert Correlation Counter Is Over Limit : Thread/ Active Directory Account Changes - A user account was created or modified. Counter: Thread/ Active Directory Account Changes Assigned To: admin
# 09	🟩	GE 1 / 300 Secs	0	**notice:** ACTIVE DIRECTORY GROUP CHANGE. Alert Correlation Counter Is Over Limit : Thread/ Active Directory Group Changes - A group or group membership was modified. Counter: Thread/ Active Directory Group Changes Assigned To: admin
# 10	🟩	GE 10 / 60 Secs	0	**warning:** COMMON THREATS. Alert Correlation Counter Is Over Limit : Thread/ Common Threats - Too Many Messages Received - Problem Should Be Investigated Counter: Thread/ Common Threats Assigned To: operations

Audit Full Alert Configuration Data

Copyright © 2014 Atris Technology All rights reserved.

Screen Generation Time: 0.094 Seconds. - Go To Top... | Site Info...

How does Atris SIEM Service fortify your GLBA and SOX compliance requirements?

- Track logons/logoffs: Monitor activity including unauthorized access as well as unusual activity from authorized personnel.
- Track failed logons: When excessive, failed logon attempts serve as separate triggers for real-time alerts and reporting. An automated notification can be sent to your help-desk as an alert to take action.
- Identify changes to management access rights, such as increased privileges, modified user accounts or adding/ removing members from a user group.
- Monitor access to audit logs and protect against audit log manipulation. Automated, real-time monitoring of information system trace log data will generate alerts for proactive management.
- Audit system event changes: Monitor and report instances where local system processes have changed (i.e. system startups/shutdowns, edits attempted on scheduled processes, etc.).

No Impact to Customer Data

Atris SIEM Service is cloud-based with all data protected by 256-bit encryption and secure authentication. We only track user log activity related to insider threat (or user negligence) and no customer data leaves your datacenter: The risk to exposing customer data is nullified!

Try a fully-functional free version of Atris SIEM for 30 days

We are convinced that our approach to SIEM will blaze a trail for the software industry to offer enterprise-capable critical banking system applications at an attractive price point to regional/ community banks and credit unions. To fully appreciate the benefits of Atris SIEM Service, we offer a complimentary 30-day trial utilizing your data for real-time monitoring.

Take advantage of our 30-day trial offer today by visiting www.atris.com.

ATRIS TECHNOLOGY
3405 NW 97th BLVD
Building A, Suite 200, Gainesville, FL 32606
Direct: (352) 331-3100
Toll free: (800) 393-1079