PRODUCT OVERVIEW

LogRhythm and LOGbinder for Exchange: Security Intelligence for Microsoft Exchange Server

LogRhythm
The Security Intelligence Company

LogRhythm and LOGbinder have developed an integrated security intelligence solution for Microsoft Exchange Server. As the dominant email communication platform, Exchange increasingly hosts an organization's most scrutinized business communication, making it critical for compliance and security requirements to monitor and audit Exchange activity.

Exchange audit activity includes:

- Mailbox activities, such as:
  - View, Update, Delete, Create, Send As, SendOnBehalf, Copy and Move actions by owners, non-owners and administrators
- Administrator activities, such as:
  - Exporting mailboxes
  - Copying entire mailbox databases
  - Changing Exchange security configurations
  - Accessing control changes to groups, roles and permissions
  - Modifying Exchange policies involving data retention, mobile devices, information rights and federation

Security Intelligence for Exchange Server

- ☑ Monitor non-owner access to mailboxes
- ☑ Monitor privileged user activity
- ☑ Respond to access control and configuration changes for groups, roles and permissions
- ☑ Track modifications to Exchange policies
- ☑ Automate mailbox audit policy configuration

Monitoring Exchange security events is critical for identifying threats and enforcing compliance controls such as separation of duties, privileged user activity monitoring, security configuration change control, confidentiality requirements and data protection accountability. LOGbinder analyzes Exchange's audit logs, producing an easy-to-understand, plain-English translation of the audit events. LogRhythm automatically normalizes Exchange audit events received from LOGbinder and categorizes them according to LogRhythm's Machine Data Intelligence Fabric, making it easy for infosec staff to identify important changes in Exchange security posture, analyze suspicious events, and investigate security incidents involving access to confidential information in Exchange. With Exchange security activity now in LogRhythm, Exchange events can be correlated with security intelligence collected from the rest of the enterprise to identify patterns of suspicious activity that cross application boundaries.

LogRhythm

LogRhythm uniquely combines next-gen SIEM, Log Management, File Integrity Monitoring and Machine Analytics, with Endpoint Monitoring and Network Forensics, in a unified Security Intelligence Platform. The LogRhythm solution gives customers profound visibility into threats and risks in areas that were previously exposed. Designed to help prevent breaches before they happen, LogRhythm's Security Intelligence Platform accurately detects an extensive range of early indicators of compromise, enabling rapid response and mitigation. The deep visibility and understanding delivered by LogRhythm empowers enterprises to secure their networks and comply with regulatory requirements. LogRhythm delivers:

- Next-generation SIEM and Log Management
- Independent Endpoint Forensics and File Integrity Monitoring
- Network Forensics with Application ID and Full Packet Capture
- State-of-the art Machine Analytics
- Advanced Correlation and Pattern Recognition
- Multi-dimensional User / Endpoint / Network Threat Detection
- Contextualized, Unstructured, and Precision Search
- Large data set analysis via visual analytics, pivot, and drill-down
- Incident response automation with Smart**Response**™
- End-to-end incident response orchestration

LOGbinder

The Exchange audit log is internal to Microsoft Exchange and inaccessible via normal means of log collection. LOGbinder for Exchange bridges the gap between the Exchange audit log and LogRhythm by extracting and translating the cryptic data in raw Exchange audit entries. LOGbinder then turns the raw Exchange audit event into an easy-to-understand event and sends the clarified event to LogRhythm via Syslog. LOGbinder is a small, efficient Windows service that monitors the internal Exchange audit log without making any changes to an organization's Exchange installation. LOGbinder installs on a non-production member of the domain that can "see" the Exchange server in just a few minutes. LOGbinder can automatically configure mailbox audit policy to ensure that auditing is consistently configured on appropriate mailboxes by organizational unit or group membership.

The tight integration between LogRhythm and LOGbinder combine LOGbinder's ability to extract and translate the cryptic and proprietary logs within Exchange into easy-to-understand event information with the threat management capabilities of LogRhythm's Security Intelligence Platform. The combined offering empowers customers to detect internal and external threats, identify behavioral anomalies, enhance security, and enforce compliance.

Protecting Confidential Data

Challenge Microsoft's Exchange is a broadly used, sophisticated communications platform used to create and manage many large, unstructured files containing complex and often confidential data. While Exchange is a leading and often mission-critical tool for these purposes, the sensitivity of the communications it enables and the data it houses poses significant security risks. Exchange's internal audit logs make it difficult to enforce user access controls and prevent data exfiltration.

Solution LOGbinder can translate Exchange audit events into Windows event logs and forward them to LogRhythm for real-time behavioral analytics, helping identify suspicious activity and unauthorized access to data and user accounts.

Additional Benefit Automatic mailbox audit configuration ensures LogRhythm can generate a high-priority alarm and initiate an out-of-the-box Smart**Response**™ plugin to automatically disable an Active Directory Account if a user is improperly accessing or modifying data. This action can be completely automated or it can require as many as three levels of authorization.

Tracking Privileged User Activity

Challenge Privileged users often have direct access to confidential data within Exchange, as well as administrative capabilities to create accounts and modify permissions, privileges and access within the platform. Exchange audit logs fail to translate record IDs, making it impossible to identify which object or user is associated with an event.

Solution LOGbinder converts proprietary Exchange audit events into Windows event logs and sends them via Syslog to LogRhythm. LogRhythm's real-time analytics can identify and alert on insider threats, such as a suspicious privileged user creating a new Exchange account with escalated privileges.

Additional Benefit LogRhythm's right-click correlation allows instant access to user account details and enables further investigation of user behavior within Exchange, associated with other system activity across the IT environment.

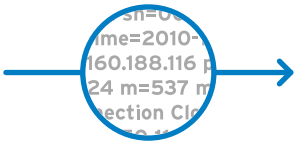
LOGbinder™

Exchange Security Intelligence

- Access by Unauthorized Users
- Access to Confidential Information
- Security Changes
- Privileged User Activity

Other Log, Security, and Machine Data

LogRhythm Forensic Sensor Data



Machine Data Intelligence

Automatically collect and process data from across the distributed environment

SmartResponse™

Automatically take action and respond to events and alarms

LogRhythm®

Security Intelligence Platform

- Next Generation Security Operations Center
- Security Analytics
- SIEM & Log Management
- Network Monitoring and Forensics
- Endpoint Monitoring and Forensics
- Behavioral Analytics (e.g. UBA, NBAD, EDR)

LogRhythm® Labs