PRODUCT OVERVIEW

LogRhythm and LOGbinder SP: Security Intelligence for SharePoint

LogRhythm
The Security Intelligence Company

LogRhythm and LOGbinder have developed an integrated security intelligence solution for SharePoint. As the dominant platform for documents and other unstructured data, organizations need to monitor activity across all users and administrators within SharePoint for compliance and security requirements. LOGbinder for SharePoint (LOGbinder SP) sends SharePoint audit events to LogRhythm for continuous compliance and enterprise security intelligence.

SharePoint audit activity includes:
- Viewing of confidential documents and lists
- Modification and deletion of objects
- Permission changes and administrative authority changes
- Role and group membership changes
- Audit log integrity events
- Exporting of SharePoint data

Security Intelligence for SharePoint

- ☑ Track access to confidential information
- ☑ Monitor changes to sensitive documents
- ☑ Respond to security changes
- ☑ Track privileged user activity

SharePoint security events are critical to compliance controls such as separation of duties reporting, privileged user activity monitoring, and security configuration change control. LOGbinder SP analyzes SharePoint's audit logs and resolves the user and object IDs as well as other cryptic codes, producing an easy-to-understand, plain-English translation of the SharePoint audit events. LogRhythm automatically normalizes SharePoint audit events received from LOGbinder and categorizes them according to LogRhythm's advanced security event taxonomy making it easy for infosec staff to identify important changes in SharePoint security posture, analyze suspicious events, investigate security incidents involving SharePoint data and document access to confidential information in SharePoint. LogRhythm also correlates SharePoint events with security intelligence collected from the rest of the enterprise to isolate patterns of suspicious activity that cross application boundaries.

LogRhythm

LogRhythm, a leader in security intelligence and analytics, empowers organizations around the globe to rapidly detect, respond to and neutralize damaging cyber threats. The company's award-winning Security Intelligence Platform unifies next-generation SIEM, log management, network and endpoint forensics, and advanced security analytics. In addition to protecting customers from the risks associated with cyber threats, LogRhythm provides innovative compliance automation and assurance, and enhanced IT intelligence. LogRhythm delivers:

- Next Generation SIEM and Log Management
- Independent Host 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 / Host / Network Behavior Anomaly Detection
- Rapid, Intelligent Search
- Large data set analysis via visual analytics, pivot, and drill down
- Workflow enabled automatic response via LogRhythm's Smart**Response**™
- Integrated Case Management

LOGbinder

The SharePoint audit log is internal to SharePoint and inaccessible via normal means of log collection. LOGbinder SP™ bridges the gap between the SharePoint audit log and LogRhythm by translating the cryptic data in raw SharePoint audit entries. For each event, LOGbinder SP™ resolves the user and object IDs and other cryptic codes. LOGbinder SP then turns the raw SharePoint audit event into a fully translated and easy to understand event and sends the (clarified) event to LogRhythm via Syslog. LOGbinder SP™ is a small, efficient Windows service that monitors the internal SharePoint audit log without making any changes to your SharePoint installation. LOGbinder SP installs on a non-production member of the farm or on any one of the existing servers in your SharePoint farm in just a few minutes and allows you to quickly configure auditing on any or all of the server's site collections.

LogRhythm and LOGbinder SP™ are tightly integrated, combining LOGbinder's ability to translate the cryptic and proprietary logs within SharePoint into easy-to-understand event information with the threat management capabilities of LogRhythm. 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 SharePoint is a broadly used platform for sharing large, unstructured files containing confidential data, and while it is a great tool for collaboration, it also poses significant security risks to organizations. SharePoint's internal audit logs are highly cryptic making it difficult to enforce user access controls and prevent data exfiltration.

Solution LOGbinder SP can translate SharePoint audit events into Windows event logs and forward them to LogRhythm for advanced correlation and real-time behavioral analytics across the universe of log data to identify suspicious activity and unauthorized access.

Additional Benefit 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.

Tacking Privileged User Activity

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

Solution LOGbinder SP converts the proprietary SharePoint audit events into Windows event logs and sends these logs via Syslog to LogRhythm. LogRhythm's advanced correlation can identify and alert on insider threats such as a suspicious privileged user creating a new SharePoint 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 SharePoint associated with other system activity across the IT environment.