Knowing who is responsible for what is happening in your IT environment is a critical component of maintaining a secure network. And while discovering the identity responsible for specific activities is a necessary step in the forensic investigation process, in many situations, that information is not contained within the available machine data. LogRhythm's Identity Analytics employs a number of capabilities for capturing identity information to ensure that important event context is available for both real-time machine analytics and rapid access during the course of an investigation.

**Exposing the “Who” in Anonymous Log and Machine Data**

Analysts need to be able to quickly identify the user associated with suspicious activity, but the majority of machine data does not include any reference to identity. For example, firewall logs, Netflow, IPS events, endpoint security events, and other data generated by perimeter devices typically only include Layer 3 or host-level information. When investigating activity where identity attribution is missing, analysts are constrained by the lack of this critical context. Attempting to manually uncover identity information is a time-consuming and complex process. LogRhythm's Identity Inference Engine™ solves this problem by combining already collected machine data with advanced analytics to automatically identify the “who” behind otherwise anonymous data.

The Identity Inference Engine™ leverages authentication, access, DHCP, and other data sources to correlate associative data tied to an identity. Data is continuously analyzed via identity inference algorithms that deliver a real-time and historic mapping of identity to hosts. This allows LogRhythm to expose the identity data behind both current and historic activity where it was previously absent.

LogRhythm's Identity Inference Engine™ does not require any third-party integrations. By leveraging the data already collected by their LogRhythm deployment, customers are able to immediately enjoy the benefits without any complex configuration or setup. The Identity Inference Engine™ delivers the context needed to streamline the forensic analysis process, expedite incident recognition and response, and significantly reduce risk.

---

"LogRhythm's Identity Inference Engine automatically retrieves user information associated with network assets, saving me the time and effort involved in manually looking up users in our asset management database."

*Vaughn Adams*

Senior Manager of IT

InterDigital

---

Figure 1 - Identity Inference results in LogRhythm
Understanding Identity Context

Audit logs often contain information related to two separate identities. One is the user performing an action and the other is the identity on which the action is being performed. As LogRhythm processes data, it distinguishes between the two, creating a clear distinction between the origin and impacted identities. For example, when user “seth.goldhammer” logs in and changes the password for the user, “jeffrey.smith,” there are two identities associated with the activity. LogRhythm is able to recognize that “seth.goldhammer” was the logged-in Origin user actively changing the impacted account, “jeffrey.smith.” This difference is critical when an analyst performs forensic analysis to distinguish between activities performed by an account versus auditing the changes made to an account. Without this distinction, a search for “jeffrey.smith” will result in an overly broad query containing data from when “jeffrey.smith” was the logged-in user and when actions were performed on the account “jeffrey.smith.” Understanding the context of each identity is critical for effective analytics.

Relevant identity context increases the accuracy of real-time analytical rules. For example, in order to recognize when someone changes another user’s password, a real-time analytics engine needs to detect when a password is modified, and then recognize that the user account changing the password is not the same as the user account whose password is being changed. LogRhythm automatically derives extensive metadata from every event, regardless of the source, clearly labeling common events such as password modifications which makes it easy to correlate the event against all relevant identity context. As a result, LogRhythm’s real-time analytical rules can look for any password modification events where the origin login user does not equal the account modified, regardless of whether or not it is tied to an Active Directory domain, local computer, network device, etc.

Accurate identity context not only delivers greater efficiency for forensic search and real time analytics performed by the AI Engine, it also ensures accuracy in compliance reporting and enforcement. Many compliance regulations specify requirements for auditing changes to user accounts. PCI-DSS, NIST 800-53, GPG-13, ISO 27001 and others include specific controls for recognizing account management activity, such as when accounts are modified, when privileges are escalated or revoked, or when accounts are created or disabled. LogRhythm’s ability to derive identity context within log data allows auditors to quickly generate compliance reports containing required information such as the account modified and the identity responsible for making the modification.

Group-Based Identity Analytics

LogRhythm integrates with user directories such as Active Directory to learn the group membership of individual users, including users whose group membership stems from nested groups. Users can take advantage of this capability by setting group filters within the console, including searches, reports, and rules used for real-time analysis. For example, LogRhythm can monitor access to sensitive files by unauthorized users, such as HR documents, by detecting users that are not part of an authorized HR group.
LogRhythm's integration with user directories provides additional contextual information during the course of a forensic investigation. In large organizations, it is very difficult to understand who each user is and their role within the company. LogRhythm provides a quick method of querying the user directory to learn additional attributes of the user, such as department, title, and email address. The additional information enables analysts to perform rapid forensics for use cases where identity context is a necessary component. This include use cases such as verifying if a user accessing HR documents is an authorized member of the HR group, or investigating activity by a user whose account has been active from a new location to determine if the account is compromised.

![User Information Table](image)

**File Integrity Monitoring with Identity Information**

LogRhythm incorporates integrated File Integrity Monitoring (FIM) within its Security Intelligence Platform. One important capability delivered by FIM is to capture the identity of the user accessing, modifying and/or deleting a file or directory. This activity is captured in real time and can be easily correlated against all other activity associated with that identity to deliver greater understanding of an event. For example, LogRhythm can detect when a user accesses a sensitive file while accessing an unauthorized cloud storage platform. Once the suspicious activity is detected, an out-of-the-box SmartResponse™ plug-in can be triggered to automatically disable the user account to prevent data exfiltration.

**The Value of LogRhythm’s Identity Analytics**

So what is the true value of LogRhythm's Identity Analytics? By extracting and adding identity details to provide relevant context even when analyzing anonymous log data, LogRhythm expedites forensic investigations and uncovers critical details tied to important events. LogRhythm's Identity Analytics provides the additional context needed to detect critical events, including compromised credentials, misuse of privileged accounts, insider theft, data exfiltration, specific compliance violations and other suspicious user activity.