Identropy Product Integration Brief: Exabeam+SailPoint

Identropy's integration of SailPoint's IdentityIQ solution and Exabeam's User and Entity Behavior Analytics merges Identity Governance and Administration with next-generation Security Information Management in order to significantly enhance an organization's security posture. It is no longer adequate to know "who has access to what", today security professionals must also know what users are doing with their access and to be able to take immediate corrective steps to prevent data breaches. Below are three distinct integrations that are the first step towards a significantly enhanced identity-based security posture.

Integration 1: Enrich Identity Context

Allows the identity context in Exabeam to be enriched by SailPoint specific data. Such examples include ability to export 1) user-types such as employees, contractors, vendors and partners, and 2) Account tags such as service, privileged, and/or inactive.

Integration 2: Additional Watch Lists

Passes critical data elements from SailPoint for use in Exabeam Watch Lists. This also allows certain types of accounts to be more closely monitored.

Disabled Accounts - Every user disabled in SailPoint (manually or automated) will be put into a watch list on Exabeam. This is to ensure that disabled users either separated by plan or unplanned are monitored and there is no activity.

Service Accounts - Exabeam has an out of box watch list for accounts that Exabeam knows as service accounts (these are mostly coming from Active Directory). SailPoint aggregates accounts from more systems than just AD and tags a Service Account for each of these systems. This task will put the user (identity) associated with/responsible for each service account into a separate watch list in Exabeam. This is to ensure that a user who has ownership of service accounts is identified if any of the service accounts owned by that identity are detected as being compromised in Exabeam.

Privileged Accounts - SailPoint aggregates accounts from more systems than just AD and tags a Privileged Account on each system. This task will put the user (identity) associated with/responsible for each of the privileged accounts into separate watch list in Exabeam. This is to ensure that Exabeam is made aware of a user who has a privileged account on a target system (that may not be AD) and is not known by Exabeam. An example would be a user considered a regular user on AD, but a privileged user on RACF.

Integration 3: Remediation According to Risk

Allows organizations to take corrective actions more quickly when a user has been identified in Exabeam as meeting a set risk score threshold. For example, if a user has met a risk score threshold that has been set at 300, the user will be passed to SailPoint as a candidate for remediation. Actions such as disablement of the account or an access review of the user can be chosen as the appropriate corrective action.

Request a Call From Our Team!

7600 Burnet Road, Suite 505 Austin, TX 78757 | Ph. 512-861-1673 | info@identropy.com | www.identropy.com