Middleware data

Middleware describes a software layer of the prototypical three-tier enterprise application that typically implements data transformations, analysis, and business logic. Middleware accesses databases for persistent storage and relies on web apps for the user interface. Middleware is often developed on the J2EE platform. In the Common Information Model, middleware data is typically mapped to the Interprocess messaging data model.

Middleware data can help operations teams diagnose problems with three-tier applications that involve the interaction between web, middleware, and database servers. Security teams can use log data to vet application integrity, identify suspicious behavior, and find specific vulnerabilities. It can also be used for user and customer transaction monitoring and to identify abnormal transactions, unknown user interaction with third party accounts, and the sequence of exact transaction patterns that match known fraudulent profiles.

Application

When your Splunk deployment is ingesting middleware data, you can use it to accomplish security and compliance, IT Ops, and application delivery use cases.

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud).