



LogRhythm's powerful rules engine enables users to specify contextual attributes of logs and events such that alerts can be triggered when concerning activity occurs. In the example above, this organization wants to be alerted anytime anyone, except the CFO (Philip Johnson), executes a transaction in their corporate financial system that exceeds \$200,000. Empowered with this level of insight and real-time alerting, LogRhythm customers gain unprecedented visibility to potential fraud and other insider threats.