

Gurukul Risk Analytics (GRA) Technical Training



DATA SHEET

Gurukul Risk Analytics' technical training prepares end users, managers, SOC analysts and data scientists to leverage the highest value from GRA implementations. Gurukul offers custom designed classes held on-site at your location, standard classes conducted regionally or at our headquarters conveniently located near the Los Angeles International Airport.

Learn to

- Define data sources and import data
- Import users or identities
- Create resources and resource groups
- Create accounts and entitlements
- Import activity data from big data
- Learn about accounts types and linkages
- Run analytics job for anomaly detection job and risk scoring
- Configure GRA for identity analytics
- Use Miner™ to perform contextual search on big data for investigations
- Manage tickets and cases in GRA

GRA Features and Benefits

- 360° view of identity, access, activity, and alerts for on-premises and cloud applications
- Over 300+ machine learning models ready to use out of the box
- User and entity behavior analytics (UEBA) predict and detect unknown threats
- Identity analytics (IdA) reduces risk from excess access and outliers
- Identify anomalous behaviors across users, accounts, applications and devices by leveraging behavior analytics
- Self-audits for employees and partners

GRA Feature Highlights

Prioritized Alerts

GRA offers a unique identity-centric view which provides risk-based prioritized alerts for actionable first step in your investigation and forensics process. The GRA dashboard provides customizable views of your organization's risk through contextual visualizations, highlighting high-risk users, resources and transactions, based on behavior anomalies and dynamic peer group analytics.

Risk and Threat Intelligence

GRA provides actionable intelligence, detecting risky behaviors before incidents occur. GRA's patent pending self-learning behavior-based algorithms consolidate identity profiles with machine data and alerts from defense-in-depth security solutions, creating context-aware timeline visualizations. GRA further extends the value of this cross-correlated data by creating behavior baselines and dynamic peer group analysis to prevent, detect and remediate previously unknown anomalies.

Self-Audit™

GRA's unique Self-Audit™ feature set provides end users and partners with a customizable online view of their identity, access and risk-ranked activity. GRA's Self-Audit™ extends traditional information security programs into the business with a two-way collaboration, showing end users and partners what they have accessed, when they accessed it, from what geo-location, and with what device; highlighting anomalous transactions with reports similar to a credit card statement.

Identity Analytics

GRA's Identity Analytics provides the capability to analyze accounts and entitlements (high privileged, shared & regular) for outlier intelligence and to identify excess access risk. Behavior-based machine learning for identity and access often results in radical reductions for accounts and access entitlements. Identity is a threat plane requiring identity and access data science that predicts and prevents security risks, assists with high privilege access monitoring, excess access, compliance, and intelligent provisioning. Identity analytics cleanse, manage, secure, and govern identities and their associated access to critical data and assets.

Course Syllabus

- Introduction to GRA
 - GRA Use cases
 - GRA Features and Benefits
 - GRA Architecture
- GRA Environment Setup
- Data Required for GRA
 - User imports
 - Resource imports
 - Account imports
 - Entitlement imports
 - Activity imports
- Identity Analytics
- Activity Monitoring and Reporting
- User & Entity Behavior Analytics
- Miner™ for Raw Search
- Monitoring High Risk Users
- Self-Audits
- Case Management
- Advanced GRA Configurations

Duration: 2 or 3 Days

Hands-on Labs and Demos

- Configuring Data Sources
- Configuring User Imports
- Configuring Resources Groups
- Configuring Resources
- Configuring Resource Attributes
- Configuring Account Imports
- Configuring Account Entitlement Imports
- Configuring Real-time Activity Imports
- How to link Rogue or Orphan Accounts
- Walk-through Application Analytics Dashboard
- Walk-through Activity Monitoring (Miner)
- Configuring Anomaly Detection Jobs
- Walk-through Predictive Security Dashboard
- Walk-through High-Risk Users Dashboard
- Walk-through Case Management Functionality
- Creating GRA Users and Roles
- Walk-through GRA Advanced Configuration Settings

Awards

