Gurucul Risk Analytics

Data Sheet

Eine wichtige Ursache moderner IT-Bedrohungsszenarien beinhaltet die Kompromittierung oder den Missbrauch von Identitäten. Benutzer haben viele Konten und Zugangsrechte, häufig zu viele, was eine günstige Ausgangslage für Cyber Kriminalität, Insider- und komplexe Attacken darstellt. Während CIOs einen einfachen Datenzugriff und einfache Funktionsweisen fordern, versuchen CISOs den Zugriff mit deklarativen Methoden und Kontrollen einzuschränken. Das Ergebnis sind zunehmende Datendiebstähle und Sicherheitsaufwände, da präventive Abwehrmethoden immer ineffektiver werden. Das immer größer werdende Datenvolumen verlangt nach Data Sciences (Extraktion von Wissen aus Daten).

Pioneers of Innovation in Identity, UEBA & SaaS Analytics

Warum sollten Sie Gurucul Risk Analytics (GRA) nutzen?

- Analyse der Zugangsrechte und deren Missbrauch durch Identitätszentrische Verhaltensanalyse aus großen Datenmengen
- Modellierung „guten Verhaltens" um unbekanntes, schlechtes Verhalten durch den Einsatz dynamischer Peer-Groups, Cluster- und Ausreißeranalysen sichtbar zu machen
- Nutzung prädiktiver Sicherheitsanalytik um Vorfälle mit einem Risikowert zu versehen und den Fokus auf die Fehlerkorrektur zu lenken
- Optimierte Nutzung von Mitarbeitern und Zeit durch Anwendung von Machine Learning
- Durch risiko-basierte Zugangskontrollen die Angriffsfläche von Benutzerkonten reduzieren und verwalten
- Verhaltensanalyse für hybride Umgebungen mit lokalen Rechenzentren und Cloud Anwendungen
- Aufdecken von Insider Bedrohung, Kompromittierung und Missbrauch von Benutzerkonten, sowie Datenausleitung (Exfiltration = nicht autorisierter Transfer von Daten)

Über Gurucul:

Gurucul Risk Analytics (GRA) unterstützt Unternehmen beim Schutz gegen Insider-Bedrohungen, Account-Kompromittierung und Datenexfiltration. Die User and Entity Behavior Analytics (UEBA), Identity Analytics und Fraud Analytics Technologie des Unternehmens nutzen Machine Learning und prädiktive Anomalie-Erkennungsalgorithmen, um bösartige Aktivitäten zu erkennen und zu stoppen.

KOGIT
Secure Identity Management

Gurucul Risk Analytics

Was sind Guruculs Kernmodule?

Für die Analyse von Zugangsrechten, Bedrohung und Cloud-Nutzung verwendet Gurucul Risk Analytics drei Komponenten. Diese kombinieren auf einzigartige Art und Weise Data Science Methoden für die Verhaltensanalyse und Identity Access Intelligence.

Behavior Based Identity & Security Analytics and Intelligence established since 2009

Access Analytics Platform™ (AAP)

Access Analytics PlatformTM (AAP) ermöglicht risiko-basierte Compliance und Provisioning.

- 360° Echtzeit Sichten im Kontext Identität, Zugangsrechte und Aktivitäten
- Bessere Identity Access Intelligence und Rollen durch Einsatz von Machine Learning auf die Verhaltensanalyse
- Massive Verringerung von Benutzerkonten und Zugängen durch Anwendung des ausgewerteten Nutzungsverhaltens
- Erkennung von privilegierten Zugriffen inklusive Reporting über obsolete, verwaiste und nicht benötigte Zugänge
- Risiko-basierte Rezertifizierungskampagnen und dynamisches Access Provisioning reduzieren Aufwand und Fehler
- Erkennung von Ausreißern in Zugangsberechtigungen anhand von Nutzung und dynamischen Peer-Groups

Highest rated by market leading analyst firms: Gartner, Forrester, 451 Group, Kuppinger Cole

Cloud Analytics Platform™ (CAP)

Cloud Analytics PlatformTM (CAP) bietet Sichtbarkeit für Zugänge zu Cloud-Anwendungen und Anomalien der Nutzung

- Kontext-basierte, volle Sichtbarkeit für Cloud-Anwendungen bezüglich Identitäten, Zugangsrechte und Aktivitäten
- Cloud-2-Cloud Konnektoren für die gängigen SaaS-Dienste
- Erkennung von Anomalien bei privilegierten Zugängen mit detaillierten Informationen zu Ausreißerzugriffen
- Risiko-Scoring betont Kompromittierung, Kompromittierung von Konten, Insider-Bedrohungen und Datenverlust
- Verwaltung/Management der Cloud-Konten durch Identity Access Intelligence und Risiko-basierte Rezertifizierungen
- Wertschöpfung für hybride Umgebung durch Nutzungsanalyse für lokale Rechenzentren und Cloud

KOGIT
Secure Identity Management

Gurucul Risk Analytics

Most customers recognized for outstanding business value and thought leadership

Threat Analytics Platform™ (TAP)

Threat Analytics PlatformTM (TAP) bietet vorhersagende Risiko-Klassifizierung durch Nutzungsanalysen

- Zeitstrahl mit Risiko-Klassifizierung für die Vorhersage, Erkennung und Behinderung von Insider und fortschrittlichen Bedrohungen
- Identitäts-zentrierte Nutzungsanalysen zur Erkennung von Kompromittierung und Missbrauch
- Proaktive Auslösung von Notfallalarmen bei Anomalien und Überschreiten bestimmter Risikoschwellwerte
- Erkennung von Anomalien für Missbrauch, geteilte Nutzung oder Übernahme hoch privilegierter Konten
- Konfigurierbare Dashboards und Richtlinien zur Optimierung des Risikomodells
- Ergonomische GUI zur Verwaltung der Incidents, oder Integration in ein anderes Ticket-System
- Portal für Self-Audits unterstützt das Risikobewusstsein der Anwender für Identitätsdiebstahl

Largest Machine Learning Library, Analytics Transparency and Big Data Agnostic

Was macht Gurucul Risk Analytics effektiver als andere Lösungen?

Die Kernarchitektur baut auf PIBAE™ auf

PIBAE = Predictive Identity-based Behavior Anomaly Engine

- Maschinenlernen-Algorithmen für die Verhaltens- und Nutzungsanalyse arbeiten mit bis zu 254 Attributen eines Identitätsprofils
- Selbst lernende und Trainings-Algorithmen klassifizieren das Risiko von Transaktionen
- Dynamische Peer Groups optimieren die Genauigkeit der Cluster und Ausreißeranalytik
- Berücksichtigung von zeitlich sich ändernden Normen wie Versetzungen, Beförderungen, neue akzeptierte Arbeitsverfahren
- Entworfen für große Datenmengen ausgelegt auf Basis von Big Data Technologie und einem flexiblen Metadaten Framework
- Integration und Nutzung von IAM und PAM als Quelldaten
- Mit ausgelieferte Algorithmen lernen und erkennen anomales Verhalten sofort nach der Inbetriebnahme
- Automatisiertes Mapping von Aktivitäten und Konten zu Identitäten durch fuzzy logic und Linked Data Analyse
- Die Big Data Architektur verarbeitet historische Daten um die Phase des Selbst-Lernen und Trainings zu verkürzen

KOGIT
Secure Identity Management

Gurucul Risk Analytics

Ergebnisse, Features und Reviews

- Am zweiten Betriebstag von GRA in einer Firma des produktiven Gewerbes wurden 2 gekaperte Accounts in der Forschungsabteilung entdeckt.
- Finanzindustrie: durch den Einsatz von GRA konnte die Anzahl von Benutzerkonten um 83% reduziert werden. Zudem wurden intelligente Rollen definiert und ein dynamisches Provisioning auf Basis risikobasierter Verhaltensanalyse erstellt.
- GRA findet häufig Missbrauch privilegierter Zugangsrechte und anormales Verhaltensmuster in unerwarteten Einsatzgebieten heraus. Sogenannte unbekannte Unbekannte.
- Ein gängiges Verhalten ausscheidender Mitarbeiter ist, noch schnell Daten und Informationen mitzunehmen. GRA unterstützt dies zu erkennen, bevor die Daten exfiltriert werden.
- Erkennung von Zugang zu Cloud-Anwendungen, die einem ausgetretenen Mitarbeiter weiterhin zur Verfügung stehen.

Cybersecurity Excellence Awards – Most Innovative Cybersecurity Company – Finalist

Welche Deployment-Optionen gibt es?

- GRA Appliance ist vorkonfiguriert und einsatzbereit zur Nutzung im lokalen Rechenzentrum
- GRA virtuelle Maschinen Images können im eignen RZ oder in der privaten Cloud betrieben werden.
- Das Modul CAP ist cloud-basiert mit Konnektoren für beliebte SaaS-Anwendungen
- GRA kann auch auf beliebiger Hardware des Kunden installiert werden und bereits vorhandene Data Lakes nutzen.
- GRA kann auch als Managed Service mit rund um die Uhr Service bezogen werden
- Wartung, Support, Training und Professional Service sind verfügbar

Gängige Anwendungsfälle:

- Security Investigations and Risk Analytics (SIEM)
- Identity und Access Management (IAM) und Privileged Account Management (PAM)
- Data Exfiltration, Data Loss Prevention (DLP) and Insider Threats
- Cloud Access Security Intelligence (CASI)
- Online Fraud Detection (OFD)

KONTAKT

KOGIT GmbH | Rheinstr. 40-42 | 64283 Darmstadt
Telefon: +49 6151 7869-0 | info@kogit.de | www.kogit.de

KOGIT
Secure Identity Management