KuppingerCole Report

EXECUTIVE VIEW

by Mike Small | February 2016

Gurucul Predictive Risk Analytics

Gurucul Predictive Risk Analytics provides an interesting approach that combines access governance, risk management and the detection of cyber threats. Unlike other solutions that focus on network traffic or technical vulnerabilities this solution focuses on identity, access and user activity to detect and prioritize risk.

by **Mike Small**
mike.small@kuppingercole.com
February 2016

Content

Related Research Documents

Advisory Note: Real Time Security Intelligence - 71033

Blog: Real-time Security Intelligence – more than just "next generation SIEM"

Leadership Compass: Access Governance - 70948

Advisory Note: Identity & Access Management/Governance Blueprint - 70839

Advisory Note: Access Governance Architectures - 71039

1 Introduction

Detecting and managing attacks on IT systems is a serious problem. Cyber criminals are using increasingly sophisticated techniques to infiltrate organizational IT systems to commit crimes including data theft, denial of service and blackmail. However, statistics show most data breaches are detected by agents outside of the organization rather than internal security tools.

Traditional perimeter security devices like firewalls, IDS (Intrusion Detections Systems) and IPS (Intrusion Prevention Systems) are widely deployed. These tools are effective at controlling certain kinds of weaknesses for known threats, patterns and signatures. They also generate alerts when suspicious events occur; however, the volume of these events is such that it is almost impossible to investigate each as they occur. While these devices remain an essential part of the defence for the agile connected business, they are not able to detect a range of threats including the use of compromised credentials, insider threats, data exfiltration, access misuse and zero day attacks.

SIEM (Security Information and Event Management) is often promoted as a solution to these problems. However in reality, SIEM is a set of tools that can be configured and used to analyse event data after the fact and to produce reports for auditing and compliance purposes. While SIEM is a core security technology it has not been successful at providing actionable security intelligence in time to avert loss or damage.

External attacks now involve a complex process, often including an element of social engineering, which exploits compromised or illicit user credentials to gain access to data. This is partly because of the strength of conventional network defences against direct frontal attack, and also because the use of apparently legitimate credentials bypasses other security controls like encryption. Furthermore, insider threats continue to be a real problem and these invariably involve the misuse of access rights. For these reasons identity and access controls have become the new perimeter.

The most effective way of detecting illegitimate access to data is through the monitoring of user identity, access and activity. Even more importantly, better access governance is essential to reduce the risks of data theft. Some traditional SIEM vendors are starting to include analysis of user activity logs in their products. However, recognizing what is abnormal versus normal remains a problem. Big Data machine learning technology provides a potential solution to this by identifying identity, access and activity patterns that are common among peer groups of users.

What is needed is the integration of user identity, access and activity analysis into cyber-defence to enhance threat prediction and detection as well as to enable remedial action to be taken before damage is done. This requires techniques taken from big data infrastructure and business intelligence machine learning to analyse the massive amount and variety of data from the many sources to raise alarms only where there is a high confidence that the threat from the anomalies detected is real.

The volume of threats to IT systems, their potential impact and the challenges in discriminating between real threats and false alarms are the reasons why a new approach is needed. The need to calibrate what is normal to reduce the signal-to-noise ratio in order to detect anomalies remains a challenge and accomplishing this using bespoke rules within some tools requires considerable skill.

It is important to look for a solution that can easily build on the knowledge and experience of the IT security community, vendors, and service providers. End user organizations should always opt for solutions that include managed services and pre-configured analytics, not just bare tools.

2 Product Description

Gurucul solutions was founded in 2010 in Los Angeles CA where it is a privately held company.

Gurucul predictive risk analytics uses advanced machine learning algorithms to identify abnormal patterns and anomalies in user identity, access and activity behaviour in order to identify potential threats and reduce the risks from excess access and outliers. It integrates behaviour-based risk scoring for adaptive access governance with conventional provisioning tools to identify and automate the remediation of excessive accounts, entitlements and risks. It also uses data from multiple sources to calibrate what is normal and to predict and detect unknown threats using dynamic peer groups with clustering and outlier using machine learning models (150+) to detect anomalies. These anomalies are then processed through predictive machine learning models to score risk on a normalized basis.

2.1 Predictive Identity Based Behaviour Anomaly Engine™

Gurucul's products are built on an analytical framework called Predictive Identity Based Behaviour Anomaly Engine™ (PIBAE). PIBAE uses identity as the core and overlays activity, alerts, intelligence, and access to provide predictive security analytics and day zero anomaly detection. PIBAE is a framework that combines user behaviour intelligence, big data analytics, and leverages identity as a threat surface to provide Actionable Risk Intelligence™.

PIBAE is powered by Gurucul's patented machine learning models that run against hundreds of attributes to build a behaviour baseline for an entity or user and compare it against dynamically created peer groups to detect anomalous patterns.

These patterns are evaluated using internal risk modelling algorithms to determine a risk score for an entity or user. Using this framework, the products and solutions provide a proactive approach to predict, detect and respond to cybercriminal activity, under-the-radar cyber campaigns as well as insider threats.

Gurucul Risk Analytics has three integrated components that together provide a hybrid behaviour analytics range of solutions.

2.1.1 Access Analytics Platform™ (AAP)

This enables risk based compliance and access provisioning including:

- A real time contextual view of identities, access and activities.
- Identity access intelligence and roles from behaviour analytics using machine learning.
- Matching user accounts and entitlements to needs based on actual behaviour.
- Detection of high privileged access and reporting on obsolete and orphan access rights.
- Identification of accounts with access activity that is very different from their peers.

2.1.2 Cloud Analytics Platform™ (CAP)

This provides visibility of cloud access and related anomalies including:

- Visibility of activities and access to cloud apps related to identities.
- Detection of High Privilege Access (HPA) account anomalies.
- Risk scoring of identity, access, and activities that helps to identify compromised and hijacked accounts, insider threats and data leakage.
- Ready to use connectors for popular SaaS applications.

2.1.3 Threat Analytics Platform™ (TAP)

This provides behaviour based predictive risk scoring:

- A risk scored time line to detect and predict insider and advanced persistent threats.
- Identity based behaviour analysis to detect hijacked accounts and unauthorized activities.
- Actionable alerts for anomalous behaviour and risk scores, plus case management.
- Detection of misuse, sharing and takeover of High Privilege Access (HPA) accounts.
- User self-audit improves user awareness and helps to detect and deter identity theft.

2.1.4 Multiple Dashboards

The above three platforms, when integrated together, provide multiple dashboards to identify and manage threats as well as to remediate abnormalities. These dashboards include:

- Insider threats – the risk associated with user entitlements and behaviours.
- DLP Alerts – how users are using data.
- Cloud Analytics – how cloud services are being used
- High Privilege Accounts – activities related to administrative accounts
- Cyber Fraud – potentially fraudulent activities
- Access Analytics – managing entitlements
- End point security – where risky behaviours emanate from

2.1.5 Deployment Options

The products can be deployed in a number of ways, an interruption of service is not required and they work with existing infrastructure:

- GRA appliances pre-loaded ready to be provisioned on premise.
- GRA virtual machine images that can be provisioned on existing servers or private cloud.
- CAP is delivered as a cloud service
- GRA can be deployed directly on existing hardware
- GRA is also available as a managed security service.

2.2 Essential Characteristics

Gurucul Predictive Risk Analytics provides functionality that spans Access Governance and Security Intelligence. This section compares the functionality provided by the Gurucul solutions with the essential characteristics for these market segments.

2.2.1 Access Governance

Access Governance is concerned with providing the answers to three key questions:

- Who has access to what?
- Who has accessed what?
- Who has granted that access?

For the answers to these questions to be useful access governance tools need to take account of how the organization actually operates as well as its policies for compliance and risk. In the past, some organizations attempted to build their access governance on a theoretical basis. This approach was not successful because it did not take account of the practical realities and complexities of their operation.

The features expected for access governance tools include: role management, policy management, rule definition and analysis, workflows management, attestation and remediation. Dashboards for executives and extended auditing and reporting capabilities are also commonly a part of these tools. Risk management features are important but not yet a standard feature of all products in the market.

The Gurucul Access Analytics platform integrated with a third party provisioning solution provides a strong match with many of the expected features. It is particularly strong in the area of risk scoring and managing access based on risk.

2.2.2 Multiple sources of data

Gurucul Risk Analytics consumes data from multiple technologies such as HR Systems, Identity & Access Management solutions, log aggregators, applications, network devices and other endpoints. It normalizes this data into a consistent format using big data infrastructure, executes correlation algorithms, builds behaviour baselines for each identity and its respective peer groups, and then uses predictive modelling to identify insider threats, fraud, and misuse of access rights.

2.2.3 Access Analytics

The analytics platforms are built upon Gurucul's patented machine learning models (150+) that run against hundreds of attributes to build a behaviour baseline for an entity or user and compare it against dynamically created peer groups. This identifies the actual accounts and entitlements that are being used by people with similar characteristics in the performance of their work and to detect anomalous access patterns. The customer can further "train" the system by providing feedback on the validity of detected anomalies.

The actual patterns detected are assigned a risk score that describes the level of risk associated with them. A textual description is provided for the risk score to clarify the kind of risk as well as a timeline associated with that risk. The user can alter the scoring to better match their own specific circumstances and add or remove their own risk patterns.

2.2.4 Security Intelligence

Access governance provides an important foundation for security intelligence. Cyber-criminals now exploit human and technical weaknesses to infiltrate organizational networks and to use apparently legitimate protocols and access rights to access and exfiltrate data. In order to detect this, you need a detailed understanding of individuals' access rights and normal patterns of access to be combined with the traditional network activity monitoring data.

Four methods of data ingestion are supported (Flat Files, Databases, APIs and Streams) across User, Resource, Activity, plus Accounts, Roles & Entitlements primary data types. Data source examples include: Identity Management (IDM), Privilege Access Management (PAM), Directories, SIEMs, DLP, FW/VPN/NGFW, Threat Intel Feeds, Vulnerability Assessments, Cloud Apps, Network Flow, Databases, Authentication, Social Media, File Storage, Telecommunications, and OS/Mobile.

Machine learning algorithms (supervised and unsupervised, regression, classification, clustering, and dimensionality reduction) have been developed into 150+ models with the ability for customers to customize risk weightings and behavior models. Customers can also create custom behavior models with side-by-side model testing on data sources. Data sources focus on 254 attributes for identity, access and activity and can be customized and expanded. Rules are also available with linked data analysis, and ability to customize per customer requirements. The solution can perform out-of-the-box with no customization or tuning for proof of concepts, testing data sources or production deployments.

Dashboards with color-coding and normalized risk scores quickly highlight to predict and detect unknown threats, highlight areas of excess access risk and access outliers, and engage employees and partners in a 2-way collaborative security relationship via self-audits. Risk scores are based on knowledge obtained from collaborative insider threat research with the Carnegie Mellon University CERT group on models of risky behaviour. Identity is a threat plane that requires the removal of excess access risks and the detection of compromise or misuse.

Gurucul Predictive Risk Analytics provides this functionality with a strong focus on access patterns. It should be integrated with the other relevant security intelligence tools to enhance the Cyber Defence / Security Operations Centre.

2.2.5 Automated response, remediation and recovery

Gurucul Predictive Risk Analytics includes a workflow capability to manage the remediation of detected anomalies and risks. This covers both the adjustment of access rights as well as managing access related incidents. It integrates with market leading trouble ticketing systems and identity provisioning tools. In conjunction with identity provisioning tools it provides the capability to automate the remediation of entitlements based on various criteria such as the assessed level of risk. The threshold levels and other parameters associated with automated remediation can be configured.

2.2.6 Scalability

The potential volume and rate of data that a security analytics tool has to deal with is enormous – scalability is therefore very important. Gurucul predictive risk analytics are built from the ground up on big data infrastructure and also integrate with customer deployed Big Data technologies to ensure massive scalability.

2.2.7 Integration

Gurucul Risk Analytics consists of a set of integrated platforms that work together “out of the box”. It provides connectors to ingest data from a wide range of data sources including commonly used cloud SaaS applications using cloud-to-cloud connectors.

3 Strengths and Challenges

Gurucul Predictive Risk Analytics provides an interesting approach that combines access governance, risk management as well as the prediction and detection of cyber threats. Unlike other solutions that focus on network traffic or technical vulnerabilities this solution focuses on user identity, access and activity to detect and prioritize risk. This approach makes sense since most cyber-attacks eventually involve obtaining unauthorized access to systems, applications or data through compromised user accounts. In addition insider abuse and data theft does not necessarily involve suspicious network activity.

The challenge, which is similar to that for a network activity based approach, is to calibrate what constitutes normal activity. Only then is it possible to accurately identify abnormal patterns and without this calibration the user is either overwhelmed with false alarms or real issues remain undetected. Gurucul Risk Analytics solves this problem through the use of their patented machine learning models and use of dynamic peer groups. The extent to which this can replace professional services and deep knowledge of the tools, tactics and procedures used by cyber-security teams remains to be seen.

So Gurucul Risk Analytics can provide an important component of the organizational cyber defence centre. It does not replace the traditional firewalls, intrusion prevention and vulnerability detection systems. It does provide an important tool to identify and counter identity based threats.

Strengths	Challenges
• Access Governance functionality using machine learning to calibrate normal user activity for accounts and entitlements. • Access entitlements can be managed using the risk associated with behaviour patterns. • Threat prediction, detection and prioritization based on user behaviour analytics. • Automation of remediation workflows and integration with related solutions.	• Effectiveness of machine learning approach needs to be proven for a wide range of security use cases. • Needs to form part of a complete cyber-defence approach. Partnerships or convergence with other complementary vendors is expected. • Professional services are a critical component of success in this area for IAM integration.

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Straße 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com