DATA SHEET

GURUCUL

Gurucul Next Generation SIEM

Uninhibited Security Visibility, Noise Reduction, and Risk-Driven Prioritization to Automate Investigations and Response Without Escalating Costs

Business Problems

The evolving hybrid workforce, continued adoption of cloud-native applications, and business at a global scale has introduced security gaps within organizations. As threat actor groups operate with support of adversarial nations, their focus on penetrating defenses and evading current security solutions means initial compromise is inevitable. This puts the burden on security engineers and analysts, often working as part of a security operations center (SOC), to identify and respond to threats that are already inside the network, whether on-premises or in the cloud. Current SIEM and XDR solutions are fundamentally flawed in several ways.

Traditional SIEM solutions are built on ingesting log data and log analytics, while other types of analytics are a poor afterthought. SIEM solutions also charge users based on amount of data ingested, which can quickly and unpredictably scale costs way above planned budgets. This forces security teams to limit data, leading to poor visibility for the very security capability they already paid for!

Most XDR solutions are focused primarily on what the endpoint sees but fail to properly incorporate and analyze all the other telemetry for identifying an attack campaign to provide a more comprehensive response. They offer mostly rule-based analytics, which limits their ability to find new and emerging threats and variants. This slows down security teams and forces them to manually correlate and investigate advanced and targeted attack campaigns that have the most potential to do damage to an organization.

> *“Gurucul really stood out because the analytics engine was the most powerful. The machine learning algorithms are the strongest. We saw results very, very quickly.”*
>
> *- WIliam Scandrett, CISO, Allina Health*

Gurucul Next Generation SIEM

Gurucul Next Generation SIEM (NGSIEM) is focused on unburdening security teams from floods of alerts and false positives, leveraging automation to drastically reduce Mean-Time-To-Detect (MTTD), and prioritizing investigations and response actions to lower Mean-Time-To-Remediate (MTTR). In addition, Gurucul NGSIEM provides the necessary capabilities to achieve or exceed compliance requirements and strongly maps to the MITRE

> *SIEM solutions are complex technologies as they centralize a variety of capabilities, functions and features into a single platform to aid a user in detecting unexpected activities and events in their environments.*
>
> *- Gartner Critical Capabilities for SIEM Report, Published 1 July, 2021.*

Attack Framework. Gurucul also works natively within any cloud environment and is the only vendor that supports cross-cloud analytics for poly-cloud threat detection and response.

Gurucul NGSIEM improves data collection and infrastructure visibility, while automating and consolidating manual tasks related to correlation, analysis, investigation, and response actions. It is also one of the only solutions that automatically includes out-of-the-box threat content powered by threat intelligence and open trained machine learning (ML) models. This delivers immediate automated threat detection upon deployment.

Further, Gurucul NGSIEM uniquely incorporates an enterprise-level risk engine that goes beyond other solutions to help security teams with prioritizing their activities across the SOC lifecycle and focus security teams on the most impactful events and threats.

Detect Unknown and Emerging Threats and Variants Earlier with Gurucul STUDIO™

Gurucul STUDIO™ enables customers to easily view, customize, and build new advanced ML models from our fully transparent and open library of 2500+ out-of-the-box models. This rapidly improves an organization's security posture against new and emerging threats and variants.

Gurucul STUDIO™ provides:

- **Full transparency and viewability of our models and how they work** to educate analysts, and confirm and trust their effectiveness
- **An intuitive graphical interface** that enables security professionals with no coding and a minimal knowledge of data science to create custom models
- **Gurucul ML model community sharing** allows for customers to share their models with our community and crowdsource this data for use with our own research team to add to our library

How Does Gurucul NGSIEM Compare?

Feature	Gurucul NGSIEM	Other NGSIEM	Traditional SIEM	Comment
Cloud-native, highly scalable, open architecture	●	◐	◔	Not lifted/shifted to cloud
Included Out-of-The-Box (OOTB) Threat Content	●	—	—	Powered by Threat Intel, analytics & machine learning
Automated data pipelines & OOTB 3rd party integrations	●	◔	◔	400+, including threat intel feeds, user/accounts, etc.
Multi-cloud deployable and analytics	●	◔	◔	Native support for AWS, Azure, GCP, etc. Cross-Cloud Analytics
User and Entity Behavioral Analytics	●	◕	◔	Complete baselining, monitoring w/ supporting ML models
Identity Security & Privileged Access Analytics	●	◔	—	Complete analytics vs. just Active Directory Correlation
Full library of trained & rule-based ML models	●	◔	◔	2500+, mapped to industry, security frameworks, etc.
Open and customizable trained ML models	●	—	—	Create, customize, crowdsourced ML-based analytics
Risk-prioritized alerting	●	◐	◐	Risk scoring vs. aggregated CVE/ CVSS scores
Full library of compliance reporting	◕	●	●	Dashboards, reports, queries, alerts
Full library of response playbooks (SOAR)	◕	◐	◔	Library of OOTB playbooks
Customizable response playbooks (SOAR)	●	◐	◐	For the Traditional SIEMS that even have it
RBAC for Cloud & data masking capabilities	●	◕	◐	Same RBAC for cloud or on-prem, data masking
Consolidated views w/option for add-on features	●	◐	◕	Reduces investigation time &seamless feature turn-up
Predictable and scalable licensing model	●	◔	◐	By asset vs. data ingestion

Gartner Disclaimer Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Why Choose Gurucul Next Generation SIEM?

Get Full Visibility Without Escalating Costs

- Asset-Based Licensing, not Data Usage
- Consolidation of Data into a Single Console
- Any Input, Device, Application and Source Normalized for Security and Less Storage

Leverage Depth of Analytics for Advanced Detection

- Automatically Adapts to New and Emerging Threats
- Out-of-the-Box Threat Content (not extra)
- Open, Customizable and Adaptive Behavioral, Multi-Cloud, Identity-Access, IoT Analytical Machine Learning Models (over 2500)

Increase Operational Efficiency and Improve ROI

- Risk-Driven Prioritization Means Less Chasing of False Positives
- Reduce Investigation Time with Improved Context
- Unburden Senior Analysts and Reduce Resource Requirements

Enjoy Automated Eradication of Threats

- Dynamic and Targeted Playbooks for Automation
- Risk Scoring via Enterprise-Class Risk Engine
- Mitigate the Full Attack Campaign Before It Impacts the Business

About Gurucul

Gurucul is a global cyber security company that is changing the way organizations protect their most valuable assets, data and information from insider and external threats both on-premises and in the cloud. Gurucul's real-time Cloud-Native Security Analytics and Operations Platform provides customers with Next Generation SIEM, XDR, UEBA, and Identity Analytics in a single unified platform. It combines machine learning behavior profiling with predictive risk-scoring algorithms to predict, prevent, and detect breaches. Gurucul technology is used by Global 1000 companies and government agencies to fight cybercrimes, IP theft, insider threat and account compromise as well as for log aggregation, compliance and risk-based security orchestration and automation for real-time extended detection and response. The company is based in Los Angeles. To learn more, visit Gurucul and follow us on LinkedIn and Twitter. To learn more, visit gurucul.com and follow us on LinkedIn and Twitter.

Gurucul | 222 North Pacific Coast Highway, Suite 1322 | El Segundo, CA 90245 | 213-259-8472 | sales@gurucul.com | www.gurucul.com