

Analytics Driven, Simple,
Accurate and Actionable
Cyber Security Solution

CYBER
ANALYTICS



happiest minds

The Mindful IT Company

Born **Digital** . Born **Agile**

Overview

Cyberattacks are increasingly getting more frequent, more sophisticated and more widespread than ever before. With more than 50 billion connected devices expected in 2020 compared to current 10 billion, the surface area for potential attacks is expected to grow 10 times larger in the next five years. The new age cyber threats are driven by external attackers or insiders with malicious intent. One of the biggest challenges organizations are facing when it comes to threat detection and risk mitigation is gaining visibility into their internal environment, as the traditional security platforms and products are incompetent in tracking or analysing the user behavior.

We at Happiest Minds believe that Machine Learning and Artificial Intelligence driven Behavioral Analytics is the fulcrum for helping Predict, Prevent and Defeat cyberattacks in this age of increasing attacks/ threats like Ransomware attacks and Advanced Persistent Threats. Cyber Analytics Platform from Happiest Minds is an enterprise grade security analytics and visualization platform focused on behavioral analytics of high velocity, real-time contextual enterprise data. Combining Big Data Technologies, Machine Learning and patented Algorithms, the Cyber Analytics platform helps discover insightful information and actionable cyber threat intelligence around security risks, targeted attacks and more.

Key Obstacles in the Cyber Threat Hunting Space

1

Finding out the "unknowns" that do not fit into known patterns

2

Moving away from signature based or heuristics based tools

3

Ability to process large volumes of data intelligence with high speed

4

Bringing out the real-time threat posture

5

Integration challenges with respect to siloes of multiple security controls

6

Shortage of trained resources to perform risk analysis

7

Keeping abreast on evolving threats and vulnerabilities

8

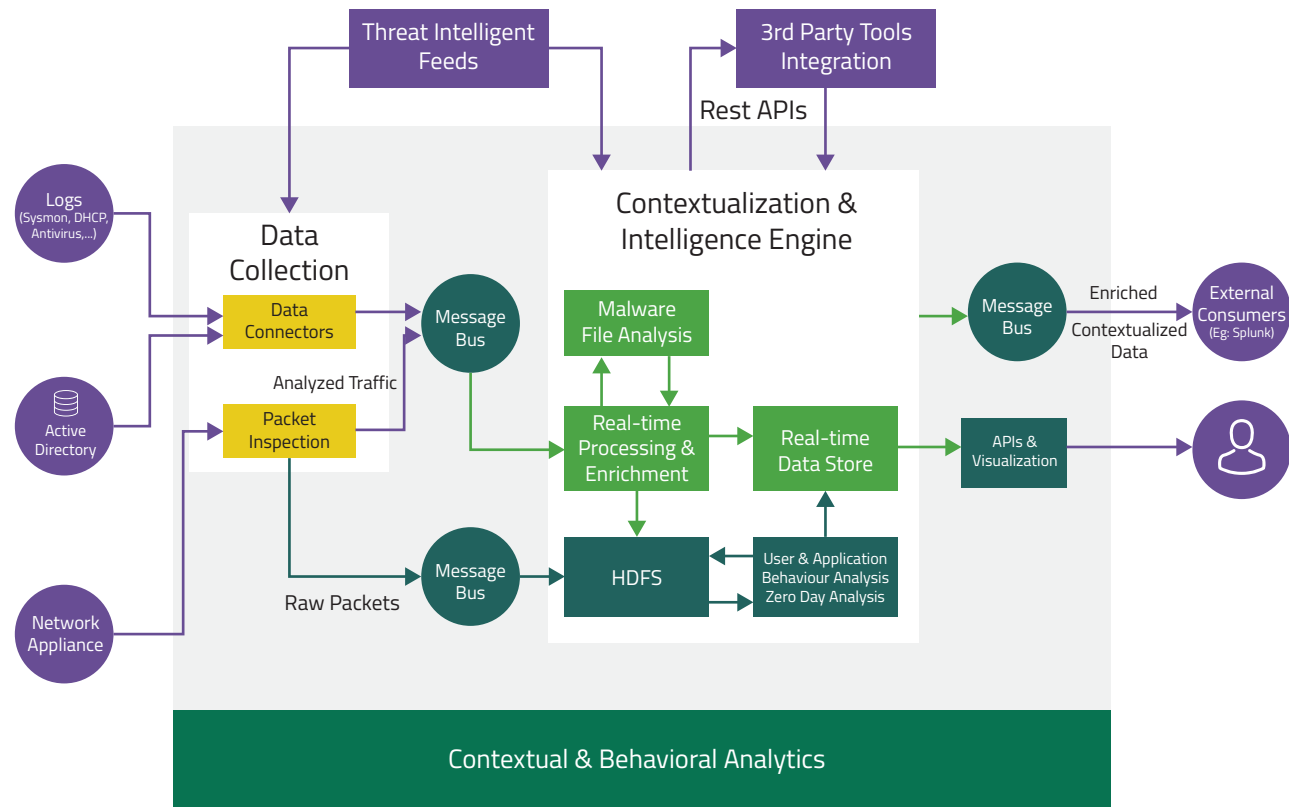
Optimizing the accuracy of alerts

Why **Next Generation** Cyber Analytics Solution?

The Cyber Analytics Solution leverages Machine learning, Big Data, Trend Analysis, User Behavioral analysis (UBA), Entity Behavioral Analysis (EBA) and other techniques to identify anomalous behaviour, activities or trends of individual users, systems, and/or applications in an enterprise. The platform can monitor user accounts, end point devices and can be embedded in applications and networks in an organization. It combines the data collected from various network & end points to derive intelligent insights on the potential security risks in organizations that the cyber criminals may exploit. The self-learning platform continually adapts with repetitive usage and helps organizations build better security posture to defend the ever evolving cyber threat landscape. It helps enterprises to instrument a portfolio of security management, automation, and orchestration; simultaneously enabling threat hunting and driving rapid Incident Response.actionable cyber threat intelligence around security risks, targeted attacks and more.

Storage Data Management for Real Time Forensic Analysis

Unified Platform for Integration and Collaboration



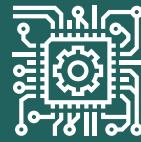
Features



User / entity behavior profiling, segmentation and visualization



High risk user/ entity identification, visualization and outlier detection



Machine learning based anomaly detection in internal connections and assigning a risk score



Data exfiltration and anomaly detection in external connections along with graphical representation of why an outlier led to an alert



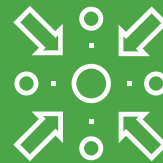
Advanced threat hunting capabilities an "exhaustive" & "fast" search capability to look for outliers / anomalies



Data Analytics with extended user or entity intelligence covering Logon / log off events, AD events, Remote login patterns and Network usage



Network analytics with reporting on Network bandwidth usage, Connection count, DNS resolutions, to and fro Traffic from sources of bad reputation



Analysing exclusive behavior patterns through machine learning and subsequent reduction false positives over a period of time



Dynamic entity link analysis with User Mapping, Detection & highlighting hidden relationships between users, IP addresses, domain demonstration using Network Graph



Reports and visualization using intuitive analytics dashboards, Compounded risk scores and Meta data with drill down capability on all reports

Benefits



Real-time detection upon occurrence of unusual activities



Multidimensional understanding about users and analysts based on Machine learning.



Artificial Intelligence: Disambiguation between Anomalous and Malicious behavior



Searching & Hunting: Rich User Experience for Collaborative Discovery



Reinforcement learning to automate Kill-Chain mapping and to distinguish malicious from anomalous.



Signature-less behavior based analytics for detecting insider and targeted cyber attacks



User and entity centric monitoring across hosts, network and applications



Proactive defense against zero-day attacks such as ransomware and rapid response

Key Differentiators



High Velocity (>10Gbps) Real Time Analysis



Enterprise grade, Horizontally Scalable architecture



Offers Unique proposition combining the network & log centric behaviors



Integration with existing Security systems, including SIEMs, Firewalls & Endpoints



Machine Learning Models & Intelligent Algorithms



Open standards based architecture that can support multiple data sources



Open Source Big Data Technologies - Kafka, Elastic Search, Spark, Hadoop



End to end cyber security offering - your partner for end to end "cyber security" needs



Rich Pool of cyber security and analytics experts



Flexible Delivery and pricing models

Our Solutions

Cyber Risk Protection Platform

Happiest Minds cyber risk protection platform leverages multiple technologies employed together to effectively address all the cyber security risks; from detection to triage, response and remediation.

Threat Vigil

Threat Vigil is one of the leading threat management solutions that offers an on-demand, cloud based, penetration testing platform, developed by Happiest Minds Technologies for various enterprise segments.

Cyber Vigil

CyberVigil is a comprehensive cyber security solution platform that can address multiple security requirements in an easy to deploy and use model.

Identity Vigil

IdentityVigil is one of the leading identity management solutions that helps organizations efficiently meet their security, regulatory and business access needs, through an end-to-end holistic IAG solution.

Compliance Vigil

ComplianceVigil solution provides a platform for risk and compliance management wherein the framework, management, automation and monitoring of the R&C is bundled into one single platform and delivered from the cloud.

Alliances



**Write to us at
business@happiestminds.com**

About Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable **digital transformation** for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, **AI & Cognitive Computing**, **Internet of Things**, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/ hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

www.happiestminds.com

