happiest minds
The Mindful IT Company
Born Digital . Born Agile

The Complete Guide to

Security Orchestration, Automation and Response (SOAR)

by

Varsharani Kallimath
Chetankumar Savalagimath

Contents

Introduction

Gartner defines SOAR as a technology that enables the organization to take inputs from various source and apply workflow aligned to process and procedure.

These can be orchestrated via integrations with other technologies and automated to achieve the desired outcome and greater visibility. Additional capabilities include case and incident management features, the ability to manage threat intelligence, dashboards, and reporting, analytics that can be applied across various functions. SOAR tools provide machine-powered assistance to human analysts to improve the efficiency and consistency of people and processes by significantly enhancing security operations activities like threat detection and response.

Why SOAR?

Like many new tools for cyber security, it is crucial to know what problems drove for invention of SOAR before deep diving into the definition of SOAR.
The five key problems the SOAR market has evolved to address are as follows:

01

Organizations are being forced to achieve workload with less skilled analysts and high expectations.

02

Alerts consume most of the analyst time with similar analysis and false alarms and performing the same tasks to determine the accuracy of the alerts.

03

Security incidents are becoming more expensive, pushing organizations to find new ways to reduce the meantime to detection and the meantime to resolution further.

04

Security operations are naturally difficult to measure and manage effectively.

05

Tribal knowledge is genetically difficult to codify and often leaves the organization with personnel changes.

What SOAR can do?

One of the added advantages of SOAR is its flexibility. SOAR can be used to simplify any number of common tasks, like updating threat databases and responding to alerts.

Key applications:

Manage Vulnerabilities: Correlating log data with threat intelligence to understand what attackers are using and identify vulnerable elements of your infrastructure before they can be compromised.

Coordinate investigations: Unify security data easily and retrieve relevant third-party threat intelligence when you need it. Instant access to external data sources helps analysts in making a precise decision in each investigation.

Respond to incidents: Playbooks, a set of rules enables SOAR platforms to act automatically when an incident occurs. This functionality helps in setting up an automated response for the most common incident types.

Streamline collaboration: Incident investigation and other security processes can grind to a halt when teams aren't able to collaborate easily, such as when teams throughout an organization store data in different formats and use different software. SOAR helps you eliminate these barriers to collaboration.

What SOAR is Not:

A SOAR solution is not a replacement for skilled analysts. Deploying a SOAR solution to replace analysts will inevitably create more risk rather than mitigation. Instead, a SOAR solution should be viewed as an enabler for the security program and security analysts alike.

SOAR solutions are not designed to ingest a large volume of raw events. Instead, SOAR solutions are designed to pick up the incident where SIEM functionality ends, providing an automated and orchestrated response throughout the Identification Phase, as well as the Containment, Eradication and Recovery Phases.

SOAR is a solution for mitigating security threats through automation which is programmed to collect data about security threats from various sources and respond quickly to the low-level security events without human assistance.

SOAR functions:

Aggregation: The ability to aggregate data across different sources in the form of alerts, or inputs from other technologies such as an alert from a SIEM tool or an email sent to a mailbox.

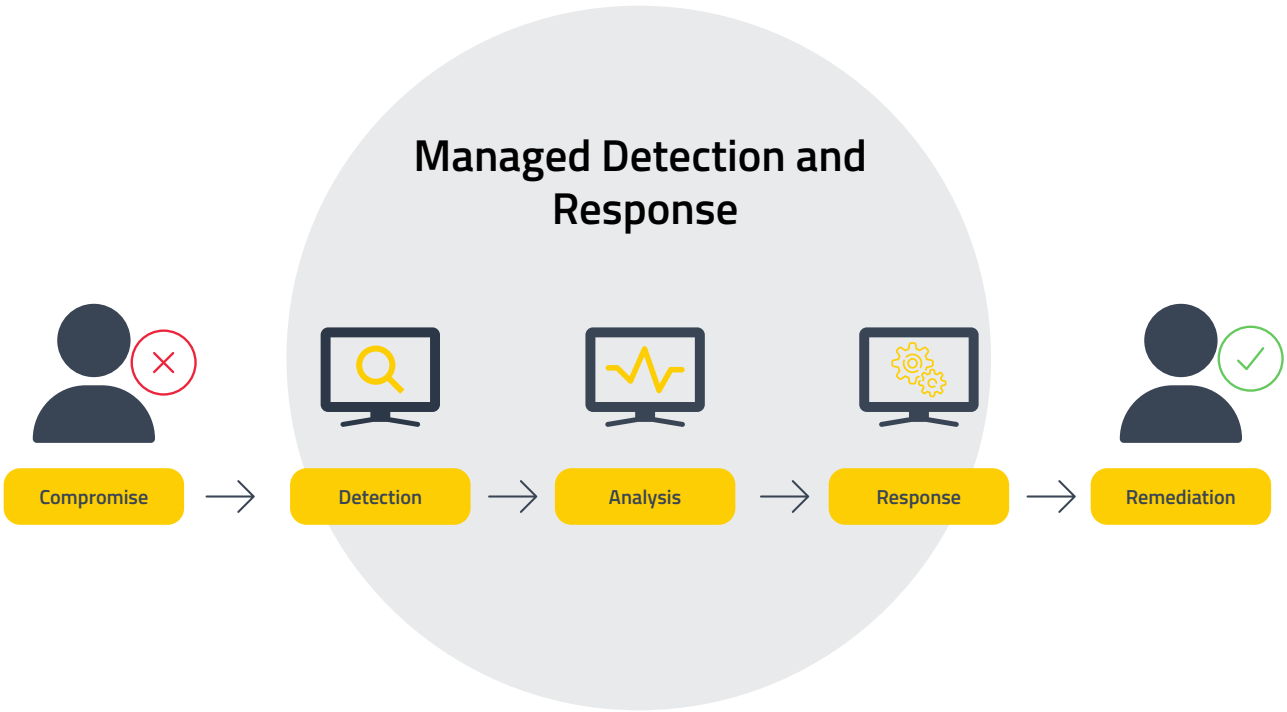
Enrichment: Additional insights during data collection and processing, SOAR solutions help in integrating external threat intelligence to perform internal contextual lookups or run processes to gather further data rendering to defined actions.

Orchestration: Arranging tasks to optimize a structured workflow by gathering information from a different source and consolidating it. SOAR solutions integrate different security tools and platforms so they can work together. Technology integrations are the best and most common method used to support technology orchestration.

Automation: This concept enables software to complete a single task or function without human involvement. Automation is not an alternative for human analysts. Instead, it reduces the analyst's time spend on simple, repetitive tasks.

Instead of wasting time on tedious manual tasks and investigating false positives, members of SOC (Security Operations Center) team can utilize their expertise to respond to events quickly and effectively.

Response: Manual or automated response provides canned resolution to programmatically defined activities. SOAR automates repetitive tasks, prioritizes critical events and streamlines security processes to decrease response times drastically.



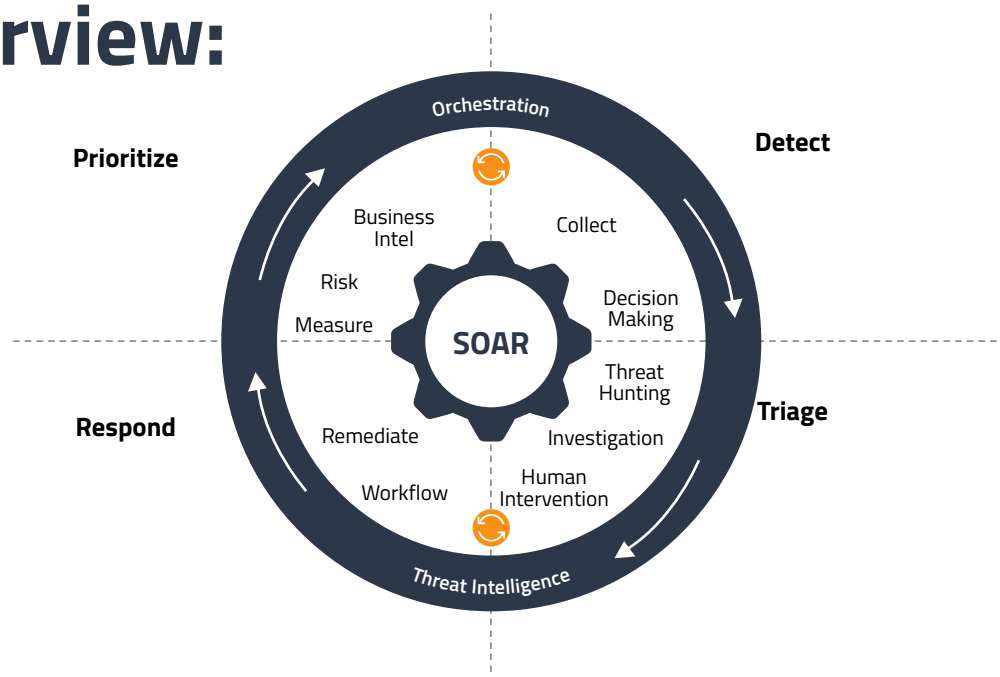
SOAR benefits for delivering MDR services.

SOAR's ability to orchestrate and automate are actions taken by security products without any need of human intervention. This is one of its greatest strength that allows SOAR to integrate with any security process or tool that is already in use that can enhance the performance to add usefulness to each product.

To address scalability problems, SOAR is integrated with existing security technologies.	The integration of SOAR improves the ability of MSSP's to detect and neutralize threats and attacks.
To unify asset databases, help-desk systems, configuration management systems, and other IT management tools it acts as a single "pane of glass".	SOAR accelerates responsiveness to alerts triggered by arming MSSP's with the visibility and ability to react decisively to new threats or attacks such as SOAR automated workflow spans for threat intelligence through the case and ticket management and provide risk and relevance between alerts.
MSSP's excess an ample amount of time dealing with false positives, because there are a greater number of alerts every day. SOAR can automate the handling of such alerts, which helps analysts to focus on where decisions are needed.	SOAR automates manual work of the analyst to validate the legitimacy of the alerts such as new users found in the infrastructure or removing and updating rules and thus reduces the time consumption.

SOAR overview:

Security Orchestration, Automation and Response: AN Overview



Managed Detection and Response (MDR) security delivery service providers face many challenges in terms of both technical and human-related issues due to advanced security threats.

The solution that relies on static signature and pattern matching is incapable of detecting and responding to today's advanced security threats. Hence, many MSSP's (Managed Security Service Providers) are going behind SOAR solution to improve their detection and response capabilities.

Developments in SOAR

SOAR is an Orchestrion, automation and responding system which can be developed in all its 3 Layers from the stage of data injection to the stage of response accusation, SOAR platform can expand the capabilities of their software with technologies like machine learning. Machine learning complements existing SOAR functionality by giving the software the means to adapt to changes in the environment. SOAR platforms can learn what is and isn't normal for automation instead of relying on static threshold-based rules. Once these baselines are established, software updates them periodically as and when the environment changes, increasing its accuracy and reducing the number of false positives.

SOAR has seen significant improvements which include process orchestration, automation of tasks or workflows. This helps in data completeness and providing a better context for alerts which reduce the amount of manual work necessary to remediate threats. Also using SOAR the security team members who are not comfortable with scripting languages can use graphical playbook creation tools, while with advanced scripting knowledge retain the ability to write scripts by hand.

Critical Components of SOAR Technology:

When evaluating different SOAR platforms, each component should be considered as it plays an important role in the function.

01 **Customizability and Flexibility:** An effective SOAR solution should be capable enough of being the single tool on top of the security stack. It should be enabled to implement in a manner that is optimized for CSIRT teams, as well as SOC's, MSSP's and security teams. Data input from a different source, including machine to machine, email, user submissions, and manual input should be supported.

In every SOAR solution there will be few default integrations readily available but not all the organization's security products support, for that reason SOAR solution should be flexible enough to create bi-directional integrations with security and analytics platforms as per the customer's requirement.

02

Process Workflows: One of the key benefits of a SOAR solution is its capability of automation and orchestration of processes workflows to achieve force multiplication and reduce the burden of repetitive tasks performed by analysts day-to-day. The process workflows implementation should be flexible enough to support almost any process which may need to be codified within the solution. Workflows should support the use of both custom and built-in integrations, as well as the manual task creations which to be completed by an analyst.

03

Incident Management: Orchestration and automation of security products provide clear value to any security program. SOAR solution should include additional features to manage the entire IR lifecycle and to maximize the time and monetary investment. This should include case management which involves collecting, distributing and analyzing data tied to specific security incidents, to allow teams to effectively respond. A SOAR platform helps organizations to reduce the meantime to detect and mean time to respond by enabling alerts to be qualified and remediated in minutes rather than days and weeks.

04

Threat intelligence: Threat intelligence is a critical component in effective and efficient incident response. These technologies support the vulnerability remediation. Threat intelligence must go above and beyond modest feeds to be truly effective in today's threat landscape, as a SOAR solution has access to not only the indicators but also to the incident information which can provide the added context, it is in an inimitable position to gather actionable threat intelligence.

05

Collaboration and Information Sharing: Incident response to a security alert is an equal potential responsibility of an individuals in an organization similarly SOAR solution need to support collaboration and information sharing among team members in a controlled manner.

SOAR Applications:

01 **Proactive threat hunting:** Since threat hunting usually requires analysts to rapidly coordinate among multiple security tools, it presents a great opportunity for orchestration with immediate impact. SOAR tools can enable security teams to ingest third-party threat feeds and automate 'search and destroy' workflows that scan for potential vulnerabilities across environments.

02 **Standardize and iterate incident processes:** Security teams need to minimize 'quality variance' in incident management and response. SOAR workflows are a great first step in this direction, allowing for partial/full codification of best-practice processes and guaranteeing that security analysts don't have to start from scratch each time they encounter a specific incident. With deployment maturity, SOAR tools will also allow teams to quickly iterate upon these processes by spotting gaps and areas for improvement.

03 **Improve investigation quality:** Multiple data points in this report suggest that security teams struggle with gathering incident context and leveraging full visibility of data at their clearance. SOAR tools can help improve investigation quality by enabling faster resolution of false positives, prioritizing incidents and risk through correlated information from multiple tools and freeing up analyst time by obviating the need to learn the detailed vernacular of many security products.

04 **Accelerate and scale incident response:** SOAR offers coordinated automation to an industry that is currently affected by important but repeatable, high-quantity tasks. SOAR tools allow SOC's to rely on automation for the grunt-work and leverage rich, correlated information for decision-making and investigation.

05 **Security operations and maintenance:** In addition to automating repetitive tasks, SOAR tools can also help security teams simplify system checks, maintenance, upgrades, and general security operations. These practices rely on workflows as much as response, and standardization are needed. Automated execution will increase accuracy and better plug gaps that leave systems vulnerable.

SOAR Use Cases:

Use cases for SOAR will vary depending on the environment and are limited only by the creativity of the organization architecture.

Sample case study

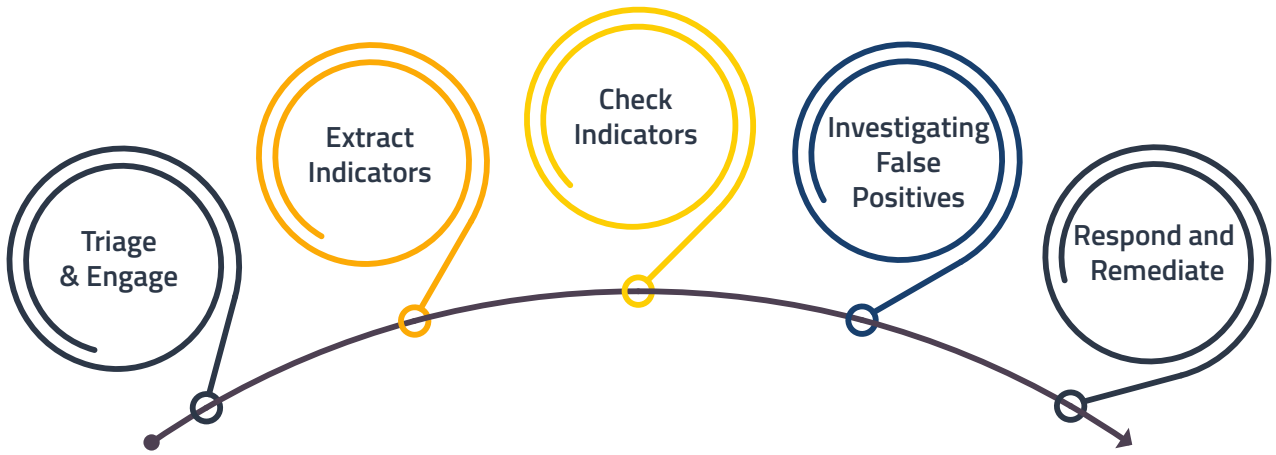
Phishing Attack:

The challenge: Phishing is the most extensive cyberattack out there today. According to the Verizon Data Breach Digest, phishing attacks play a role in 92 percent of security breaches today. This means security teams are spending more time trying to identify and remediate these attacks. But as the volume of attacks continues to grow, it's difficult to keep up. Analysts need to act faster on phishing responses, handles large volumes, standardized to deal with repeated attacks, and still customizable to deal with unique attacks.

As part of the triage process, the SOAR platform extracts compromised indicators. With a quick scan of the header and content of the email, the SOAR platform assigns an incident severity and checks for bad reputations by cross-referencing the data against external threat intelligence databases. If any malicious indicators found, affected users are informed with instructions on what to do. The SOAR platform also scans all email accounts and endpoints to identify malicious instances and delete and adds the malicious, compromised indicators to blacklists tracked by other security tools.

In cases where malicious indicators are not detected, the SOAR platform checks if any attachments found in the suspected email and detonate them in a sandbox for further analysis. If nothing malicious detected, the SOAR platform forwards the incident to the IT security team for manual investigation. If the team is satisfied that the email is not malicious, the SOAR platform sends an email to the recipients, notifying them of the false alarm.

Here is the workflow:

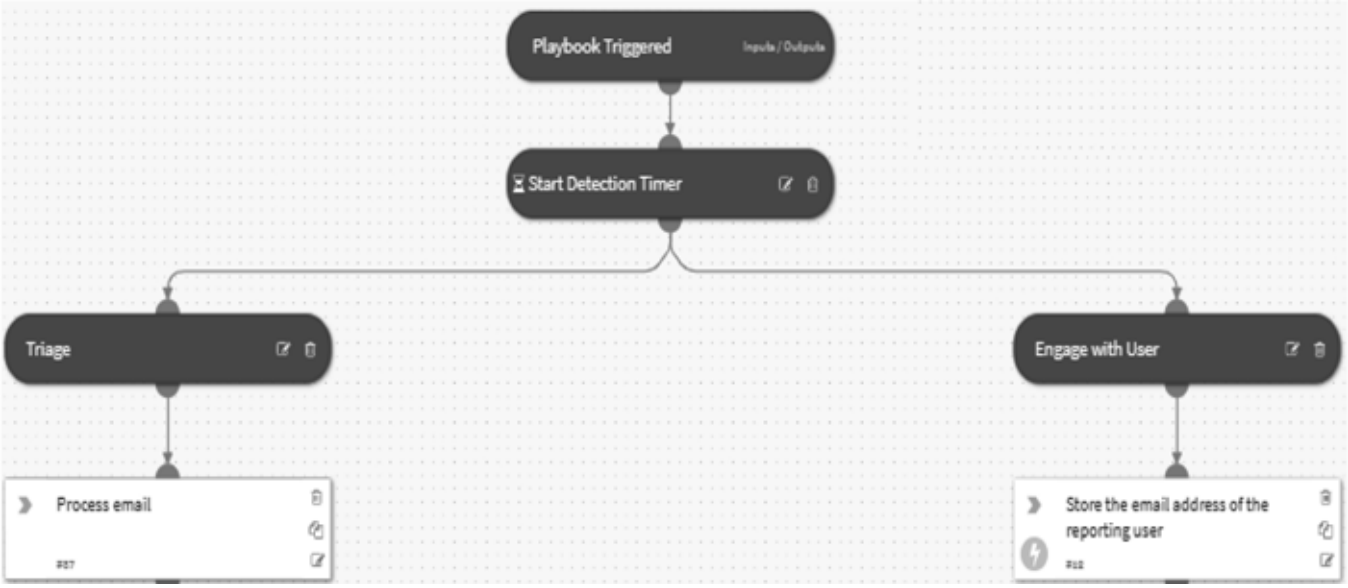


Phishing Playbook:

Triage and Engage

When an employee sends suspected phishing email, it's essential to consider it as malicious until proven. Apprising the employee of the email receipt puts them at ease, and initial triage helps check the intensity of the phishing attack in question.

Steps: Save the employee email account that sent the alert and acknowledge. Enhance the account with details from Active Directory and add phishing email data to relevant context entities.



Extract Indicators

Kickstart initial investigation by extracting common indicators that help to break the phishing email down to constituent parts.

Steps: Extract the URL and IP address and from the phishing email.

Check Indicators

By enriching the extracted indicators with a reputation from integrated security tools, the analysts can provide the required context, and this is the first branch where indicator malicious are checked.

Steps: Enrich data with a reputation from sources like File, URL, and IP. Use conditional tasks to check if the malicious indicator was found.

Investigating False Positives

Many steps to be involved with a comprehensive check for false positives because the alternative is still far more malicious. The steps can be automated, which even increases the level of robustness while reducing analyst effort and manual effort.

Steps:

- If no malicious indicators were found on the initial check, run a check on Sandbox.
- If Sandbox results provide positive feedback, manually inspect the sender's domain distance to check closeness with the company's domains.
- If nothing suspicious found with the domain, check whether the hostname URL is altered or not.
- If the mail clears all the tests, conduct one final round of manual investigation and if needed, get another security analyst help.
- Close the investigation by sending an email to the employee in question marking the email as safe.

Responding to Verified Phishing Attempt:

The analysts must move to contain and respond to the threat immediately if the mail is flagged during the false-positive check.

This end-to-end response ensures that it not only respond to current attack but also possible of preventing knock-on attacks in the kill chain.

The email attachments should be investigated for further threats, and the attacks spread should be studied and condensed. The employees should be notified about the confirmed malice.

Steps:

- Send an email to the employee about the email is malicious and is being responded to.
- Search and delete all the phishing mail from other mailboxes.
- If the mail had an attachment and was extracted, ensure the extracted file is investigated for malicious Indicators of Compromise using the tools at your disposal.
- Close the investigation if there was no attachment.

SOAR providers:

Gartner mentions the following providers in their SOAR Market Guide: ATAR Labs, Ayehu, Cyberbit, CyberSponse, D3 Security, Demisto, DFLabs, EclecticIQ, IBM, Splunk, Rapid7, Resolve, ServiceNow, Siemplify, Swimlane, Syncurity, ThreatConnect, and ThreatQuotient.

Key Findings

01 The SOAR technology market aims to converge security orchestration and automation (SOA), security incident response (SIR) and threat intelligence platform (TIP) capabilities into single solutions.

02 SOAR functionality consolidates data sources, uses the information provided by threat intelligence feeds, and automates responses to improve efficiency and effectiveness. While traditional SIEM solutions can “say” something, those that incorporate SOAR can also “do” something.

03 Early adopters of SOAR technologies have been organizations and managed security service providers with mature security operations centers (SOCs) that understood the benefits of incorporating SOAR capabilities into their operations. However, use cases implemented by early adopters have not evolved over the last 12 months and are stuck in a rut, limiting the long-term potential for SOAR in security operations.

04 SOAR solutions are not “plug-and-play.” Even though solutions have a library of out-of-the-box use cases and integrations, buyers are reporting multiweek professional services engagements to implement their initial use cases, as every organization’s processes and technologies deployed are different.

05 Orchestration and automation are starting to be localized in point security technologies, usually in the form of predefined, automated workflows. This is not the same as a full-featured SOAR solution.

06 As per Gartner’s recommendation, Security and risk management leaders overseeing security operations should pr epare for their SOAR implementations by having a starting set of defined processes and workflows that can be implemented. Out-of-the-box plays, and integrations are a starting point but can rarely be implemented without some customizations.

Author Bio

Chetankumar Savalagimath has over 7+ years of experience in Information Security and Enterprise IT Security Operations, System Integration, Managed Services, Infrastructure Design & Architecture, and Technical Pre-sales. He is currently a part of the Infrastructure Management and Security Services business unit in Happiest Minds Technologies Pvt Ltd. He is responsible for designing, Engineering, offering solutions and pre-sales. he has wide-ranging interests in Security solution automation and Building Advanced Security operation center.

Varsharani Kallimath has over 5+ years of experience in Information security on a wide range of security tools and technologies. She is currently part of the Infrastructure Management and Security Services business unit in Happiest Minds Technologies Pvt Ltd. She is responsible for designing, engineering and developing solutions. She also is interested in Cyber Security forensics and Security automation.

Business Contact **business@happiestminds.com**

happiest minds
The Mindful IT Company
Born Digital . Born Agile

www.happiestminds.com

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transfor-mation 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 manage-ment 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 the U.S., UK, The Netherlands, Australia and Middle East.