Managed.sa

Cybersecurity Orchestrator

Digital Forensics and Investigations

Threat Intelligence

Managed Detection and Response (MDR)

Orchestrator

Operations Services

Managed.sa
Cybersecurity Orchestrator

Digital Forensics and Investigations

DFIR integrates two discrete cybersecurity disciplines:

Digital forensics, the investigation of cyberthreats, primarily to gather digital evidence for litigating cybercriminals; and incident response, the detection and mitigation of cyberattacks in progress. Combining these two disciplines helps security teams stop threats faster, while preserving evidence that might otherwise be lost in the urgency of threat mitigation.

Managed.sa
Cybersecurity Orchestrator

Key Features

1. Incident Identification and Triage

DFIR helps quickly identify and prioritize security incidents based on severity and impact.

2. Digital Evidence Collection and Preservation

Focuses on securely collecting and preserving digital evidence from compromised systems for legal or investigative purposes.

3. Root Cause Analysis

Uses forensic techniques to determine the origin, methods, and scope of an attack.

4. Containment, Eradication, and Recovery

Involves steps to isolate threats, remove malicious artifacts, and restore systems to a secure state.

5. Post-Incident Reporting and Documentation

Provides detailed reports on incidents, including the timeline of events, actions taken, and lessons learned.

Benefi ts of the service

01
Rapid Threat Mitigation
Helps organizations quickly respond to and contain threats, reducing the risk of widespread damage.

02
Enhanced Security Posture
Provides insights into vulnerabilities and weaknesses, allowing organizations to strengthen their defenses against future attacks.

03
Legal and Regulatory Compliance
Ensures that evidence is collected and handled in a way that supports legal actions and meets compliance standards.

04
Informed Decision-Making
Offers detailed forensic analysis, enabling businesses to make data-driven decisions about security improvements.

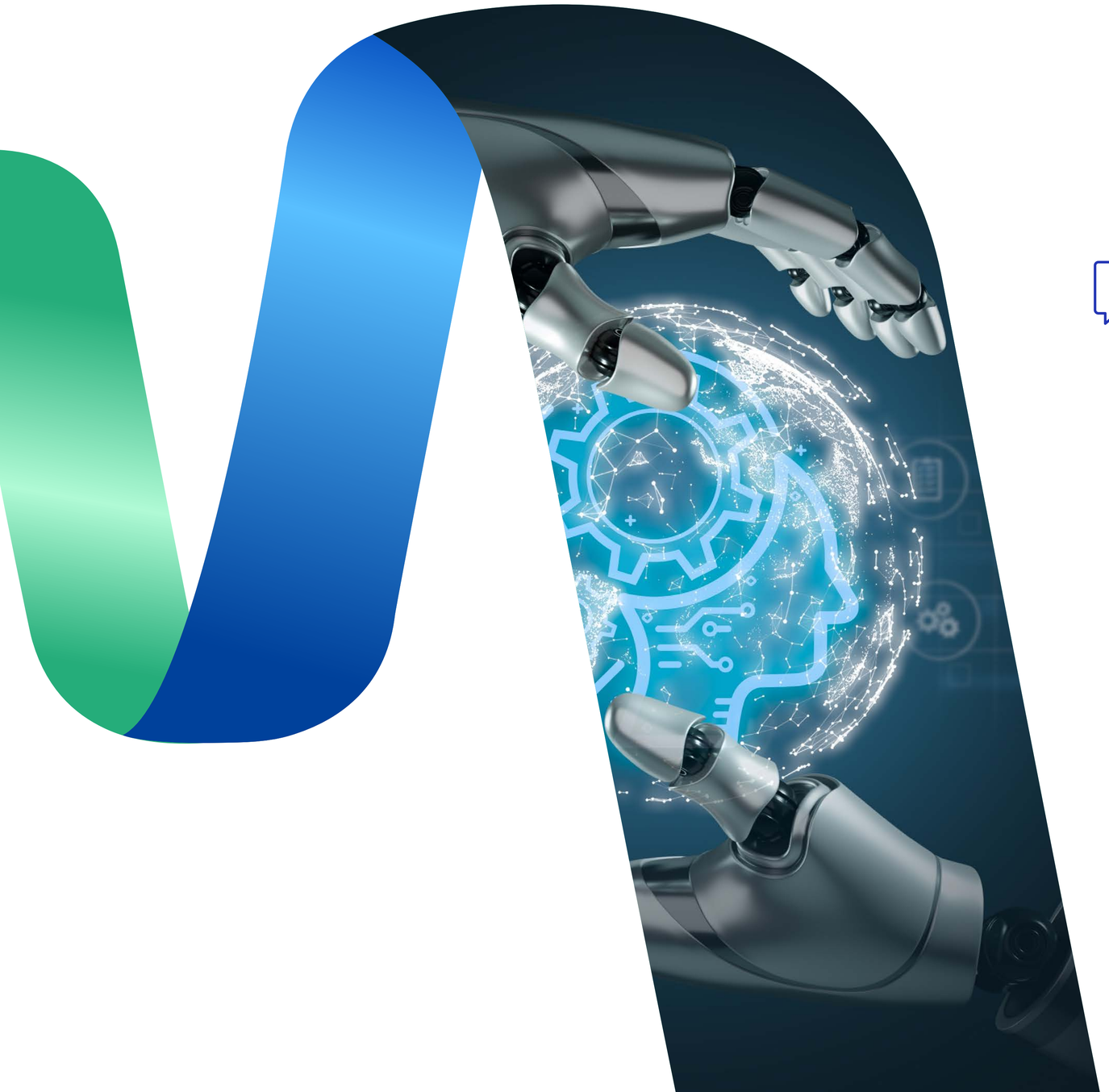
05
Minimized Business Disruption
By containing threats effi ciently, DFIR reduces operational downtime and helps organizations recover faster from cyber incidents.

Managed.sa
Cybersecurity Orchestrator

Who Should Use This Service?

All Organizations should use DFIR services. It’s essential for companies that need to quickly detect, respond to, and recover from cyber incidents, as well as those requiring forensic investigations for legal, compliance, or internal purposes. DFIR services are crucial for enhancing security resilience and minimizing the impact of cyberattacks.

Managed.sa
Cybersecurity Orchestrator



Threat Intelligence

Our Thread Intelligence service is designed to keep organizations ahead of cyber risks. By weaving together a rich array of open and closed sources, encompassing a wide array of evidence-based details about cyber-attacks, cybersecurity experts can learn from past attacks to better safeguard the future.

From zero-day exploits to phishing and man-in-the-middle attacks, insights into attack mechanisms and detection strategies reveal how various attacks could impact your business and provide actionable insights on defending against them.

Threat intelligence allows security teams to proactively defend against emerging threats and improve incident response, enabling them to take eff ective, data-driven actions to prevent cyberattacks before they occur. It can also help an organization detect and respond to attacks in progress faster.

Managed.sa
Cybersecurity Orchestrator

Key Features

1. Real-Time Data and Alerts

Threat intelligence provides real-time data and alerts on emerging cyber threats, vulnerabilities, and attack vectors.

2. Actionable Insights

Threat intelligence delivers actionable insights, offering context about threats such as attack methods, indicators of compromise (IOCs), and recommended mitigation strategies.

3. Threat Context and Attribution

Provides context around specific threats, including their origin, motivations, and potential impact, as well as attribution to specific threat actors.

4. Integration with Security Tools

Threat intelligence can be integrated with SIEMs, firewalls, and other security tools to enhance automated detection, correlation, and response.

5. Historical Data and Trend Analysis

Off ers access to historical threat data and analysis of long-term trends in the threat landscape.

Key Features

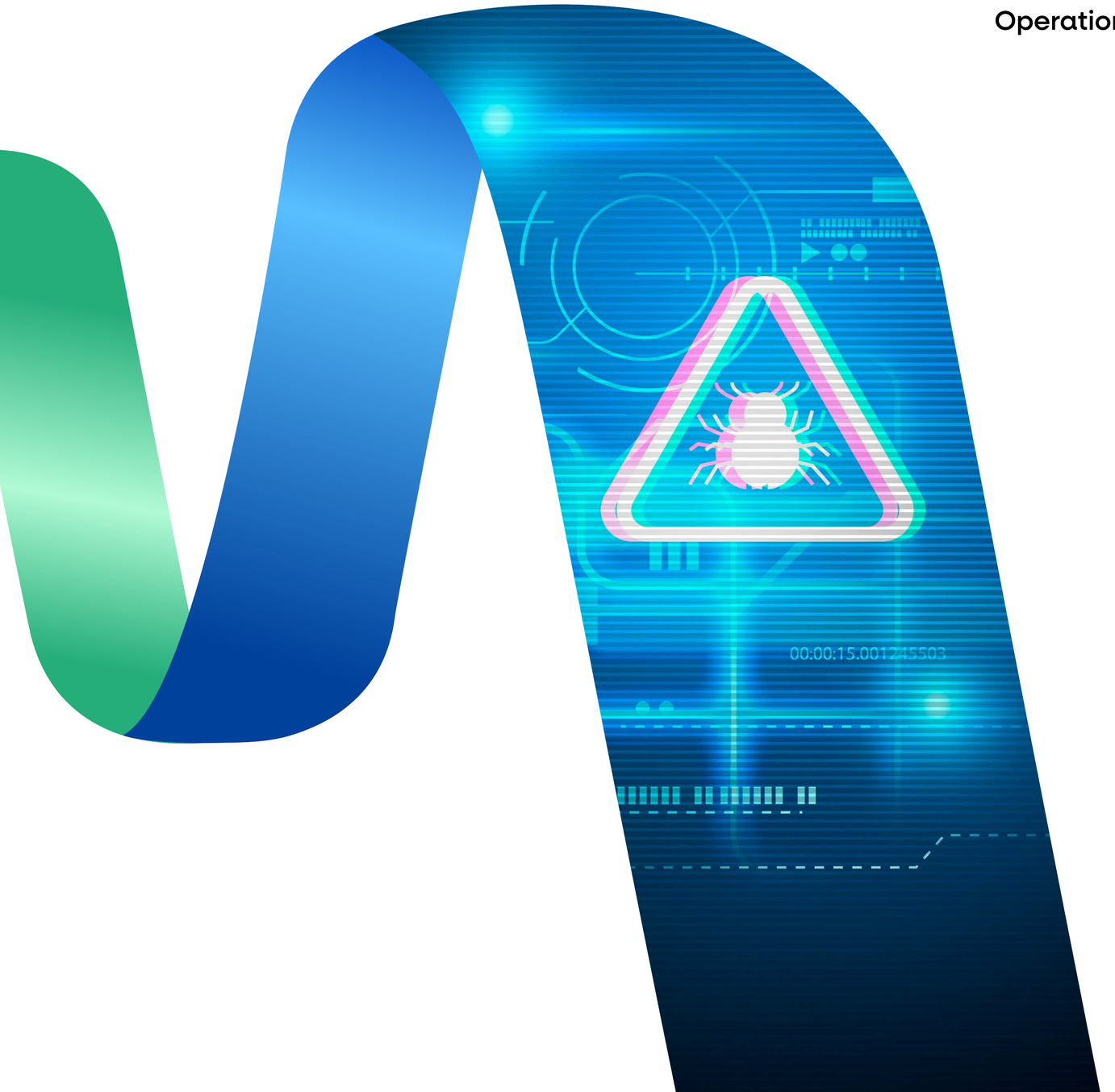
1. Enables organizations to stay ahead of potential attacks by responding to threats as they emerge, reducing the chances of compromise.
2. **Proactive Defense:** By off ering insight into emerging threats and trends, threat intelligence enables organizations to anticipate attacks and improve their overall security posture.
3. **Risk Reduction:** Informed decisions based on threat intelligence help minimize vulnerabilities and reduce the risk of successful attacks.
4. Helps security teams prioritize responses and implement targeted defensive measures, making their efforts more efficient and focused.
5. Enables organizations to better understand who may be targeting them and why, which can guide more strategic defenses and responses.
6. Automates threat detection and response processes, allowing for faster reaction times and reduced workload on security teams.
7. Helps organizations predict future attacks and vulnerabilities, allowing them to prepare more robust defenses and identify patterns in attackers' behaviors.

Managed.sa
Cybersecurity Orchestrator

Who Should Use This Service?

Organizations that have a sensitive structure should use threat intelligence to stay ahead of evolving cyber threats by gaining actionable insights, enabling proactive defense strategies, and reducing the risk of attacks. It enhances threat detection and incident response while improving overall security posture. Additionally, it helps prioritize and allocate resources effi ciently to mitigate the most critical risks.

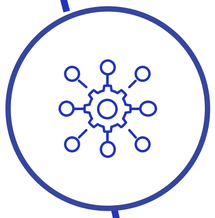
Managed.sa
Cybersecurity Orchestrator



Managed Detection and Response (MDR)

Managed Services MDR service provides 24x7 Threat Monitoring, Detection, and Response, leveraging a combination of advanced technologies, experienced analysts, Threat Intelligence, and human expertise in monitoring, investigations, and response.

Managed.sa
Cybersecurity Orchestrator



Managed Services supports its customers to achieve the following:

1. Proactive detection of attacks.
2. Limit damage of Cyber Attacks.
3. Improve security visibility and reporting through details monitoring.
4. Root Cause Analysis (RCA) of incidents.

MDR (Managed Detection and Response)

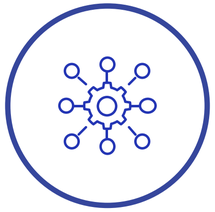
is an outsourced security service where a third-party provider handles threat detection, monitoring, and incident response on behalf of the organization, combining automated tools with human expertise for 24/7 security operations.

XDR (Extended Detection and Response)

is a security solution that integrates and correlates data across multiple security layers, such as endpoints, networks, and cloud environments, to provide unifi ed threat detection, analysis, and response. It enhances visibility and automates responses across an organization’s entire security ecosystem.

Managed.sa
Cybersecurity Orchestrator

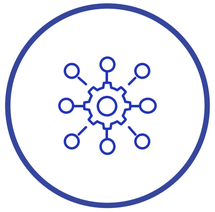
Operations • Orchestrator • **Managed Detection and Response (MDR)**



Key Features	MDR (Managed Detection and Response)	XDR (Extended Detection and Response)
Threat Detection and Monitoring	24/7 monitoring by a third-party provider using a combination of automated tools and human expertise.	Automated detection across multiple security layers (endpoints, network, cloud) using advanced analytics.
Response Capabilities	Human-driven response where security experts provide recommendations or directly remediate incidents.	Automated, integrated response actions across multiple layers, such as isolating endpoints or blocking malicious traffic.
Scope of Coverage	Focuses on specifi c environments like endpoints, networks, or applications.	Broader visibility across multiple layers (endpoints, networks, cloud, identity, etc.).
Integration with Security Tools	Can integrate with existing tools like SIEMs, EDR, and firewalls, but managed externally.	Natively integrates various security data sources (e.g., EDR, NDR, cloud) for a unifi ed view and response.
Data Correlation	Correlation of events may be limited to specific environments based on the scope of the service.	Correlates data across multiple security vectors (endpoints, network, identity, cloud) for comprehensive detection.
Management	Fully managed service, where a third-party provider handles detection and response.	Typically managed in-house or by security teams, with automation handling many detection and response tasks.
Visibility	Provides visibility into environments managed by the MDR provider.	Off ers deep, unifi ed visibility across multiple environments and security layers, all integrated into one platform.

Managed.sa
Cybersecurity Orchestrator

Operations • Orchestrator • **Managed Detection and Response (MDR)**



Benefits of the service	MDR (Managed Detection and Response)	XDR (Extended Detection and Response)
24/7 Threat Monitoring	Continuous, round-the-clock monitoring by security professionals, ensuring threats are detected and responded to quickly.	Always-on monitoring across multiple layers with automated alerts and responses.
Faster Incident Response	Human experts provide rapid response and remediation, ensuring threats are dealt with swiftly.	Automated response mechanisms allow for immediate containment and remediation across endpoints, networks, and more.
Scalability	Easily scalable for organizations without the need to hire additional security staff .	Scales across multiple security layers, providing a unifi ed view of threats with minimal manual intervention.
Customization	Can be tailored to the organization's needs with specifi c use cases, but largely managed by a third party.	Highly customizable, allowing organizations to defi ne their own detection and response rules across multiple environments.
Lower Internal Costs	Reduces the need for hiring and maintaining a full-time internal security operations team.	Reduces costs related to manual processes by leveraging automation, though it may require initial investment in tools.
Holistic Threat Visibility	Provides visibility into threats, although typically limited to specifi c environments like endpoints or networks.	Off ers deep visibility across all integrated security layers (endpoints, network, cloud), creating a more complete security picture.
Proactive Threat Hunting	Human experts actively hunt for threats based on intelligence and behavioral patterns.	Automated threat hunting identifi es suspicious behavior across multiple security layers without constant human

Managed.sa
Cybersecurity Orchestrator

Who Should Use This Service?

MDR is ideal for organizations that lack in-house security expertise and resources, and prefer to outsource their threat detection, monitoring, and incident response to a team of external experts. It's best suited for small to medium-sized businesses or companies looking for fully managed security services.

XDR is suited for organizations with established security teams and capability to deal with threat detection, monitoring, and incident response.

Managed.sa
Cybersecurity Orchestrator

Managed.sa
Cybersecurity Orchestrator

3273 Anas Ibn Malik - Al Sahafah Dist.
Riyadh 13321 - 8347
Kingdom of Saudi Arabia

+966 11 4185222

managed.sa