JIGHI MANAGED DETECTION AND RESPONSE (J-MDR)

Jighi Managed Detection & Response (J-MDR)

If your organization is looking to improve its computer incident response and cyber threat detection programs, **Jighi Managed Detection & Response (J-MDR)** is designed to be a cost-efficient way to achieve these goals.

WHY JIGHI MDR (J-MDR) IS THE FUTURE OF SOC?

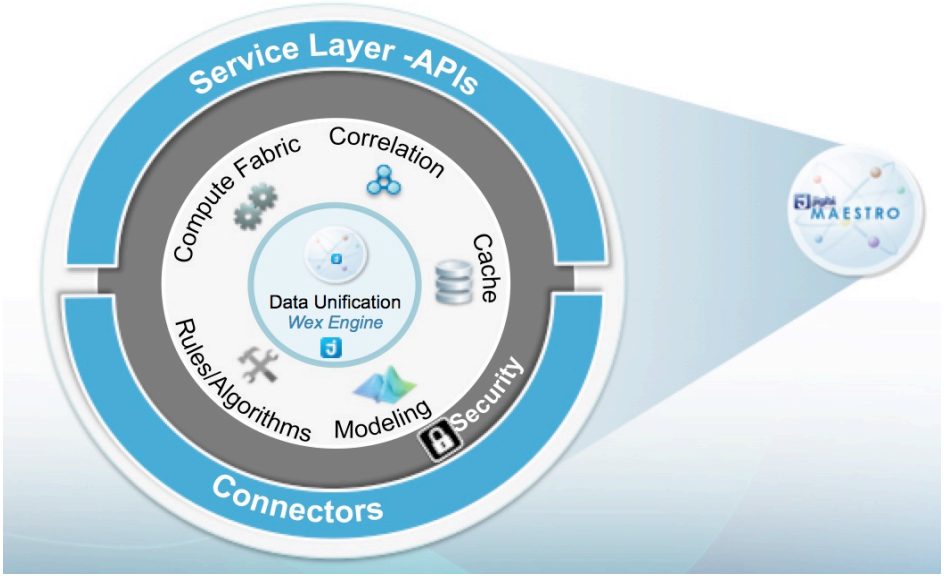
Security teams are always on the lookout to enhance their defensive capabilities against new and more potent cyber threats. However, Security Operation Centers (SOC) are failing to counter today's most innovative and dangerous threats: **targeted and unknown attacks**. J-MDR is an evolution of the standard SOC. It is adaptive and comport a machine-learning algorithm that adapts to new threats. In fact, our clients believe that J-MDR is a tectonic paradigm shift to a more robust approach to SOC deployment.

Targeted attacks are very different than last generation's most common cyber attacks. With targeted attacks, cyber criminals spend a greater amount of time exploring sophisticated attack methods to carry out long-term large-impact breaches. New malware and fresh attacker TTPs also go undetected by traditional monitoring SOC systems. Today, as the volume and sophistication of these new cyber threats grows, every organization must ask, "**Does my SOC detect and respond to targeted and unknown attacks?"**

JIGHI MANAGED DETECTION & RESPONSE (J-MDR)

VS.

OTHER MANAGED SECURITY SERVICES



Proprietary Component of J-MDR: Maestro Engine (J-Maestro)

1. Unlike most other managed security services, J-MDR is more focused on threat detection, rather **than compliance and standards.**

2. J-MDR services are delivered using the Jighi's own set of tools and technologies (J-Shield, J-Maestro, J-Central and

many other home grown modules. The tools are configured to guard Internet gateways and endpoints. They can also detect threats that have passed traditional perimeter security tools. Our methods and techniques vary depending on the customer's environment, needs and the threat landscape.

3. While some automation is used, Jighi Managed Detection and Response (J-MDR) is heavy on human's involvement to monitor networks round the clock. Humans also do analysis of security events and alert customers. Customers can expect to have direct interactions with our analysts rather than relying on a portal or a dashboard when it comes to alerting, investigating security events, case management, and other activities.

4. Jighi Managed Detection and Response service also perform incident validation and remote response. This means if you need to identify indicators of compromise, reverse engineer a piece of malware, or do some sandboxing, we'll be happy to let our innovative Enovise Lab dissect things for you.

DIFFERENCTIATED J-MDR OPERATIONAL FEATURES

Jighi Managed Detection and Response (J-MDR) may sound similar to other managed security services. But our customers say J-MDR is years ahead of the rest of managed security services or other SOCs. Below are some feature highlights:

- **Coverage**.

  With J-MDR services, we only work with event logs that our own tools provide. Managed security services can work with different types of event logs and contexts. The customer decides which of their security data is sent to the MSSP.

- **Compliance reporting.**

  If you need compliance reporting, go for a managed security service, as J-MDR does not do compliance reports. It focuses on protecting your asset and in our opinion; most standards and compliance are average.

- **The human touch.**

  One of the upsides of J-MDR offerings is that you get more human interaction with analysts. Managed security services mostly rely on portals and e-mail rather than direct communication (which can also be hacked).

- **Incident Response.**

  With J-MDR, you do NOT need a separate retainer if you want on-site incident response. Remote incident response is usually included in what you pay for the basic service. This is not true for many managed security services, where you need separate retainers for both onsite and remote incident response.

Advanced Jighi proprietary tools and artificial Intelligence enhance both Jighi and Enovise's team threat visibility.

A jighi security division

Meet us for a demo at Africa Cyber Security Conference