Managed Detection and Response (MDR)

Power up your defence mechanisms and stay ahead of the game! We provide round-the-clock guardrails to thwart intrusions and deliver uncompromised security - be it on-premise, mobile, cloud or edge.

A cyber attack can shake up your enterprise. With the modern-day hybrid infrastructure, boundaries are fluid, making it easier for hackers to gain backdoor entry, lie low, and remain hidden until they wreak havoc. It is critical that enterprises augment their cyber security with an advanced solution for dedicated 24x7 threat detection & response, to protect themselves from next-gen attacks.

Why move away from the old time-tested approach?

Traditional SIEM-based security monitoring is reactive, cannot provide the extensive coverage, analysis and maturity needed to handle the complexity of modern security breaches, and also does not address several significant problems that plague enterprises today.

How is Managed Detection and Response (MDR) any different?

Managed Detection & Response is a proactive approach that comes with a comprehensive set of security defense components starting from monitoring, threat intelligence, threat hunting to intelligent incident analysis and response.

Key challenges that MDR services address

- Access to skilled threat hunters, analysts & incident responders, to augment security team
- Evolved capabilities in contextualizing and analyzing incidents of compromise
- Advanced expertise in deep diving into logs, extensive threat research and forensics capabilities
- Expert recommendations to improve security posture

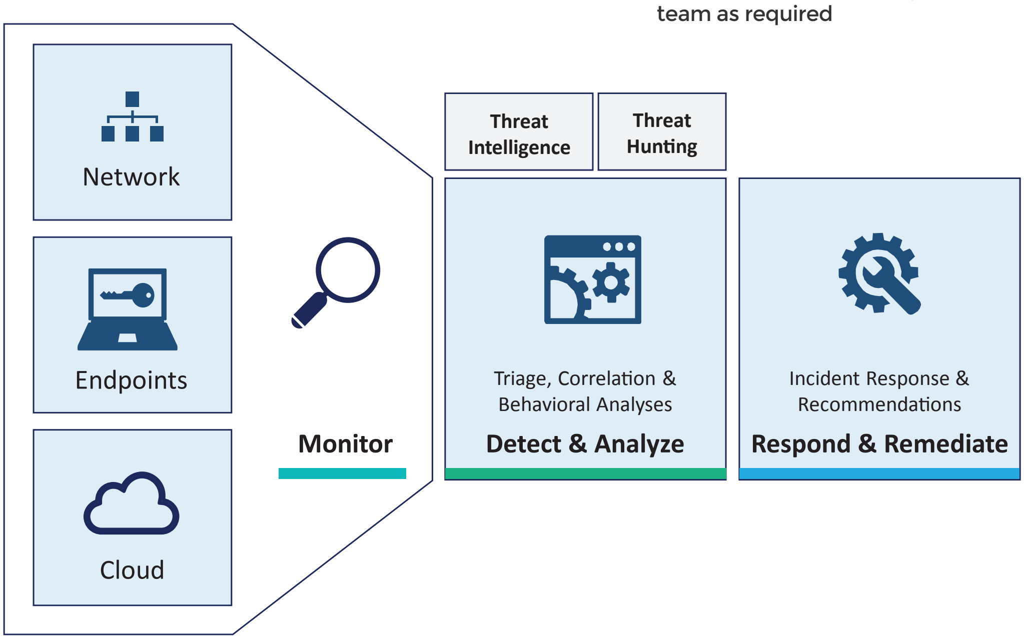
The GAVS Approach

Speed is key to immunize networks, systems & data against cyber threats, and to protect from financial & reputational loss.

GAVS' MDR service augments the capabilities of cutting-edge security solutions with an artificial intelligence-driven, integrated security approach that provides greater visibility of threat vectors across the IT landscape, constant monitoring, proactive detection, alert prioritization and accelerated incident response.

The Differentiators

- 'Follow the Sun' global delivery model
- Over 8 years of experience in frontline security operations
- 24x7 monitoring, with cyber experts available across all time zones
- Choice of flexible support hours
- Automation platform with playbooks and response workflows
- Red team well versed in the latest cyber kill chains
- Security analysts with deep domain expertise & rich consulting experience
- Curated industry-specific threat intelligence
- Periodic reviews and proactive identification of gaps & remediations to security posture
- Extended support through the Security COE team as required



MONITORING

Our analysts perform round-the-clock alert monitoring and analysis, with massive scalability to adapt to spikes in threat volumes. We use the monitoring features of our leading edge AIOps Platform Zero Incident Framework™ (ZIF), but can also leverage any in-house AI-based monitoring solution, and fine-tune suitably to the baselines & challenges evidenced in the environment.

Landscape

We use follow-the-sun approach, and have cyber experts spread across several time zones to provide 24x7x365 coverage to global customers. All areas of the infrastructure are monitored, including networks, systems, applications, cloud and accesses.

Unique Use Cases to reduce false positives

Based on the organizational context and risk landscape, specific monitoring use cases are developed. Leveraging this context, we look at type and usage of assets, user behavior and asset criticality to arrive at custom use cases, thereby reducing false positives.

Technology

Leveraging our security COE, and partnerships with some of the leading SIEM & Cyber Defense vendors, our team can sharpen existing systems or solutions being used at the enterprise.

DETECTION & ANALYSIS

The team of cyber security experts detects intrusions and conducts static & dynamic analyses to examine a sample's behavior. The team analyzes each of the steps in the expanded kill chain model, and builds capabilities to detect and mitigate attacks within each of the steps. Behavior analysis is done by dedicated SOC analysts who understand the environment's unique characteristics. Innovative techniques are used to identify real threats, and expert recommendations are provided to eliminate them. Threat Hunting and Threat Intelligence complement the Detection & Analysis phase.

Threat Hunting

Our threat hunting experts go beyond log sources, and proactively investigate the enterprise infrastructure to identify potential compromise, or for a breach activity that a hacker might initiate at a later stage. They use manual and automated approaches to look for suspicious actors that bypass security controls.

Internal

Use of machine learning models to detect anomalous behavior across endpoints, applications, networks, & user behavior, and for cyber kill chain mapping.

External

Integration of vulnerability intelligence, client specific threat intelligence, and global knowledge base of adversary tactics & techniques, to identify evidence of compromise.

On signs of a potential anomaly, our cyber hunters act immediately to inform the response team & collaborate with them for mitigation.

Global Threat Intelligence

Client Specific Threat Intel

Data
(network, apps, endpoints, users)

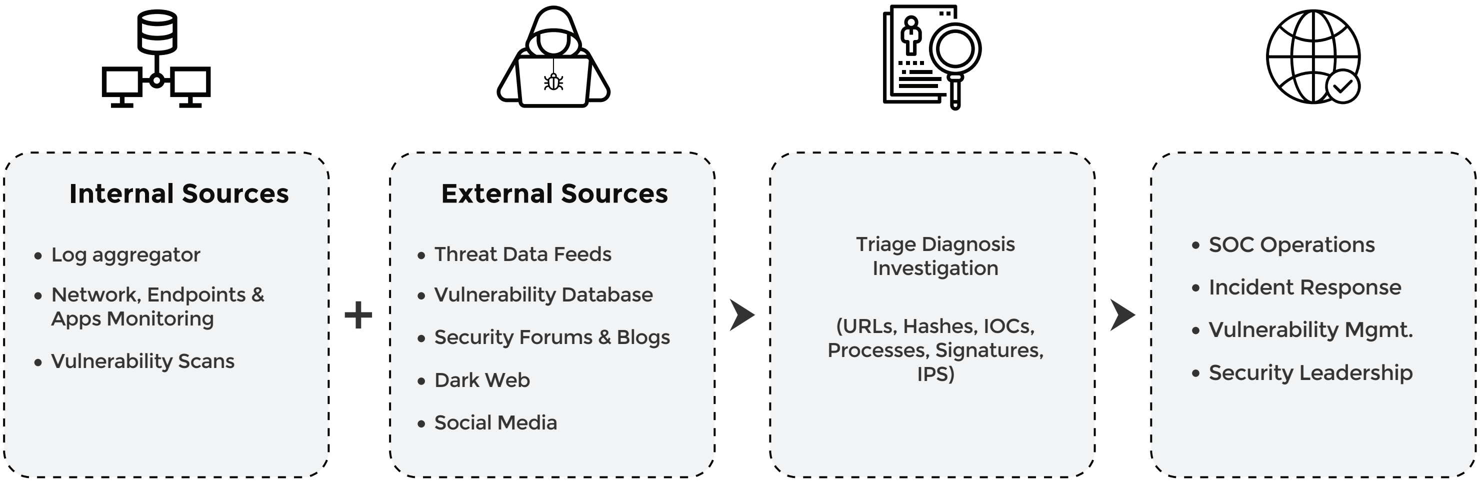
Other Data
(MITRE ATTACK, Crown Jewel Analysis)

Threat Intelligence

Our Threat Intelligence service helps accelerate detection of anomalous activity with proprietary threat intelligence, specific to the enterprise's threat landscape. Threat intelligence aggregation data is produced from various validated threat sources sharing Indicators of Compromise (IOC) information.

Analysts then enrich internal alerts with this external information and context, thereby accelerating triage, scoping, and containment of the incident.

The threat intelligence team analyzes and synthesizes data to determine the actors that are specifically targeting the organization, or its executives. The data obtained is used in conjunction with Security & IT technologies, for rapid response and mitigation of threats.



Internal Sources

- Log aggregator
- Network, Endpoints & Apps Monitoring
- Vulnerability Scans

+

External Sources

- Threat Data Feeds
- Vulnerability Database
- Security Forums & Blogs
- Dark Web
- Social Media

Triage Diagnosis Investigation

(URLs, Hashes, IOCs, Processes, Signatures, IPS)

- SOC Operations
- Incident Response
- Vulnerability Mgmt.
- Security Leadership

RESPONSE & REMEDIATION

GAVS provides 24x7 incident response coverage by bringing together the automation and remediation features of the ZIF AIOps Platform, and a team of seasoned incident responders with rich response experience in major breaches. They can rapidly investigate, contain the attack and take remedial measures, working in tandem with the enterprise's IT team. ZIF automation features include workflows and playbooks for routine aspects of incident management, triaging and response.

We work with enterprises to assess and handle each incident uniquely, while minimizing the impact of a breach. Our elite team of cyber responders perform in-depth analysis to find forensic evidence, determine scope of incident, identify the extent of impact, find systems that have been compromised, and develop an effective threat mitigation strategy for swift containment and remediation based on the attacker's activities. The team also devises strategies to improve the security posture of the enterprise and formulate tailored incident management and response plans to prevent impact from future threats.

GAVS

GAVS Technologies is focused on automation-led digital transformation services. GAVS' IP led solution, Zero Incident Framework™ is an AIOps solution that enables organizations to trend towards a Zero Incident Enterprise™.

For more information on how GAVS can help solve your business problems, write to inquiry@gavstech.com

www.gavstech.com