Product Sheet

Managed Detection Response (MDR) Service

PROTECT | DETECT | RESPOND | REMEDIATE

The corporate perimeter is melting and remote work is the new normal. The technology threat landscape is becoming more sophisticated which calls for more advanced cybersecurity skills. To address this need, an end-to-end and comprehensive threat monitoring and response solution to protect customers from any kind of cyberattacks is required; hence, we developed **AGIL Managed Detection and Response (MDR) Service**. It comprises of a modern, 100% managed Cloud Security Operations Centre (SOC) with AI infused automation playbooks and remediation methods driven by **XDR*** and **SIEM#**.

8 KEY BENEFITS

1. Simplified visualisation of complex attacks and understanding of how they progress across a kill chain
2. Automated response capabilities that can help block attacks in progress
3. Improvement of mean time to detect and/or mean time to respond
4. Aggregation and correlation of security data from multiple security controls and sources

5. Single solution by consolidating multiple security tools into a single threat detection and response solution
6. Advanced analytics that can detect and identify modern, sophisticated attacks
7. Reduction in the number of escalations to higher-skilled security analysts
8. Prioritisation of security incidents based upon severity of attack and proximity to critical business assets

Business Benefits

- Maximise ROI: Reducing the 24/7 round year in-house operating costs by providing a fully managed service.
- Single Pane of glass: Proprietary CISO dashboard which provides the view of the Security Posture across products and platforms.
- Data Ownership: Data and security alerts stay in customers' cloud environment.
- Automation: Advanced automated detection and response with our custom playbooks
- Break Security Data Silos: Bring all the security data into a single solution
- Reduce Complexity: Filtering the noise out of alerts for better security investigations using built-in ML and AI
- Fast, seamless deployment: Offering provides a FastTrack onboarding of XDR and SIEM for customers providing better value for investment

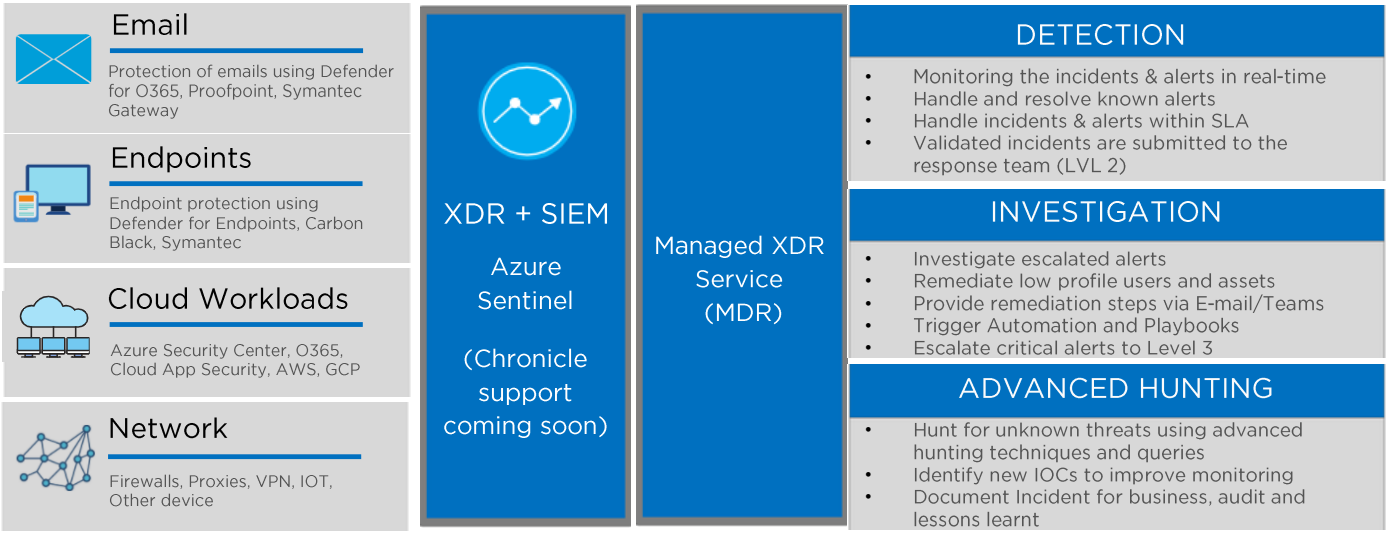
***Cross-layered detection and response (XDR)** collects & automatically correlates data across multiple security layers – email, endpoint, server, cloud workloads, and network. XDR enables faster threat detection so that our security analysts are able to respond rapidly, leading to significantly lower investigation & response times.

#Security Information and Event Management (SIEM) is a software solution that aggregates and analyses activity from many different resources across your entire IT infrastructure. SIEM collects security data from network devices, servers, domains &

ST Engineering Mission Software & Services Pte. Ltd.
www.stengg.com/cloud

DOP 0221

HOW IT WORKS



WHAT WE OFFER

FEATURES	BASIC	PREMIUM
Threat Detection & Response with a 1 hour SLA for Critical incidents	✓	✓
Threat Remediation to resolve threats in the organisation	✓	✓
Threat Hunting for proactively searching for cyber threats that are undetected	✓	✓
Microsoft XDR Deployment and configuration by ST Engineering experts	✓	✓
Basic Playbook Library onboarding for SOAR	✓	✓
Basic Data Connector Onboarding to Azure Sentinel	✓	✓
Ongoing monitoring and analysis with regular reporting (24x7)	✓	✓
CISO Dashboard as a single pane of glass for visibility across security products & different Cloud environments	✓	✓
Custom Incident Response Action Playbooks as per organisational requirements		✓
Connect data from Threat Intelligence providers into Sentinel		✓
Advanced Data Connector Onboarding from multiple sources		✓
On-Demand Premium & Advisory Support from our Cloud cyber-consulting team		✓

Detecting Attacks Fast

We see MDR as a potential path to helping our customers detect, identify, and understand complex attacks across the kill chain. This means investing in a solution with simplified visualisation across the attack chain, and advanced analytics capable of correlating signals from many sources. Organisations need automated response capabilities. This will be especially effective if there are solutions, which can block attacks and update rule sets across endpoints, networks, servers, and cloud-based workloads. With our AGIL MDR solution, we enable our customers to detect attacks fast and enable remediation with world-class automation.

Get Started with AGIL MDR today

Contact us at cloud@stengg.com for more details

We are a leading Cloud & cybersecurity services company with a strong focus on combating the newer cyber crimes and attacks across on-premise and hybrid infrastructures. As a Microsoft Gold Partner, AWS Advanced Partner, Google Cloud Premier Partner and a trusted advisor for Government & Enterprise organizations for Cloud & cybersecurity services, we power drive organisations with end-to-end cloud services. For more information please visit www.stengg.com/cloud

ST Engineering Mission Software & Services Pte. Ltd.
www.stengg.com/cloud

DOP 0221

ST Engineering