Kloudynet Managed Detection and Response (MDR) Service

Mission

Corporate perimeter is melting, and remote work is the new normal. The threat landscape is becoming more sophisticated and hence more advanced cybersecurity skills are required. Our Mission is to provide an end-to-end and comprehensive threat monitoring and response to protect customers from any kind of cyberattacks. We deliver a modern SOC with AI infused automation playbooks and remediation methods.

XDR + SIEM BENEFITS

Simplified visualization of complex attacks and understanding of how they progress across a kill chain

Automated response capabilities that can help block attacks in progress

Improvement of mean time to detect and/or mean time to respond

Aggregation and **correlation** of security data from multiple security controls and sources

PROTECT | DETECT | RESPOND | REMEDIATE

Single solution by consolidating multiple security tools into a single threat detection and response solution

Advanced analytics that can detect and identify modern, sophisticated attacks

Reduction in the number of escalations to higher-skilled security analysts

Prioritization of security incidents based upon severity of attack and proximity to critical business assets

Business Benefits

- **Maximize 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 Kloudynets custom playbooks
- **Security Data in Silos:** Bringing 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

Email
Protection of emails using Defender for O365, Proofpoint, Symantec Gateway

Endpoints
Endpoint protection using Defender for Endpoints, Carbon Black, Symantec

Cloud Workloads
Azure Security Center, O365, Cloud App Security, AWS, GCP

Network
Firewalls, Proxies, VPN, IOT, Other device

XDR + SIEM
Azure Sentinel

Kloudynet
Managed XDR Service (MDR)

DETECTION

- Monitoring the incidents & alerts in real-time
- Handle and resolve known alerts
- Handle incidents & alerts within SLA
- Validated incidents are submitted to the response team (LVL 2)

INVESTIGATION

- Investigate escalated alerts
- Remediate low profile users and assets
- Provide remediation steps via E-mail/Teams
- Trigger Automation and Playbooks
- Escalate critical alerts to Level 3

ADVANCED HUNTING

- Hunt for unknown threats using advanced hunting techniques and queries
- Identify new IOCs to improve monitoring
- Document Incident for business, audit and lessons learnt

Detecting Attacks Fast Using XDR + SIEM

We see XDR and SIEM 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 visualization across the attack chain, and advanced analytics capable of correlating signals from many sources. Organizations need automated response capabilities. This will be especially effective if XDR and SIEM solutions can block attacks and update rule sets across endpoints, networks, servers, and cloud-based workloads. With our XDR and SOC solution, we enable our customers to detect attacks fast and enable remediation with world-class automation

FEATURES	BASIC	PREMIUM
Threat Detection & Response with a 1 hour SLA for Critical incidents	✓	✓
Threat Remediation to resolve threats in the organization	✓	✓
Threat Hunting for proactively searching for cyber threats that are undetected	✓	✓
Microsoft XDR Deployment and configuration by kloudynet 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	✓	✓
Custom Incident Response Action Playbooks as per organizational requirements		✓
Connect data from Threat Intelligence providers into Sentinel		✓
Advanced Data Connector Onboarding from multiple sources		✓
On-Demand Premier & Advisory Support from our cybersecurity consulting team		✓

Getting started with Kloudynet

Kloudynet Technologies | +6 03-27807408 | sales@kloudynet.com

Kloudynet is a leading cybersecurity services company with a strong focus on combating the newer cyber crimes and attacks across on-premise and hybrid infrastructures. Kloudynet is a Microsoft Gold Partner and a trusted advisor for large enterprise organizations for cybersecurity services. For more information go to www.kloudynet.com

Gold Microsoft Partner