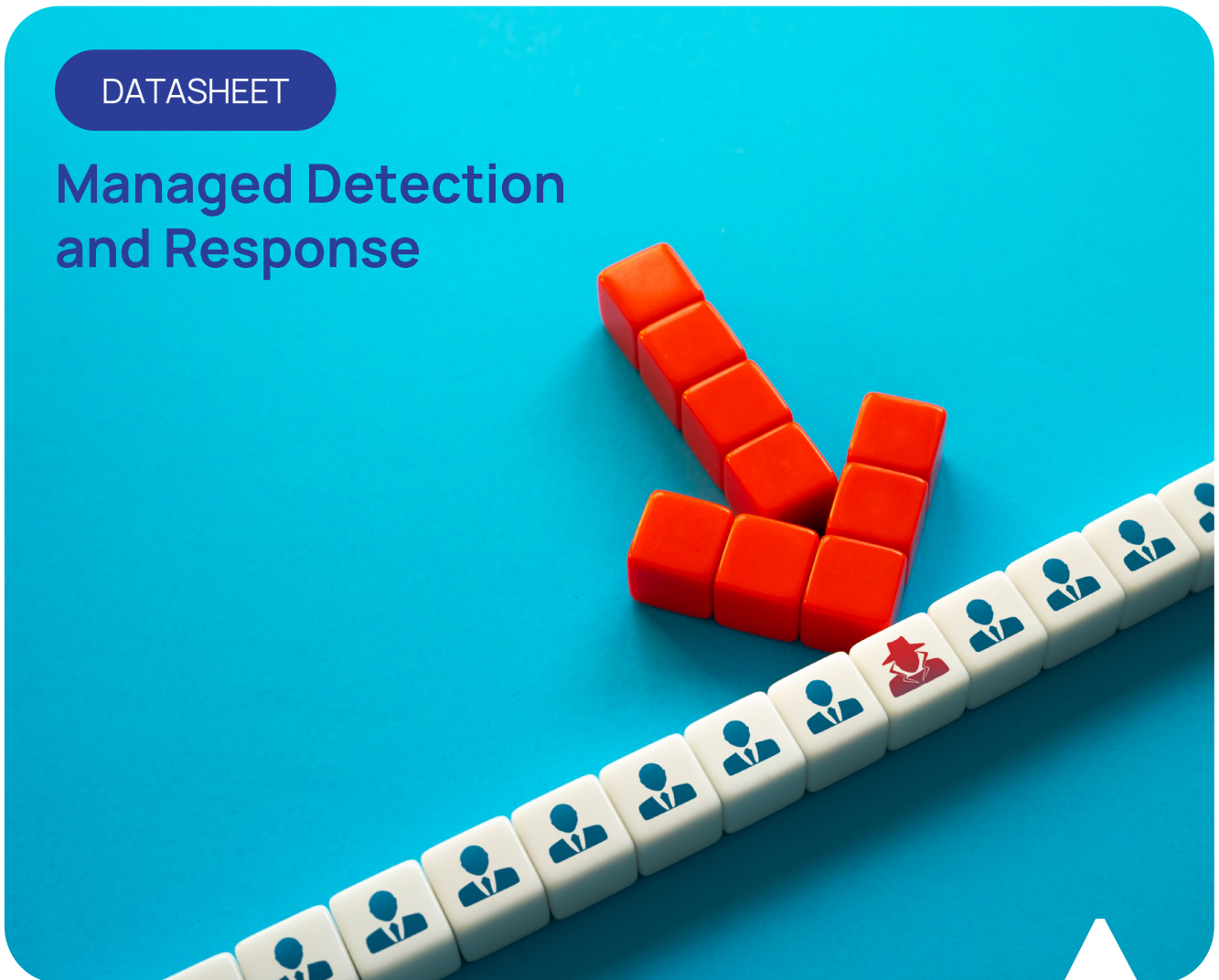


DATASHEET

Managed Detection and Response



Cybersecurity Challenges in the AI/ML Era

Today's organizations face complex cybersecurity challenges threatening their digital assets and operations. Also, the landscape is rife with factors hindering robust cybersecurity programs' establishment. Some of the main cybersecurity challenges that enterprises face are:

- **Alert fatigue-** Too many alerts often overwhelm cybersecurity teams making the security posture vulnerable.
- **Skill gap-** Finding specialists for roles like incident response and cloud security is tough, leaving organizations with a skills deficit. There are 490,513 open cybersecurity roles that take 21% longer to fill than other IT jobs.
- **Inadequate cybersecurity-** Building a strong cybersecurity program requires substantial investment toward tools, licenses, and personnel. Most organizations depend on lean security teams that lack incident handling procedures.
- **Delayed threat detection-** Cyber threats often remain undetected for extended periods, escalating the damage and cost for organizations. It takes 90 days to uncover a security incident, unless detected.
- **Detection of advanced threats-** Traditional cybersecurity struggles against sophisticated threats, such as advanced persistent threats (APTs).

Managed Security Services for Advanced Threat Detection and Response

NuSummit Cybersecurity provides complete managed security services to help organizations strengthen their security and stay safe from advanced threats. Our Managed Detection and Response (MDR) solution includes threat intelligence, proactive threat hunting, continuous security monitoring, simulated attack exercises, incident tracking, and thorough incident analysis and response capabilities. Central to our offering is a SOC led by experienced professionals, known as the NuSummit Cyber Defense Center (CDC). The CDC delivers round-the-clock managed threat detection and incident response to safeguard your enterprise from emerging threats and ensure regulatory

NuSummit Cybersecurity CDC



Automated Incident Response and Forensics



Event analysis



Automated incident responses



Anomaly detection



Incident retainers



Digital forensics



Evidence gathering



Endpoint Detection and Response



Security orchestration



Automated incident response



Threat Management



Dark web monitoring



Threat intelligence



Threat hunting



Offensive Security



Red teaming



Breach assessment



Dark web monitoring



SIEM Implementation and Engineering



Assisted SIEM deployment



New use-case development



SOC maturity assessments



Actionable Reporting



Trend analysis



Business impact reports

NuSummit Cybersecurity MDR Services

NuSummit Cybersecurity offers Managed Detection and Response services (MDR) and co-managed services that can help you improve your security posture and reduce your risk of a cyberattack. We offer two types of SOC services:

NuSummit Cybersecurity delivers turnkey security monitoring through a Security-as-a-Service (SECaaS) framework ensuring smooth deployment and management. Industry leading SIEM, EDR, and UEBA solutions are integrated into our offering to provide 360° visibility into your IT environment.

We can include software licenses into our services to create pricing efficiencies, without

compromising on quality. Our simplified scaling options eliminate the need for architectural changes, allowing easy accommodation of your enterprise's growing needs. Also, our flexible data retention schemes allow you to choose the retention period that is right for your organization. Rest assured; your data remains under your control.



NuSummit Cybersecurity Co-Managed Services

Our co-managed security services are a cost-effective way to access the benefits of MDR and elevate your existing setup without giving up control of your security ecosystem.

NuSummit Cybersecurity's security professionals will manage and operate your SIEM tools, technologies, appliances, and licenses, while you retain ownership of your licenses and subscriptions. This lets you focus on your core business while we take care of your security needs. We offer dedicated VM/Cloud instances strategically positioned within your environment or Azure instances for added security.

NuSummit Cybersecurity managed security services feature:

Co-Managed Services

Pre-existing SOC transition, optimization and operations

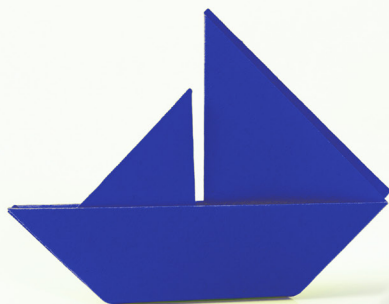
- Pre-existing setup review
- Threat modeling
- Team onboarding
- Use case tuning and playbook creation and uplift
- Ongoing operations

New SOC implementation and operations

- Business requirement and objectives
- Infra setup and license allocation
- Threat modeling
- SOC engineering
- SOC team onboarding

MDR

- Requirements gathering workshop
- Team onboarding
- Tech system discovery
- SLA-based governance reviews
- Ongoing operations



Key Highlights



Continuous Monitoring and Insights

- 24x7x365 monitoring, baselining, and anomaly detection.
- Yearly, quarterly, and monthly threat-con reviews.
- Single pane visibility through in-depth dashboards.
- Industry-specific curated threat intelligence for anomaly detection and use-case enrichment.



Enhanced Threat Readiness

- Situational awareness through threat modeling and threat hunting.
- Maintenance and operation of security monitoring infrastructure.



Streamlined Visibility and Management

- CXO assurances through KPIs and real time cybersecurity posture of an organization.
- Managed XDR or MXDR with optional perimeter firewall management and 24x7 engineer reachability.
- 24x7 support by chat/call.



Regulatory and Compliance Assurances

- Incident response aligned to NIST Cybersecurity Framework.
- Incident handling – Identify, protect, detect, respond, and recover.

Tailored MDR Solutions to Meet Your Needs: Service Packs

We offer three MDR service packs to meet the unique cybersecurity needs of your enterprise:

	Armor 1	Armor 2	Armor 3
Cybersecurity Strategic Workshop Yearly security assessment and benchmarking.			✓
Recovery and Resilience Monitoring and reporting of backups [frequency, size, last tested date]. Readiness procedures and policies.			✓
Cybersecurity Asset Management Inventory of cybersecurity control systems and critical systems capturing controls, gaps and risk.			✓
Network Vulnerability Scans and Penetration Testing Identify weaknesses in network configuration, key applications, and systems.		✓	✓
User-Centric Security Managed security awareness, phishing resilience, and multi factor authentication.		✓	✓
Dark Web Reputation Monitoring Real time alerting and scanning of thousands of internet dark web locations for stolen credentials or data.		✓	✓
24x7 Managed Endpoint Detection and Response Setup endpoint protection of core systems and compute endpoints, setup thresholds and auto containment.	✓	✓	✓
24x7 Managed SIEM and SOAR Setup log monitoring covering business critical systems, supporting infra and security system. Automated response plays based on MITRE framework.	✓	✓	✓
Remediation assistance, and Cybersecurity Tech Stack Management Provide actionable reports for fixing security issues, and managing cybersecurity technologies – tuning log sources, policy management for firewalls, among others.	✓	✓	✓
Security Analytics Dashboards and reports for showing solution effectiveness, recovery readiness, blocked threats, key risks, and upcoming actions.	✓	✓	✓

Why MDR?



Reduced noise in your environment and cost of ownership.



Easy adoption of services such as EDR, UBA, and threat modeling as your program evolves.



24x7 security coverage and geo-redundancy with SOC's in India and MEA.



Functional Security Operational Center (SOC) within 2 weeks.



Mature processes and controls including ISO 27001, ITIL Service Management, NIST Cybersecurity.



15+ years of global experience in managing mission critical SOC's for different industry verticals.

250+

MDR team

20+

MDR SIEM technologies

100+

MDR Clients

15 yrs

of service excellence

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at cybersecurity.nusummit.com or write to us at cybersales@nusummit.com.

**Dallas | Jersey City | Cupertino | Ottawa | Riyadh | Dubai
Mumbai | New Delhi | Bangalore**

© NuSummit Cybersecurity Limited. All rights reserved.

All trademarks, logos and brand names are the property of their respective owners.
All company, product and service names used are for identification purposes only.
Use of these names, trademarks and brands does not imply endorsement

Follow us at:   