# OMDR

A Service That Helps You Test Your Cybersecurity and Put That Learning to Strengthen Your Cybersecurity Posture

## *Invinsense Offensive Managed Detection and Response*

Cybersecurity is a continuous journey as attacks are a continuous process. This journey starts with having cybersecurity solutions that act as basic hygiene and provide preventive cybersecurity. Then comes detection and prevention, threat hunting and solutions and people needed for it. Once everything is done, organizations achieve a certain cybersecurity posture. Majority of the organizations stop here and a few go totest their cybersecurity posture, and very rare an organization goes beyond that and put its cybersecurity to continuous testing and implementing those results in achieving a cybersecurity posture that is dynamic and in response to the environment.

Invinsense Offensive Managed Detection and Response helps organization to test their cybersecurity tools, people and

processes with the help of our elite Red Team that thinks and acts like attacker. Red team who manages Invinsense MDR will help your cybersecurity to observe the entry of adversaries, lateral movements, attack paths and weaknesses in ITsystems and networks.

Invinsense OMDR leverages Continuous Automated Red Team (CART), RedOps, Breach & Attack Simulations (BAS), DevSecOps and Vulnerability management tools to provide you continuous cybersecurity posture to help you combat cyberattacks24x7 and provide you insight of your current minimumtime to detect (MTTD) and minimum time to responds (MTTR).

| Redops & CART | Breach & AttackSimulation | Vulnerability Management |
|---|---|---|
| › Production Environment | › Simulated Environment | › VAPT NSAR <br> › Automated Manual Testing <br> › Cloud Security Posture Appsec <br> › Static-Dynamic |

## Invinsense OMDR- Features, Deliverables and Team

| Features | Deliverables | Team |
|---|---|---|
| o Application Security Assessment | o Dynamic Security Testing | o Red Team |
| | o Static Code Analysis | |
| | o DevSecOps Process | |
| | o Web, Mobile, API | |
| o Vulnerability Assessment & Penetration Testing | o Container / Micro Services Security Testing | o Red Team |
| | o VAPT for entire infrastructure, Cloud Components | |
| | o VAPT in case of critical incident detection | |
| | o VAPT on every new product / module release | |
| | o Detailed report to be furnished to Clientmanagement on every VAPT | |
| | o Security Testing for each release | |
| o Breach and Attack Simulation | o Advanced Phishing Attack Simulation | o Red Team |
| | o Advanced malware Attack Simulation | |
| | o API Security Attack Simulation | |
| | o Database Security Simulation | |
| | o Advanced Wireless Security Testing | |
| | o Targeted User attack simulation | |
| o Red Teaming Exerciseand Automation | o Reconnaissance / information Gathering | o Red Team |
| | o Active Reconnaissance / Covert Observation | |
| | o Attack Planning and Pretexting | |
| | o Exploitation | |
| | o Post Exploitation | |
| | o Reporting | |

# Purchasing

| Unit | SKU | Description |
|---|---|---|
| Invinsense OMDR | IC ICPL-INV-OMDR-0109 | Invinsense Of Managed Detection and Response |

**About Infopercept** - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support

Infopercept | INVINSENSE