MDR

Invinsense Managed Detection and Response

Adversaries are getting organized to launch sophisticated attacks. The scale and volume of these attacks prove that there is stopping of adversaries from entering any organization. Preventive cybersecurity solutions definitely help for maintaining cyber hygiene, but they cannot stop sophisticated and coordinated attacks on their own.

Whenever an attack happens, the worst hit is a CISO who owns cybersecurity. CISO is not one person, but it means all profiles that are responsible for cybersecurity in an organization. Adversaries may enter through the weakest link but maximum damage they make is to a CISO.

Invinsense MDR services empower CISOs to enhance their security posture with 24x7 detection and response. Our blue team becomes an extended team of CISOs and help them set up integrated 24x7 security management that helps protect against known and unknown cyberattacks.

Our blue team, which consists of veteran security professionals, helps CISOs strengthen their security landscape by integrating SEIM, SOAR, Case Management, Threat Intelligence and Threat Exchange and EDR to provide Extended Detection and Response (XDR) that does detection and response along all your security elements.

Invinsense MDR Do Detection, Threat Hunting and Response For CISOS

The main objective of Invinsense MDR is to identify potential malicious activities across your technology landscape and neutralize on behalf of CISOs or in coordination of CISOs.
It is done in three different ways and combination of all the three.

1. Automated Detection And Response:

- The integration of SEIM, SOAR, Case Management, Threat Intelligence and Threat Exchange and EDR provides automated detection of indicators of potential threats and the system also has an option to neutralize the threats automatically.

2. Automated And Human Led Detection And Response:

- In this approach, the integrated security solutions generated indicators are further analyzed by our blue team. It is then neutralized by acting on it combinedly by system as well as humans.

3. Human Led Threat Hunting:

- This is completely blue team-initiated investigations of malicious indicators that cannot be detected or prevented by existing security tools and systems.

OODA Loop- The Core Framework Of Invinsense MDR

Invinsense MDR works on OODA framework for detection and response. Blue team and the integrated systems together work on OODA framework to detect, investigate and neutralize all potential and existing threats in customers' environment.

The OODA loop is a four-stage process of decision making: Observe, Orient, Decide & Act. Invinsense MDR cycle through the phases strategically and rapidly as part of the analysis and decision-making process. During a cybersecurity incident, a quick and precise reaction is crucial. The OODA loop helps blue team to decide and act rather than notify or do nothing.

At its core, the OODA loop is a process for identifying and analyzing how a living being thinks, acts, responds, and adapts to stimuli. This framework is at the core of Invinsense MDR and has numerous applications, both offensive and defensive.

Invinsene MDR - Service Features and Deliverables:

Features	Deliverables	Team
○ Log Monitoring	○ Remote Monitoring Services for Client on 24x7 basis	○ Blue Team
	○ Daily, weekly and monthly reporting to Client management	
	○ Use Case Management	
	○ Event Management	
	○ End Point Deception	
○ Threat Management	○ Threat Intelligence	○ Blue Team
	○ Threat Hunting	
	○ Threat Co-relation	
○ Incident Management	○ Incident Response	○ Blue Team
	○ Forensic Analysis (need basis)	
	○ Investigation and Remediation	
○ Management Reporting	○ Risk Analytics and Management Reporting	○ Blue Team
○ Security Automation	○ Incident Automation and Orchestration	○ Blue Team
	○ Automating L1/L2 Repeatable Takes	

SIEM	SOAR	Security Solution & EDR	Security Solution & EDR
➢ Dashboard ➢ Alerts ➢ Reports ➢ Link Analysis Visualization	➢ Playbooks ➢ Fully Automated Playbooks ➢ Semi-Automated Playbooks ➢ Manual Playbooks	➢ Block ➢ Isolate ➢ Quarantine ➢ Shell /CMD Command Execution	➢ Endpoint Isolation ➢ Firewall ➢ Email Security ➢ Database Firewall

Purchasing

Unit	SKU	Description
Invinsense MDR	ICPL-INV-MDR-0108	Invinsense 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

Imprint

Publisher

3rd floor, Optionz Complex, Chimanlal Girdharlal Rd, Opp. Regenta Central Antarim Hotel, Navrangpura, Ahmedabad, Gujarat
380009, INDIA

Contact

sos@infopercept.com
www.infopercept.com/datasheet