OXDR

Invinsense Offensive Extended Detection and Response (OXDR)

Attacker's Action to Predict Future Attacks and Test Your Defence

Invinsense Offensive Extended Detection and Response (OXDR) is a consolidated platform, which integrates various offensive security tools to help organizations act like adversaries and identify vulnerabilities in their people, processes, and technologies, both externally and internally. This capability enables organizations to predict future attacks and test the capability of defence to respond to attacks.

The platform covers Attack Surface Monitoring, Vulnerability Management, Breach and Attack Simulation and RedOps. It encompasses organizations' IT, Cloud, OT, and IoT landscapes.

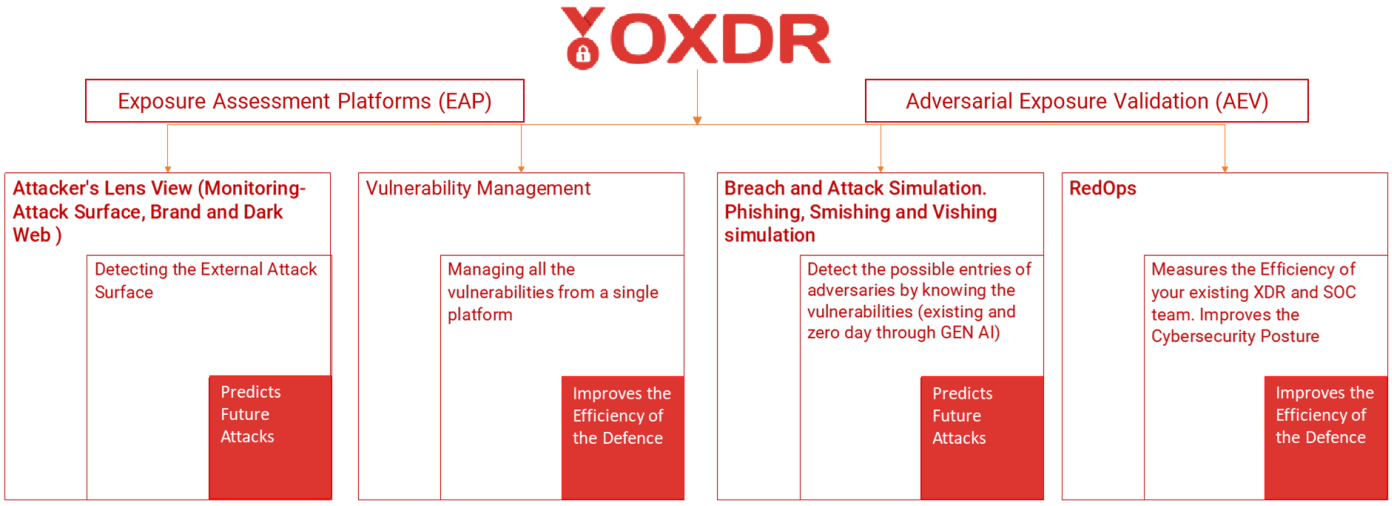


Figure 1 Invinsense OXDR for Improving the Efficiency of Your Defence and Predicting Future Attacks

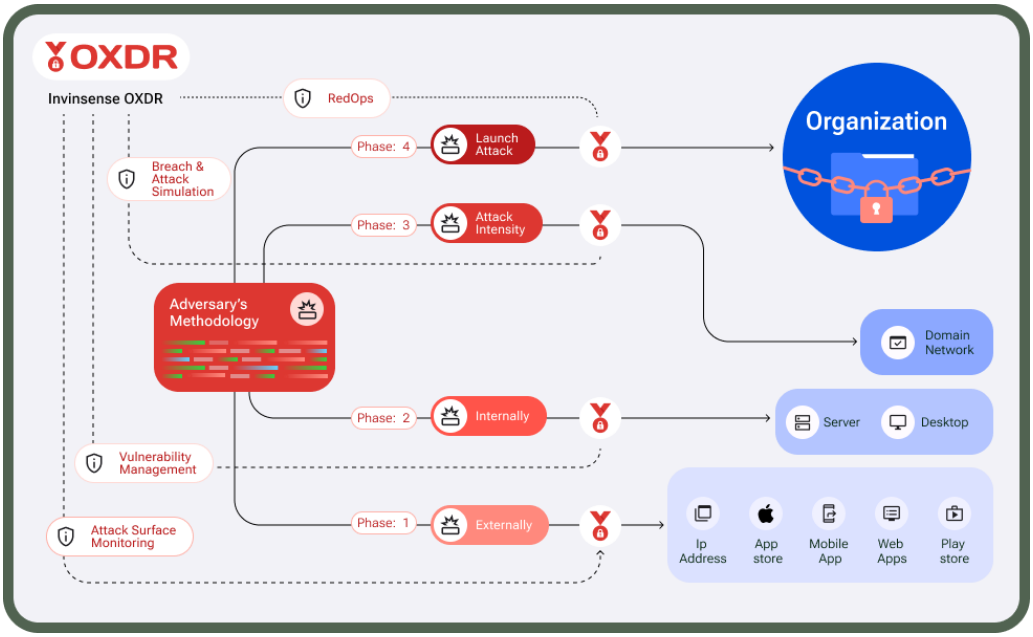


Figure 2: Invinsense OXDR in Action

Invinsense OXDR has combined all offensive security tools, mapped to the adversaries' approach to attacking an organization. In the first phase, adversaries scan the external environment and dark web for vulnerabilities or stolen credentials of the target organization. Invinsense OXDR mirrors this approach through Attack Surface Monitoring, scanning the external environment and reporting findings to the organization. In the second phase, adversaries exploit vulnerabilities to establish the foothold in the victim organization. Invinsense OXDR's vulnerability management helps organization to manage those vulnerabilities. In the third phase, adversaries use tools to attack systems; our breach and attack simulation within OXDR allows organizations to test their systems against simulated machines. In the fourth stage, adversaries execute a final blow through a combination of human and machine attacks. This stage is covered under our RedOps, where we conduct comprehensive red teaming similar to actual attacks. It also helps organizations test their existing security and its actual mean time to detect and respond.

Invinsense Attacker's Lens View :

Invinsense Attacker's Lens View continuously scans your organization's digital environment, including data on the surface web as well as the dark web, to identify potential vulnerabilities and exposures. By mapping out all the assets, including networks, applications, and devices, it provides a comprehensive view of the potential entry points that attacker might exploit. This proactive approach enables organizations to understand their risk profile better and prioritize security measures to address the most critical weaknesses.

Invinsense Attacker's Lens View includes Attack Surface Monitoring, Dark Web Monitoring, and Brand Monitoring.

Key features:

- Attack Surface Monitoring
- Dark Web Monitoring
- Open IPs, Ports
- Blacklisted IPs
- Leaked Credentials
- Subdomain Enumeration
- Passive Vulnerability Assessment
- Web Technologies
- Email Security
- Expired SSL
- Vulnerable SSL
- Open Cloud Buckets
- Stolen Credentials
- Leaked Sessions
- Source Code Leakage
- Pastebin Search
- Postman Monitoring
- Personal Information
- Malware Infected Machines
- Look Alike Domains
- Rogue Mobile App
- Social Media Profiles
- Brand Mentions

Invinsense Vulnerability Management:

Invinsense Vulnerability Management enhances your organization's security posture by maintaining a consolidated view of exposure to threats. It brings all the vulnerabilities reported across your landscapes: IT, Cloud, OT and IoT under one umbrella, providing a single, comprehensive view of all the issues present in your organization. This reduces the complexity of vulnerabilities being reported by various tools, allowing you to easily determine which vulnerabilities have been fixed and which ones are still pending.

Key features:

- Vulnerability testing using templates
- Vulnerability Tracking
- Vulnerability Resolution Timeline
- Risk Acceptance
- SLA Configuration
- RBAC for various roles
- Vulnerability Import for more than 120 Tools
- Vulnerability Deduplication
- Product Management
- Vulnerability Filtration
- Host wise Vulnerabilities
- Metrics Dashboard
- Automated evaluation of network security posture against adversaries
- Cloud Security Posture Management (CSPM)
- SAST/DAST and IAST

Invinsense Breach and Attack Simulations Including Phishing, Smishing and Vishing:

Invinsense BAS simulates real-world cyberattacks to test your organization's defences and uncover vulnerabilities within your security infrastructure. These simulations are also mapped to the MITRE ATT&CK framework. By mimicking the tactics, techniques, and procedures (TTPs) used by cybercriminals, it provides continuous, automated assessments of your organization's ability to detect, respond to, and recover from various attack scenarios. It strengthens your security posture by providing actionable insights into how well your systems can withstand actual cyber threats.

Key features:

- Smishing Attacks
- Vulnerable Employees Metrics
- Current Security Control Testing (DLP, Firewall, etc)
- Data Exfiltration Check
- Email Phishing
- Email Whaling
- Custom Phishing Templates
- Training Modules
- Vishing Attacks
- SIEM Use case creation
- Provides visibility into the attack, strengths, and weaknesses of your defence mechanism.
- Assists in detecting and responding to adversary behaviour
- Supports fine-tuning security policies and other components of your security setup
- Endpoint Testing
- SOC Team resilience check
- Use case testing

Invinsense RedOps:

Invinsense RedOps evaluates your organization's security posture using realistic attacker techniques. It provides insight into how well your organization is prepared to handle a real attack and identifies areas that require improvement. Key outcomes include determining the current minimum time to detect (MTTD) and minimum time to respond (MTTR).

Key features:

- Complete Red Team Engagement
- Identifies weaknesses in your security setups
- Assists in strategizing red team responses based on outcomes and blue team actions
- Provides security teams with hands-on experience of a real incident
- Trains security teams to handle sophisticated attacks
- Monitoring effectiveness of SOC Team (Mean Time to Detect)

Invinsense OXDR helps you continuously optimize and achieve your Continuous Threat Exposure Management (CTEM) program objectives:

CTEM represents a comprehensive approach that goes beyond occasional patching & vulnerability management and reactive detection and response.

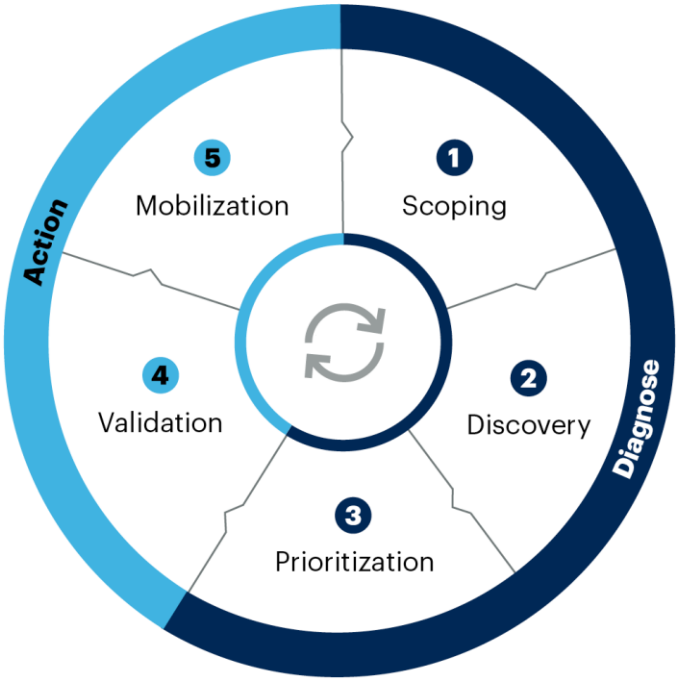
The 5 ongoing phases of CTEM:

1. Scoping
2. Discovery
3. Prioritization
4. Validation
5. Mobilization

Invinsense OXDR combines security experts, layered security technologies (both offensive & defensive capabilities) and the right processes to help customers achieve their CTEM goals, and delivers the following outcomes:

- Attack surface visibility and consistent security posture across environments (IT, IoT, Cloud, OT)
- Comprehensive exposure assessment and security validation
- Business-context aware remediation and improved risk prioritization
- Holistic threat exposure management by harmonizing security teams, processes and technologies

5 Steps in the Cycle of Continuous Threat Exposure Management



gartner.com

Gartner

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
© Infopercept Consulting Pvt. Ltd.

Publisher
3rd floor, Optionz Complex, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact
sos@infopercept.com
www.infopercept.com/knowledge/datasheets