XDR

The Litmus Test of Your Cybersecurity That Also Helps to Achieve Continuous Cybersecurity Posture.

Red Team and Breach and Attack Simulation Solution

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 to test 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.

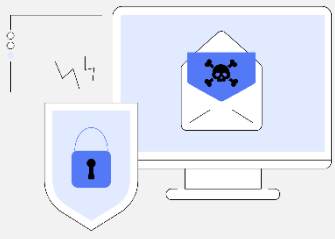
Invinsense RBAS helps organization to put their cybersecurity tools, people and processes to test and help them achieve continuous cybersecurity posture. Invinsense RBAS will help your cybersecurity systems to observe the entry of adversaries, lateral movements, attack paths, and weaknesses in IT systems and networks. The Red Ops will act like adversaries and will provide insight of current minimum time to detect (MTTD) and minimum time to respond (MTTR).

Invinsense RBAS combines everything that is needed to test your environment and make it more matured. Invinsense RBAS covers Continuous Automated Red Team (CART), RedOps, Breach & Attack Simulation (BAS), DevSecOps and Vulnerability Management.

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

Invinsnse RBAS- RedOps and Continuous Automated Red Team (CART)

Automated red teaming and RedOps of Invinsense RBAS evaluates the security posture of your organization by using realistic attacker techniques and gives a fair idea about how well your organization is prepared to handle a real attack and where do you need improvements. Major outcomes of this tool are to determine the current minimum time to detect (MTTD) and minimum time to respond (MTTR).

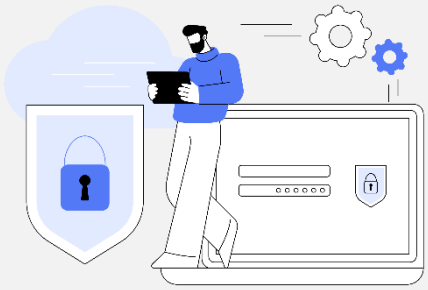


The Key Features of RedOps:

- Automation of various Red Team Attacks
- Automated Execution of various Tactics, Techniques and Procedures
- Helps to identify weak spots in your security setups
- Helps to strategies red team response, based on the outcome and action of blue team
- Gives security teams a hands-on experience of a real incident
- Trains security teams to handle such attacks which sophisticated

Invinsense RBAS- Breach and Attack Simulation (BAS)

Breach and Attack Simulations allows Invinsense RBAS to simulate attacks and assess the security posture of your organization. It is a cyber security framework used for imitating adversaries Tactics, Techniques and Procedures in a simulated environment.



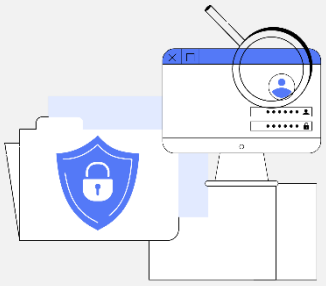
The Key Features Include:

- Leverages the MITRE ATT&CK model to identify and mimic adversary behaviours
- Automates penetration mechanism to test endpoint security against the common postcompromise adversarial technique
- Enables automated evaluation of a network security posture against adversaries
- Evaluates networks for software patch levels, security controls, and defender tools
- Reduces resources needed for assessments and offloads red teams
- Helps organizations to fine-tune behavioural-based intrusion detection systems
- Helps security teams with IoC detection and adversary response
- As an outcome of the attack simulation, you get visibility of the attack, strengths, and weaknesses of your defence mechanism
- Helps with the detection and response to adversary behaviour
- Helps fine-tune security policies and other components of your security setup

Invinsense RBAS- Vulnerability Management And Devsecops:

Clear picture of your organization's security posture is only possible by testing it continuously. Through DevSecOps, Invinsense RBAS allows you to perform security testing across IT landscape to know your security posture in real time.

Vulnerability management allows to build central repository of various security testing across the landscape.



The Key Features Include:

- Pre-commit hooks
- Commit-time testing – Static Code Analysis (SAST)
- Build-time testing and analysis – Dynamic Security Testing (DAST)
- Deployment checks
- Vulnerability testing using templates
- Vulnerability metrics, reports, and baseline self-service tools
- Removal of Deduplication when repetition of findings with same CVE and CWE
- Enables automated evaluation of a network security posture against adversaries
- Cloud Security Posture Management (CSPM)
- Vulnerability metrics, reports, and baseline self-service tools.
- Workflow and Task Management on the different vulnerabilities

Purchasing

Unit	SKU	Description
Invinsense OMDR	ICPL-INV-OMDR-0109	Red Team and Breach and Attack Simulation Solution

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, CG Rd, Opp. Regenta Hotel, Navrangpura, Ahmedabad, Gujarat 380009, INDIA

Contact

sos@infopercept.com

www.infopercept.com/knowledge/datasheets