Unified Threat Detection and Response with Invinsense XDR

The Defender's Brain of Your Cybersecurity - Invinsense XD

ingesting data from multiple security layers, providing a unified view of th
solutions with threat intelligence and threat exchange capabilities.

Traditional security solutions often operate independently, creating gaps in visibility and coordination, leading to delayed or missed detections of sophisticated threats. XDR integrates and correlates data across various security layers—endpoints, network, servers, and cloud—providing a unified, comprehensive view of the threat landscape. This enhances situational awareness, speeds up threat detection, and streamlines incident response, ultimately improving the overall effectiveness and efficiency of an organization's cybersecurity operations.

Invinsense XDR

Invinsense XDR is a scalable solution for all clouds and operational technology (OT). It follows a next-gen SIEM-based approach to ingest telemetry data from multiple data sources including organization's existing tools and its integration with the security lake ensures better computing, cost-effective storage and better detection and response by utilising the Open Cybersecurity Schema Framework (OCSF) as a foundational data schema. It is the only solution with integrated SIEM, SOAR, EDR, Threat Intelligence, Threat Exchange and Case Management features.

Key capabilities

Threat Hunting

enhances organization's cybersecurity by proactively identifying and mitigating advanced threats before they can cause significant damage. Improves detection capabilities, reduces response times, and helps to fortify defenses against future attacks

Automated Response

significantly reduces incident response times by swiftly executing predefined actions, minimizing the impact of threats. Enhances efficiency and consistency in handling security events, freeing up human resources for more complex tasks.

Threat Intelligence

gives actionable insights into emerging threats, enables organizations to proactively defend against potential attacks and enhances overall security posture.

Behavioural Analysis

identifies anomalous activities and potential threats based on deviations from normal behavior patterns. Improves the detection of sophisticated attacks and insider threats that might bypass traditional security measures.

Cloud Workload Protection

secures applications and data across diverse cloud environments by providing visibility, threat detection, and automated response capabilities. Ensures compliance and reduces risk by protecting against vulnerabilities, misconfigurations, and unauthorized access.

Efficient IoC and indicators database

helps detect and respond to security breaches by providing a centralized repository of known threat indicators, enabling faster threat detection and mitigation, and enhancing overall cybersecurity posture.

Automatic correlation

helps find relationships between attributes and indicators from malware, attacks campaigns or analysis.

Data-sharing

with third-party security tools and trust-groups

Pre-built and Customizable playbooks

for common security use cases. Helps standardize incident response procedures and ensure consistency.

Real-Time Monitoring and Alerts

triggers automated responses based on predefined rules. Alerts can be sent to relevant team members to ensure timely action.

Security and Access Control

including role-based access control (RBAC) and audit logging, to prevent unauthorized user access to the platform

Security Configuration Assessment

maps the configuration with CIS bench mark and detects the endpoints lacking proper configuration to improve the security posture of the organisation.

Package level vulnerability identification

allows for early detection of security risks within dependencies, enabling faster remediation. It enables proactive mitigation of known issues, enhancing overall application security.

IOC blocking capabilities via single Console

centralizes threat management, enabling rapid, streamlined defense against indicators of compromise across systems.

Multiple form factors (on prem, bring your own cloud and SAAS model)

provides flexibility to meet diverse operational needs, ensuring optimal performance and scalability across varied environments.

Key Benefits

Holistic Threat Detection

Integrates data from multiple sources to form a comprehensive view of the threat landscape, much like how the human brain processes information from various senses.

Contextual Analysis

Provides context to security events by correlating data across endpoints, network, servers, and cloud, enabling a deeper understanding of potential threats.

Offload SOC Team

Automates routine tasks and responses to threats, similar to how reflex actions are processed by the brain, allowing for quicker and more efficient incident response.

Prevention First

Utilizes advanced analytics to proactively identify and mitigate threats before they can cause significant harm, akin to the brain's ability to anticipate and react to danger.

Continuous Learning and Adaptation

Continuous updates and improved security measures based on new treats and vulnerabilities, mirroring the brain's ability to learn and adapt to new situations.

In numbers

500+
use cases built around various technologies

4000+
rules for achieving various use cases

25+
threat Intelligence feeds including, CertIn and FS-ISAC

90+
custom use cases created by threat research team for capturing IOC/IOA.

100+
readily available SOAR playbook for task automation

Invinsense XDR Features:

Invinsense EDR

- Endpoint Protection
- Automated Response
- UBA
- Advance Telemetry
- Leteral Movement Protection
- AMTD + Ransomware Protection
- File Integrity Monitoring
- CIS Benchmark
- Custom Benchmark
- Vulnerability Detection for Endpoint
- End Of Life Software
- Disk Encryption
- Forensic Capability
- Defender Management
- Endpoint Firewall Management
- Asset Discovery
- IOC / IOA Mapping
- Integrated Threat Intelligence
- Attack Trajectory for File less and In Memory Attacks
- Device Control
- Ransomeware Protection

SIEM	• Mitre Attack Mapping • 100+ Prebuilt Datasource Integration (Agent + Agent Less) • Custom API Integration Support with SIEM • Custom Agent + Agent less Logs Onboarding • Support Multiple Log Format (Including Custom Log Format)	• Custom Dashboards and Report • 500+ Inbuilt Use Cases on Various technologies • Real time and hostorical Event Visibility • Compliance Support and Visibility • Agentic AI • Third Party Integration for Alerting
SOAR (Automation)	• 1000+ Application Integration Support • Custom Application Support (API Integration) • No Code Workflow Builder	• Visual Playbook Editor • Improve MTTD and MTTR by X% • L1 and L2 Productivity Enhancement

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