XDR

Extended Detection and Response is effective against all kinds of cyberattacks and adversaries, but only when it gets integrated and coordinated intelligence from the key cybersecurity solutions.

An Integrated Detection and Response with Attacker's Sense

Invinsense XDR is one of the most integrated XDR that combines intelligence of the key cybersecurity solutions- - SIEM, SOAR, EDR, Case Management, Threat Intelligence, Threat Exchange, and other cybersecurity solutions. Invinsense XDR integrates these elements in such a way that it becomes a cybersecurity ecosystem that acts at the level of adversaries. This ecosystem combines automated and human efforts mapped around attacker's tactics and neutralize all kinds of threats. Its integration with threat intelligence and threat exchange makes sure that the system learns from it and becomes more agile towards similar attacks in the future

Invinsense XDR Works on The OODA Approach

The OODA loop is a four-stage process of decision making: Observe, Orient, Decide & Act. Invinsense XDR will 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 followed by Invinsense XDR is designed to help your team make decisions and take action rather than freezing up and doing nothing. At its core, the OODA loop is a process for identifying and analysing how a living being thinks, acts, responds, and adapts to stimuli. This process is invaluable to your security team and has numerous applications, both offensive and defensive.

The Key Highlights Include:

- Digital landscape of each customer is different, Invinsense OODA allows customization to fit all types of requirements.
- Offers API based integration with 200+ vendors.
- Automated mapping with MITRE ATT&CK techniques.

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

Integrated Case Management, Threat: Intelligence and Threat Exchange

Invinsense XDR also integrates case management, threat intelligence and threat exchange. Extended Detection and Response Security Incident requires scalable and customizable case management integrated with Threat Intelligence and community approach to exchange the learnings

The Key Highlights Include:

- **Collaborates**- Multiple SOC and CERT analysts can collaborate on investigations simultaneously.
- **Elaborates**- Cases and associated tasks can be created using a simple yet powerful template engine.
- **Acts**- Add one, hundreds or thousands of observables to each case that you create or import them directly from a MISP event or any alert sent to the platform.
- **Investigates** – Look for IOC's and TTP's in various threat intelligence API's
- **Exchanges** – Share your leanings to community
- **Distributes**-The new vulnerabilities across different teams.

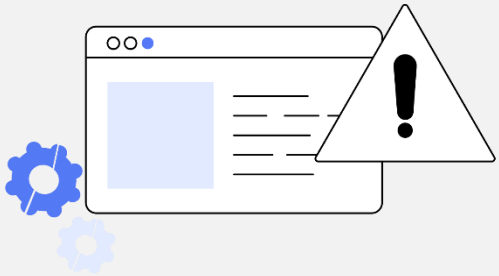
Complete Visibility and Response to Advanced Threats With EDR and SIEM

EDR and SIEM are two important components of an organization's security strategy.

The EDR component provides enhanced endpoint visibility and ensures a faster response time. it spots unknown types of malwares hence can protect your organization from advanced malware. On the other hand, SIEM is important because it collects a lot of data from various components of your network, analyzes it for any sign of malicious activities, filters, and prioritizes the alerts to provide an attack timeline that ultimately helps organizations to understand the attacks and stop them.

Weaved together EDR and SIEM offer actionable intelligence through threat patterns and active response capabilities that can block network attacks and stop lateral threat movement.

The EDR and SIEM components of Invinsense XDR are powered by Wazuh. They provide complete network visibility and help security analysts discover and investigate threats and attacks.



The Key Features:

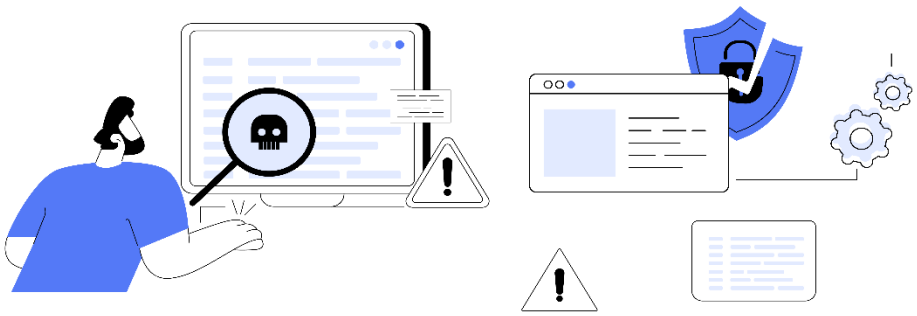
- Monitor endpoints for files, registry keys, processes, applications, open ports, network configuration, etc.
- Collect and normalize a large amount of log data from on-prem and cloud sources including endpoints, emails, applications, servers, and cloud.
- Analyze data, add context and identify threat pattern.
- Real-time visibility for security analysis and active response based on the analysis.
- Configuration assessment and policy monitoring.
- Inventory of running processes and installed applications.
- Detect malicious behaviour, malware, phishing attempts, and indicators of compromise (IoC).
- Offer a rich set of dashboards, reports, and link analysis visualization tools to provide complete visibility of the network.
- Ensure compliance adherence with real-time visibility of network and events.
- Correlate events to get a holistic view of the organization's security posture.
- Automated analysis of IPs, URLs, Domain names, Filenames, Hashes, Registry keys, DLLs.
- Automated analysis of email addresses, links, headers, attachments.
- Guided procedures for standardized incident response.
- Threat intelligence from Cortex, MISP etc.
- Comprehensive and contextual incident response.
- Enable endpoint isolation, blocking, and quarantine.
- Generate alerts and notifications through Email, SMS, ticketing system (powered by The Hive).

Invinsense XDR Is Fast, Accurate And Easy Deploy In Any Cloud (AWS, AZURE, GOOGLE) Or On- Premise Leveraging Terraform

Invinsense XDR also integrates case management, threat intelligence and threat exchange. Extended Detection and Response Security Incident requires scalable and customizable case management integrated with Threat Intelligence and community approach to exchange the learnings

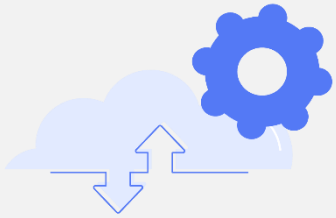
To Why Terraform:

- Codifies Your Application Infrastructure.
- Reduces human error and increases automation by provisioning infrastructure as code.
- Manages infrastructure across clouds.
- Creates reproducible infrastructure.
- Provision consistent testing, staging, and production environments with the same configuration.
- "15 minutes deployment"



Collective Security Orchestration Automation And Response

SOAR is a collection of tools that enable organizations to collect inputs from different sources like SIEM, EDR, AV etc. monitored by the security team. The SOAR component of Invinsense XDR is based on Shuffle. This provides incident analysis and response by leveraging a combination of human and machine intelligence. The incident analysis and response procedures are provided by workflows and playbooks.



The Key Features Include:

- No cap on the number of users, applications and cloud workflows.
- Workflow editor and app editor for customization.
- Detection Engineering framework.
- Private apps and integrations.
- Default and custom playbooks.
- Manual/ Semi and Fully Automated Playbooks for incident response.
- Automated remediation workflows for similar incidents.
- SMS and email alerting system.
- Hybrid email triggers, schedules and executions.
- Cloud backups.
- Data location and retention control
- Audit logging.
- Custom and controllable reporting.
- Risk-based overview
- Multiple dashboards e.g., Compliance, Management.

Purchasing

Unit	SKU	Description
Invinsense XDR	ICPL-INV-XDR-0107	An Integrated Detection and Response with Attacker's Sense

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