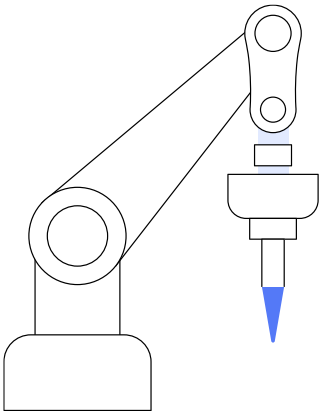
Infopercept

Invinsense® UEBA
Behavioral Analytics and Insider Threat Detection for Critical Infrastructure

Behavior-Centric Threat Detection Across Industrial and Enterprise Systems

Invinsense® User and Entity Behavior Analytics (UEBA) solution brings a modern layer of behavioral intelligence to security operations for critical infrastructure sectors including energy, utilities, manufacturing, and industrial control systems. Unlike traditional, rule-based detection methods, Invinsense UEBA applies machine learning and AI to model behavioral baselines and dynamically identify anomalies across users, systems, and network entities.

By continuously monitoring operator activities, remote logins, SCADA control commands, privileged account actions, and OT/IT interactions, Invinsense UEBA uncovers hidden threats like insider attacks, privilege misuse, data exfiltration, and command misuse that often evade traditional tools.



Key Benefits

- Real-Time Detection of Anomalous Behaviors and Insider Threats
- Dynamic Behavioral Profiling Using AI/ML
- Low-and-Slow Attack Detection and Account Compromise Alerts
- Seamless Integration with SIEM, SOAR, and IAM Systems
- SCADA and OT-Aware Behavioral Monitoring
- Automated Threat Response and Policy Enforcement
- Privileged User Activity Auditing and Risk Scoring
- Improved Threat Visibility and Reduced False Positives

Key Capabilities

Behavioral Intelligence for Modern Cyber Defense

Anomaly Detection Using Baseline Behavior Models
ML-driven baselining of users, applications, endpoints, and network activity.

Real-Time Anomaly Scoring
Prioritized alerting based on behavioral deviations across IT and OT environments.

Privileged Access Monitoring
Detects misuse, escalation, and unauthorized command execution across SCADA and remote interfaces.

Compromised Account Identification
Flags unusual login patterns, geographic anomalies, and device mismatches.

Integration and Correlation-Driven Analytics

SIEM, SOAR & IAM Integration
Enriches behavioral data with context from security alerts, access logs, and automation workflows.

SCADA & Load Dispatch Visibility
Understands operational workflows to detect unusual command behavior and operator intent anomalies.

Cross-Domain Correlation
Links user activity to network, endpoint, and application behavior for unified threat detection.

Automated Incident Handling and Response

Trigger-Based Alerting & Escalation
Automatically flags critical deviations and initiates response.

Access Revocation & Session Termination
Responds to high-risk events by locking users or disconnecting sessions.

Case Management Integration
Escalates anomalies into SOAR workflows or case tracking systems.

Deployment Flexibility

Cloud-Based: Scalable, centrally managed deployments

On-Premises: For compliance-sensitive and air-gapped environments

Hybrid: Unified visibility across distributed IT/OT environments

Security Outcomes Delivered

- Early Detection of Insider Threats and Account Compromise
- Real-Time Behavioral Anomaly Alerting with Automated Response
- Improved SOC Efficiency with ML-Driven Prioritization
- Enhanced Threat Visibility Across Critical Infrastructure Systems
- Reduced False Positives and Alert Fatigue

Invinsense UEBA is your behavioral security layer for uncovering the unseen—delivering intelligence-driven protection for the most critical assets and people in your environment.

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