

Ai-powered User Behavior Analytics

▶ Detect threats and respond in real time

Our insider threat management platform provides a highly configurable alerting subsystem that includes both customizable rules (based on generic behavioral indicators of potential insider threats) and an AI-powered user behavior analytics module for detecting anomalies in the routines of internal users.



Predefined and custom alerts

Ekran System provides rule-based incident flagging. Its collection of alert templates covers the most common insider threat indicators.



Automated incident response

Ekran System allows you to set up automated incident response actions. These vary from warning messages obligating users to acknowledge their actions to application termination and user blocking.



User and entity behavior analytics (UEBA)

User and entity behavior analytics (UEBA) Ekran's alert system includes an artificial intelligence module that establishes baseline user behavior to detect abnormal user activity and possible account compromise.

▶ Ekran System AI analyzes user behavior

The Ekran System UEBA module establishes baseline user behavior to detect abnormal user activity and possible account compromise. In this example, we analyze the working hours of a user and create a baseline from this data.

Customer highlights



The dashboard interface includes a sidebar with navigation options: Monitoring Results, Forensic Export History, Reports, Interactive Monitoring, Health Monitoring, Password Management, Client Management, Tenant Management, User Management, Access Management, Alert Management, User Behavior Analysis, USB Monitoring, and Audit Log.

The main dashboard area displays several widgets:

- Clients:** A pie chart showing 3 licensed clients and 2 unlicensed clients. A red alert message states "ATTENTION: Not all Clients are licensed!". A button "INSTALL MORE CLIENTS" is visible.
- Memory Usage:** A line graph showing memory usage over time, with a peak of 200 MB and a duration of 2 minutes.
- Sessions Outside of Work Hours:** A bar chart showing session counts for dates from 03/13/2023 to 03/20/2023.
- Storage Usage:** A diagram showing storage usage for Database (39.33 GB) and Binary Data (20.07 GB). A smaller value of 0.07 GB is also indicated.
- Latest Live Sessions:** A table with columns: START, CLIENT NAME, and USER NAME.

START	CLIENT NAME	USER NAME
03/20/2023 12:00:2...	WINServer2019	WINSERVER2019/A...
03/20/2023 12:00:0...	UbuntuVM	user
- Rarely Used Computers:** A section for identifying rarely used computers.

▶ Security team detects threats and responds in real time

In Ekran System, you can easily view sessions in which behavioral anomalies are detected and respond to risky user activity. Moreover, you can get a report on all risky sessions. Notifications are delivered via email.

The screenshot displays the 'ALERT MANAGEMENT' interface. At the top, there are panels for 'Properties' (with 'Enable rule' checked and 'Name' set to 'Unusual working hours') and 'Conditions' (with 'Unusual work hours' checked and severity set to 'High'). Below these is a table of alerts:

RI...	NAME	DESCRIPTION	ASSIGNED TO	STATE	NOTIFICATION	EMAIL RECIPL...
<input type="checkbox"/>	upload xlsx files		All Clients	Disabled	None	
<input type="checkbox"/>	Upload passwo...		All Clients	Enabled	None	
<input type="checkbox"/>	testalert		All Clients	Disabled	None	
<input type="checkbox"/>	Proxy Anonymi...	This is an alert ...		Enabled	None	
<input type="checkbox"/>	Manual data sa...	This is an alert ...		Enabled	None	
<input type="checkbox"/>	License genera...	This is an alert ...		Enabled	None	
<input type="checkbox"/>	Keyboard man...			Enabled	None	
<input type="checkbox"/>				Disabled	None	
<input type="checkbox"/>				Enabled	None	
<input type="checkbox"/>				Enabled	None	
<input type="checkbox"/>				Enabled	None	

Below the table are three configuration panels: 'Email Notifications' (with three unchecked options), 'Additional Actions' (with 'Show warning message to user' unchecked and 'Block user in the current session' checked), and a pagination control showing page 1 of 3.

▶ The most complete set of supported platforms



“ One of the fastest solutions that I have installed and configured. I can recommend EKTRAN as a good, light and efficient solution.”

▶ Licensing

Ekran System® is licensed based on the number of endpoints and is offered in Standard and Enterprise Editions. The Enterprise Edition includes several enterprise-grade maintenance and integration features.



Visit us at <https://www.ekransystem.com>

/EkranSys

/ekransysteminc

/ekran-system

/Ekran System

Ekran System® Inc.

60 Kendrick St. Suite 201 Needham,
MA 02494, USA