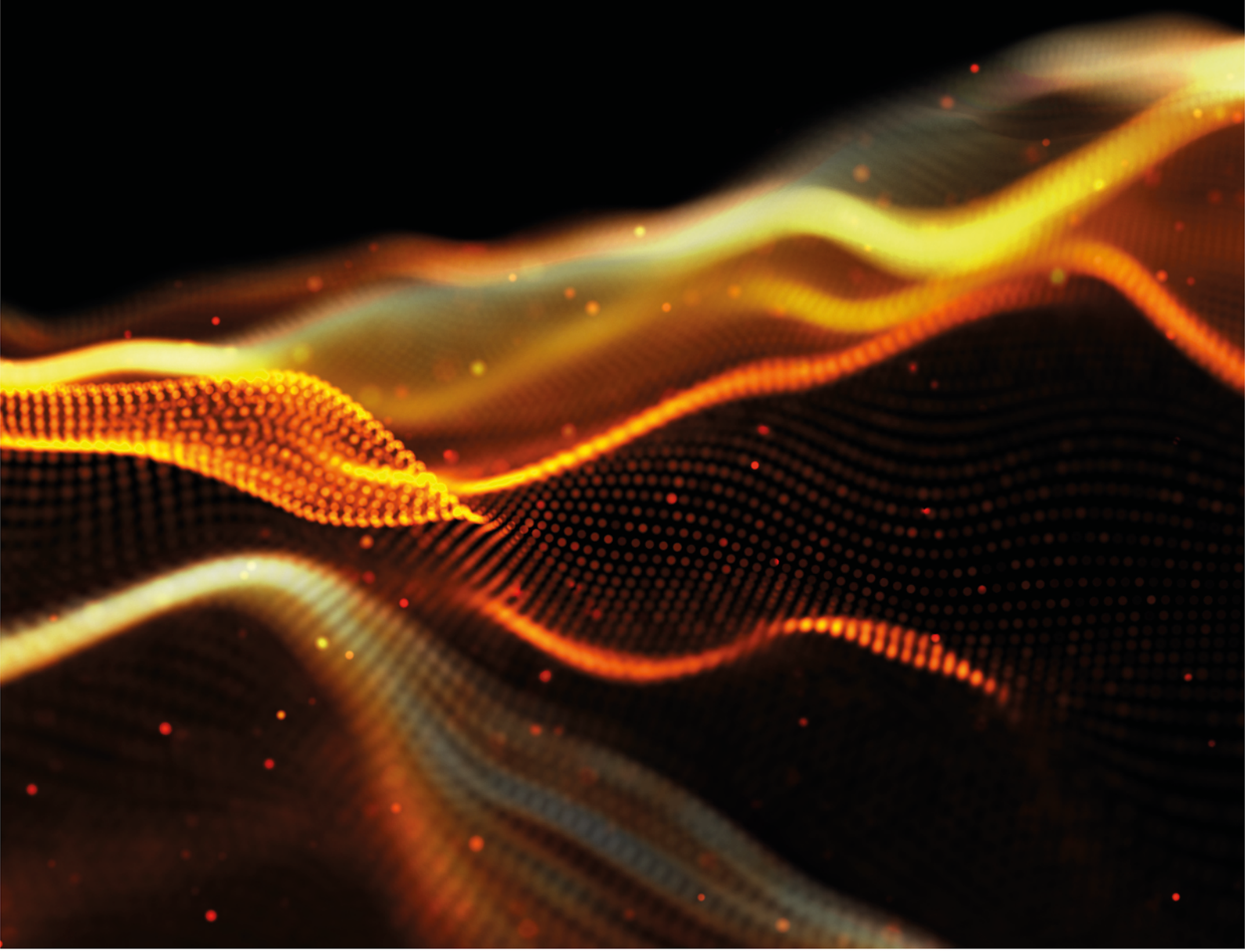
EKRAN®

WHITE PAPER

5 LEVELS OF USER BEHAVIOR MONITORING



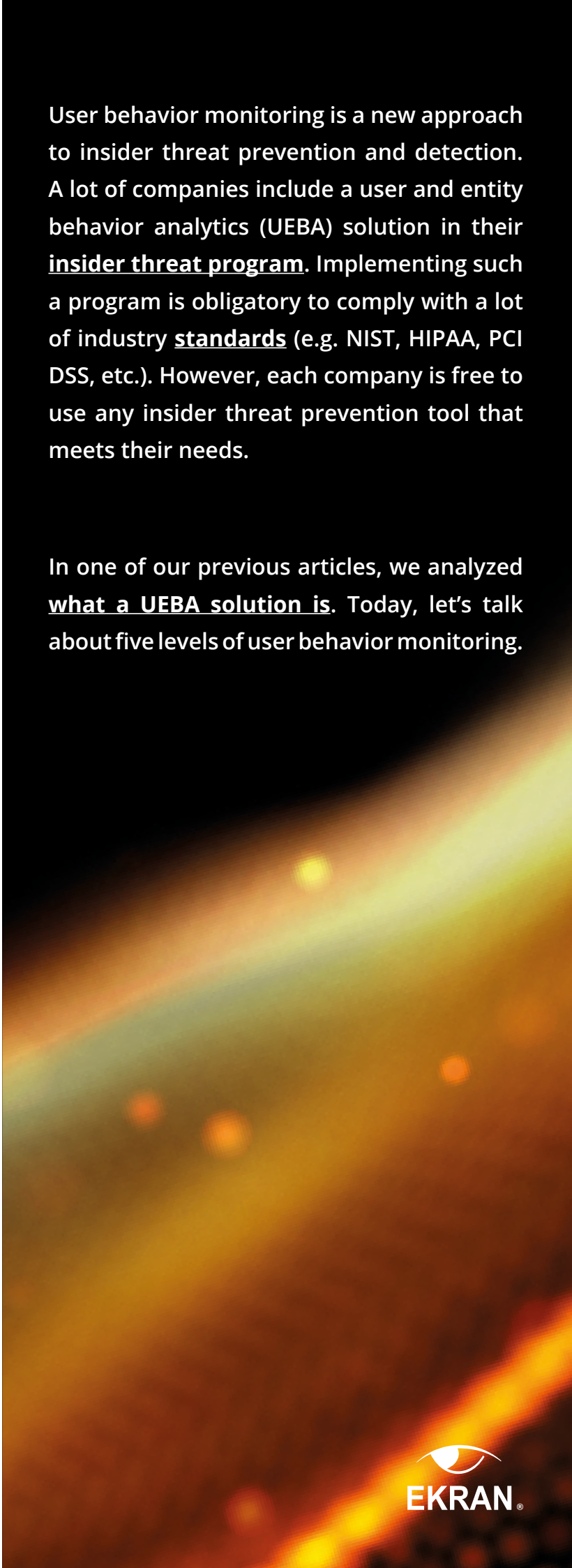
www.ekransystem.com

info@ekransystem.com

TABLE OF CONTENTS

User behavior monitoring is a new approach to insider threat prevention and detection. A lot of companies include a user and entity behavior analytics (UEBA) solution in their **insider threat program**. Implementing such a program is obligatory to comply with a lot of industry **standards** (e.g. NIST, HIPAA, PCI DSS, etc.). However, each company is free to use any insider threat prevention tool that meets their needs.

In one of our previous articles, we analyzed **what a UEBA solution is**. Today, let's talk about five levels of user behavior monitoring.



WHAT IS UEBA?

User and entity behavior analytics refers to technology for profiling user and entity behavior and detecting anomalies. UEBA software is based on machine learning algorithms or advanced statistical models. By analyzing user and entity actions, this software creates a baseline of users' normal behavior and detects patterns that lead to cybersecurity violations.

A UEBA system allows you to take your insider threat protection program to the next level. It enforces traditional monitoring and detection tools with a proactive approach to threat detection and constant self-improvement.

Gartner predicts that by 2022, UEBA technologies will be embedded in 80% of threat detection and incident prioritization solutions.

5 levels of user behavior analytics

LEVEL 1: GATHERING HELPFUL CONTEXT

The first stage of user behavior monitoring is collecting data on the system, entities, and events the UEBA solution needs to analyze.

Each UEBA solution records a unique dataset according to the use cases it covers. For example, UEBA software might collect the following information about users' activity:

- log in and log off times
- requests to access sensitive assets
- visited websites
- started applications
- connected USB devices
- keystroke dynamics
- and more

The effectiveness of all other levels of behavior monitoring fully depends on the data a UEBA system analyzes.

Some UEBA solutions are able to collect the necessary information by themselves. However, it's best to create a **dedicated** user activity monitoring **program** for that. There are two key reasons:

- A standalone solution has more tools for monitoring and recording data.
- Data from monitoring software is useful for insider threat detection, conducting investigations, etc.

LEVEL 2: DETECTING THREATS

After a user behavior analytics solution has gathered information on normal user behavior, UEBA becomes useful for insider threat detection. Data analysis allows the

software to detect suspicious actions and establish patterns for various categories of users (ordinary employees, privileged users, third-party contractors, security officers).

How can you use a UEBA solution?

UEBA software can aid your insider threat strategy by allowing you to do several things:

- **Detect threats based on real-time user actions.** For example, the Ekran System UEBA module analyzes work hours of each employee and gets to know normal times for logging in and out. If a user tries to log in at an unusual time (e.g. in the middle of the night), Ekran can notify a security officer or block this attempt.

- **Prioritize security alerts.** Based on the analysis of user behavior, a UEBA module creates a list of suspicious user actions. When it's integrated into an SIEM or threat detection system, a UEBA can sort rule-based alerts from the least to the most dangerous. This functionality is especially useful for enterprises, where a threat detection solution can produce hundreds of alerts per day.

- **Improve investigation efficiency.** Comparing normal user behavior with malicious actions that led to an insider threat saves a lot of time for security officers. Such a comparison allows you to determine what exact action turned a threat into an attack.

  At this stage, a UEBA solution makes your insider threat security tools more effective, but it isn't useful on its own. It still requires an accurate description of the violation it has to detect, mechanisms for alerting, and tools for further investigation.

  It's best to integrate such user behavior analytics with other cybersecurity solutions for better protection.

LEVEL 3: CREATING AN EMPLOYEE BEHAVIORAL PROFILE

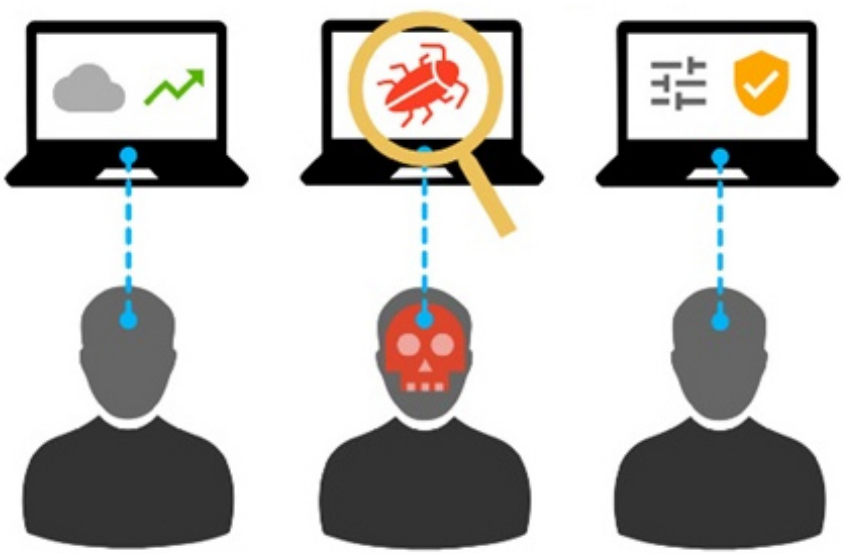
In psychology, a behavioral profile describes characteristics and behavioral patterns of individuals or groups. In insider threat detection, behavioral profiles are used to create a baseline of user behavior. This baseline helps the system detect abnormal user

actions. Also, using the baseline, a security officer can outline a **portrait of a malicious insider**.

A user profile contains a set of actions typical for a certain employee based on monitoring data collected during the baseline period. If there's a change in this behavior, the solution compares it to the typical behavior of other users in the peer group and known patterns of insider threats, then alerts a security officer f there are any red flags.

Such functionality is useful for **incident anticipation**. It's also the basis for your behavior monitoring program.

Employee behavioral profiles help you identify malicious insiders before they harm your system



Additionally, machine learning and semantic analysis algorithms allow for **detecting human emotion** in written texts (emails, messages, documents, etc). This is helpful for detecting a disgruntled employee before they turn into a malicious insider.

Portraits of insiders are based on investigations of previous security violations. By analyzing them, a UEBA figures out patterns that indicate malicious intent. These can be a useful addition for **alert-based incident response**.

How does behavioral profiling work?

A UEBA system analyzes collected data in order to determine normal user and entity behavior and establish patterns that indicate malicious activity. Depending on the amount of data collected and the complexity of the analysis, establishing baseline user behavior may take from one week to several months.

At this stage, it's best to combine automatic behavior analysis with inputs from security officers. Manual investigation helps to avoid false-positive alarms in the future.

When are behavioral profiles helpful?

Using behavior profiles, a UEBA can detect:

- malicious activity
- compromised accounts
- potential attackers
- privilege misuse
- access misuse

At this stage, there are legal and moral issues you need to consider. Sometimes, it takes years for a loyal employee to turn into a malicious insider. Some companies suggest monitoring not only employee activity at work but also social media activity. If you do this, make sure it's reflected in your cybersecurity policy and your employees are aware of it.

Behavior profiles are useful for detecting:

LEVEL 4: GETTING AN EARLY WARNING

Levels 4 and 5 represent the most powerful types of user behavior analytics. Using machine learning and statistical analysis, they predict cybersecurity violations based on collected data. The main difference between these levels lies in when the UEBA solution uncovers a potential trespasser. Level 4 and 5 systems are useful for detecting:

- fraud
- data exfiltration
- intellectual property theft
- espionage
- privilege abuse

At level 4, a UEBA solution picks up anomalies in employee behavior that indicate malicious intent. An early warning means an incident is detected before data loss happens — usually when an attacker is only planning malicious actions. At this point, a rogue employee has decided to steal or corrupt company data but hasn't yet decided on the time, tools, scale, etc.

A UEBA solution can pick up early signs of malicious intent: working late for no obvious reason, accessing sensitive data the employee didn't need before, connecting various USB devices, etc.

Advanced UEBA solutions can detect:

When working with a UEBA solution of this level, you have to be careful how you interpret the results of analysis. User and entity profiling and machine learning analysis can produce false positives. It's best to review behavior profiles manually, especially for users with access privileges.

If a user consistently breaks cybersecurity rules (e.g. logs into a server outside work hours to work from home), the UEBA solution will mark such behavior as normal. However, such actions expose the network and may lead to a data leak.

Therefore, it's best to conduct an additional analysis before taking any action based on a UEBA alert. In these cases, organizations still have to rely partly on their own rules instead of purely relying on statistical analysis and profiling.

LEVEL 5: FORESEEING INSIDER THREATS

At the final level, a UEBA solution is able to create an **insider risk score** for users long before they commit an attack. This is done without any input from a security officer. An insider threat prediction is usually based on:

- a user's behavior profile
- patterns of insider attacks
- predictive models for various types of attacks
- performance assessment
- data provided by HR, accounting, and legal systems

Indicators of a turn toward negative behavior are best detected through psycholinguistic indicators, such as emails and messages, posts on social media, and text shared via other channels.

Can you trust such a system completely?

Though a UEBA is a useful tool for a security officer, its results should be closely checked before any actions are taken. False-positive results are highly possible at this level.

In order to decrease their number, you can:

- **constantly provide the algorithm with new monitoring data.** The more corporate systems are integrated into this process, the better the results you'll get.
- **allow for gradual model growth.** As you hire new employees and create new job positions, the UEBA module needs to be allowed to create new employee profiles and associate them with existing ones.
- **provide the software with automatic and manual feedback.** The algorithm should always compare its predictions with real user actions. Also, a security officer should correct this comparison if needed.
- **conduct long-term and short-term baselining.** Such training will teach the algorithm to predict violations using both recent and past contexts.

CONCLUSION

User behavior monitoring is effective for detecting and preventing insider threats. Combining it with more traditional cybersecurity tools provides you with a clear picture of your network and user actions.

The choice of a suitable level of user behavior monitoring depends on the use cases a company needs to cover. Ekran System is equipped with a vast toolset for **insider threat detection**:

- constant **user activity monitoring and session recording**
- **identity** and **access management**
- **alerting** on suspicious events (in addition to a UEBA module)