EKRAN.

Staying Protected from Insider Risk: Practical Steps for Organizations

Yevhen Zhurer

Head of Business Development
Ekran System

Ekran System at a glance

EKRAN.

Our industry recognition

Gartner
Included in the Gartner 2022 Market Guide for Insider Risk Management Solutions

NIST
Mentioned in NIST Special Publication

Microsoft Azure
Value Added Partner

kuppingercole ANALYSTS
INCLUDED IN 2021 KUPPINGERCOLE LEADERSHIP COMPASS FOR PAM

Our customers

VISA

ups

SAMSUNG

Deloitte.

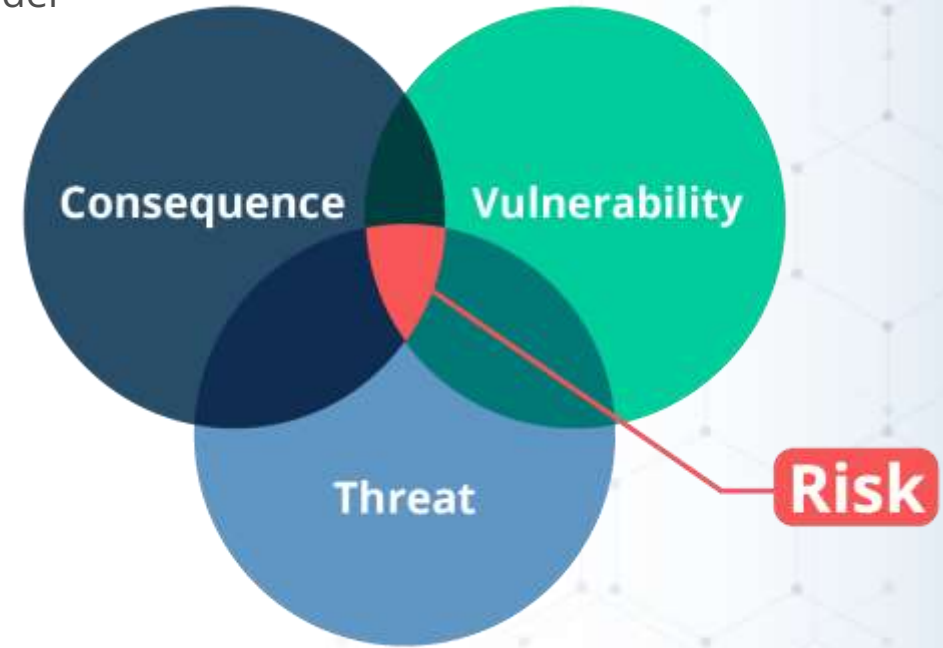
Agenda

- Why pay attention to insider risks and threats?
- Goals of insider risk management
- Cybersecurity compliance with Ekran System
- Identify and assess insider risks
- Deter insider risks at the early stages

Why pay attention to insider risks and threats?

The possible impact of experiencing an insider threat:

- Financial losses
- Reputational damage
- Leaked data and intellectual property
- Customer churn
- Additional compliance audits



Goals of insider risk management

01 **Be aware of insider risks** and threats relevant to your organization

02 **Monitor existing threats** and prevent possible damage from them

03 **Demonstrate compliance** with cybersecurity standards, laws, and regulations

04 **Deter insider activity** before it turns into an insider attack

05 **Detect suspicious behavior** that may indicate the start of an attack

06 **Disrupt security incidents** to limit damage from them

Cybersecurity compliance with Ekran System

Robust capabilities for user activity monitoring, privileged access control, and security incident response make Ekran System a reliable software for complying with:

BSI Information technology in process monitoring and control	ISO 27001 Major controls	GDPR Articles
Restrict external access (e.g. Internet, intranet, maintenance) to the process control network	Organization of information security	Principles relating to processing of personal data
Design, manage, and revoke external access to the process control systems	Access control	Responsibility of the controller
Provide access only to features needed for operation	Operations security	Security of processing
Provide secure system-based authentication mechanisms	Supplier relationships	Data protection impact assessment
	Information security incident management	Tasks of the data protection officer

Identify insider risks during security risk assessment

- Generate reports on past security incidents and risky user activity
- Watch user session records to determine causes and possible consequences of those incidents
- Revise access control rules for accessing sensitive resources

Deter insider risks at the early stages: employee awareness training

- Collect examples of insider threats from user session records
- Educate employees in real time with warning messages about their risky activity
- Evaluate training results by analyzing received alerts and notifications
- Generate periodic and ad hoc reports to prepare for the next training session

Deter insider risks at the early stages with PAM

- Configure a unique list of access privileges for user groups and particular users
- Check identities of privileged and third party employees with multifactor authentication
- Enforce secondary authentication to distinguish users of shared accounts
- Automate password and secret management
- Generate temporary credentials or manually approve access to the most sensitive resources

Detect any insider activity with UAM

- Monitor and record the activity of any user on any endpoint within the protected perimeter
- Enable offline activity monitoring and data synchronization upon Internet connection
- Manage the connection and usage of USB devices
- Collect metadata on user activity to understand the context and user intent behind any incident
- Protect recorded data from intrusion by monitoring users with any level of privilege
- Export monitoring records in protected format for forensic investigations

Respond to insider threats ASAP

- Configure security rules and real time notifications about violations
- Define which threats should be stopped automatically with Ekran System, and which ones need the attention of the security officer
- Kill threatening processes and block users in real time
- Integrate Ekran System with your SIEM to see the full picture of a security incident
- Investigate security incidents by revising records and reports on the incident

Handle insider risks with Ekran System

EKRAN.

Thank you!

yevhen.zhurer@ekransystem.com
ekransystem.com

→ **Meet me at the SOFTPROM Booth in Hall 7!**