Effectively Managing Insider Risks and Meeting NIS2 Requirements

with Ekran System

Ekran System®
Presented by Anna & Alex

The risks within your walls

Your invisible enemies. Who are they?

Malicious insiders - 25%

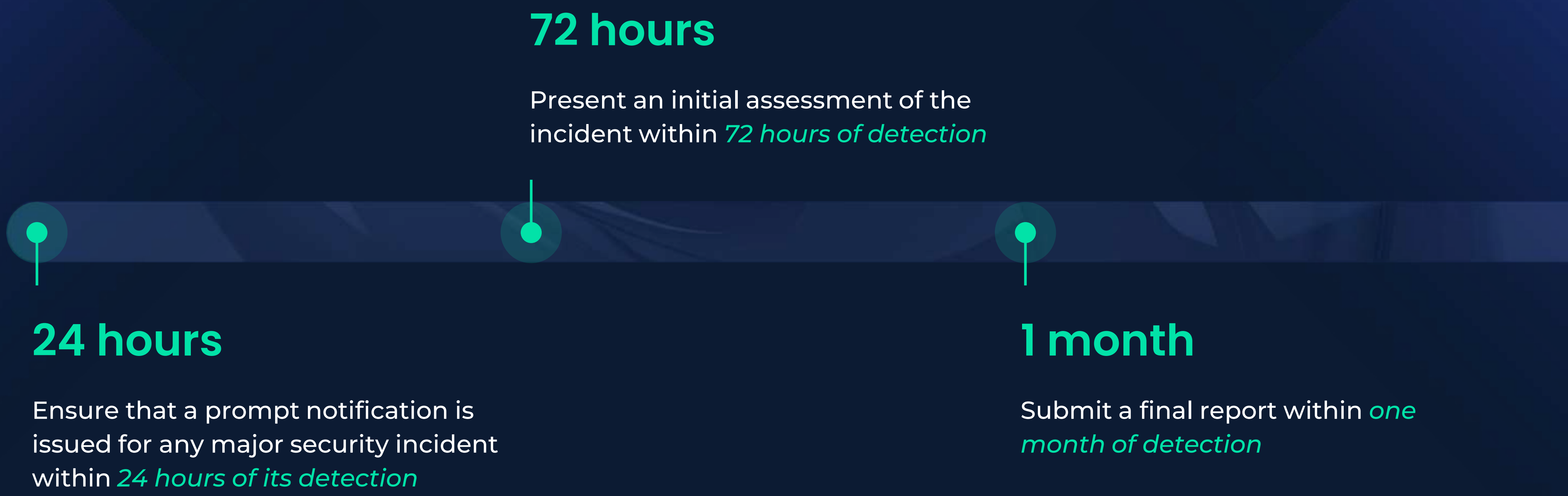
Outsmarted insiders - 20%

Negligent insiders - 55%

NIS2 becomes mandatory in the EU

> After **17 October 2024**, failure to comply with the NIS2 directive can result in **financial penalties** and sanctions against top management.

NIS2 reporting requirements



24 hours

Ensure that a prompt notification is issued for any major security incident within *24 hours of its detection*

72 hours

Present an initial assessment of the incident within *72 hours of detection*

1 month

Submit a final report within *one month of detection*

Non-compliance with NIS2 will cost you

Additionally, national authorities retain the authority to impose **additional penalties**, such as penalty payments, aimed at compelling essential or critical institutions to cease any identified violations of the directive.

Up to €10 M or min. 2%

Up to **10 million euros** or **minimum 2%** of the company's total annual global turnover in the previous fiscal year.

€20 M or 4%

In severe instances, they may escalate to as much as **20 million euros** or **4%** of the previous year's global turnover.

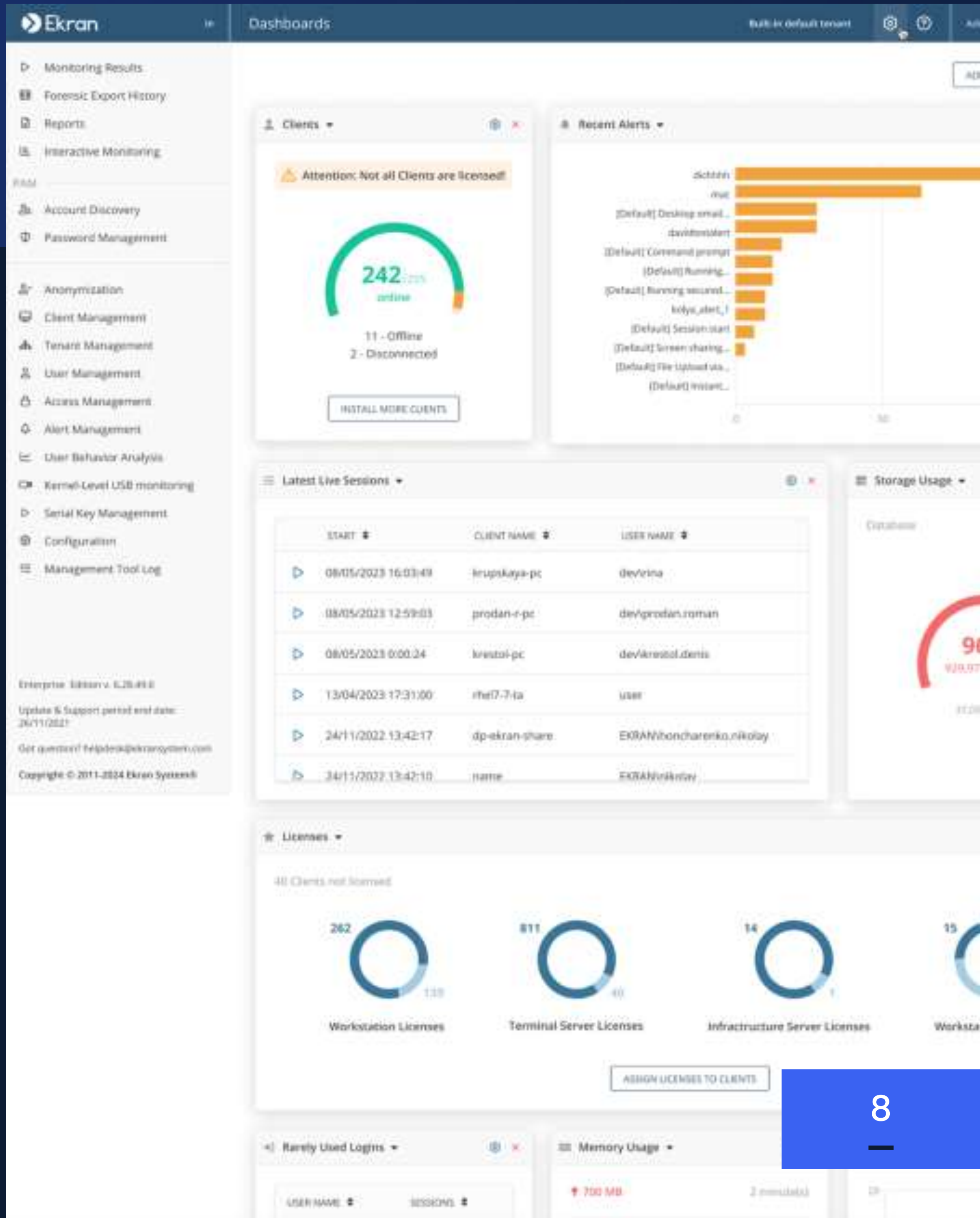
The essence of NIS2

The NIS2 directive requires you to have a **security system within your walls**. It establishes the legal framework that mandates organizations to monitor and secure their critical infrastructures against cyber threats and internal risks.

Ekran system

Introducing Ekran System

- Manage insider risks
- Meet NIS2 requirements



Enterprise Edition v. 6.28.49.0

Update & Support period end date: 26/11/2021

Got question? helpdesk@ekransystem.com

Copyright © 2011-2024 Ekran System®

Latest Live Sessions

START	CLIENT NAME	USER NAME
08/05/2023 16:03:49	krupskaya-pc	dev\irina
08/05/2023 12:59:03	prodan-r-pc	dev\prodan.roman
08/05/2023 0:00:24	krestol-pc	dev\krestol.denis
13/04/2023 17:31:00	rhel7-7-ta	user
24/11/2022 13:42:17	dp-ekran-share	EKRAN\boncharenko.nikolay
24/11/2022 13:42:10	name	EKRAN\nikolay

Secure access, monitor activities, and boost productivity — all in one

PAM

01 Privileged account and session management (PASM); Endpoint access management

02 Privilege elevation and delegation management (PEDM); Secrets management

03 Remote privileged access management (RPAM); MFA

UAM

01 Real-time user activity monitoring

02 Alerts for security incidents and suspicious activities;
Rule-based detection of abnormal activity

03 Searchable records of all third-party user activity

Productivity

01 Productive vs. Idle time tracking

02 Productivity dashboards with granular view

03 Customizable productivity reports; Power BI integration

NIS2 requirement	Measures to implement					
Policies on risk analysis and information system security	Leverage user activity monitoring to enhance visibility into IT infrastructure and detect insider threats, vulnerabilities, and other cybersecurity risks.	Granularly manage user access and monitor privileged users to prevent the risk of unauthorized activity.	Develop policies and procedures for identifying, assessing, and prioritizing cybersecurity risks.	Establish information system security policies.	Implement an information security management system (ISMS) based on ISO 27001.	Conduct an inventory of your sensitive assets and software.
Incident handling and reporting	Enable real-time detection of malicious user activity and other cybersecurity threats.	Implement and automate prompt response to security threats.	Ensure incident investigation with recorded session export for forensic purposes.	Develop an incident response plan (IRP) outlining the steps to be taken in the event of various types of security incidents.	Swiftly report cybersecurity incidents to the relevant regulators and authorities, according to Article 23 of the NI2 Directive.	Document your incident reporting procedures.
Business continuity, such as backup management and disaster recovery, and crisis management	Promptly detect security events that could potentially lead to a crisis.	Leverage user session recordings and activity logs to assess the impact on systems and data and to develop recovery plans and procedures.	Reduce the risk of unauthorized activity that may disrupt business operations by getting hold of access privileges in your IT infrastructure.	Facilitate communication by providing accurate and detailed information about a crisis and its impact.	Establish a business continuity plan (BCP) that includes provisions for backup management, disaster recovery, and crisis management.	Implement regular backup procedures for critical data and systems.
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	Secure RDP connections of third-party vendors, partners, and other supply chain entities accessing your IT infrastructure.	Implement measures to detect unauthorized data access, data exfiltration, or other remote user anomalous behavior of your third parties.	Verify and manage the identities of supply chain members accessing your infrastructure.	Protect access to sensitive data and critical systems by providing third-party vendors with one-time passwords and limiting their user session time in your IT infrastructure.	Conduct a supply chain risk assessment by issuing questionnaires and performing on-site visits with your supply chain representatives.	Outline the expected security requirements in service-level agreements with your third parties to enhance accountability.
Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure	Limit access to critical development infrastructure.	Monitor and record user activity within the development environment to check if users adhere to the established security policies.	Configure rules to receive alerts about the use of suspicious apps in the development environment or automatically shut suspicious apps down.	Thoroughly assess supplied software products and services during the acquisition process.	Establish a patch management process and a vulnerability disclosure policy (VDP) to address emerging weak spots.	Adopt the coding standards and practices to eliminate security risks during software development.

NIS2 requirement	Measures to implement					
Policies and procedures to assess the effectiveness of cybersecurity risk management measures	Monitor how your employees and other users stick to data security policies and other cybersecurity rules in your organization.	Use your user activity audit logs to assess how cybersecurity measures work in your organization.	Develop policies outlining how you assess your cybersecurity risk management measures.	Define key performance indicators to measure the effectiveness of specific cybersecurity controls and risk management efforts.	Conduct regular internal and external security audits to identify gaps and areas for improvement.	Maintain detailed documentation of your security assessment processes, findings, and actions taken.
Basic cyber hygiene practices and cybersecurity training	Get visibility into user actions and behaviors to identify and address any lapses in basic cyber hygiene practices and detect policy violations.	Monitor user actions during penetration testing to provide targeted feedback to users and promote adherence to cybersecurity best practices.	Use recorded user sessions to develop materials and case studies for cybersecurity awareness training initiatives.	Nurture users' cybersecurity habits by displaying warning messages in response to forbidden actions.	Conduct regular cybersecurity training covering basic cybersecurity practices, cyber threats, and attack vectors.	Facilitate collaboration between your employees, IT team, and security experts to share cybersecurity knowledge and discuss any questions and security concerns.
Policies and procedures regarding the use of cryptography and encryption	Encrypt user activity monitoring data, connections, and other sensitive records.	Encrypt passwords and user secrets in your organization.	Encrypt all usernames and aliases during user activity monitoring to protect user privacy.	Encrypt sensitive files, databases, and storage systems.	Create clear policies outlining which assets need encryption and which algorithms your organization uses.	Implement secure communication protocols such as SSL and TLS to safeguard your data in transit.
Human resources security, access control policies, and asset management	Ensure human resources security by detecting and investigating any unauthorized or suspicious activities carried out by employees.	Control access to sensitive assets and implement the principle of least privilege.	Capture users' interactions with critical assets and systems to ensure asset tracking, accountability, and protection.	Maintain a comprehensive inventory of all assets, including hardware and software.	Conduct background checks on job applicants to make sure they are not a security risk.	Establish procedures for employee departures, including revoking access and collecting company assets.
Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	Mitigate the risk of unauthorized access and account compromise with the help of two-factor authentication.	Establish a secure access request and approval workflow and enhance authentication procedures in your organization.	Take control of your employees' passwords by implementing password management solutions.	Ensure secure communication by encrypting all communication channels, especially for sensitive information.	Develop a separate, secure system for emergency communication, such as a dedicated phone line, satellite phone, or a specific application.	Train employees on secure communication practices, like recognizing phishing attempts and avoiding sharing sensitive information over unencrypted channels.

Benefits of using Ekran System for NIS2 compliance

- Manage privileged accounts and sessions
- Secure and control access to critical endpoints
- Verify user identities
- Detect and disrupt insider threats
- Promptly respond to incidents
- Get full network visibility

Download our ebook

Ultimate Guide
to NIS2 Compliance

Customer success story

cecabank

Cecabank ensures Swift CSP compliance with the help of Ekran System

cecabank

SWIFT account protection

Industry:

Banking

Location:

Spain

Market:

Spain, UK, France, Germany, Hong Kong

Challenges:

- Ensure a high level of financial data protection
- Meet SWIFT CSP requirements
- Reduce the risk of SWIFT account compromise
- Detect compromised SWIFT credentials

The solution

- Track all logins with the Ekran System agent on a CITRIX server
- Record all login attempts with Syteca's optical character recognition algorithm
- Log user activity and forward records to the customer's SIEM system for further analysis

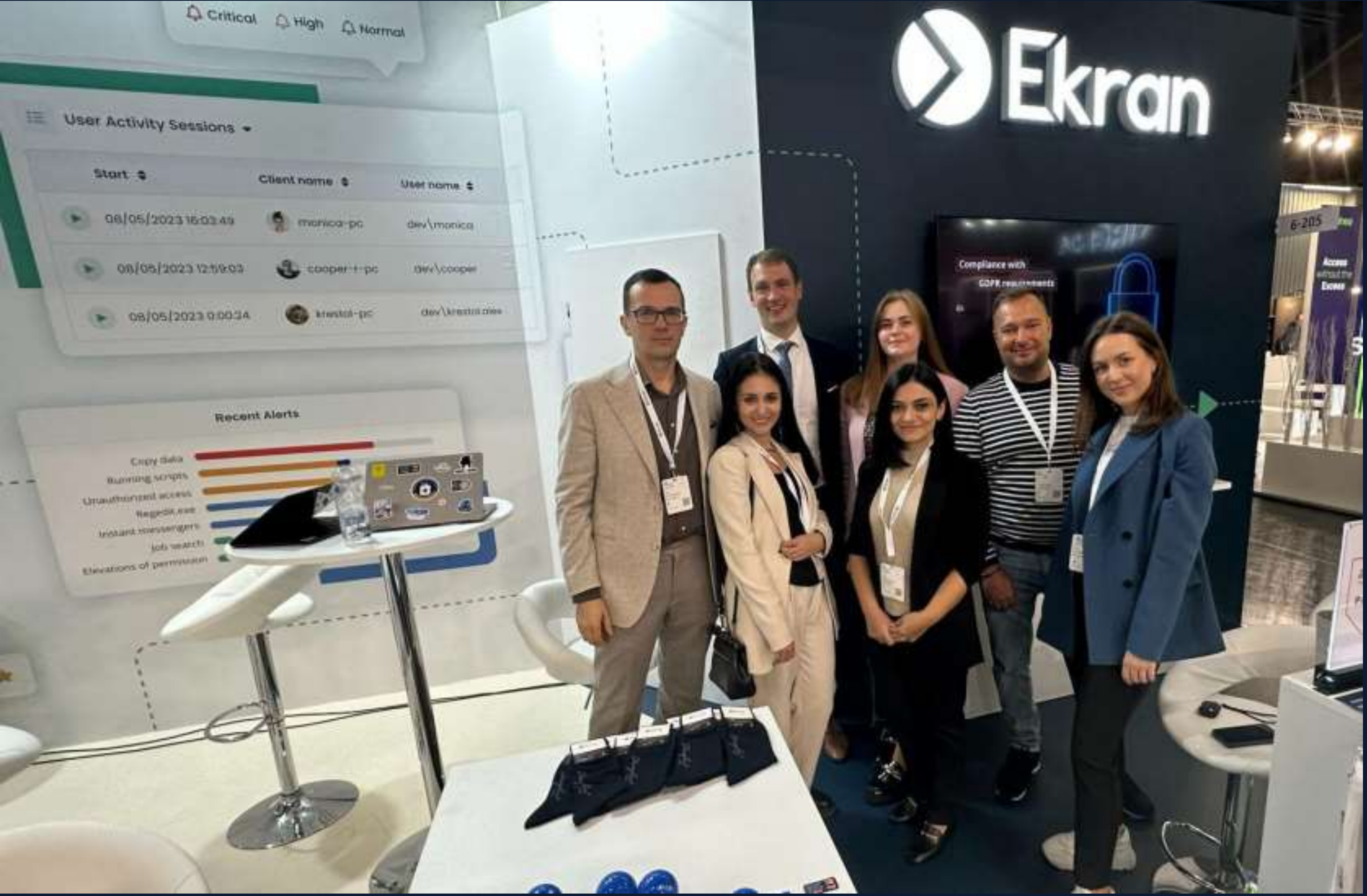
The result

- ✓ Compliance with SWIFT CSP requirements
- ✓ User activity transparency within the SWIFT environment
- ✓ Ability to prevent and detect attacks in the SWIFT environment in the early stages

Ekran System customized some of their functionality to help us solve our security tasks.

Now, monitoring and auditing users accessing the SWIFT network through our environment is much easier.

Security Architect at Cecabank



Founded

in 2013

Offices

USA, Poland, Germany, Ukraine

Customers

2500+

300+ partners

in 56 countries

About Ekran System

The future of our company

Ekran System is becoming

Syteca

arriving this October

New name, more advanced platform, same reliable team

Syteca

Thank you!

For more information email us at:

sales@ekransystem.com

marketing@ekransystem.com

support@ekransystem.com