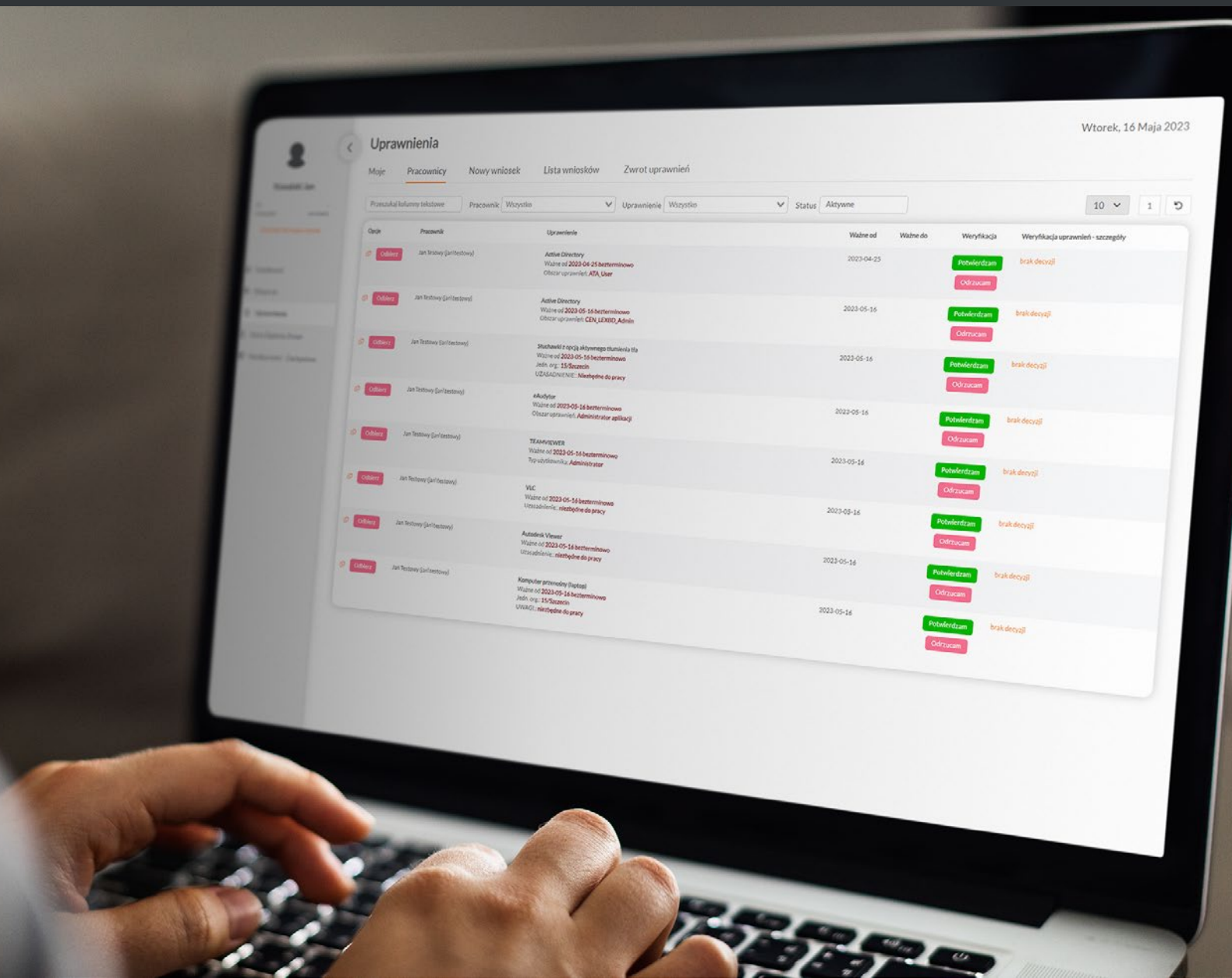
eauditor IAM

IDENTITY ACCESS MANAGEMENT (IAM)

Comprehensive software that automates the processes of granting, verifying and revoking authorizations to IT systems.



BENEFITS OF IMPLEMENTING THE SYSTEM

eauditor IAM

SECURITY

The implementation of the system ensures the possibility of ongoing monitoring of authorizations by superiors by providing them with easy access (via the Employee Panel) to the authorizations held by employees. Employees also have access to authorizations and can apply for the removal of unjustified authorizations. The increase in security results from transferring supervision over authorizations to lower levels of the organizational structure.

ACTIVE AUTHORIZATION PREVIEW

Managers can check the authorizations their subordinates have to IT systems at any time. Access to the view is possible in the Employee Panel. Employees can also verify their authorizations.

AUTOMATIZATION

The system enables acceleration of the processes of granting, withdrawing and auditing authorizations to IT systems. Thanks to this, entities employing several thousand employees can significantly shorten the processing time of authorization applications. The applicant does not need to know who is responsible for considering the application. As a result of defining the relations between the files, the system automatically indicates the person considering it. Verification of the compliance of authorizations is carried out in two stages - by the direct superior and the IT department.

SIMPLE APPLICATION FOR PERMISSIONS

The applicant does not need to know who is responsible for considering the application. As a result of defining the relationship between the files, the system automatically indicates the person considering it. Verification of the compliance of authorizations is carried out in two stages - by the direct superior and the IT department. This allows to limit the number of employees with incorrect access to IT systems.

NOTIFICATIONS

Each participant in the authorization management process receives automatic email notifications regarding the creation and change of the authorization application status. There is no need to log into the system to verify the application status.

AUDIT

The system allows you to define cyclical verification of already granted authorizations to IT systems. The verification process is automated and regularly reminds about the need to conduct an audit. Thanks to this, decision-makers are sure that the verification will take place on time.

BENEFITS OF IMPLEMENTING THE SYSTEM

eauditor IAM

INTEGRATION

MS Active Directory/eHelpDesk

The system's built-in integration mechanisms with services and products streamline the work of the system administrator. It is possible to: automatically import the organizational structure, import employee data, directly send tickets to technical support departments or view current permissions in the Employee Panel.

EMPLOYEE PANEL

The Employee Panel is a web application available to employees from the computer desktop (icon) without having to log in. The panel automatically identifies the logged in user and authenticates them using SSO.

A SYSTEM ADAPTED TO EVERY INDUSTRY

The strength of the system is its full configurability at the implementation stage. It is possible to create records and authorization definitions independently. It can be used in the area of handling requests for access to, for example, production machines or rooms.

PURPOSE OF THE SYSTEM

The system's task is to simplify and automate the process of managing authorizations.

The system allows for the implementation of the following processes:

- requesting permissions to individual systems/applications,
- requesting permissions to groups of permissions/profiles,
- requesting the return of permissions,
- verification of formal permissions,
- verification of actual permissions,
- ongoing monitoring of permissions,
- performing an audit of permissions,
- requesting changes to software,
- physical and automatic granting of permissions in other systems/services.

FOR WHOM?

The system is designed for entities with a large, complex and distributed infrastructure. Quick benefits from implementing the system are visible in entities with over a thousand employees who have access to IT resources.

FILES

Dictionary lists necessary for editing and creating an application. The system administrator can independently define files, enter data into them, modify them, create any connections between them and enter comments within them, which will be displayed when creating an application.

DEFINITIONS OF PERMISSIONS

Defined files are used to create definitions of authorizations for individual IT systems and profiles (groups of systems). A properly defined request will be directed to the appropriate support group in the eHelpDesk system.

APPROVAL TEMPLATES

Defining approval templates allows you to clearly define the person or people responsible for accepting or rejecting the application. Email notifications are also defined, which inform all process participants about the current stage and status of the application.

OPENING BALANCE AUDIT

The function is used to verify current (current) authorizations granted to employees. After importing data to the system, the administrator can check the compliance of granted access to IT systems.

NEW APPLICATION

Application form enabling the registration of the following information:
applicant, person to whom the application relates, subject of the application, expiry date of the authorization.

LIST OF APPLICATIONS

View containing a list of applications divided into current statuses. From the list of applications, it is possible to make changes to the application, change the approver, track the application history, and divide the list by the subject of the application.

PREVIEW OF GRANTED PERMISSIONS

The manager (supervisor) has a preview of the permissions granted to all of his subordinates. The employee has a preview of all of his permissions. The view of current permissions allows you to create a duplicate application for an existing permission.

RETURN OF PRIVILEGES

The decision-maker can at any time withdraw selected or all permissions from employees. The employee can apply for their return within the scope of their permissions. This prevents unauthorized access to programs and resources, thus increasing the level of IT security.

VERIFICATION OF PERMISSIONS

The system enables two-step verification of granted authorizations:

- **formal verification** – consists of confirmation of authorizations by the employee's direct superior. The system enables automatic generation of notifications about the need to conduct formal verification. After formal verification, it is possible to start the actual verification process.
- **actual verification** – is carried out by the technical support department. It consists of checking authorizations that have already been formally verified. The IT department confirms or rejects the authorizations.

APPLICATION PROCESS

eauditor IAM

1 NEW APPLICATION FOR AUTHORIZATION

The applicant creates a new application after logging into the system or from the employee panel.

2 SELECTION OF THE EMPLOYEE OR GROUP OF EMPLOYEES TO WHOM THE APPLICATION APPLIES

The applicant selects the employee or group of employees to whom the application applies from the available list.

3 SELECTING THE SUBJECT OF THE APPLICATION

The applicant indicates, in accordance with the definition of authorizations, the subject of the authorization request. Within one form, he or she can apply for the granting of multiple authorizations, even if the acceptance is made by different verifying persons.

4 INDICATION OF THE VALIDITY PERIOD OF THE AUTHORIZATIONS

The applicant sets the validity period of the authorization (indefinite period or indicates a specific time period).

5 COMPLETION OF REQUIRED PARAMETERS

The applicant completes the required fields in the application, which are defined in the approval templates.

6 SENDING THE APPLICATION

The requesting person sends the request, which is then forwarded in the appropriate order to the people indicated in the approval templates.

7 ACCEPTANCE OR REJECTION OF THE APPLICATION

The decision-maker receives an e-mail notification of pending applications. After logging into the system or from the employee panel, they accept or reject the application.

8 EMAIL NOTIFICATION

Each participant in the process is informed about changes in the application status via e-mail notifications.

9 EXECUTION OF THE APPLICATION

Information about the acceptance of the application by the business owner is forwarded to the specific support group to generate authorization.

10 GENERATING PERMISSIONS

The IT department assigns real (physical) permissions to IT systems. It is possible to automatically generate permissions using scripts (e.g. creating a domain account, setting a password, access rights to shared folders, creating an e-mail account, etc.). The list of possibilities for generating permissions is unlimited as a result of using the PowerShell engine.

SECURITY

The system was assessed for compliance with OWASP Application Security Verification Standard (ASVS), version 4.0.3 at level 2, excluding points requiring source code analysis.

OWASP ASVS defines best practices for testing application security mechanisms and web applications.

PURCHASING MODEL AND LICENSING

The system is offered in a subscription model (12/24/36M) or perpetual license. The price of the system depends on the number of system administrators (the number of accounts for people authorized to administer the system) and the number of users appearing in the processes (in practice, this number is equal to the number of people in MS Active Directory).

INSTALLATION/RUN/IMPLEMENTATION

- The system implementation process begins with a thorough analysis of the type and number of systems, types of authorizations and application processing methods.
- The system installation and configuration is performed remotely in the client's infrastructure.
- The implementation process consists of creating files and connections between them and defining all processes. The next step includes conducting the so-called opening balance of authorizations - data is imported from current systems containing authorizations (if any), MS Active Directory and the necessary integrations are created. The process of creating the opening balance can be created multiple times until error-free authorization lists are obtained. After creating the opening balance of authorizations, a two-stage verification is carried out (formal verification and actual verification).
- After completing the implementation process, the system's operation is monitored for a period of 3 months and the necessary corrections are introduced.

INTEGRATION

The system is integrated with the following services/products:

- Microsoft Active Directory - in terms of importing the organizational structure and people (employees), login authentication,
- CAS - in terms of login authentication,
- Employee Panel - in terms of requesting, reviewing and accepting permissions,
- eHelpDesk - in terms of processing requests for permissions.

Please contact us

www.eauditor.eu/en/IAM