

Cybercom

CESP

Cybercom Enhanced Security Platform

Cybercom Enhanced Security Platform, CESP, is an integrated platform that provides comprehensive security functions for high assurance applications that require high level of security and protection. CESP has been developed based on the latest technology to be able to create a robust and flexible solution that conforms to the highest standard of performance and security.



Executive Summary

There are a large number of systems where the confidentiality, integrity and availability of the applications and all the data are of great importance. Typically, this can be assured by implementing the system within a closed network environment with very limited access to applications and data for external users.

However, the expanding demand for service oriented applications increases the need for opening up these systems for bidirectional communication with external users and services. Opening up these systems for external users and services is not a trivial task. Thus, there is a need for a security layer which enables communication with internal applications and data while not compromising the integrity, confidentiality and availability of the system.

Cybercom Enhanced Security Platform, CESP, is an integrated platform that provides comprehensive security functions for high assurance applications that require high level of security and protection.

The Solution

Cybercom Enhanced Security Platform, CESP, is an integrated platform that provides comprehensive security functions for high assurance applications that require high level of security and protection.

CESP has all the necessary components that together form a unique security layer for services and information. CESP contains the following seven components:

- Authentication - Assures that only trusted users can get access to the system
- Access Control - Make sure that authorized users only can access data he/she has the right to see. Also controls the ability to update data
- Logging - Collects information about all user activity in the system
- Control and Audit - Functions that can be used to control and monitor user activity in real time and to analyze logs and to perform audits.
- Secure Communication - Secure system for communications across network boundaries
- Server Management - Manages all services on all servers
- Notification - Notify senders and receivers in pre-defined situations in a secure and reliable way

Authentication using CESP-ID

Authentication is needed in order to assure that only trusted users can get access to the system. In CESP, authentication of user is done using CESP-ID. CESP-ID is a flexible authentication solution that provides secure authentication of users and enables Single Sign-On between applications and organizations.

CESP-ID assures that an actor has been identified, authenticated, and assigned different attributes. This assertion is a signed proof and it can then be used to gain access to an application instead of requesting a new authentication from the actor. In CESP-ID this assertion is based on the SAML standard.

CESP-ID is based on the Security Assertion Markup Language (SAML) 2.0, which is an XML-based standard for exchanging authentication data between security domains. CESP-ID supports several different authentication mechanisms and can be integrated with Trusted Security Server for providing verification of electronic ID (EID).

Access Control with CESP-Access

Access control ensures that an authorized user only can access data or a service that he/she has the right to see and use. Access control in CESP is performed by CESP-Access. Once the user has been uniquely identified, his/her ability to access data or application is checked.

In CESP, access is based on user attributes with a technique called Attribute Based Access Control (ABAC). The application can, based on these attributes, grant access to the information based on its own access policies. This way of granting access give much more flexibility than traditional access control based on groups or roles. This flexible access control system also reduce the burden of an extensive administration of groups and roles when a lot of different applications can be accessed using the CESP-ID Single Sign-On functionality.

Logging using CESP-Log

Logging is a central activity in a secure application in order to detect unwanted behavior in the system. CESP-Log is the module that is responsible for the logging service in CESP.

Logs are collected from all different levels in the system, from operating system, network components, database systems and application components. All log information is encrypted and signed and sent to a central log service where it is saved in a protected repository using signed log chains.

The local log agent can receive logs even if the central log service is not active or if the communication to the central service is down. The log agent handles this kind of situation by buffering the information locally. The log agent transmits this buffered data when the communication with the central server has been resumed.

Analyze Logs using CESP-Audit

The benefit of having a central storage of log records from all systems within a domain is that it enables a more complete log analysis. CESP-Audit analyses all logs that have been collected by CESP-Log.

Based on this analysis alert can be generated and sent out according to pre-configured rules. It is also possible to create graphical reports to visualize the logs and to be able to study different activities in detail. An administrator can create such reports using an intuitive graphical interface. Report creation can be scheduled so that standard reports can be sent out on a regular basis to predefined recipients.

The analysis of logs is performed in two steps. In the first step, the log files that has been collected by CESP-Log are normalized and predefined information from the log files are extracted. The next step is the analysis of the data using the report generator.



About Cybercom

The Cybercom Group is a high-tech consultancy that offers global sourcing for end-to-end solutions. The Group established itself as a world-class supplier in these segments: security, portal solutions, mobile services, and embedded systems.

Thanks to its extensive industry and operations experience, Cybercom can offer strategic and technological expertise to these markets: telecom, industry, media, public sector, retail, and banking and financial services.

The Group employs 2,000 persons and runs projects worldwide. Cybercom has 28 offices in 11 countries. Since 1999, Cybercom's share has been quoted on the NASDAQ OMX Nordic Exchange. The company was launched in 1995.

Contact Details

For further information, please contact:

Henrik Johansson, Business Unit Manager
henrik.johansson@cybercomgroup.com
+46 70 825 00 80

or visit our website www.cybercom.com