CSI Emergency Request 2020

Secure Emergency and Privileged activities in SAP

Also available as Software as a Service

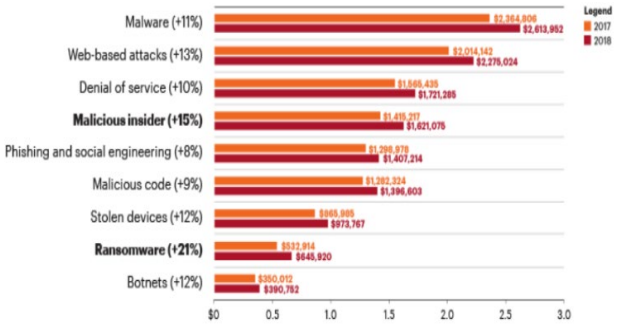
Emergency and privileged Access Management for SAP© systems

SAP users with broad access are considered "the keys to the kingdom" for attackers. People-based attacks have increased the most. Therefore, this is one of the key items in data security.

CSI Emergency Request (CSI ER in short) manages and controls all emergency and privileged activities in SAP systems.

The automated emergency procedure mitigates risks and lowers a timely response of the intervention team when emergencies in the SAP systems needs to be solved. IT provides temporary broad access to the SAP systems for the team to solve the issue with full evidence logging for monitoring and auditing this usage.

Also, all activities of the other privileged SAP users (like SAP*, DDIC) are logged and can be monitored and reviewed.



CSI Emergency Request:

Allows permitted users to request an emergency session through a dedicated SAP user ID. With automated credential creation and login for the requestor. The emergency user performed actions are traced to monitor, detect (mis)usage, review and audit the emergency session. The owners of the emergency user(s) are informed via email.

Safeguards the logging. Logging is kept outside the SAP system.

Can be integrating with a ticketing system.

Logs all emergency and privileged user activities

Logs all activities and included old and new values for table changes.

Focusses on the user experience, with multi-language support and web-based application, dashboards and reports.

Includes monitoring and follow up of which Emergency sessions has not (yet) been reviewed.

Features

- Secures the emergency accounts since no credentials are shared
- Logging is kept outside the SAP system
- All changes are logged, with old and new value(s) for comparison
- Full audit trail available
- Multi language support
- Web based application
- User Behaviour Analytics with dashboarding and reports
- Identifies more critical emergency sessions that should receive the attention of the compliance team
- Monitoring on review of sessions

CSI tools - audit and security software for SAP environments
Security Research Center Herent | Bieststraat 2 | B-3020 Herent | Belgium
Tel: +32 16 308 000

www.csi-tools.com

Observe. Think. Act.

Includes User Behaviour Analytics: Overview reports exist that list all transaction codes of multiple sessions. These reports provide full insight in why emergency sessions are used in a very detailed and transparent way.

Identifies more critical emergency sessions that should receive the attention of the compliance team:

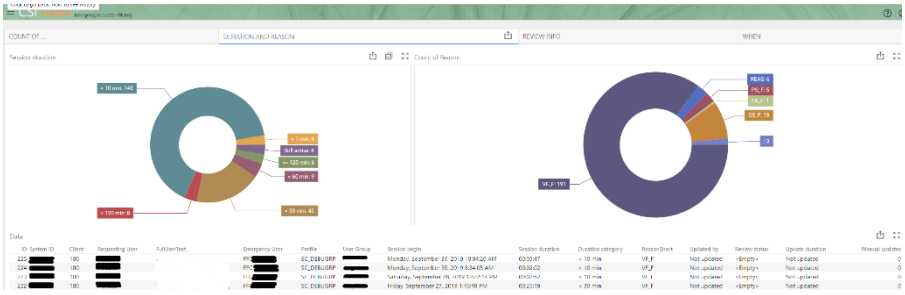
- Definition of critical items per emergency session.
- Classification of transactions that should be reviewed. These analyses work cross all emergency sessions selected.

Provides insight in criticality during reporting and analysis. Items that can be used are:

- SAP Users
- ER Profiles
- User Groups
- Duration of a session
- Out-of-Office hours: e.g. From Friday 8pm till Monday 6 am

Dashboards that list overview ER sessions (all sessions or critical items only):

- Top Users
- Top ER Profiles
- Duration
- Timeline frequency
- Reason
- Review status



Value proposition of CSI Emergency Request

Efficient (ROI)

- Web based user interface to reduce time on implementation and maintenance
- Timely response when emergencies in SAP needs to be solved.

Effective

- Safeguarding of login credentials
- Full audit log available
- Automate time consuming processes
- Allow flexibility in providing broad access rights when needed, without manual interaction and with full evidence.

Tuned for business readiness

- Be in control of exceptional situations and privileged users and what users are doing.
- Fully adjustable to rapidly respond to changes in the internal business environment
- organizations can identify and react quickly to control failures/weaknesses, noncompliance, and adverse events in a timely manner so that action can be taken.