Do you know who is reading your email right now?

IDECSI provides real-time detection of data breaches – you know the instant anyone fraudulently accesses your applications

IDECSI
Enterprise Security

Office 365, Microsoft Exchange, G Suite
Many other applications

Continuously monitoring all access to applications, the IDECSI ACCESS ANALYZER identifies suspicious behaviour and immediately alerts the user

Flash Audit

- One-off health check of email system
- Analysis of mailboxes and platform config
- Thorough report of all vulnerabilities

Breaches detected

Malicious email forwarding rules

Abuse of administrative privileges

Weak passwords and compromised credentials

Password interception over malicious WiFi

Employee lifecycle management

Configuration errors

Keyloggers, malware

Immediate ROI

Installation and configuration within hours, agentless

Immediate report of existing vulnerabilities
- Out-of-date configuration
- Unexpected forwarding rules
- Unwanted send-as permissions

Learning period during which IDECSI ACCESS ANALYSER learns normal user behaviour

Real-time alerting for any potentially malicious activities not matching dynamically learned user profile

No additional constraints imposed – no new passwords or smart keys

Completely secure

IDECSI ACCESS ANALYSER requires only read-only access to logs

No configuration capabilities to your platform

No access to document content, email content or other confidential information

Self checking – any change to IDECSI configuration alerted in real-time

User centric design

The user is directly alerted of potential breaches*

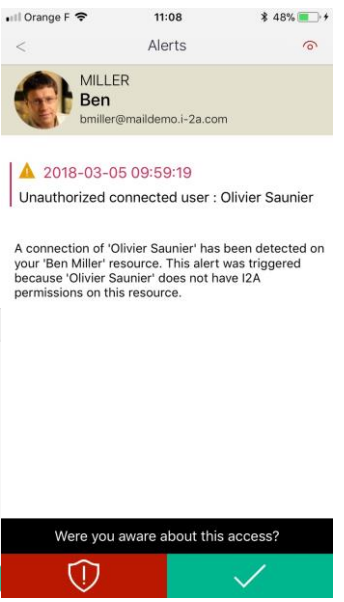
The user confirms a genuine breach

Only then does the security team engage

Minimal false positives

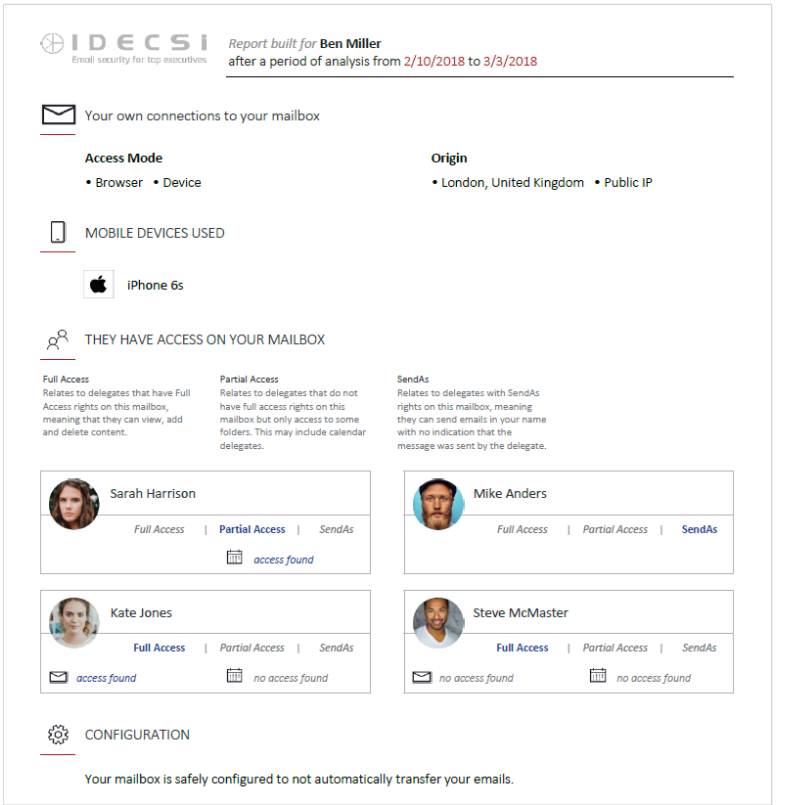
Users become intimately involved with their own security

* Security team decides which alerts the user sees



70 major customers, including 20 in the Fortune 500

BELGIUM PRIME MINISTER'S OFFICE · ENGIE · SANOFI · SOCIETE GENERALE · SNCF · L'ORÉAL · SFR



Report shows how resource is normally accessed, who has permissions to access, who has used those permissions

The right protection for everyone

Real-time Premium Protection

- Real-time notification of all fraudulent access and malicious reconfiguration
- Monitoring of alerts to support user in confirming correct action to take
- Managing config changes, weekly report

Real-time Protection

- Real-time notification of all fraudulent access and malicious reconfiguration
- Designed for those with sensitive information in their mailboxes and other applications

Permanent Audit

- Constant collection of logs
- One-page report available at any time
- Complete information on configuration and access over the previous weeks or months

Flash Audit

- One-off health check of email system
- Analysis of mailboxes and platform config
- Thorough report of all vulnerabilities

Applications protected

Office 365 · Dropbox · OpenText (The Content Experts) · OneDrive · Exchange · G Suite · SharePoint · SAP

New applications continuously being added

Proprietary applications supported

Operational model

The IDECSI ACCESS ANALYZER constantly collects logs and config objects from all protected applications to analyse all operations, taking into account
• IP range • user-id • time range • device used • simultaneous sessions
• IP geo-position • actions taken • device geo-location (if enabled).

All operations are cross-checked with
• the user's dynamically learned profile
• the context of the action
• proprietary registry of application vulnerabilities.

IDECSI's big data platform uses machine learning to identify suspicious behaviour with exceptional accuracy.

Depending on the nature of the activity, the user or the security team alerted.

prix de l'innovation des assises 2010 — Assises of Security Innovation Prize

Golden Cloud Innovation Prize

T Night Gold Medal

Lauréat Innovation IT 2017 — Innovation IT – CRIP / CTO

Patented in Europe & USA

Visit www.idecsi.com
or email contact@idecsi.com

Highly flexible

Logs and detailed information from the IDECSI ACCESS ANALYSER are available for many months.

Alerts and other information can be sent to a SIEM. There is no need to store the detailed application level logs in the SIEM, significantly reducing SIEM storage costs.

Easy-to-use administration platform can be managed by internal security teams – providing additional protection with outsourced IT.

Alerts and notifications can be displayed directly in an existing centralized security administration console.