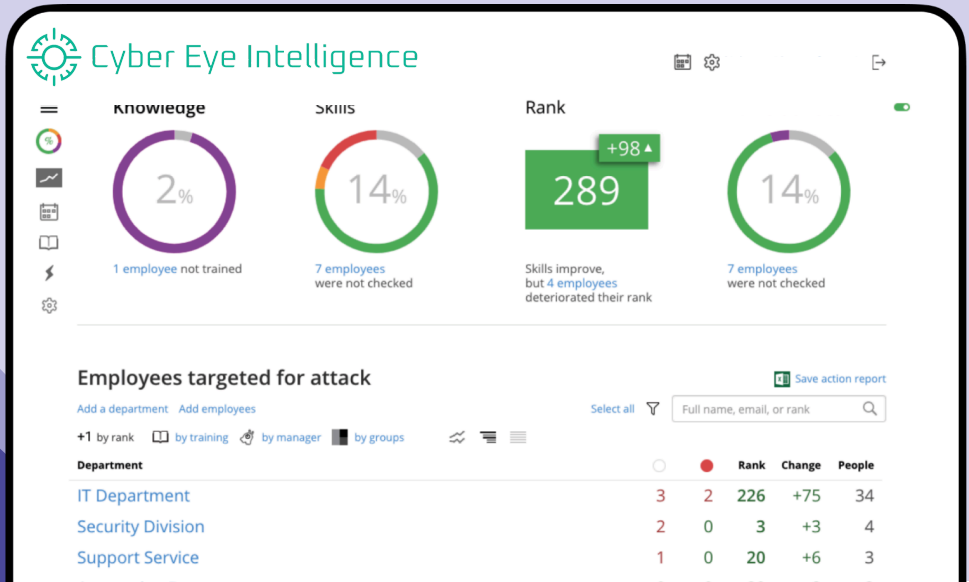
SiberSentinel

Cyber Eye Intelligence

AttackAvert

Platform to automate continuous employee learning and skill training for information and physical security



Humans were the cause of 68% of information security incidents in 2024

Source: Verizon Data Breach Investigations Report

To reach corporate systems containing valuable data, scammers need to only hack a single user who already has the necessary rights.

Scammers usually attack employees via email, sites, social networks, messengers, mobile devices, offices and workspaces.

Email

Messengers

Sites

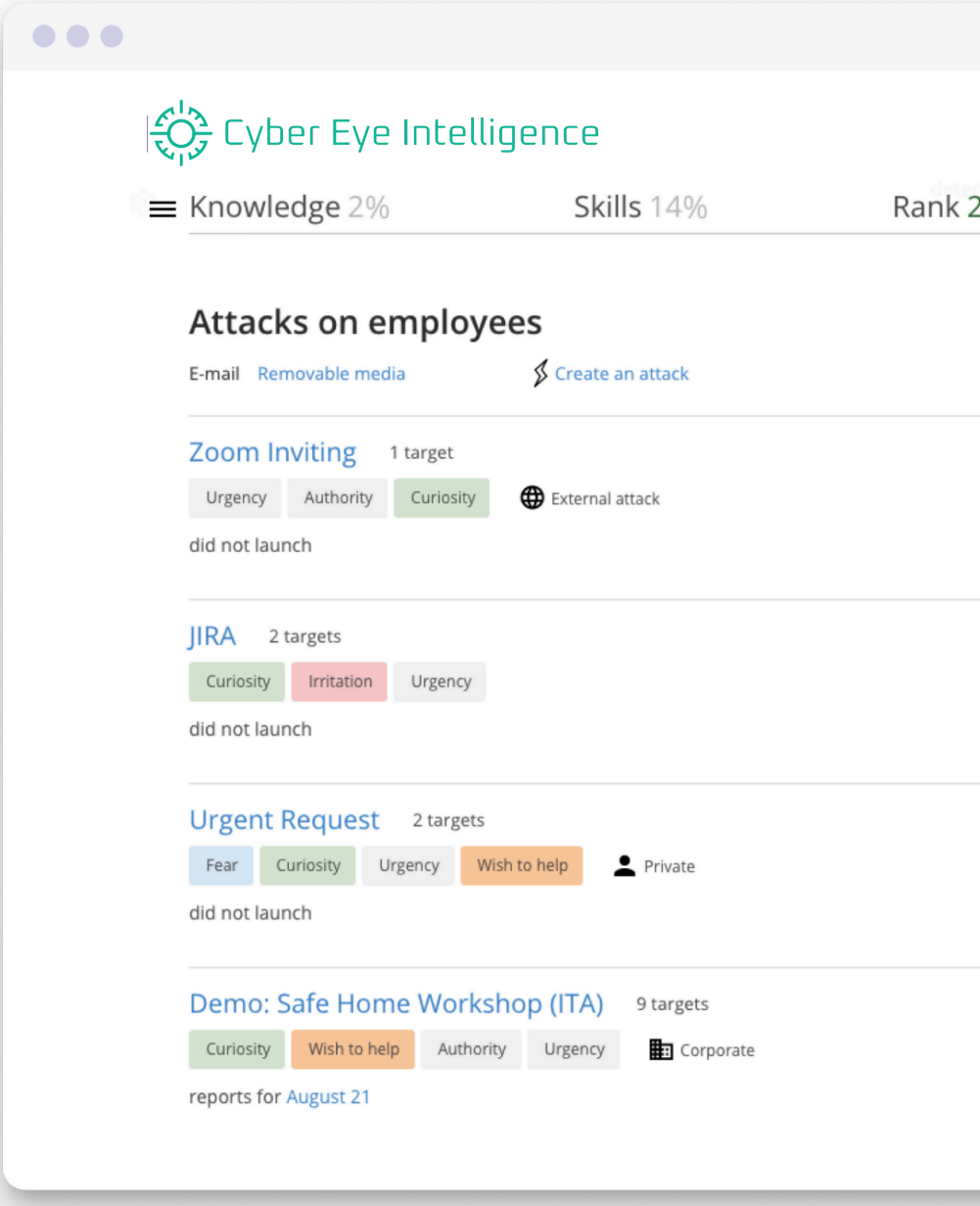
Mobile devices

Social networks

Office, workspaces

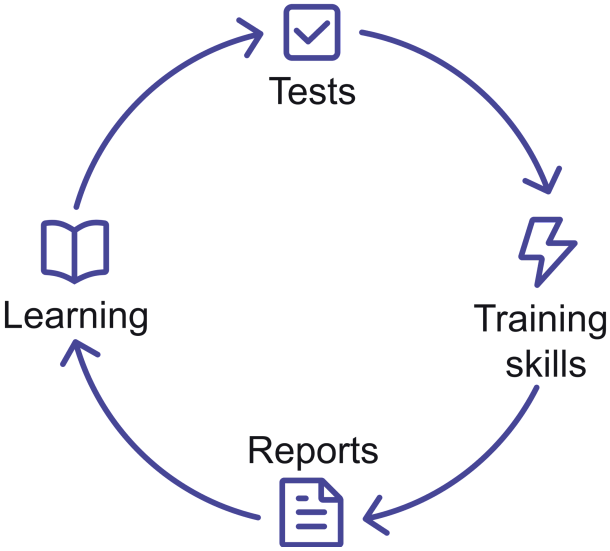
A platform to protect against employee-directed cyber attacks

- Supports the security team with creating an automated awareness process to reduce security risks.
- Contains electronic courses and tests, as well as scenarios and templates to simlulate cyber attacks
- Supports the development of employee skills to counter all types of digital attacks:
  - via email,
  - websites,
  - USB devices,
  - spoofed Wi-Fi access points,
  - social networking and instant messa
- Platform content is regularly updated to address the latest threats.


Cyber Eye Intelligence
Knowledge 2%
Skills 14%
Rank 2
Attacks on employees
E-mail
Removable media
Create an attack
Zoom Inviting
1 target
Urgency
Authority
Curiosity
External attack
did not launch
JIRA
2 targets
Curiosity
Irritation
Urgency
did not launch
Urgent Request
2 targets
Fear
Curiosity
Urgency
Wish to help
Private
did not launch
Demo: Safe Home Workshop (ITA)
9 targets
Curiosity
Wish to help
Authority
Urgency
Corporate
reports for August 21

Create an automated awareness process to reduce security risks

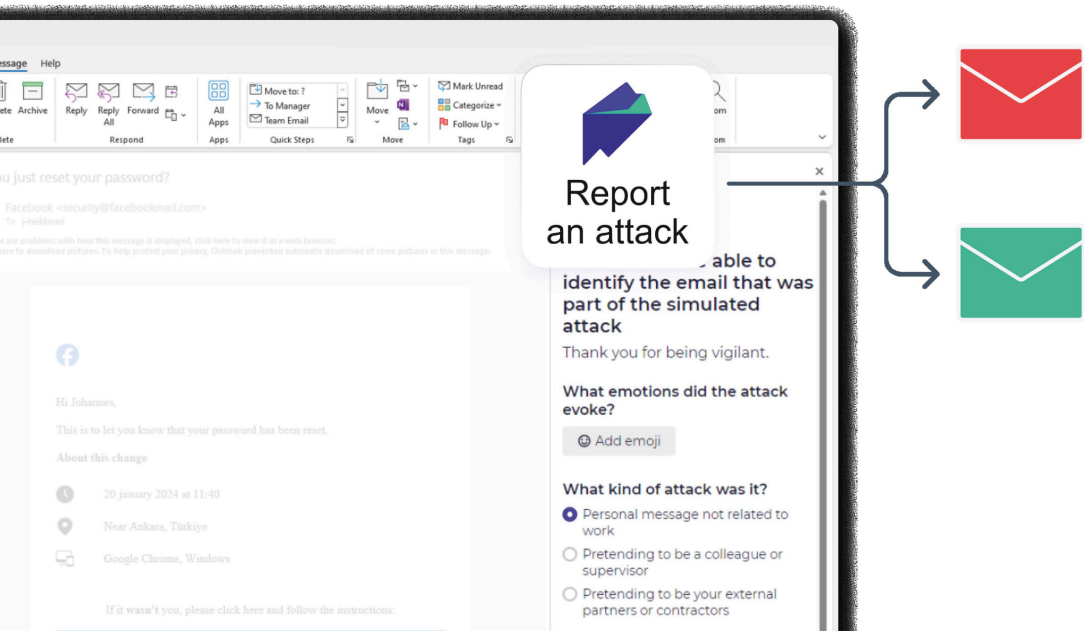
- Traditional distance learning and mandatory testing to raise security awareness issues.
- Continuously manage employee skills through simulated attacks.
- Determine the security level of an employee, department, and the entire organization.



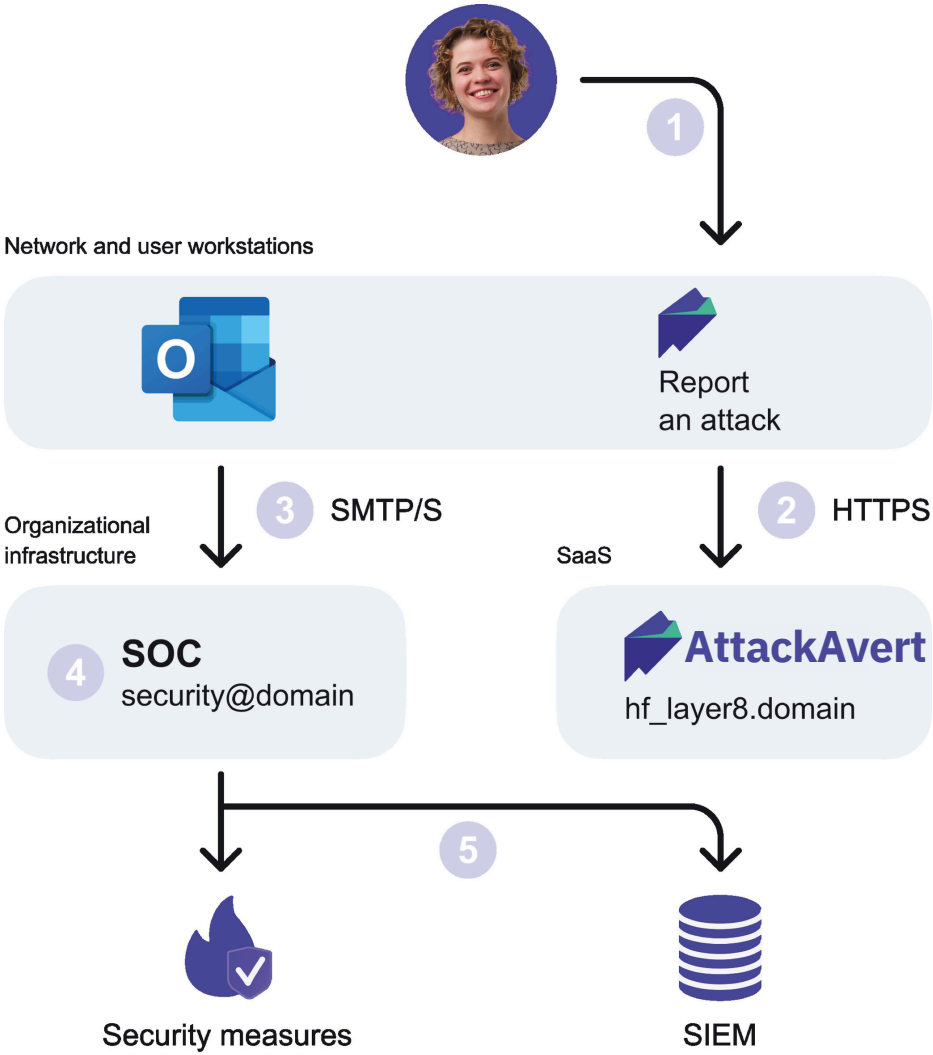
AttackAvert can be used as an LMS: upload your courses and assign them to employees.

AttackAvert enables employees to quickly report attacks and protect the organization

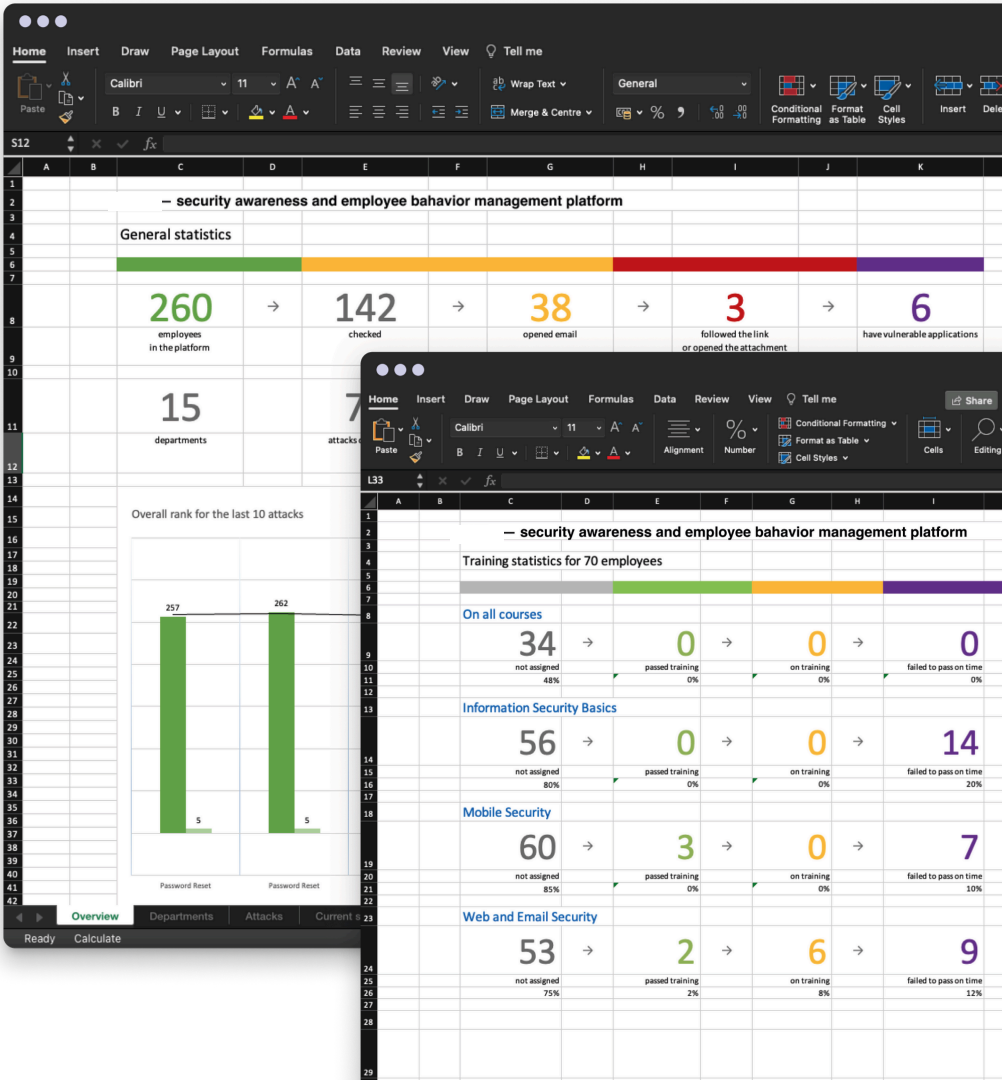
- Install a plugin in your mail client to enable an employee to report suspicious emails with a single click.
- The employee sends an email via a secure channel to whoever needs it, with attachments and important information.
- It is possible to filter simulated and real emails.



Enhance SOC processes by integrating employee reports



Effortlessly evaluate the effectiveness of the process and provide reports during audits



Integrating AttackAvert with security tools and IT systems increases the security posture of your company

Scenario	Security tool or IT system	Method
Reactive learning	Antivirus, DLP, Security Email Gateway, Web Security Gateway, vulnerability scanner	API
Assign training and view results from a single console	IRP/SOAR	API
Notification of unwanted emails, websites, and attachments	Plugin for email clients, plugin for browsers	plug-in
Training in an external system	LMS	API
Send security events to the monitoring system	SIEM	syslog
Compatibility with information security products	Antivirus, DLP	N/A
Block unwanted emails	Security Email Gateway	API
Access control taking into account the employee's skill level	IDM	API
Import a list of employees	Directory Service HRM/ERP	LDAP(S) API

Contact us at info@cybereyeintel.com to schedule an online demonstration of the AttackAvert platform

Cyber Eye Intelligence

SiberSentinel

19th Floor, OneWest, Financial District,
Nanakaramguda, Hyderabad - 500008
Telangana, INDIA
Email : info@sibersentinel.com