OutThink

World's first Cyber Security Culture platform

hello@outthinkthreats.com
www.outthinkthreats.com

Activate
Behavioural
Change

Using an innovative cognitive learning methodology and robust socio-technical principles, OutThink empowers you to build a risk aware culture and enables the implementation of ENISA's Cyber Security Culture (CSC) framework.

enisa

BUILD A RISK AWARE CYBER SECURITY CULTURE (CSC)

There is industry-wide recognition that traditional security awareness raising campaigns (e.g. legacy CBT, phishing simulations) are not, in themselves, affording sufficient protection against ever evolving human focused cyber attacks. CSC is broader in both scope and application than security awareness, being concerned with making cyber security considerations an integral part of employees' behaviours and conduct, embedding them in their day-to-day actions.

ENISA CSC IMPLEMENTATION GUIDE	OUTTHINK PLATFORM FUNCTIONALITY
Step 1. Set up your core CSC work group Tasked with strategy, ensuring evidence-based approach to CSC and implementation of CSC activities.	Recruitment of cyber security champions - members of the CSC work group, responsible for implementation of CSC activities Advanced metrics to support envidence-based approach
Step 2. Business understanding and risk assessment Talk to employees to identify existing CSC, beliefs and practices; this will drive and shape subseq. activities.	Assessment of human factor risk, feedback gathering to identify existing CSC, beliefs and practices; activate human sensors
Step 3. Define main goals, target audience and success criteria for your CSC programme	Identify target audience, associated risk profiles and core training requirements; success criteria and goals defined at onboarding stage
Step 4. Gap analysis between as-is and goals Calculating your CSC as-is current state, a prerequisite for quantifying the impact of CSC activities.	Assessment of as-is current state CSC - knowledge, attitudes, people's perception, current level of protection (key security controls in place across the oganisation)
Step 5. Select one or more activities To close the gap between the current as-is and your goal Create or buy tools to implement.	OutThink provides security awareness training, phishing simulations, policy attestation, live workshops, executive briefing sessions
Step 6. Run your selected activities + talk to employees to identify existing CSC; this will drive and shape subsequent activities.	Delivery of relevant, tailored cognitive security awareness training via the OutThink social platform, enabling two-way communication
Step 7. Rerun as-is and analyse the results	Assessment of human factor risk; relevant metric and dashboards to track short and long term CSC improvement
Step 8. Review and consider your results before deciding on next action	Review actionable intelligence and metrics data Meaningful reports for the executive management team

The ultimate goal of security awareness is to achieve lasting behavioural change and build a risk aware Cyber Security Culture in your organisation. The OutThink platform is successfully used by organisations around the world to enable this transformation.

hello@outthinkthreats.com
www.outthinkthreats.com

Outthink Ltd
+44 (0) 203 389 5669

3rd Floor, 86-90 Paul Street
London, EC2A 4NE, UK