THALES CYBER AND CONSULTING

Cyber Human Error Assessment Tool (CHEAT®)

KEY BENEFITS

- **SECURITY:** Discover cyber vulnerabilities that other approaches miss; improving your security posture
- **SPEED:** Human error database and automated reporting greatly accelerates the time from investigation to report
- **MITIGATION:** Risk reduction and avoidance actions identified and graded, allowing for prioritised treatment

INTRODUCTION

Recent studies have shown that around 60% of all cyber-attacks are caused by insiders and that the overwhelming majority of Insider Threat security breaches – a worrying 95% can be attributed at least in part to human error. Defence strategies which primarily focus on technology only provide partial protection against attack. There is a clear need in the cyber security market for a more rigorous and structured approach.

INTRODUCING CYBER HUMAN ERROR ASSESSMENT TOOL (CHEAT®)

Thales has developed a unique methodology and accompanying tools which assess and mitigate human errors as part of cyber vulnerability investigations and post-incident investigations.

OUR APPROACH

Data is collected at interview or by use of questionnaires with key members of your staff. This allows a large number of human threat error indicators to be identified and assessed across the dimensions of organisation, people, technology and environment. These data, triangulated by the tool, are analysed by Human Factors experts. Risks are graded according to severity, and a number of mitigation recommendations are generated, together with an indication of their ease of implementation.

APPLICABILITY

CHEAT® can be used across multiple industries. The tool is personalised to the different domains in which it is used. For example, enterprise clients may place more emphasis on the business case aspects of risk, while defence clients will prefer to receive recommendations couched in terms of those standards which they commonly adhere to.

FUTURE DEVELOPMENT

The CHEAT® methodology and tool are constantly being refined and developed as their use becomes more widespread. As more data is gathered, we intend to provide further useful features such as benchmarking across departments / organisations. Enhanced automation will be introduced as we learn which outcomes and outputs are most valued by clients.

BUSINESS MODEL

Thales can be engaged to provide Cyber Vulnerability Investigations (CVIs) using CHEAT®. Engagements are fixed price according to the size of your organisation and the extent of estate. Contact us for further details, or to request a quotation.

https://www.thalesgroup.com/en/tcc-uk

SUMMARY OF SERVICES

- Vulnerability Inspection
- Human Error Threat Indication
- Risk Identification
- Risks Scored for Probability and Impact
- Risk Avoidance and Mitigation Actions
- Actions Graded by Ease of Implementation
- Methodology and Tools Tailored by Domain
- Comprehensive Report Output

WHY THALES?

- Extensive, Long Pedigree in Human Factors
- Comprehensive Cyber and Audit Skills
- Expertise in Psychology, Safety, HF Design
- Transparent and Affordable
- Unique Approach to Human Cyber Aspects

MARKETS AND CUSTOMERS

CHEAT® is applicable across all of the markets which Thales Cyber and Consulting serves – Defence, Secure Government, Central Government, Critical National Infrastructure and Regulated Industries. Customers who hold data and who may be subject to attacks which target their people will benefit from the additional coverage that CHEAT® brings to Vulnerability Audits and Inspections.

CASE STUDIES

After initial development and testing in 2015/16, 7 CHEAT® assessments were completed or started in the first year (2017). The approach continues to be popular with our clients. For example:

CHEAT® was used to assess the team responsible for part of a Royal Navy major equipment programme. CHEAT® generated 60 specific recommendations, prioritised by their importance. A number of other bespoke recommendations were proposed.

CHEAT® was used to assess the impact of an attempted cyber-attack on the secure networks department of a major defence contractor. Questionnaires were distributed and in-depth interviews were conducted with senior members of staff. The CHEAT® team made a number of suggestions including simple, cost-efficient adjustments to the company's cyber security policy.

A Formula 1 automotive company were assessed. Prioritised recommendations were provided and discussed with the client. This informed the efficient allocation of resources to tackle the most important threats to their competitive information and customer data. Thales was on hand to support them in the implementation of the key recommendations.

THALES UK – 350 Longwater Avenue, Green Park, Reading, RG2 6GF
E thalescyberandconsulting@uk.thalesgroup.com

https://www.thalesgroup.com/en/tcc-uk

THALES