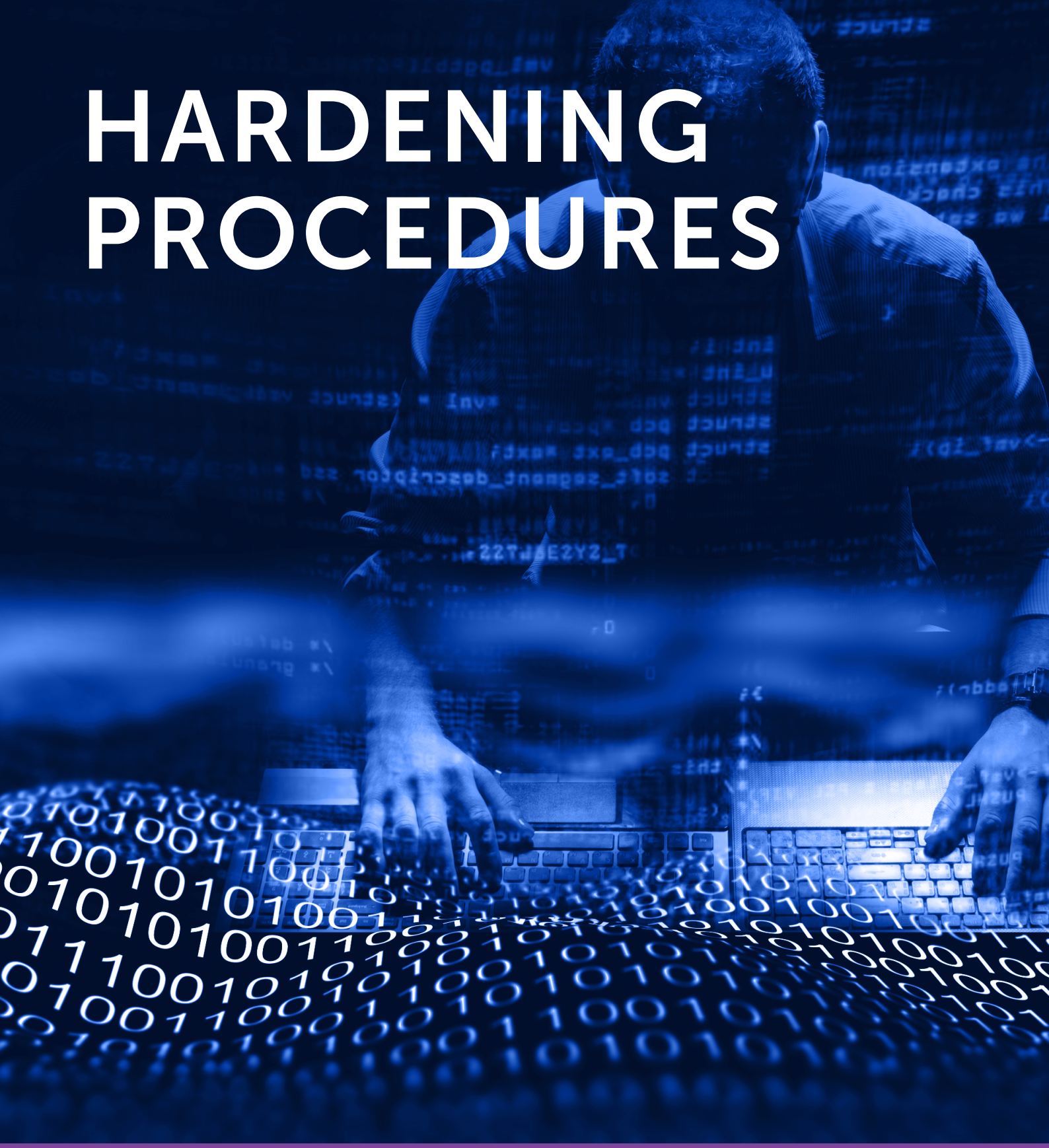
# HARDENING PROCEDURES



COMSEC

# What is Hardening Procedures?

Software vendors provide solutions with a basic configuration that focuses on ease of implementation rather than security. Most vendors publish a security appendix for those products to help the system owner implement product security.

Hardening procedures are documents based on common security practices and security best practices regarding a specific system or application. Those procedures are designed to reduce the system's attack surface and mitigate potential vulnerabilities that might be exploited in various circumstances.

# Comsec's Hardening Procedures

Hardening procedures are documents containing topics relevant to hardening with regard to key settings in information security. These can include permissions, access control, password and account management policies, disabling of unneeded services and features, activating security mechanisms, etc.

Comsec's hardening procedures are based on vendors' official recommendations and validated with in-depth research on specific topics, testing of those hardening topics in Comsec's cyber security labs considering common security practices and security best practices. Our hardening procedures take into consideration the compensating controls that might be implemented in a client's environment and provide a secure platform for application deployment.

# Why Comsec

The Comsec team has a valuable knowledgebase and experience, with members from the fields of IT and security, and has demonstrated experience with the products in question.

Comsec is monitoring the cyber security world and updating its procedures based on the changing risk factors and new attack vectors.

# Clients Challenge

## “A CHAIN IS ONLY AS STRONG AS ITS WEAKEST LINK“

Systems that are delivered by vendors with their default (vanilla) configuration are designed for ease of configuration and implementation rather than for resilience against cyber-attacks.

Default configuration or custom configuration performed by a person with weak knowledge and experience in security might expose the system to unnecessary risk that could be mitigated by implementing proper hardening procedures.

## Comsec UK

33rd floor, Euston Tower
286 Euston Road
London, NW1 3DP, England
Tel: +44 (0) 2034638727
info@comsecglobal.com

## Comsec BV

Hogehilweg 4
1101 CC Amsterdam
The Netherlands
Tel: +31 (0) 102881010
info@comsecglobal.com

## Comsec HQ

Yegia Kapayim St. 21D
P.O.Box 3474, Petach-Tikva
Israel 49130
Tel: +972 (0) 39234646
info@comsecglobal.com


COMSEC