a lightweight cybersecurity framework for thorough protection

60% of all cyber attacks or breaches in 2016 were aimed at SMEs

68% of SMEs have no systematic approach for ensuring cybersecurity

60% of SMEs who were victims of cyber attacks did not recover and shut down within 6 months

Cyber threats to SMEs
Small and medium-sized enterprises (SME) are the new big target for cyber attacks. SMEs see themselves confronted with a large variety of cyber threats.

Solution: The SMESEC framework
SMESEC is a lightweight cybersecurity framework for protecting SMEs against cyber threats. As an SME, you find vulnerabilities and address them with simple tutorials, tools, and lessons-learned — all by yourself.

Benefits of using the SMESEC framework for your enterprise

Do it yourself
Step-by-step guidance for meeting customer requirements and standards

Keep the investment small
Cost-effective tutorials and tools suitable for a busy environment

Keep it simple
Practices adapted to your company instead of complicated formal policies and procedures

Sources:

The Lightweight Cybersecurity SMESEC Framework

Awareness & Training Tutorials

Definition & Recommendation Tools

Lessons from Testing & Validation

Vulnerability Discovery & Resolution Tools

Threat Protection & Response Tools

Cyber threats to SMEs
Small and medium-sized enterprises (SME) are the new big target for cyber attacks. SMEs see themselves confronted with a large variety of cyber threats.

68% of SMEs have no systematic approach for ensuring cybersecurity

60% of SMEs who were victims of cyber attacks did not recover and shut down within 6 months

Solution: The SMESEC framework
SMESEC is a lightweight cybersecurity framework for protecting SMEs against cyber threats. As an SME, you find vulnerabilities and address them with simple tutorials, tools, and lessons-learned — all by yourself.

Benefits of using the SMESEC framework for your enterprise

Do it yourself
Step-by-step guidance for meeting customer requirements and standards

Keep the investment small
Cost-effective tutorials and tools suitable for a busy environment

Keep it simple
Practices adapted to your company instead of complicated formal policies and procedures

Sources: