PROTECTIVE
PROACTIVE RISK MANAGEMENT

ENHANCED THREAT AWARENESS TOOL

Through Improved Security Monitoring and Shared Threat Intelligence

FIND OUT MORE

www.protective-h2020.eu

@protective

office@protective.eu

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 700071.

PROJECT **OVERVIEW**

PROTECTIVE is designed to improve an organisations ongoing awareness of the risk posed to its business by cyber security attacks. PROTECTIVE makes two key contributions to achieve this enhanced situational awareness. Firstly it increases the computer security incident response team's (CSIRT) threat awareness through improved security monitoring and increased sharing of threat intelligence between organisations within a community. Secondly it ranks critical alerts based on the potential damage the attack can inflict on the threatened assets and hence to the organisations business. High impact alerts that target important hosts will have a higher priority than other alerts. Through the combination of these two measures organisations are better prepared to handle incoming attacks, malware outbreaks and their security problems and to guide the development of the prevention and remediation processes.

The PROTECTIVE system is designed to provide solutions for public domain CSIRTs and SME's who both have needs outside the mainstream of cyber security solution provision. Public CSIRTs needs arise in part because commercial tools do not address their unique requirements. This has created a shortfall, clearly articulated by ENISA, of tools with the required analytical and visualisation capabilities to enable public CSIRTs provide optimised services to their constituency. SME's also are vulnerable to cybercrime as they have limited resources to protect themselves and often a limited understanding of what needs to be done. Two pilots will be conducted to evaluate and validate the PROTECTIVE outcomes with CSIRTs from 3 National Research and Educational Networks (NRENs) and with SMEs via a managed security service provider (MSSP).

PROJECT **OBJECTIVES**

PROTECTIVE will develop a comprehensive solution to raise organisational cyber situational awareness (CSA) through:

Enhancement of security alert correlation and prioritisation

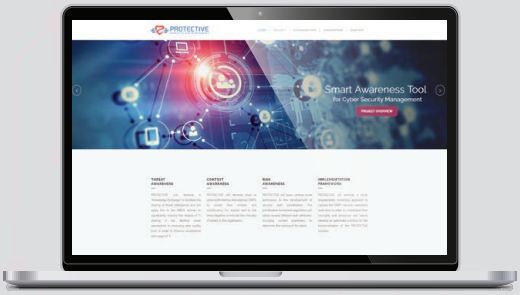
Linking of the relevance/criticality of an organizations assets to its business/mission

Establishment of a threat intelligence sharing community

These three elements will be tightly woven to provide an integrated CSA platform that will be developed firstly for CSIRTs in the NREN community and later applied for further validation within the SME end-user community.

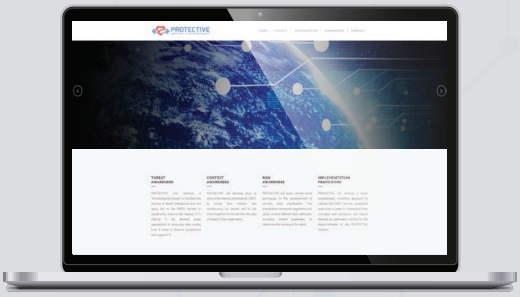
PROTECTIVE
PROACTIVE RISK MANAGEMENT

TECHNOLOGY OBJECTIVES



- **ENHANCE SECURITY MONITORING** THROUGH IMPROVED INCIDENT CORRELATION AND PRIORITISATION
- **ESTABLISH THE CRITICALITY OF AN ORGANISATIONS** ASSETS TO ITS MISSION
- DEVELOP **TOOLS AND TECHNIQUES** TO ESTABLISH COMMUNITY THREAT INTELLIGENCE SHARING
- **IMPROVE TRUST** IN THE DATA QUALITY OF SHARED INTELLIGENCE
- **DEVELOP SOFTWARE FRAMEWORK** TO SUPPORT INFORMATION FLOW PROCESSING

PILOT OBJECTIVES



- **DEMONSTRATE THE OPERATIONAL EFFICIENCY** OF THE DEVELOPED SOLUTION IN AN **NREN** ENVIRONMENT
- EVALUATE THE DEVELOPED SOLUTIONS TO **SUPPORT SME SECURITY MANAGEMENT**

www.protective-h2020.eu
@protective
office@protective.eu