**Securityaware.me Training Platform**

Interactive training courses

Securityaware.me is an online platform for creating and managing interactive training courses using real infrastructures and methods (servers, computers, networks etc.). Contrary to other e-learning platforms, Securityaware.me focuses only on cybersecurity. All hosted courses are created by experts from security companies and institutes around Europe and include training material for many different security topics and levels of expertise.

**Security Information and Event Manager XL-SIEM**

Real-time alerts for securing the SME

The SMESEC XLSIEM is a platform for collecting cybersecurity alerts and deviations from correct behaviour in a system. The information comes from the correlation of several monitoring tools focusing in different areas of the target system. The tool provides real-time analysis of the alerts and information about them in an easy and accessible way. In contrast to other SIEM tools, the XLSIEM guides end-users with concrete and actionable recommendations of what to do against specific alerts, and protect better their organization.

**Cybersecurity Coach CYSEC**

Assess, plan, and track improvements in cybersecurity

CYSEC provides SMEs with the ability to assess, plan, and track improvements in cybersecurity in a simple, do-it-yourself fashion. For an SME that is aware of cyber risks, CYSEC easily understandable cybersecurity advice and offers a personalized, self-adaptive journey of building cybersecurity capabilities to protect the SME. For the open cybersecurity expert community serving SMEs, CYSEC gives insights into how cybersecurity practices are adopted and a channel for helping SMEs to solve their difficult challenges.

**CybersecurityZone**

AI and protectionheuristics for comprehensive of workstations and servers

SMYSEC CybersecurityZone from Bitdefender gives small and medium-sized companies a unified approach to security management that addresses the scalability and performance challenges your organization is facing today. CybersecurityZone is architected from the ground up to unify security control over virtualized, physical, and mobile environments. It protects all the things that keep your business going: workstations, servers, mailboxes and mobile devices. It is incredibly easy to set up and light on your resources.
Early Warning Intrusion Detection System EWIS

Light intrusion detection that is also able to attract attacks away from the systems

EWIS is a honeypot-based intrusion detection solution tailored for SMEs. It can run in parallel with the real system, attracting attacks away from the SME’s systems. EWIS also provides a graphical interface visualizing the events that are captured by our sensors, this interface is part of the final SMESEC framework.

SMESEC framework is part of the final sensors, this interface visualizing the events that are captured by our sensors, this interface is part of the final SMESEC framework.

Features
- Emulates production services like the ones SMEs are using.
- Non-intrusive detection of malicious network events.
- Visual representation of real-time and passed network events.
- Complete visibility and control over the web traffic.

Citrix Application Delivery Controller

Complete visibility and control over the web traffic

Citrix Application Delivery Controller, which provides solutions for granting SMEs the visibility and control they need over encrypted traffic, thus ensuring compliance with their privacy, regulatory, and acceptable user behaviour. To keep users safe inside an organization, all communications must be inspected, not just clear-text traffic. Without, organizations are at risk from attacks: Hackers can infiltrate malware and steal data across multiple endpoints in the guise of encrypted traffic.

Features
- Selectively decrypts traffic according to URL category, reputation, or customer list.
- Blocks malicious websites such as malware, spam, and phishing sites.
- Analytics, visibility, and reporting for communication networks and user data.

IBM Anti-ROP Compiler Plugin

Protect software with the moving target defence technology

IBM Anti-ROP Compiler Plugin (Shakedown) allows compiling a C/C++ program with binary shuffling enabled so that the resulting executable is different for each build. The shuffling prevents buffer overflow and ROP attacks scale out: an exploit that targets one instance of the application will not successfully execute on other instances.

Features
- No modifications to project’s source code is required.
- Generates many versions of single binary executable, all different in binary layout but identical in functionality.
- Performs different types of randomizations to make it difficult for the attacker to circumvent.

Test-as-a-Service TaAS

Automated security testing for IoT

The TaAS (Test as a Service) allows SMEs to develop standards-based interoperable and secure products with short time-to-market and low engineering and financial overhead. TaAS offers capabilities to verify and validate the potentiality of vulnerabilities related to oneM2M and LoRa security requirements. Our motivation is to meet the market requirements related to sensors and IoT platforms domain. For example, TaAS analyzes the LoRa network attack for the susceptibility of LoRa devices to different types of attacks using commercial off-the-shelf hardware and executes the appropriate security test cases.

Features
- Automated on the shelf security testing.
- Non-regression report.
- Instant security problem detection.

SMESEC FRAMEWORK

How secure is your company?

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 767257 (SMESEC). This work is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments presented herein do not necessarily reflect the official views of these funding bodies.

Contact project leader: Jose Francisco Ruiz, Atos Spain SA, jose.ruizr.external@atos.net

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement H2020-854578. This work is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments presented herein do not necessarily reflect the official views of these funding bodies.

Contact project leader: Jose Francisco Ruiz, Atos Spain SA, jose.ruizr.external@atos.net