Securityaware.me Training Platform

Interactive training courses

Securityaware.me is an online platform for creating and managing interactive training courses using real infrastructures and testbeds (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.

Features

Hosts courses that are open to the public or made available privately to selected registered users.

Provides course managers with the ability to create their own space, host their own private or public courses to present a personalized training experience to their users.

The training courses can be executed directly in Securityaware.me or exported to be inserted in other learning management systems (e.g. Moodle).

❝ I learned the basics of Spam and Phishing. ❞
Amalia Kakaroumpa, Myrtian Blue Events

❝ I created a full list of courses to train my employees. ❞
Alexis Pantziaros, In4Capital

Security Information and Event Manager XL-SIEM

Real-time alerts for securing the SME

The SMESEC XL-SIEM 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 XL-SIEM guides end-users with concrete and actionable recommendations of what to do against specific alerts and protect better their organization.

Features

Provides total control for creating relevant alarms and full event history.

Lets the user aggregate different sources of SMESEC input data to provide a good insight of attacks.

Recommendations guide the user to the right tools and actions to be performed.

❝ For the first time, I felt to be in control. ❞
Rodrigo Diaz, ATOS

❝ It was easy to understand what happens and take immediate action. ❞
Olmo Rayón, WorldSensing

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 offers 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.
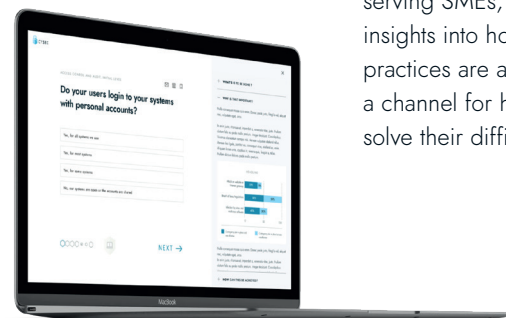
Features

The what, why, and how for each cybersecurity improvement in the SME.

Recommends the next step in the SME's improvement journey.

Awards badges that certify your SME's achievements in getting protected.

❝ CYSEC gave us holistic awareness about cybersecurity. ❞
Andreas Last, GridPocket

❝ The CYSEC tool provided valuable insight into the security of the company blevely just doing a quick survey. ❞
Jordi Cucurull, Scytl

GravityZone

AI and protectionheuristics for comprehensive of workstations and servers

SMESESC GravityZone 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. GravityZone 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 install and light on your resources.
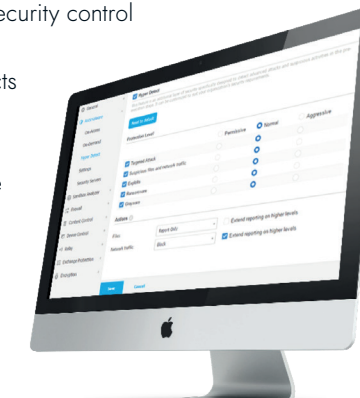
Features

Comprehensive security and efficient management with layered protection for the SME's endpoints.

Artificial intelligence and machine learning perfected for best protection and best performance.

Web-based security for full control and enhanced business productivity.

❝ I now spend less than one hour a month on security because GravityZone takes care of almost everything. ❞
Denis Muckensturm, Les Jardins de Gaïa

❝ It's an additional layer of security that protects us from the most advanced attacks. ❞
Simon Gassmann, Quilvest Switzerland

SMESEC

CYBERSECURITY FOR SMALL AND MEDIUM-SIZED ENTERPRISES

a lightweight cybersecurity framework for thorough protection

Vulnerability Discovery & Resolution Tools

lightweight defenses against Cyber threats

Lessons from Testing & Validation

Awareness & Training Tutorials

THE SMESEC FRAMEWORK

Threat Protection & Response Tools

Definition & Recommendation Tools

The SMESEC framework s based on up-to-date information about Cybersecurity. The SMESEC framework provides SMEs with the ability to build Cybersecurity itself with just little investment and without complicated policies and procedures. SMESEC makes Cybersecurity accessible for SME and helps to prevent and mitigate cyber risks of a large part of the European economy.

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.

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.

> « I gained new insights into the overall security events in the system. »
> A Greek company in the defence sector

> « It was easy to retrieve and query for security events. »
> Christos Tranoris, sense.city

Citrix Application Delivery Controller

Complete visibility and control over the web traffic

SMESEC partially integrates the industry-leading 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.

> « We could see issues right away and address them proactively. »
> Christos Tranoris, Swiss ABB unit

> « With Citrix, giving users access was as simple as checking a box, and it all worked. »
> Ayd Asraf, Aramex

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.
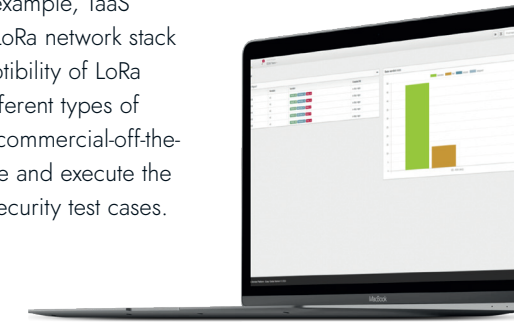
Features

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.

> « We successfully used it on industrial IoT devices. »
> Olmo Rayón, Worldsensing

> « A simple compiler wrapper allowed me to do the shuffling. »
> Olmo Rayón, Worldsensing

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 stack for the susceptibility of LoRa devices to different types of attacks using commercial-off-the-shelf hardware and execute the appropriate security test cases.
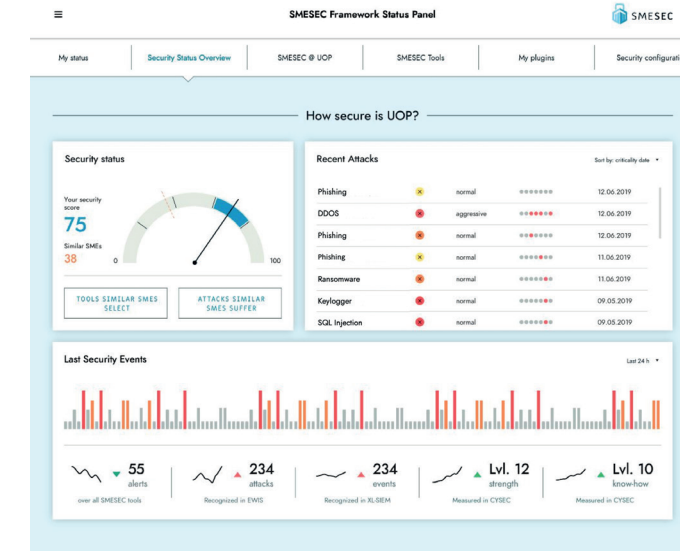
Features

Automated on the shelve security testing.

Non-regression report.

Instant security problem detection.

> « We saw the improvement of our product security after each testing phase. »
> Samuel Dupont, Bioceanor

> « The automated cloud-based testing procedure allows me to continue working while the tests are executed. »
> Bruno Legeard, Smartesting

SMESEC FRAMEWORK

How secure is your company?
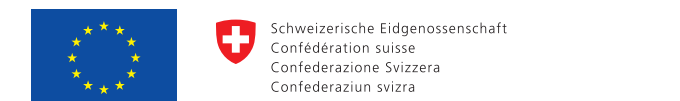
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740787 (SMESEC). This work is supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 17.00067. The opinions expressed and arguments employed 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