ISECOM STAR

Security certification for secure connectivity

White paper

Executive Summary

In today’s dynamic business environment, there are several business risks, which if not addressed could lead to failing of systems on which your customers rely. Security testing and analysis is a big part of identifying suck risks. The way the information is stored, managed, accessed and shared has changed with much dependence on the Internet and cloud-based infrastructure and services that the security of on-premise data is quite passé. Malware, spyware and other risks of data theft and abuse are wide-spread.

The systems that provide remote connectivity solutions need to be secure and standards-based. Remote access VPN technologies requires the networks and devices to talk to each other, but its basis should be secure communications.

Introduction

VPN (virtual private network) and tunneling are techniques that allow, among other benefits, to encrypt data links between yourself and another computer. This computer might belong to your organization, a trusted person or organization, or a commercial VPN service. Tunneling encapsulates a specific stream of data within an encrypted protocol, making everything that travels through the tunnel unreadable to anyone along the transmission path. Using a VPN or other form of tunneling to encrypt data is one of the best way to ensure that it will not be seen by anyone other than you and people you trust. Another major benefit of this technique is the authentication of remote parties.

STAR Certification OSSTMM 3.0

The Security Test Audit Report (STAR) is a certification obtained by assessing a product by authorized third-party auditors. By going through an OSSTMM 3.0 audit process, a business assures that security parameters are tested and implemented effectively.

By achieving the STAR Certification, service providers of every size will be able to give prospective customers a greater understanding of their levels of security controls.

OSSTMM OSSTMM OSSTMM OSSTMM OSSTMM OSSTMM OSSTMM
STAR
CERTIFIED OSSTMM 3.0
SECURITY TEST AUDIT REPORT

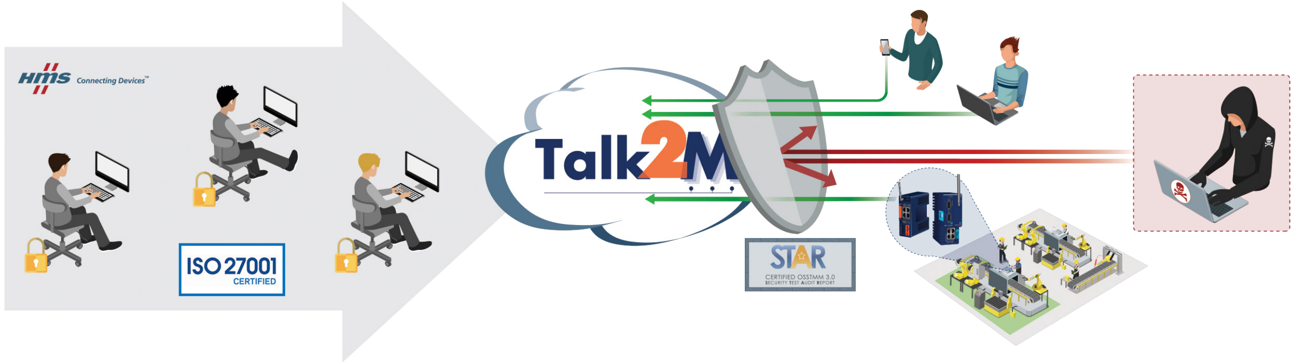
ISECOM and OSSTMM

ISECOM is an independent security research organization which creates and maintains the Open Source Security Testing Methodology Manual (OSSTMM). Back in January 2001, the Institute for Security and Open Methodologies (ISECOM), an open community and a non-profit organization began with the release of the OSSTMM. It was a move to improve how security was tested and implemented.
OSSTMM is to test the operational security of physical locations, people and forms of communications. The interconnectedness between people, processes, systems, and software create a complex web, which is difficult to keep a tab on, but proper security measures helps mitigate many of the risks.

Safety is primary – who would you rely on for the safety of you and your customer's data? Today, hacking and outright attacks are common.

Problem Definition

Today's technology environment is highly complex with security at each level, layer and location at risk. Technical risk can easily translate into business risk, so its identification on time is required to mitigate it. Unauthorized access and blatant security attacks threaten business, as customers invariably become the ultimate victims of the attack with their data being compromised.



Solution Details

How is the certification obtained?

OSSTMM certification is the assurance of an organization's security according to the thorough tests within the OSSTMM standard and is available per vector and channel for organizations or parts of organizations that maintain a level of a minimum of 90% validated yearly from an independent third-party auditor. Validation of security tests or quarterly metrics is subject to the ISECOM validation requirements to assure consistency and integrity.

What the audit covers?

Its elaborate steps include posture review, logistics, active detection verification, visibility audit, access verification, trust verification, controls verification, process verification, configuration and training verification, property validation, segregation review, exposure verification, competitive intelligence scouting, quarantine verification, privileges audit, survivability validation and service continuity and end survey, alert and log review task.

Purpose of ISECOM OSSTMM audit report

The report provides a standard reporting scheme based on a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way. It also provides guidelines which when followed will allow the auditor to provide a certified OSSTMM audit.

Business benefits

- Cloud based infrastructure needs security as its base. When that is ensured, the business shows preparedness for an eventuality of a security attack. The certification helps with this preparedness.
- To meet business goals, data protection is one of the most important aspects to be looked into. Vulnerability of devices, networks and infrastructure to attacks and breaches can result in customer moving away from your products and services.
- Following industry best practices such as adherence to security protocols instils confidence in customers.
- The certification provides a high level of trustworthiness in the business. With specific test information, the scope and a clear statement of the security metrics and details for comparisons with previous security tests or industry test averages, it provides prospective customers with a greater understanding of their levels of security controls in place
- It also enables effective comparison across other organizations in applicable sectors and it is focused on the strategic and operational business benefits as well as effective partnership
- The certification serves as a proof of a factual test
- With understandable metrics, it is known whether the required parameters are met or not
- Since, it holds the analyst responsible for the test, error or negligence in audit is highly unlikely

eWON Talk2M and Argos is STAR security certified

Remote connectivity solutions require high levels of quality and security parameters to be met, especially for industrial equipment. Data exchange and utilization of services over the cloud makes it all work. When data exchange on cloud is secure, customers have more confidence on the solution provider. Scrutiny and detailed audit of the systems and processes through a certification process ensures this security.

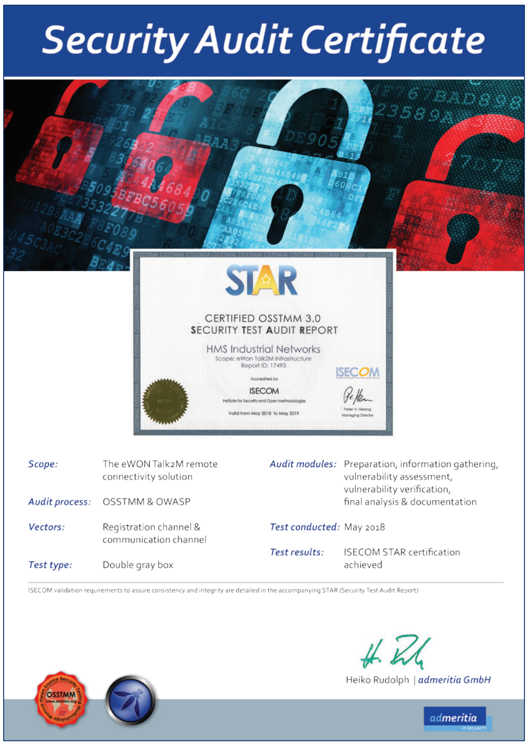
HMS is a provider of quality gateways/routers that takes away the burden of on-premise monitoring and control, which can be done remotely, saving cost and time. HMS Industrial Networks' remote connectivity solution, eWON Talk2M and Argos remote connectivity solution are both ISECOM STAR security certified.

The Talk2M infrastructure is as integrated element in the remote access solution where the Argos is part of a remote management /dashboard solution. They are fully redundant network of distributed servers (VPN and IIoT) , and other services that act as the secure meeting place for eWON devices and users.

Reach out to us to know about our services and how we follow and maintain global standards of security.

[ii] http://www.isecom.org/about-us.html

[iii] http://isecom.org/mirror/STAR.3.pdf



Security Audit Certificate

STAR

CERTIFIED OSSTMM 3.0
SECURITY TEST AUDIT REPORT

HMS Industrial Networks
Scope: eWon Talk2M Infrastructure
Report ID: 17493

Accredited by
ISECOM
Institute for Security and Open Methodologies
Valid from May 2018 to May 2019

ISECOM

Peter V. Herzog
Managing Director

Scope: The eWON Talk2M remote connectivity solution

Audit process: OSSTMM & OWASP

Vectors: Registration channel & communication channel

Test type: Double gray box

Audit modules: Preparation, information gathering, vulnerability assessment, vulnerability verification, final analysis & documentation

Test conducted: May 2018

Test results: ISECOM STAR certification achieved

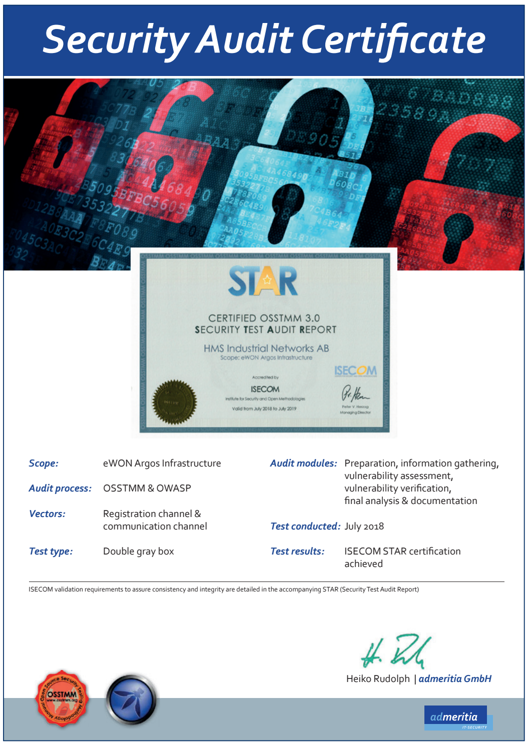
ISECOM validation requirements to assure consistency and integrity are detailed in the accompanying STAR (Security Test Audit Report)

Heiko Rudolph | *admeritia GmbH*

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

admeritia
IT-SECURITY

Talk2m: *ISECOM STAR certified*



Security Audit Certificate

STAR

CERTIFIED OSSTMM 3.0
SECURITY TEST AUDIT REPORT

HMS Industrial Networks AB
Scope: eWON Argos Infrastructure

Accredited by
ISECOM
Institute for Security and Open Methodologies
Valid from July 2018 to July 2019

ISECOM

Peter V. Herzog
Managing Director

Scope: eWON Argos Infrastructure

Audit process: OSSTMM & OWASP

Vectors: Registration channel & communication channel

Test type: Double gray box

Audit modules: Preparation, information gathering, vulnerability assessment, vulnerability verification, final analysis & documentation

Test conducted: July 2018

Test results: ISECOM STAR certification achieved

ISECOM validation requirements to assure consistency and integrity are detailed in the accompanying STAR (Security Test Audit Report)

Heiko Rudolph | *admeritia GmbH*

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

admeritia
IT-SECURITY

Argos: *ISECOM STAR certified*