Vulnerability Management

Vulnerability Management helps you identify, assess and manage vulnerabilities in your IT.

What can we help you with?

- Selection and implementation of a suitable tool
- Setting up vulnerability management processes
- Technology integration (SIEM, Service Desk and CMDB, etc.)

- Creation and customization of "Vulnerability Analysis and Evaluation" reports
- Hardening and compliance checks

Why choose Aricoma?

We have been implementing VM products since 2010 and have completed **dozens of implementation and integration projects**. We design and develop custom integrations that we test in our environment. We have **hardened more than 40 different platforms**. We are a partner of Tenable, whose technology we brought to the Czech Republic.

Security is our DNA

Identification of vulnerabilities

VM allows you to identify vulnerabilities in network infrastructure, applications and systems.

Rapid response to threats

Active vulnerability monitoring allows you to react quickly to new threats and ensures that you can respond immediately to potential security threats.

Prioritisation of patches

Vulnerability management provides you with mechanisms to prioritise patches by importance, helping you to focus your resources on the most critical area. A key role in effectively eliminating vulnerabilities is played by prioritization, which takes into account other important parameters than just CVSS. First of all, it provides up-to-date information from Threat Intelligence, information about the potential for exploitation and defines its severity or specifies the type of vulnerable system.

Risk reduction

Regular vulnerability scanning and patching help to reduce the risk of a successful attack and minimize the potential impact on your organization.

Compliance with the regulations

Many security regulations and standards require regular identification and management of vulnerabilities. VM will help you meet these requirements efficiently.

Improving response to events

Vulnerabilities identified and patched as part of vulnerability management can reduce the chances of successful attacks and also make it easier to detect security incidents.

Ensuring business continuity

Vulnerability management plays a key role in ensuring business continuity by helping to minimize the risk of interruptions to business. Identifying and fixing system vulnerabilities prevents unauthorized access to critical data, reducing the likelihood of attacks that could disrupt your business continuity.

It doesn't end with the installation of the equipment

For us, the project does not end with the installation of the scanner. VM covers a range of specific areas and we can help you in each of them. We can set up the entire process to be fully automated, while still serving to effectively eliminate vulnerabilities and prevent security incidents.

Tenable Cyber Exposure Platform

We offer a broad portfolio of Vulnerability Management products that together provide a Cyber Exposure Score. This term is used by Tenable to assess the likelihood of a vulnerability being exploited that could lead to a serious security incident.

Vulnerability Acceptance

Patching Control

Integration with Technologies

Ticketing System

Privileged Access Management

Automation

Virtual Patching

VM as a Service

Vulnerability Scanner

Vulnerability Analysis

Vulnerability Management

Compliance check

Vulnerability Reporting

Interfacing with Processes

Patch Management

Change Management

System Hardening

Compliance with Standards

Customization of Policies

Penetration Tests

Customization of Reports