Vulnerability Management

> 23 000 VULNERABILITIES DETECTED IN 2020

20 % CVSS 9+

EXPLOIT AVAILABLE FOR 33 %

THERE WAS NO REPAIR FOR 22 %

AEC

Vulnerability management is a complete process involving the detection, analysis and evaluation of vulnerabilities, including removing them. From the point of view of system security, Vulnerability Management is absolutely key, and therefore every company should have it in place. Vulnerability scanners or Vulnerability Management tools can be used to easily and quickly detect vulnerabilities on a network.

How can we help you?

- Choosing and implementing a suitable tool
- Setting up the vulnerability management processes
- Technological integration (SIEM, Service Desk, CMDB and others)
- Creating and customising reports
- Vulnerability analysis and evaluation
- Hardening and compliance checks

Why choose AEC?

- We have been implementing VM products since 2010.
- We have dozens of implementation and integration projects behind us.
- We design and develop our own integrations, which we test in our environment.
- We have done hardening on more than 40 different platforms.
- We are a platinum partner of Tenable, whose technology we brought to the Czech Republic.
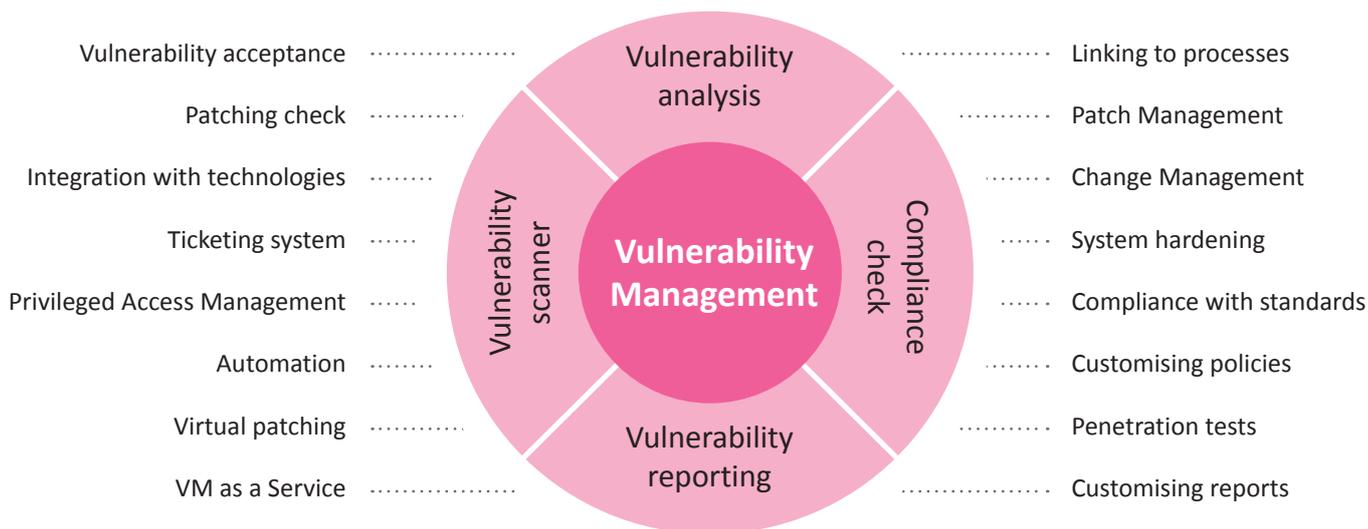
Don't be inundated with critical vulnerabilities

Prioritisation is a key function for effectively removing vulnerabilities. If the output of your vulnerability management is hundreds of critical items that you merely report to asset owners, there is no real removal of vulnerabilities. A suitable tool for Vulnerability Management must make the administrators' work easier, not the other way around! Prioritisation is cru-

cial, as it takes into account other important parameters than just CVSS. Above all, it provides up-to-date information from Threat Intelligence, information on the possibility of exploitation and defines its difficulty or specifies the type of vulnerable system.

Severity of vulnerability	Misuse vector	Possibility of exploitation	Information from Threat Intelligence

Vulnerability priority

Installing the equipment is not the end for us

We are a stable partner in the field of security. For us, the project does not end with simply installing a scanner. Vulnerability Management includes a whole host of specific areas and we can help you in each one. We can set up the entire process so that it is fully automated, while serving to effectively remove vulnerabilities and prevent security incidents.

Vulnerability acceptance · · · · · · · · · · · · · · · · · · Linking to processes

Patching check · · · · · · · · · · · Patch Management

Integration with technologies · · · · · · · · Change Management

Ticketing system · · · · · · System hardening

Privileged Access Management · · · · · Compliance with standards

Automation · · · · · · · · Customising policies

Virtual patching · · · · · · · · · · · Penetration tests

VM as a Service · · · · · · · · · · · · · · · · Customising reports

Vulnerability analysis

Vulnerability scanner

Vulnerability Management

Compliance check

Vulnerability reporting

Tenable Cyber Exposure Platform

As a platinum partner of Tenable, we offer a wide portfolio of products for Vulnerability Management and together they provide the "Cyber Exposure" score. This term is used by Tenable to assess the likelihood of exploiting a vulnerability that could lead to a serious security incident.

Tenable third party information and data

Assets

Vulnerabilities

Threats

tenable Lumin
Determining, reporting and comparing your Cyber Exposure score

tenable.sc
On-Premise Vulnerability Management

tenable.io
Vulnerability management in the cloud

NESSUS SCANNER	NESSUS NETWORK MONITOR	NESSUS AGENT	INDUSTRIAL SECURITY	CONTAINER SECURITY	PCI ASV	WEB APP SCANNING

Tenable third party information and data

CMDB

IT Systems Management

Governance, Risk and Compliance

Full visibility across all assets

Prioritisation and fully customisable reports

Flexibility: Cloud or On-Premise