

# Vulnerability Management

Vulnerability Management vám pomůže identifikovat, hodnotit a spravovat zranitelnosti vašich informačních technologií.

## S čím vám pomůžeme?

- Výběr a implementace vhodného nástroje
- Nastavení procesů řízení zranitelností
- Technologické integrace (SIEM, Service Desk, CMDB a další)
- Vytvoření a customizace reportů
- Analýza a vyhodnocení zranitelností
- Hardening a kontroly souladu (compliance)

## Proč zvolit Aricomu?

Produkty VM implementujeme od roku 2010 a máme za sebou **desítky implementačních a integračních projektů**. Navrhujeme a vyvíjíme **vlastní integrace**, které testujeme v našem prostředí. Provedli jsme **hardening více než 40 různých platforem**. Jsme partnerem společnosti Tenable, jejíž technologii jsme do Česka přinesli.



## Identifikace zranitelnosti

VM vám umožní identifikovat zranitelnosti v síťové infrastruktuře, aplikacích a systémech.

## Rychlá odezva na hrozby

Aktivní monitorování zranitelností vám umožní rychlou reakci na nové hrozby a zajistí, že můžete okamžitě reagovat na potenciální bezpečnostní hrozby.

## Prioritizace oprav

Řízení zranitelností vám poskytne mechanismy pro prioritizaci oprav podle důležitosti, což vám pomůže zaměřit své zdroje na nejkritičtější oblast. Klíčovou funkcí pro faktické odstranění zranitelností je prioritizace, která zohledňuje i další důležité parametry než jen CVSS. Především poskytuje aktuální informace z Threat Intelligence, informace o možnosti exploitace a definuje její náročnost nebo upřesňuje typ zranitelného systému.

## Snížení rizika

Pravidelné skenování a opravování zranitelností vede ke snížení rizika úspěšného útoku a minimálního potenciálního dopadu na vaši organizaci.

## Soulad s regulacemi

Mnoho bezpečnostních předpisů a standardů vyžaduje pravidelnou identifikaci a správu zranitelností. VM vám pomůže plnit tyto požadavky efektivně.

## Zlepšení reakce na události

Zranitelnosti identifikované a opravené v rámci správy zranitelnosti mohou snížit šance na úspěchy útoků a také usnadnit odhalení bezpečnostních incidentů.

## Zajištění kontinuity podnikání

Správa zranitelnosti hraje klíčovou roli v zajištění kontinuity provozu tím, že pomáhá minimalizovat riziko přerušení provozu. Identifikace a oprava zranitelností systémů zabrání neoprávněnému přístupu k důležitým datům, což snižuje pravděpodobnost útoků, které by mohly narušit kontinuitu vašeho podnikání.

## Instalaci zařízení to pro nás nekončí

Projekt pro nás nekončí pouhou instalací skeneru. VM zahrnuje celou řadu specifických oblastí a v každé z nich vám dokážeme pomoci. Celý proces umíme nastavit tak, aby byl plně automatizovaný, a přitom sloužil k efektivnímu odstraňování zranitelností a předcházení bezpečnostním incidentům.

### Tenable Cyber Exposure Platform

Nabízíme široké portfolio produktů v oblasti Vulnerability Managementu, které dohromady poskytují tzv. Cyber Exposure skóre. Tento termín používá Tenable pro hodnocení pravděpodobnosti zneužití zranitelnosti, které může vést až k závažnému bezpečnostnímu incidentu.

