# Article information:

Introduction to Vulnerability Management – BMC Software | Blogs
<https://www.bmc.com/blogs/vulnerability-management/>

# Article summary:

1. Vulnerability management is the practice of identifying, classifying, prioritizing, remediating, and mitigating vulnerabilities within a technology system.

2. A vulnerability management program should take into account security threats, technologies used, legal and geographic limitations, customer and market requirements, and other factors.

3. Automated discovery capabilities can help manage security gaps by identifying known vulnerabilities and prompting the installation of security patches before the infrastructure is used in the security sensitive SDLC pipeline.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article provides an overview of vulnerability management as it relates to enterprise technologies. The article does a good job of outlining the components of a vulnerability management program and providing examples of how automated discovery capabilities can help identify potential vulnerabilities. However, there are some areas where the article could be improved upon.

First, while the article does mention potential risks associated with weak business processes or inadequate access controls, it fails to provide any evidence for these claims or explore counterarguments that may exist. Additionally, while the article mentions that hackers perform a cyber-attack every 39 seconds, it does not provide any sources for this statistic or explain why this number is significant in relation to vulnerability management programs.

Furthermore, while the article does provide some information on how to prioritize and automate vulnerability management programs, it fails to discuss any potential drawbacks or risks associated with such approaches. Additionally, there is no discussion on how organizations can ensure that their vulnerability management programs are compliant with applicable laws or regulations.

Finally, while the article does mention that “security breaches went unnoticed for an average of 206 days” in 2019, it fails to provide any sources for this statistic or explain why this number is significant in relation to vulnerability management programs.

In conclusion, while this article provides a good overview of vulnerability management programs and their components, it could be improved upon by providing more evidence for its claims and exploring counterarguments as well as discussing potential drawbacks or risks associated with such approaches.

# Topics for further research:

* Vulnerability management program risks
* Vulnerability management compliance regulations
* Average time to detect security breach
* Impact of inadequate access controls
* Automated vulnerability management solutions
* Hacker attack statistics

# Report location:

<https://www.fullpicture.app/item/959e8783e246dfeec8ffe5e98e86800a>