

WHITE PAPER

# 10 Ways a Vulnerability Management Program Improves Your Cyber Security Defense



# A Cornerstone in a Modern Cyber Security Defense

Thousands of new vulnerabilities are discovered annually, requiring organizations to patch software and reconfigure security settings. To proactively address vulnerabilities before they are utilized in a cyberattack, organizations serious about their cyber security defense should implement a vulnerability management program.

Achieving visibility into all vulnerabilities across all ecosystems is challenging, something cybercriminals are capitalizing on by exploiting weaknesses in systems, applications, and users. With a solid vulnerability management program, you can simplify the process of identifying, categorizing, prioritizing, and remediating vulnerabilities in all types of ecosystems.

## Protecting Your Systems & Users

Vulnerability management is generally defined as the process of identifying, categorizing, prioritizing, and remediating vulnerabilities in all types of systems. Modern vulnerability management should cover systems as well as users. Historically the user - the first line of defense, but also the weakest link - has not received much attention. That is now changing.

But how do you work with vulnerability management targeting your users? The methodology is the same as for systems. Systems are scanned - users are targeted with simulated phishing attacks. Systems are patched - users are educated with awareness training.



# Maximizing Coverage in Vulnerability Management

Vulnerability management is generally defined as the process of identifying, categorizing, prioritizing, and remediating vulnerabilities in all types of systems. Modern vulnerability management should cover systems as well as users. Historically the user - the first line of defense, but also the weakest link - has not received much attention. That is now changing.

But how do you work with vulnerability management targeting your users? The methodology is the same as for systems. Systems are scanned - users are targeted with simulated phishing attacks. Systems are patched - users are educated with awareness training.

## Remediate Vulnerabilities & Strengthen Your Defense

A vulnerability management program aims to significantly increase your cyber security defense by detecting various types of vulnerabilities and potential risks, such as outdated software, misconfigurations, weak passwords, exposed functions, and services, but also users who expose your organization to risk. Modern vulnerability management is a hybrid between scanning from the outside and the use of lightweight endpoint agents. This hybrid gives extended and complete coverage, not least covering the growing remote workforce using remote devices. Increase your organization's resilience to all types of social engineering.

## Allows You to Be One Step Ahead of Attackers

Hundreds of new known vulnerabilities are detected every week, and threats and attackers are constantly changing. Most critical vulnerabilities are found in standard systems that many organizations utilize to a large extent. Your organization is continuously exposed to new threats as new devices, networks, web applications, or cloud services are added. To protect your organization from these threats and proactively detect and remediate vulnerabilities, you will need a successful vulnerability management program.



## WHITE PAPER

# 10 Ways a Vulnerability Management Program Improves Your Cyber Security Defense

## Addresses & Strengthens Weak Users

You cannot patch users, so how do you understand how vulnerable they are? The methodology is the same as for systems. By performing phishing simulations, you can identify weak users. Together with user awareness training, you will increase your organization's resilience to all types of social engineering.

## Gives Greater Visibility & Covers All Systems

A vulnerability management program offers a comprehensive solution to assess your entire IT environment and its users. The technology covers everything from software in traditional systems, network equipment, OT/SCADA, IoT, cloud and container environments to computers and applications, web applications, and APIs. Accordingly, everyone can use vulnerability management regardless of what systems they use. Your vulnerability management program should provide visibility into your entire attack surface, including the cloud.

## A Risk-Based Approach

A risk-based approach to cyber security will help you prioritize all resources, in particular high-risk vulnerabilities, in the best possible way. A risk-based approach to vulnerability management is crucial for the prioritization and efficiency of your vulnerability management program and will strengthen your cyber security defense significantly.

## Automated Defense

Monitoring an entire attack surface often requires having a significant cyber security operation. A vulnerability management platform will incorporate a largely automated process. Automation ensures continuous use, which means that you will have systematic and risk-based work that creates an excellent value for the organization.



## WHITE PAPER

# 10 Ways a Vulnerability Management Program Improves Your Cyber Security Defense

## Well-Proven Technology

There is an ever-increasing number of cyber security products on the market. Which products do you choose? This is a question that many organizations are asking themselves. Vulnerability management is based on well-proven technology that has been developed continuously for more than 20 years. When you implement a platform for vulnerability management, you can feel confident that you have made a safe, secure, and practical choice that will give great value in return. You will immediately gain insight into the vulnerabilities in your technical IT environment and identify the users that put the organization at risk.

## Demonstrate Compliance

Authorities and industry associations are placing higher and higher legal requirements and demands through legislation and other regulatory requirements. These requirements dictate organizations work systematically with information security. A vulnerability management program can help your organization create a systematic, analytical, risk-based security strategy and demonstrate compliance effectively and clearly.

## Improves Internal Communication

Many organizations lack the tools to communicate internally what risks their organization is exposed to. Many times, internal security reporting is perceived to be not completely objective. Instead, provide an accurate picture of the current security situation that can also be quantified and followed over time. The reporting from a vulnerability management platform suits the need of top management and cyber security experts.

## Instant Value in Return

The goal of many cyber security products is to prevent possible future incidents. But when will the next incident occur? How much time, money, and effort will you need to invest before that product provides a good ROI? With a vulnerability management program, you will immediately gain insight into the vulnerabilities that exist in your IT environment, as well as identifying the users that expose your organization to risk. Thus, you instantly get great value from working with a vulnerability management program.

# Why Holm Security?



## Leading Attack Vector Coverage

The broadest coverage of attack vectors in the industry which includes both technical and human attack vectors.



## More Than Just Another Vendor

Your most important partner within cyber security helping you stay one step ahead of cybercriminals.



## Data Privacy

Any vulnerability data we collect is stored and encrypted in data-neutral locations so you can be assured that only you will have access to your data.

## How can we help?

Want to get in touch? We'd love you hear from you. Here's how you can reach us.



+46 8-550 05 581



[info@holmsecurity.com](mailto:info@holmsecurity.com)



[www.holmsecurity.com](http://www.holmsecurity.com)