

WHITE PAPER

# 5 Steps to Successful Vulnerability Management



# 5 Steps to Successful Vulnerability Management

Vulnerability management is a cornerstone in a modern cyber security defense. But getting started and implementing a successful security strategy for vulnerability management can be challenging. Here is our checklist to help you become successful.



## Automation & Continuity

It's important to understand that Vulnerability Management is an ongoing and never-ending process. Most organizations don't have the resources to work on an ongoing basis, so automation is a key function.

### Automated Work Process

Create an automated work process, including automatic and continuous scans running in the background.

### Proactive

Enhance your proactive day-to-day security strategy with automation.



## Risk Based Approach

Risk-based vulnerability management (RBVM) allows you to understand vulnerability threats in the context of their potential business impact. Keep it simple and instead, look at the basic metrics.

### High-Risk Vulnerabilities

Prioritize vulnerabilities based on basic metrics. Start with high-risk vulnerabilities, which require little effort to remediate, and work your way down.

### Simple Metrics

Work with simple metrics to weigh your vulnerabilities, like CVSS (Common Vulnerability System Score), exploitability in combination with how critical a system is for your organization.



## WHITE PAPER

# 5 Steps to Successful Vulnerability Management



## Ambition Level

It's important to set a realistic ambition level when working with Vulnerability Management, as it is an ongoing and never-ending process.

### Insight

The first step is to get insight into and understand the risks you face. Identifying threats is just one of the biggest steps many organizations need to take.

### Q10 Process

We recommend the Q10 work process - identify the 5-10 most critical vulnerabilities that should be solved during the upcoming quarter.



## Involve & Engage

You'll be more successful together. Don't make vulnerability management a one-man show. Co-operation is key.

### Involve

Involve system owners, development team, CISO, IT manager, etc., and let them do their part.



## Integration

Depending on how far you've come in your cybersecurity process, you might want to integrate with other tools and products in your ecosystem.

### Integrate Today

Integrate with other systems that you or your outsourcing partner is working with, for example, SIEM or ticketing solutions. If it's not integrated today - it'll be in the future.



## The Users

You're not stronger than your weakest link. Even the most well-protected systems in the world won't do you any good if your users put you at risk. Historically, most organizations have been focused on protecting systems but have forgotten about the users.

### Human Firewall

Keep your users aware and resilient through simulation of social engineering together with tailored and automated awareness training. Build your human firewall.

### Evolving Threats

Keep your users up to date with the constantly shifting and evolving threats through repeating simulations and awareness efforts.

# Find Weaknesses Where You Are the Most Vulnerable

Stay on top of your web application security by continuously detecting thousands of vulnerabilities with our Web Application Scanning. Understand your current threat landscape and adopt a proactive approach to information security. Detect vulnerabilities related to harmful code, misconfigured systems, weak passwords, exposed system information and personal data.