Vulnerability maturity model, application and environment security

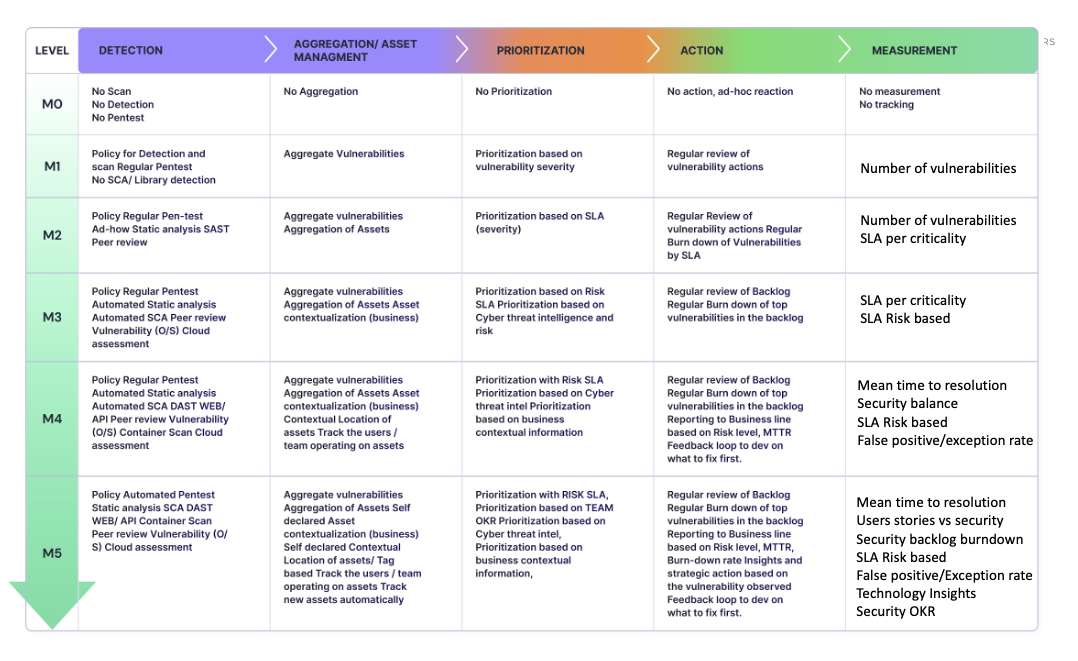
Intro:

In today's rapidly evolving threat landscape, organizations face an ever-increasing risk of cyberattacks and data breaches. Vulnerabilities are getting discovered faster than ever, with a 34% yoY increase of vulnerabilities discovery. Vulnerabilities are often tackled as they come from security scanners, leading to burnout of security professionals, with 50% of security engineers considering changing their profession entirely. To mitigate these risks, vulnerability management and triage have become an essential component of an effective cybersecurity program. Vulnerability triage, in particular, plays a critical role in identifying, prioritizing, and remediating vulnerabilities to minimize the organization's attack surface across applications, cloud and infrastructure. However, the process of vulnerability triage is not a one-size-fits-all approach and requires a maturity model that reflects the organization's current state of readiness. This article will explore the evolution of vulnerability management and triage process maturity and how organizations can enhance their capabilities to manage and mitigate cybersecurity risks effectively.

## Why:

We created the vulnerability maturity model to provide a quick and easy assessment method to define where you are in the vulnerability assessment process from triage

## Vulnerability Triage and maturity model V1



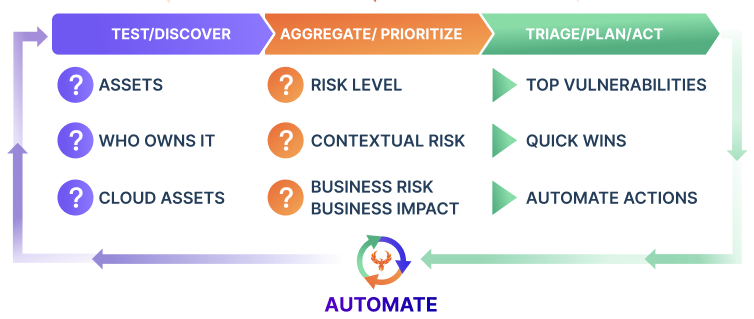
## How to assess your maturity level for vulnerabilities?

You can assess your organisation against this model [downloading the V1.0](https://docs.google.com/spreadsheets/d/1ZuCJ65TfzF6jvdLiQxITlYHsmPgjUqNVGsuqXLFNZFE/edit?usp=sharing) here, we are integrating the model inside [DSOMM](https://owasp.org/www-project-devsecops-maturity-model/) for easier integration and will be publishing a new whitepaper on this model in the upcoming months.

The model is also mapped back to [OWASP SAMM V2](https://owasp.org/www-project-samm/)

A more extended model can be found in part of the SANS [Vulnerability management model.](https://www.sans.org/blog/vulnerability-management-maturity-model/)

## What are the various areas of vulnerability triage?



* Detection/Testing = identification of artifacts and tooling integration.
* Aggregation of vulnerabilities = describe the different levels of maturity in aggregating vulnerabilities.
* Prioritization = describe the different levels of maturity for the prioritization process.
* Vulnerability Actions = Describe the actions that can be taken to resolve vulnerabilities; the actions are tied to the process implemented and the maturity of the measurements.
* Vulnerability Processes = Describe the process of vulnerability triage and remediation.
* Measurements = Describe how to measure vulnerability and processes.

Future work: we will include two other areas in the model: deduplication and correlation/contextualisation.

## What is a vulnerability triage process?

A vulnerability triage process is essential in ensuring an organization's systems and applications are secure from malicious attacks. It involves a systematic approach to identifying and prioritizing vulnerabilities based on their level of severity (at most basic level), risk (at highest maturity level), and the potential impact they could have on an organization's assets, data, and reputation. The triage process typically involves several steps, including discovery, assessment, prioritization, and scheduling of necessary work with relevant teams.

The first step in the vulnerability triage process is discovery. The process involves identifying vulnerabilities within an organization's infrastructure, applications, or systems. Identifying Vulnerabilities can be achieved through automated tools or manual analysis of code, vulnerability scan reports, and system reports. Once a vulnerability has been discovered, it is important to document the details of the vulnerability, including its location, severity, and potential impact on the organization's assets and data.

The next step is assessment, which involves analyzing the vulnerability to determine its level of severity and potential impact. The Analysis may involve testing the vulnerability to see if it can be exploited and to what extent. It is important to understand the technical details of the vulnerability, such as the root cause and potential attack vectors, as this information will inform the prioritization and scheduling of work.

Once the vulnerability has been assessed, it is prioritized based on its severity level and potential impact. Vulnerabilities are typically classified into different categories, such as critical, high, medium, and low severity. The prioritization process considers the potential impact on the organization's assets, data, and reputation and the likelihood of exploitation. This information is used to determine the level of urgency for remediation.

After prioritization, the next step is to schedule the necessary work with the relevant teams. This may involve assigning tasks to internal or external teams, such as developers, system administrators, or third-party vendors. The scheduling process considers the availability of resources and the urgency of remediation. It is important to communicate the urgency of remediation to all relevant parties to ensure the necessary work is completed within a reasonable timeframe.

Vulnerability triage process is essential in ensuring the security of an organization's infrastructure, applications, and systems. It involves a systematic approach to identifying and prioritizing vulnerabilities based on their severity level and potential impact. The process typically involves several steps, including discovery, assessment, prioritization, and scheduling of necessary work with relevant teams. Organizations can effectively manage their security risks and protect their assets, data, and reputation by following a vulnerability triage process.

## How does phoenix security help?

Phoenix security was created to help organizations quickly integrate several of those maturity elements and rapidly bring organizations to Maturity level 4, providing tools and process acceleration to incorporate the process and practices at the organizational level quickly and painlessly.

>> CTA

## What are the different maturity levels for a vulnerability process?

* Level 0: Absent - At this level, the organization does not have a formal process for vulnerability scan, triage, discovery or assessment. Identifying and remedying vulnerabilities is reactive, from random discovery, and there is no systematic approach to prioritize vulnerabilities based on their severity, risk, context or potential impact.
* Level 1: Initial - The organization has a basic process/policy for vulnerability scan and triage at this level. There is some awareness about the importance of vulnerability management, and vulnerabilities are tracked and reported to relevant teams. However, the process is still reactive, and remediation activities have no formal prioritization or scheduling.
* Level 2: Managed - At this level, the organization has a well-defined and managed process for vulnerability scan, and some level of triage. Vulnerabilities are identified and tracked systematically, and there is an initial prioritization process based on the severity and potential impact of the vulnerability. Initial steps for SLA prioritization might be in place. There is some level of aggregation of vulnerability and measurement.
* Level 3: Defined - At this level, the organization has a mature and well-defined process for vulnerability scan/test, discovery, triage and measured remediation, fully integrated into the overall security program. The process is well-documented and communicated to all relevant parties, and there are clear roles and responsibilities for vulnerability management. Vulnerabilities are prioritized based on a risk-based approach, and remediation activities are regularly monitored and reported on. There is a well-defined approach on exception management with a mitigation approach.
* Level 4: Quantitatively Managed - At this level, the organization has a fully mature process for vulnerability scan/test, discovery, triage and measured remediation, that is data-driven and quantitatively managed. Vulnerabilities are prioritized based on a comprehensive risk assessment that considers the likelihood and potential impact of exploitation. There is ongoing monitoring and reporting on vulnerability management metrics, and the process is continually optimized based on data-driven insights. There is a well defined approach on exception management, rapid and systematic threat modeling with mitigation approach.
* Level 5: Optimizing - At this level, the organization has a fully optimized and mature process for vulnerability scan/test, discovery, triage and measured remediation, that is continually tested and benchmarked, refined and improved. The process is fully integrated into the overall security program, with ongoing collaboration and communication across all relevant teams. The organization leverages the latest tools and techniques to identify and prioritize vulnerabilities, and there is a culture of continuous improvement and innovation in vulnerability management. There is a well defined approach to exception management and rapid and systematic threat modeling with mitigations

## How does triaging differ between application security and infrastructure security?

1. Complexity of Vulnerabilities: Application security vulnerabilities tend to be more complex and require a deeper understanding of the application's underlying code and architecture. This makes it more challenging to identify and prioritize vulnerabilities, as it requires a higher level of technical expertise and specialized tools. On the other hand, infrastructure security vulnerabilities tend to be more straightforward and easier to identify and remediate.
2. Speed of Remediation: In application security, the speed of remediation is critical due to the fast-paced nature of software development. Applications are often updated and deployed frequently, so vulnerabilities must be addressed quickly to avoid disruption to development cycles. In infrastructure security, remediation tends to be more planned and scheduled, as infrastructure changes typically require more lead time.
3. Tools and Processes: The tools and processes used in application security often differ from those used in infrastructure security. For example, application security may rely on automated tools to identify vulnerabilities in code. In contrast, infrastructure security may rely on manual checks and audits to identify vulnerabilities in network configurations and device settings.
4. Risk Assessment: Risk assessment in application security often requires a deeper understanding of the application's functionality and potential impact on the organization's assets and data. In infrastructure security, risk assessment focuses on the potential impact on the organization's network and devices.
5. Collaboration: Collaboration between development and security teams is critical in application security, as developers need to understand the implications of vulnerabilities in their code and applications. Collaboration may be more limited in infrastructure security, as infrastructure changes tend to be managed by dedicated IT teams.

In summary, while there are some similarities in the triage process between application and infrastructure security, several key differences exist. Application security tends to be more complex and requires higher technical expertise, while infrastructure security tends to be more straightforward. The speed of remediation, tools and processes, risk assessment, and collaboration are all factors that can impact the triage process in different ways in these two areas of security.

## Conclusions

Vulnerability triage is a complex process that can be broken down into several aspects. Trying to tackle everything at a high maturity level can be overwhelming and lead to dissatisfaction. Starting with a limited scope, defining several activities around vulnerability management is key to progress systematically towards a higher maturity level.

## Phoenix security perspective

From running vulnerability management at scale for application security and cloud security, we learned many lessons about what works and does not work. Every organization has its process, maturity and procedures. Phoenix security is here to help every organization progress on the journey of vulnerability evolution and resolution of vulnerabilities without burnout. You can schedule a free consultation with one of our experts to assess your organization's maturity level. To know more about how we can automate the discovery of assets, triage and prioritization, schedule a demo call with us.