Vulnerability Management processes Eklamot

May 2022

Contents

1. Introduction

The main purpose of this document is to present updated process of Vulnerability Management. Document contains an extensive description of the process, including:

- **Main target,**
- **Detailed steps of VM process,**
- **Parties engaged**
- **KPIs.**

2. Vulnerability Management – Main target and detailed steps of VM process

Main target of structured Vulnerability Management process is to ensure safety of infrastructure by identifying, acting on and reporting known vulnerabilities.

System Administrator performs scanning on **regular basis** (we recommend at least one per week) Issues that have been found critical by the tool (and confirmed by the Security team) are prioritised which was neglected in previous version of the VM process.

Detailed steps of VM process

1. Performing scanning with Nessus tool by Security Team

2. Are there any new detected Vulnerabilities? – Security team performs check to confirm if there are new detected Vulnerabilities.

3. If there is none – process ought to stop there and is set to repeat.

4. If yes, impact vulnerability should be assessed (by Nessus or by Security team) and passed with scanning report to appropriate System Administrator – If scanning will result in detection of vulnerability then weakness should be assessed for its business disruption potential. Risk-categorized vulnerability with report should be sent to System Administrator responsible for given system.

5. Report analysis performed by System Administrator – Report analysis is performed by an Administrator responsible for given system – road map to resolution should be prepared with issues marked as critical handled at first.

6. Should this issue be derogated? System Admin decides if vulnerability needs to be derogated due to business interests.

7. Preparing derogation request – If yes, System Admin should inquire a derogation to Security Team with clearly stated rationale.

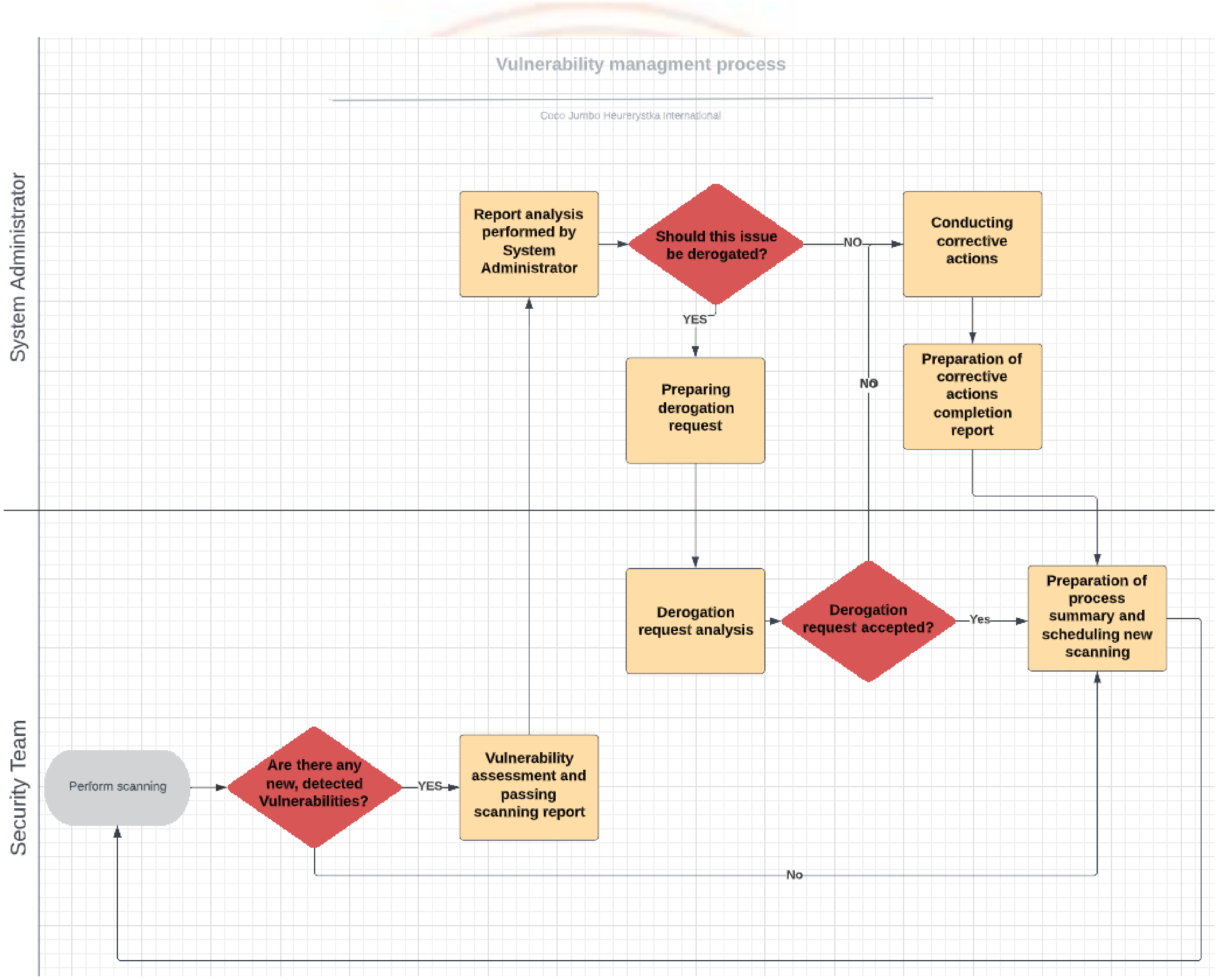
8. Conducting corrective actions – If vulnerability should not be derogated, System Administrator should initiate corrective actions working on par with road map prepared earlier.

9. Corrective actions completion report – After performing appropriate corrective actions system administrator should prepare report with description of actions taken.

10. Derogation request analysis – Security team analyses and formulates an opinion regarding requested derogation for a given vulnerability.

11. Derogation request accepted? – If derogation request submitted by a System Administrator was accepted, the Security Team prepares a process summary. In case of vulnerability being too impactful to derogate, the process ought to continue from step 8.

12. Preparation of process summary Security team prepares a summary of process with description of identified vulnerability, level of impact and action taken.


Vulnerability managment process
Coco Jumbo Heurerystka International
System Administrator
Security Team
Report analysis performed by System Administrator
Should this issue be derogated?
NO
Conducting corrective actions
YES
Preparing derogation request
NO
Preparation of corrective actions completion report
Derogation request analysis
Derogation request accepted?
Yes
Preparation of process summary and scheduling new scanning
Perform scanning
Are there any new, detected Vulnerabilities?
YES
Vulnerability assessment and passing scanning report
No

3. Key Performance Indicators (KPI)

Key performance Indicators are focused on identifying efficiency of VM process and potential existing weak links and bottlenecks which should be main focus of VM process analysis.

Lp.	KPI	Description
1	# of detected vulnerabilities	Number of vulnerabilities found by scanner
2	# of requests for derogation submitted	Number of requests submitted by SysAdmins
3	# of false-positive	Number of vulnerabilities flagged mistakenly
4	Average times needed to close a vulnerability in a given month	Average time needed to resolve a vulnerability (from scanning to prepared end-report)
5	# of detected critical vulnerabilities	Number of vulnerabilities found highly impactful (by safety Team)
6	% of detected vulnerabilities that were found critical	Share of critical vulnerabilities in total # of detected vulnerabilities

4. Revision of process and KPI set

Using data collected within reporting process and feedback provided by KPI this process should be revised at least once per year to ensure that there are no design flaws, and if any will be identified, applicable actions should be taken to restore full capabilities of the process.