Genpact

Threat & Vulnerability Management Process

Version v2.7

22/09/2020

Document Ownership – Rohit Kohli

NOTICE

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by Genpact, nor is this document (in whole or in part) to be reproduced or furnished to third parties or made public without the prior express written permission of Genpact.

Version Control

Version No.	Released On	Change Type	Author/owner	Approver	Date of next review
1	10-Jan-2007	No changes	SOC Team	Vikas Jain	31-Jan-2008
1	01-Jan-2008	No changes	SOC Team	Vikas Jain	31-Dec-2008
1	01-Jan-2009	No changes	Samrat Nandi	Vikas Jain	31-Dec-2009
1.1	10-Aug-2009	Change in KC path (KC migrated to Knowledge@Genpact	Srinivas Kalava	Vikas Jain	31-Dec-2009
1.2	31-Dec-2009	Reviewed with no Changes.	Sukumar	Prashant Srivastava	01-Jun-2010
1.2	30-May-2010	Reviewed with no Changes.	Md.Ateef	Prashant Srivastava	31-Dec-2011
1.2	31-Dec-2011	Reviewed with no Changes.	Md.Ateef	Prashant Srivastava	30-Dec-2012
1.2	30-Dec-2012	Reviewed with no Changes.	Neeraj Kumar	Prashant Srivastava	31-Dec-2013
2.0	01-Jul-2013	Added, DB, Network, PCI	Neeraj Kumar	Prashant Srivastava	31-Dec-2013
2.0	30-Dec-2013	Reviewed with no Changes.	Shalva Narayan	Uma Sekhar Avvari	31-Dec-2014
2.0	08-Oct-2014	Added Rescanning for Leftover devices	Prakash Jaiswal	Uma Sekhar Avvari	31-Dec-2015
2.1	20-May-2015	Updated Process flowcharts, remediation process	Rohit Kohli	Ramachandra Hegde	31-Dec-2015
2.2	31-Dec-2015	Reviewed with no Changes.	Rohit Kohli	Ramachandra Hegde	31-Dec-2016
2.3	30-May-2016	Restructured the document with addition of AppSec, VA, PT and configuration review	Rohit Kohli	Ramachandra Hegde	31-Dec-2016
2.4	10-13-2016	Remediation Scope / Timelines	Rohit Kohli	Ramachandra Hegde	31-Dec-2016
2.4	01-20-2017	No Change	Rohit Kohli	Ramachandra Hegde	31-Dec-2017

2.4	01-30-2018	No Change	Rohit Kohli	Ramachandra Hegde	31-Dec-2018
2.5	03-25-2018	Updated approach to risk-based remediation of vulnerabilities and asset risk scoring	Rohit Kohli	Ramachandra Hegde	31-Dec-2018
2.5	01-02-2019	No Change	Rohit Kohli	Ramachandra Hegde	31-Dec-2019
2.6	06-02-2020	Added asset priority assignment, Updated exception handling Updated VA/PT schedule	Rohit Kohli	Ramachandra Hegde	05-02-2021
2.7	22-09-2020	Added Exception Management process & Helpmate catalog workflow	Rohit Kohli	Ramachandra Hegde	21-09-2021

Table of Contents

Purpose

This document establishes the Threat and Vulnerability Management Process of Genpact. This document sets out the approach to manage network and application security by defining fundamental controls and objectives. This document is both owned and maintained by Information Security Team (hereafter referred as “InfoSec”). This process document is reviewed and approved by Genpact's CISO.

Scope

Threat and Vulnerability management process document is applicable to all the network infrastructure devices and applications managed by Genpact and its subsidiaries which includes but not limited to:

- Network/ security devices
- Servers
- Endpoints
- Voice systems
- Wireless connected systems
- Web application
- Thick client applications
- Mobile applications
- Other software and applications running on Genpact owned systems

Stake Holders

Domain leads and the members of the following teams are responsible to adhere to this process

- Information Security Team (InfoSec)
- Enterprise Application Group (EAG)
- End User Computing (EUC)
- Server Management Group (SMG)
- Network Management Group (NMG)
- Poles Support Team (PST)
- Security Operation Center (SOC)

- System Center Configuration Manager (SCCM)

Refer Appendix A for team wise roles and responsibilities

Compliance

Compliance with Threat and Vulnerability Management policy is mandatory, failure to comply with this policy will result in non-compliance with customer and regulatory requirements.

Activities

Major activities covered under this policy are Vulnerability Assessment, Penetration Testing, Application Security Assessment, Security Code Review and Configuration Review.

Vulnerability Assessment:

Vulnerability assessment (VA) is the process to identify all the known vulnerabilities existing on a particular device, Internal VA should be conducted with authentication, External VA should be conducted without authentication.

Penetration Testing:

Penetration Testing (PT) is the process to run exploits on the known vulnerabilities with the purpose to gain additional information or access on the targeted systems.

It is mandatory to conduct PT on all the PCI and critical rated devices, at least on a yearly basis.

Refer to Appendix B for the list of Do's and Don'ts

Configuration Review:

Configuration Review (CR) is the process to assess the current configurations of the devices, servers and applications as per Genpact's hardening guidelines.

In absence of Genpact's hardening guidelines CIS Benchmark will be applicable.

It is mandatory to conduct CR on critical devices/ services/ applications at least on a yearly basis.

Dynamic Application Security Assessment (DAST):

Application Security Assessment (AppSec) is the process to assess the current security posture of a given application as per the OWASP and SANS top 25, in line with Genpact's InfoSec policies.

It is mandatory to perform DAST on the critical and high severity applications at least on a yearly basis.

Secure Code Review:

Secure Code Review (SCR) is the process to identify security related issues in an application by analyzing the application source code in reference with OWASP secure coding guidelines.

It is mandatory to perform SCR on all critical and high severity applications at least on a yearly basis. Scope is limited only to Internet facing applications and platform developed for customer applications.

Vulnerability Assessment Frequency and Schedule

Internet Facing Applications

	Code Review	Dynamic Assessment	VAPT	Configuration Review
Critical	On code change	6 Months	6 Months	6 Months
High	6 Months	6 Months	6 Months	6 Months
Medium	6 Months	Yearly	Yearly	Yearly
Low	Yearly	Yearly	Yearly	Yearly

Internal Applications

	Code Review	Dynamic Assessment	VAPT	Configuration Review
Critical	On code change	Yearly	Yearly	Yearly
High	Yearly	Yearly	Yearly	Yearly
Medium	Yearly	Yearly	Yearly	Yearly
Low	N/A	Every 2 year	Yearly	Yearly

Vulnerability Assessment Schedule – Infrastructure

Tasks	Frequency	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
VA	Monthly	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Third party PT (Internal and Internet facing)	Yearly									✓	✓		
PCI Systems	Yearly		✓	✓	✓								
Internal PT						**YEARLY**							
Key Infrastructure Security Projects						✓	✓						
Network - Server Zone, DMZ, Cloud Environment						✓	✓					✓	✓
Key clients								✓	✓	✓			
Major Changes	On Demand												

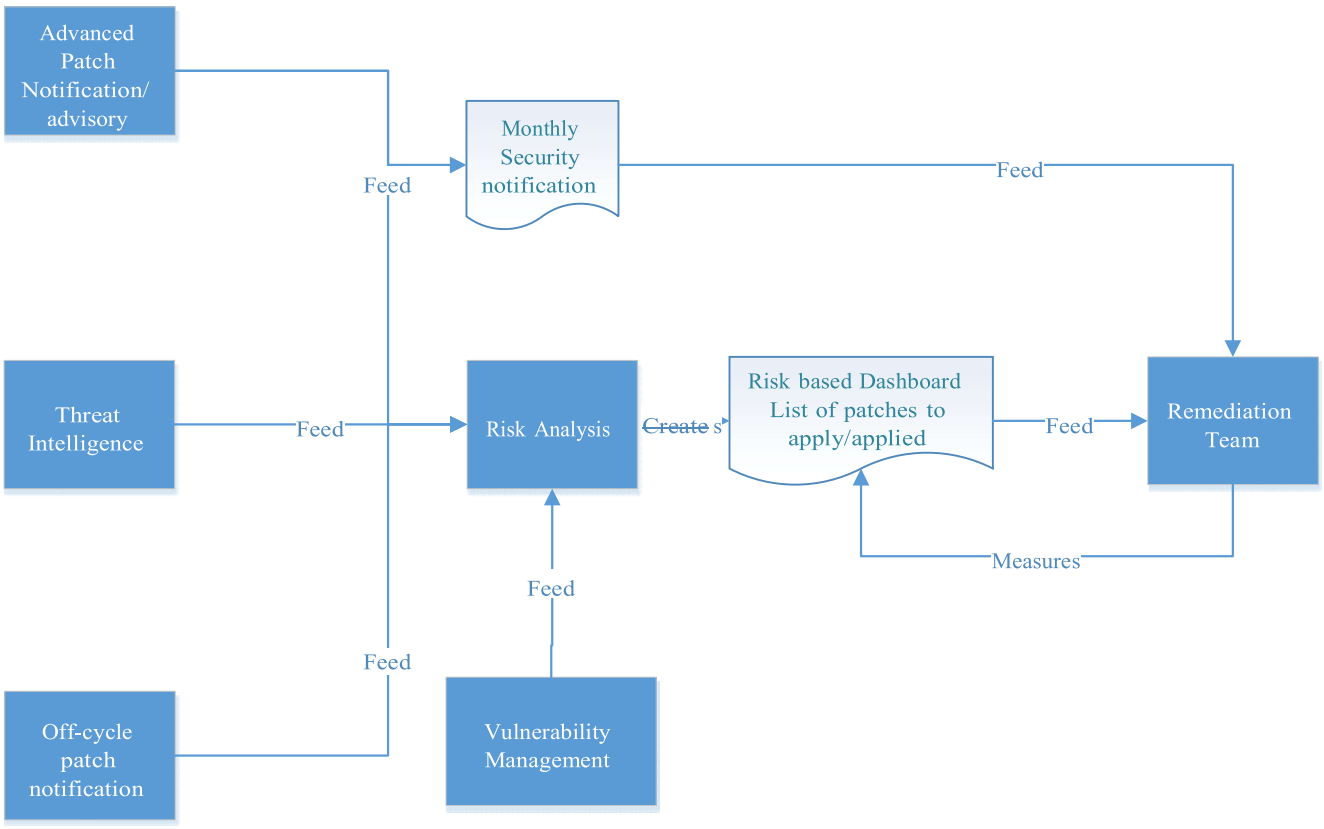
✓ Planned

Process Overview

Linkage between Patch and Vulnerability Management

Genpact InfoSec team has registered with US-Cert, NVD, FS ISAC etc. to receive daily security notification on security issues and vulnerabilities. The team relies on the preliminary analysis of these organizations and takes into consideration security advisory basis business impact, severity, urgency and applicability to the Genpact environment. Based on these information, InfoSec team provide the list of applicable patches in the form of advisory to the remediation team on Monthly basis (Microsoft advisory in second week of month and Non-Microsoft advisory last week of month) to mitigate the vulnerabilities.

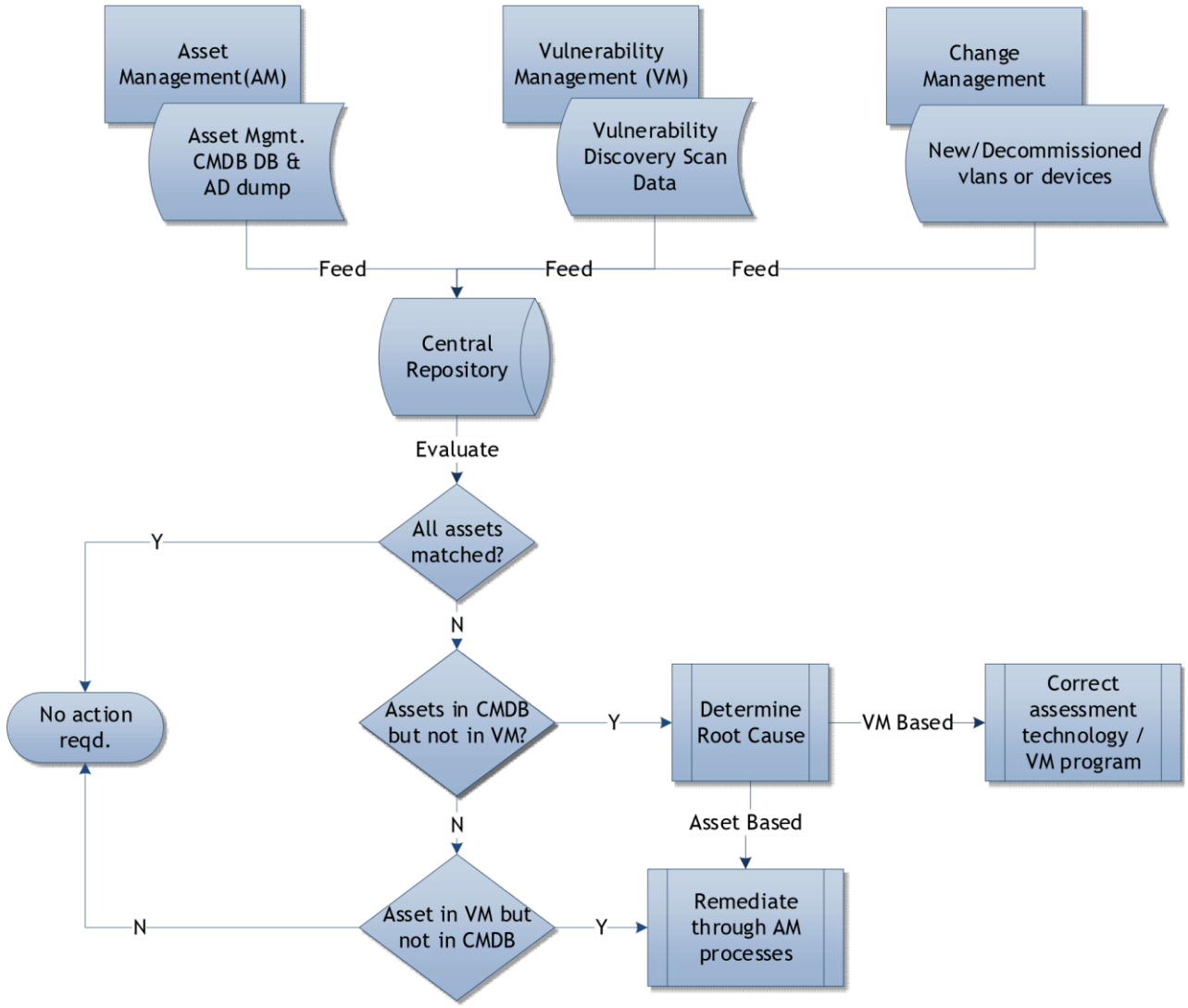
A Software-as-a-Service based Vulnerability and Risk Intelligence (VRI) platform has been implemented in order to accurately measure risk and prioritize remediation efforts.



Remediation progress can be monitored in VRI platform using:

- Search function IN VRI tool can be used to validate closed/open status of CVE IDs
- Leverage data available in VRI for reporting monthly patch compliance

Asset Inventory Reconciliation



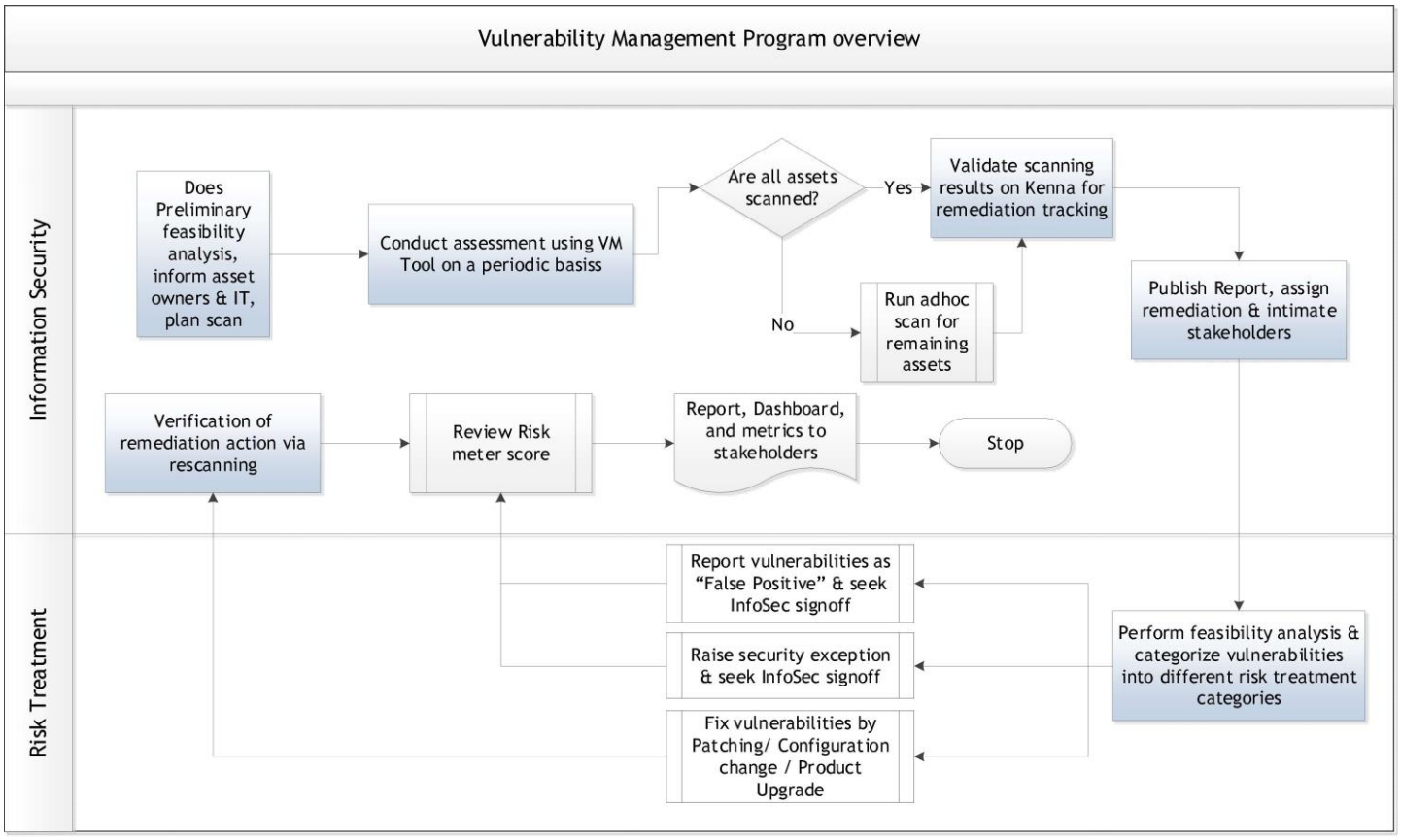
The assets reconciliation will be performed on a monthly basis using multiple data sources and compared with actual assets scanned.

The external sources used:

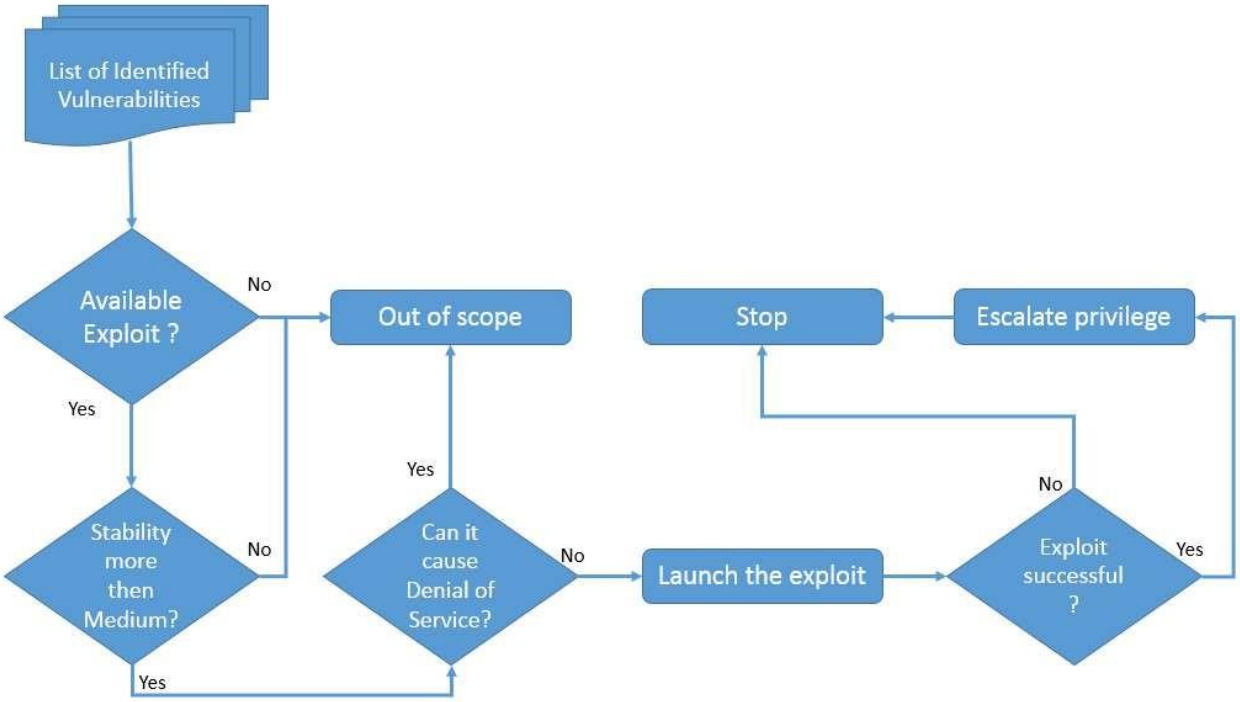
- Monthly Baseline created based on: Active Directory dump, UCMDB, Assets Management
- Change Management – changes related to VLANs (new, decommissioned, moved) and changes related to addition/decommission of servers and network equipment

All founded defects (assets not covered in scans) after determining the root cause, will be covered in next weekly scan.

Vulnerability Management Program Overview



Penetration Testing Process



Vulnerability Remediation Overview

Vulnerability Risk Intelligence (VRI) platform is an intelligence driven vulnerability remediation technology that helps drive the risk score (meter) of vulnerabilities impacting overall Genpact risk posture.
Risk Meter is an asset-based measure of the security risk possessed by a group of assets, based on the following factors:

- Adjusted CVSS: CVSS scores are adjusted automatically to reflect the probability of breach or impact of vulnerability.
- Exploit Analytics: If a vulnerability has known exploits or breaches or have a popular target in recent cyberattacks.
- Asset Priority: Criticality of the asset in our infrastructure. The asset priority is assigned as per below table: -

S.No.	Device Type	Asset Priority
1.	Network/ security devices	10
2.	Servers	10
3.	Endpoints	7

Asset scores are based on the highest vulnerability that exists on the asset and is multiplied by the Asset Priority. External facing assets represent a higher risk and therefore will receive a score increase (+200)

- Green = Score between 0 - 330
- Yellow = Score between 340 - 660
- Red = Score between 670 - 1000

Vulnerability scores:

- Green = Score between 0 - 33
- Yellow = Score between 34 - 66
- Red = Score between 67 - 100

Remediation Team will focus on vulnerabilities that provide the greatest reduction in risk based on real-world threats, not just internal weaknesses.

VRI "Top Fixes" dashboard provide the exact "fix" required to be applied in order to decrease/maintain risk meter score in green area. Remediation team will perform preliminary analysis & classify vulnerabilities into determined state. Some examples of the determined state include:

- Patched, Configuration change, remediated, or fixed o Risk Acceptance o False positive
- Mitigation through technology or existing effective controls

Remediation progress can be monitored in VRI platform using:

- Search function for specific closed/open vulnerabilities in a period ☐ Dashboard (historical Risk Information section)

Handling exceptions:

- Remediation team will revert with action plan and timelines for closure of identified vulnerabilities
- All approved exceptions will be imported and tracked in VRI
- Risk meter score will automatically get adjusted once a vulnerability status is set to "Risk Acceptance"

Remediation Timelines

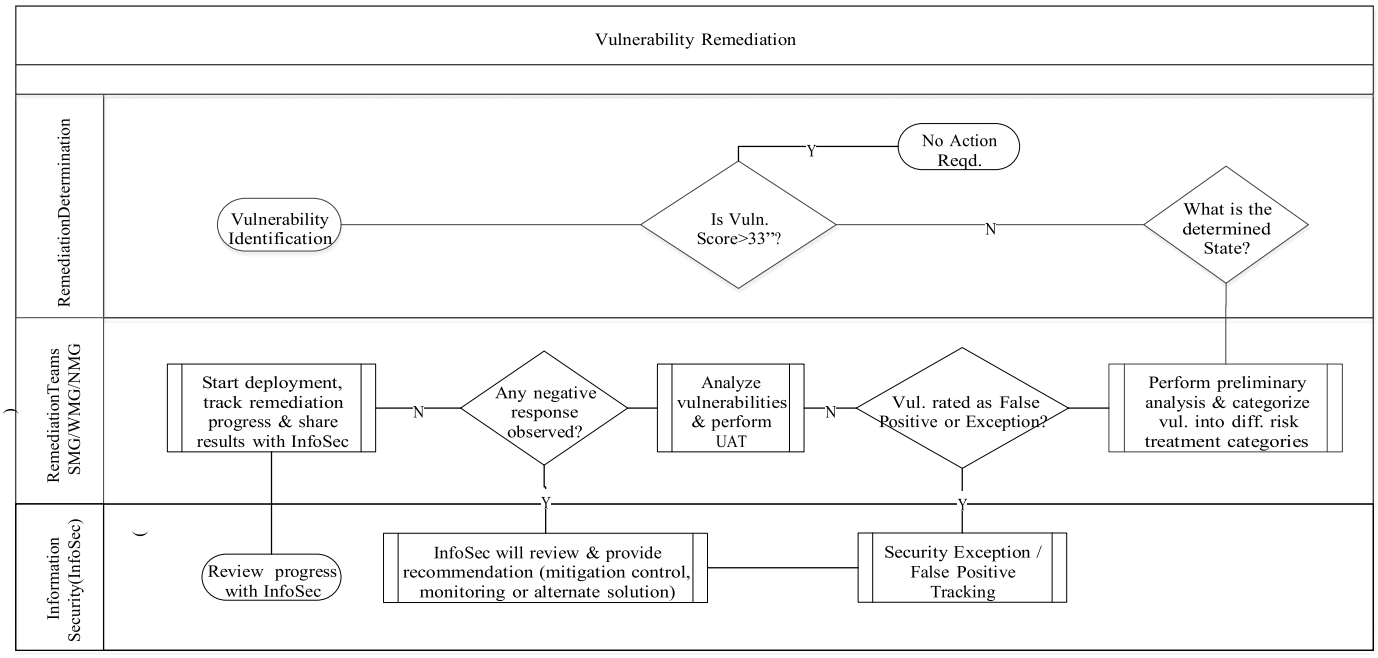
Risk Meter	Score	Timelines (Days)
Red	670 - 1000	Within 30 Days
Yellow	340 - 660	Within 30 Days
Green	0 - 330	Within 60 Days

* We have to maintain risk meter score green.

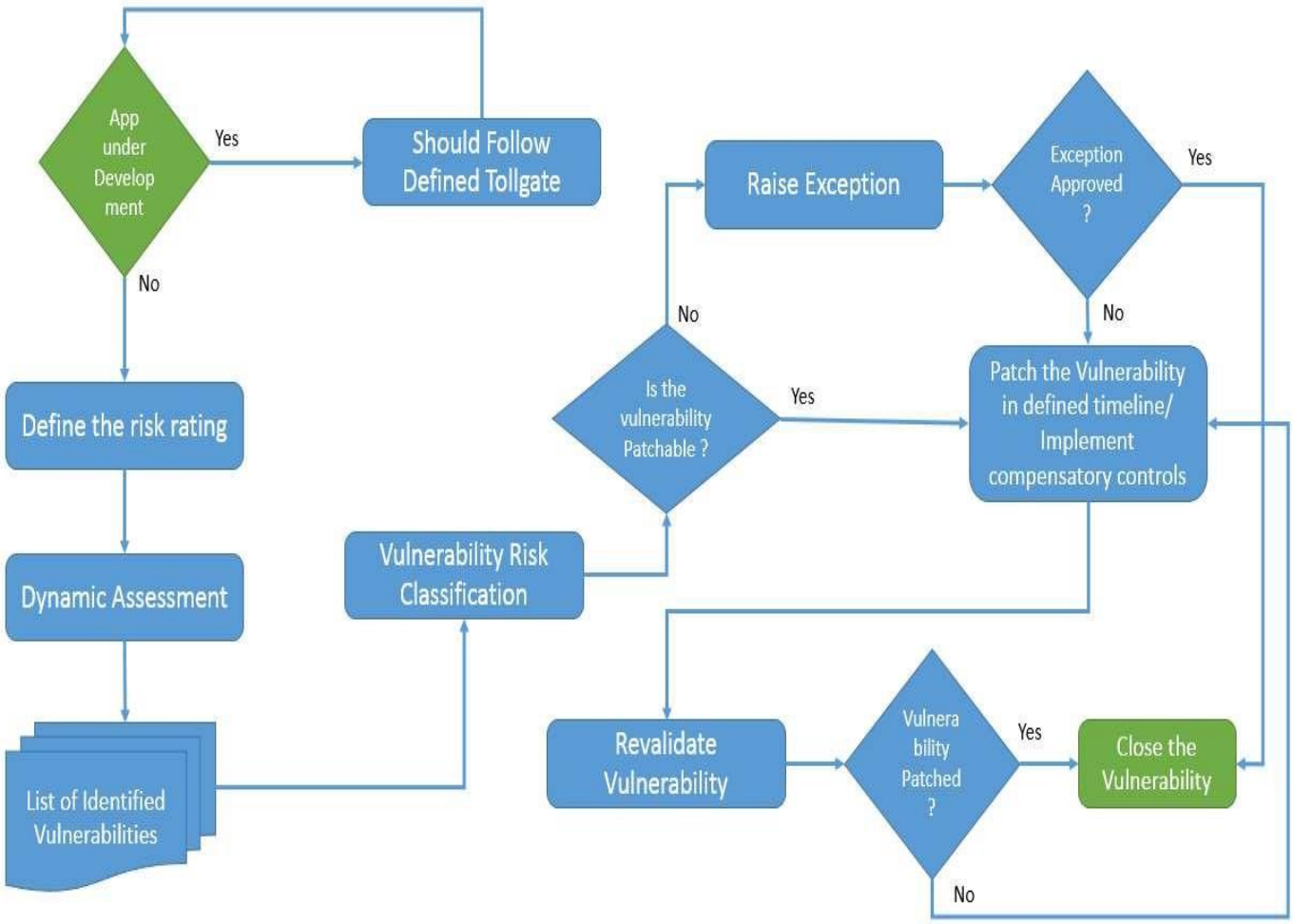
Critical Asset – Remediation Prioritization

- Genpact categorize certain category of servers (Active Directory, Exchange, O365, FTP, File Server, DNS, DHCP, Web Server, Federation, Single Sign ON (SSO), Two Factor Authentication (RSA), and Identity & Access Management Servers) hosted in shared server zone and PDMZ as business critical.
- Information security team basis the asset risk register has adjusted the asset priority for difference type of assets which helps drive focus remediation of assets with high risk score

Vulnerability Remediation



Application Security Assessment



RACI Matrix

Process	Task	Responsibility	Accountability	Consulted	Informed
Patch Notification	Risk Analysis of Threat Intelligence & Security Advisories	InfoSec	InfoSec	-	Remediation / Operations
	Publish Report on off-cycle patch remediation	InfoSec	InfoSec	-	Remediation / Operations
	Tracking Remediation	SOC Operations	SOC Operations	InfoSec	Remediation / Operations
Asset Inventory Reconciliation	Collection of Asset Data from CMDB	InfoSec	InfoSec	IT Asset Mgmt. Team	SOC Operations
	Validation of Workstation, Servers, & Network devices	InfoSec	InfoSec	IT Asset Mgmt. Team	SOC Operations
Vulnerability Management	Vulnerability Scanning and Identification	InfoSec	InfoSec	-	SOC Operations
	Risk Re-Ranking	InfoSec	InfoSec	SOC Operations	Remediation
	Risk Treatment Classification	Remediation	Remediation	SOC Operations	SOC Operations
	Reporting of program KPIs and metrics	InfoSec	InfoSec	Remediation	EUC, NMG, SMG
	Program enhancement requests	InfoSec	InfoSec	SOC Operations	Remediation
Vulnerability Remediation	Assignment of remediation to different stakeholders	SOC Operations	InfoSec		
	Patch Implementation	Remediation	SOC Operations	InfoSec	InfoSec
	Security Exception	Remediation	SOC Operations	InfoSec	InfoSec
	Software Upgrade	Remediation	SOC Operations	InfoSec	InfoSec
	Configuration Change	Remediation	SOC Operations	InfoSec	InfoSec
	Tracking of remediation actions	SOC Operations	InfoSec	InfoSec	InfoSec

Detection

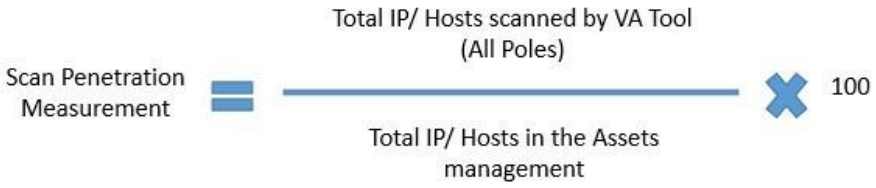
- Running VA scans across Infra on given VLANs
- Quarterly Reconciliation of VLANs and Assets across Infra and Business
- Measuring Scan Penetration every month for coverage of Assets
- Conducting Configuration reviews of server, OS, network devices and critical applications
- Performing Application vulnerability assessment on frequent intervals
- Performing source code review of business critical applications to identify vulnerable source code

Incidence Logging/ Escalation

All issues related to incidents and escalations are to be resolved as per Genpact's Incident Management Process

Control Mechanism

- Weekly and Fortnightly Review of new discovered vulnerabilities & monitor remediation progress
- Monthly Report Out for VA and Monthly Compliance Metric
- Closure/Remediation Tracking by respective functions
- Scan penetration measurement



*Asset CMDB= All AD Active Machine + SMG CMDB (All sub domain CMDB) + Network Devices (Data & Voice) excluding Wireless Access Point+ All Security Devices (NIDS/NIPS/Firewall/SIEM)

Exception Handling

- For marking any vulnerability as False Positive, approval needs to be taken from InfoSec and application manager.
- For vulnerabilities with no fix available, approval needs to be taken from InfoSec till the time a fix is available other than the stipulated time frame of the OEM/ Industry Standard.
- Any exceptions for identified vulnerability needs to be approved by InfoSec Team and tracked by SOC Operations team
- All exception should be raised, and documentation needs to be maintained by SOC Operations team.
- Risk arising due to End of Life (EOL), End of Support (EOS) and application dependencies shall be assessed in conjunction with existing and compensatory controls vis-à-vis risk to information system by Infosec, Business, IT teams and shall be owned by system owner for a specific period. The risk will be re-assessed post expiry of the specified period
- Exception for inability to remediate the vulnerabilities recommended by Kenna requires careful due diligence. A workflow has been created in Helpmate to include the stake holder's approval to manage and approve exceptions wrt OS, application and N/W devices vulnerabilities.
- Conditions where a request for not applying patches as recommended are:
    - Conflict with the Application
    - End of Support System
    - Vendor recommendation
    - Others

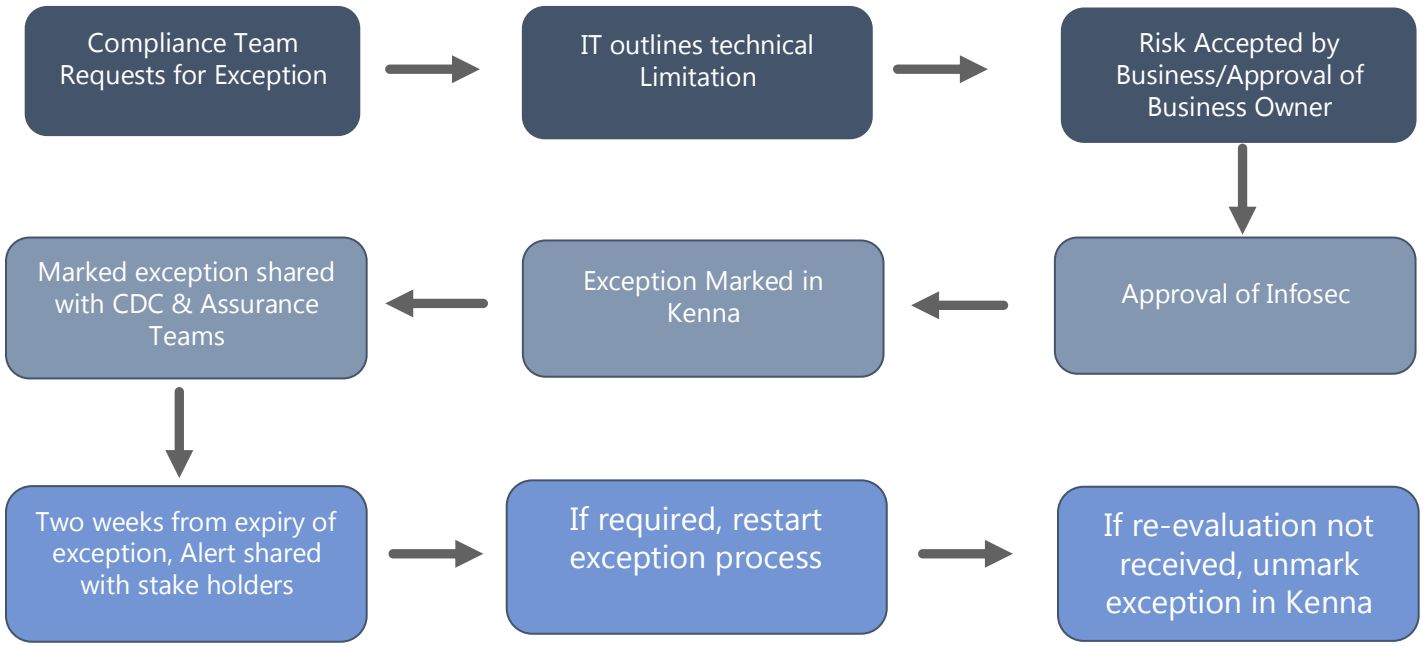
- The Helpmate exception workflow catalog can be initiated by a member of Compliance team after due consideration that, applying a security fix as recommend by Vulnerability scanner/Kenna/ OEM will have severe impact on the business productivity. Additionally, compensatory control that will be implemented along with duration for which exception is sought needs to be indicated in the workflow. The workflow for the catalog can be reached at: Helpmate>Catalog>Threat and Vulnerability Management Exceptions

Post approval by the stake holders, an exception will be marked in the Kenna, which will include hosts against which CVE based exception has been granted along with duration for which exception has been sought.

Post the expiry of exception period, the vulnerability will be re-activated in Kenna, if no further exception is needed or remediation has been done as recommended. In case the remediation has not been undertaken, an approval process will be reinitiated through the Helpmate catalog. Roles and responsibilities of various stakeholders will be as follows:

- Exception can only be raised by Compliance team/ Digital Team
- IT team outlines technical limitation
- Business owner Accepts the Risk
- Infosec approves the risk acceptance
- Risk acceptance marked in Kenna

Threat and Vulnerability Management Exceptions Workflow



Success Measure

- Timely closure of vulnerabilities by remediation teams
- Closure of identified vulnerabilities within defined timeline
- Target 90% scanning penetration
-

Potential Risk Points

- Any critical alert not attended on time can lead to serious security breach
- Identified vulnerabilities are not closed within agreed timelines
- Assets are not scanned consecutively for 2 scan frequency
- Vulnerabilities are reopened post validation confirmation

References

Genpact Information Security Policy Document

Appendix A - Roles & Responsibilities

This section defines the roles and responsibilities of different teams involved in the process:

Information Security Team (InfoSec)

- Perform threat analysis and dissemination services
- Conduct and ensure enterprise wide vulnerability scan
- Monitor enterprise wide vulnerability remediation progress
- Provide aggregated reporting on enterprise wide vulnerability findings status
- Work with different entities on reviewing risk and defining acceptable mitigation controls
- Identification & escalation of critical vulnerability enterprise wide
- Perform risk re-ranking for prioritized remediation & adjust risk rating based upon potential impact to Genpact
- Maintain and publish secure coding guidelines and standards for secure configuration of network devices, operating systems and other critical software

- Perform ad hoc vulnerability scanning on critical assets/ applications
- Perform penetration testing on critical assets/ applications
- Perform dynamic and static application security assessment as per the available schedule
- Perform configuration review on servers, network devices, applications and databases
- Perform firewall rule base review and publish recommendations to NMG
- Share a comprehensive report for the identified application vulnerabilities with application team
- Maintain vulnerability scanning schedule (Internal / External)
- Publish threat intelligence for critical vulnerabilities
- Engage third party vendors for external VAPT of critical infrastructure devices
- Maintain and update Vulnerability Management process document

SOC Operations

- Maintain approved list of false positives and security risk exceptions
- Perform revalidation scanning to verify remediation of identified vulnerabilities
- Maintain and publish vulnerability scorecard to InfoSec and Genpact management

Remediation Teams (WMG / SMG / EAG / NMG)

- Perform preliminary review of vulnerabilities
- Determine false positives and seek InfoSec and SOC approval
- Seek exception from InfoSec for the vulnerabilities with “No Solution” or application dependency
- Seek downtime from business for vulnerability remediation, if required
- Perform vulnerability remediation by security patch installation, configuration adjustment, software removal or by modifying firewall rules
- Highlight the challenges faced to patch the vulnerability to InfoSec and SOC
- Maintain remediation tracker and share progress with InfoSec, SOC & EUC operations team

Application Team

- Perform incremental secure code review of the applications
- Track and ensure the remediation of identified vulnerabilities
- Request InfoSec for application dynamic assessment on completion of application development
- Maintain remediation tracker and share the progress with application owners and InfoSec
- Seek InfoSec approval for deploying the application in production environment
- Seek exception from InfoSec for the vulnerabilities with application dependencies

Appendix B - Do's and Don'ts for Penetration Testing

Considering the criticality of penetration testing activity and its impact on the environment, following few things are to be kept in mind while performing the activity.

- All the Penetration Testing activities should be explicitly approved by management and InfoSec manager
- Penetration testing should not be conducted on peak hours
- Stability of exploits for production system should be either 'High' or 'Excellent'
- Any exploit downloaded from Internet should be checked for malicious script before executing
- Any exploit that may resulting into Denial of Service or crash PoC (Proof of Concept) should not be used
- Persistent modules of exploits are not be used
- Pivoting to another system post exploitation is not permitted
- Exploit evidence should be limited to Ipconfig / ifconfig output
- Access, deletion or modification of any files/folders on the exploited systems is not permitted
- All the scripts, backdoors or executables uploaded on the exploited systems should be removed post analysis of target system
- Persistent module of exploiting a system should not be used
- Disrupting any of the running services on compromised system is not permitted