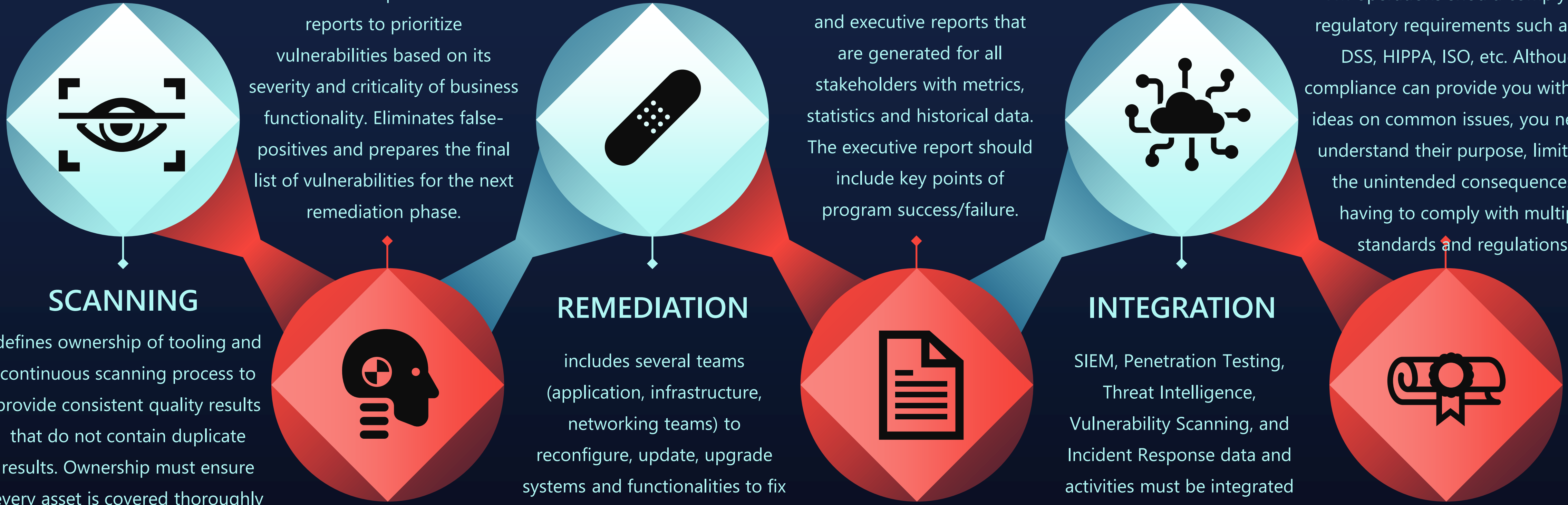
VULNERABILITY MANAGEMENT PROGRAM KEY FACTORS



SCANNING

defines ownership of tooling and continuous scanning process to provide consistent quality results that do not contain duplicate results. Ownership must ensure every asset is covered thoroughly in the scanning process on a regular period with proper agent deployments and scan profile coverage.

ASSESSMENT

includes review process of scan reports to prioritize vulnerabilities based on its severity and criticality of business functionality. Eliminates false-positives and prepares the final list of vulnerabilities for the next remediation phase.

REMEDIATION

includes several teams (application, infrastructure, networking teams) to reconfigure, update, upgrade systems and functionalities to fix vulnerabilities. Remediation owner takes responsibilities of remediation progress tracking.

REPORTING

includes tactical, technical, and executive reports that are generated for all stakeholders with metrics, statistics and historical data. The executive report should include key points of program success/failure.

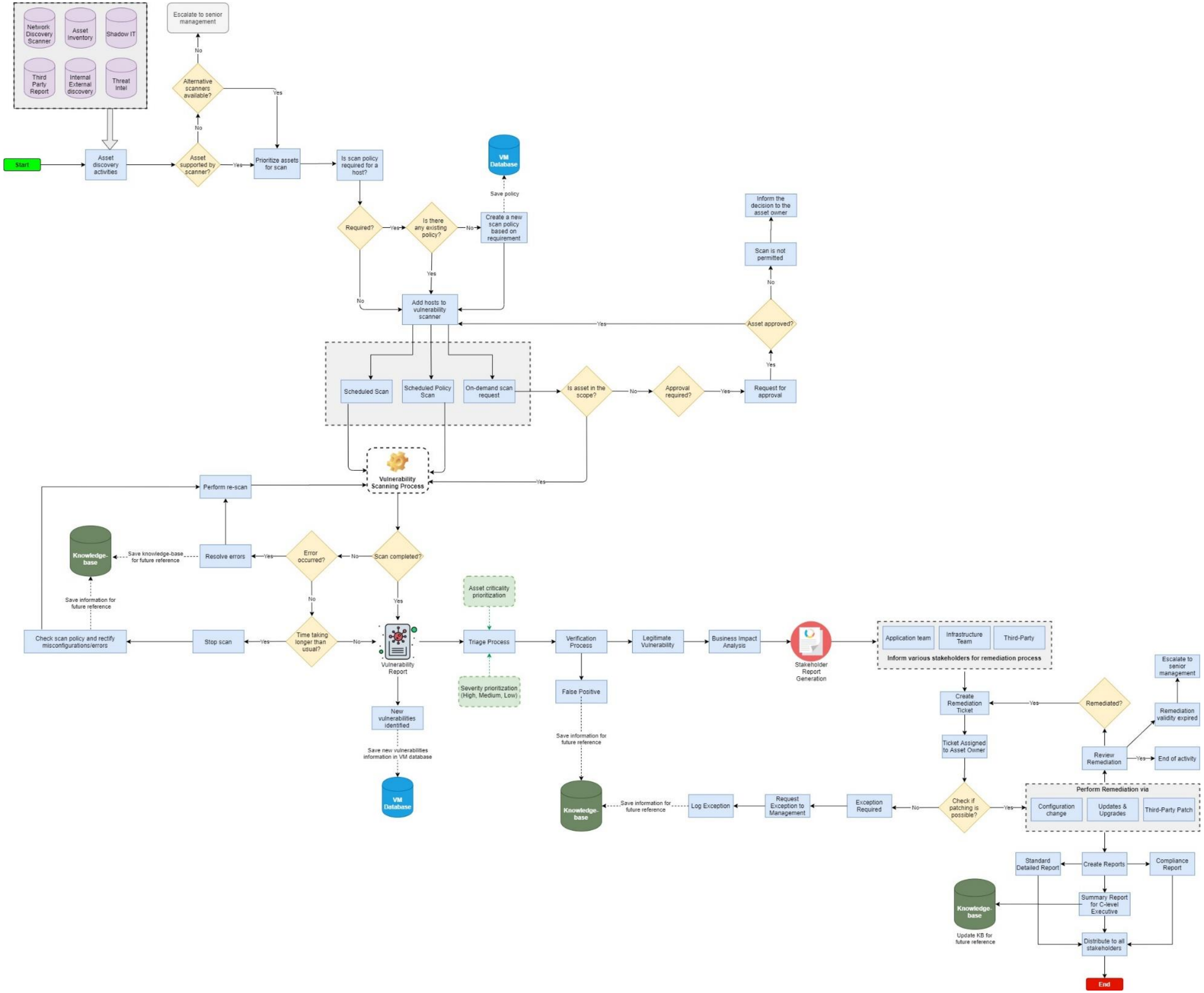
INTEGRATION

SIEM, Penetration Testing, Threat Intelligence, Vulnerability Scanning, and Incident Response data and activities must be integrated and filtered to get the consistent, maximum and actionable output.

GOVERNANCE & COMPLIANCE

VM operations should comply with regulatory requirements such as PCI-DSS, HIPPA, ISO, etc. Although compliance can provide you with useful ideas on common issues, you need to understand their purpose, limits and the unintended consequences of having to comply with multiple standards and regulations.

Chintan Gurjar
InfosecNinja.blogspot.com
chintangurjar@outlook.com


Network Discovery Scanner
Asset Inventory
Shadow IT
Third Party Report
Internal External discovery
Threat Intel
Escalate to senior management
No
Alternative scanners available?
Yes
No
Start
Asset discovery activities
Asset supported by scanner?
Yes
Prioritize assets for scan
Is scan policy required for a host?
VM Database
Save policy
Required?
Yes
Is there any existing policy?
No
Create a new scan policy based on requirement
No
Yes
Add hosts to vulnerability scanner
Inform the decision to the asset owner
Scan is not permitted
No
Asset approved?
Yes
Yes
Scheduled Scan
Scheduled Policy Scan
On-demand scan request
Is asset in the scope?
No
Approval required?
Yes
Request for approval
Yes
Vulnerability Scanning Process
Perform re-scan
Knowledge-base
Save knowledge-base for future reference
Resolve errors
Yes
Error occurred?
No
Scan completed?
Save information for future reference
No
Yes
Asset criticality prioritization
Check scan policy and rectify misconfigurations/errors
Stop scan
Yes
Time taking longer than usual?
No
Vulnerability Report
Triage Process
Verification Process
Legitimate Vulnerability
Business Impact Analysis
Stakeholder Report Generation
Application team
Infrastructure Team
Third-Party
Inform various stakeholders for remediation process
Severity prioritization (High, Medium, Low)
False Positive
New vulnerabilities identified
Save new vulnerabilities information in VM database
VM Database
Save information for future reference
Knowledge-base
Save information for future reference
Log Exception
Request Exception to Management
Exception Required
No
Check if patching is possible?
Yes
Create Remediation Ticket
Yes
Remediated?
Escalate to senior management
Remediation validity expired
Ticket Assigned to Asset Owner
Review Remediation
Yes
End of activity
Perform Remediation via
Configuration change
Updates & Upgrades
Third-Party Patch
Standard Detailed Report
Create Reports
Compliance Report
Knowledge-base
Summary Report for C-level Executive
Update KB for future reference
Distribute to all stakeholders
End