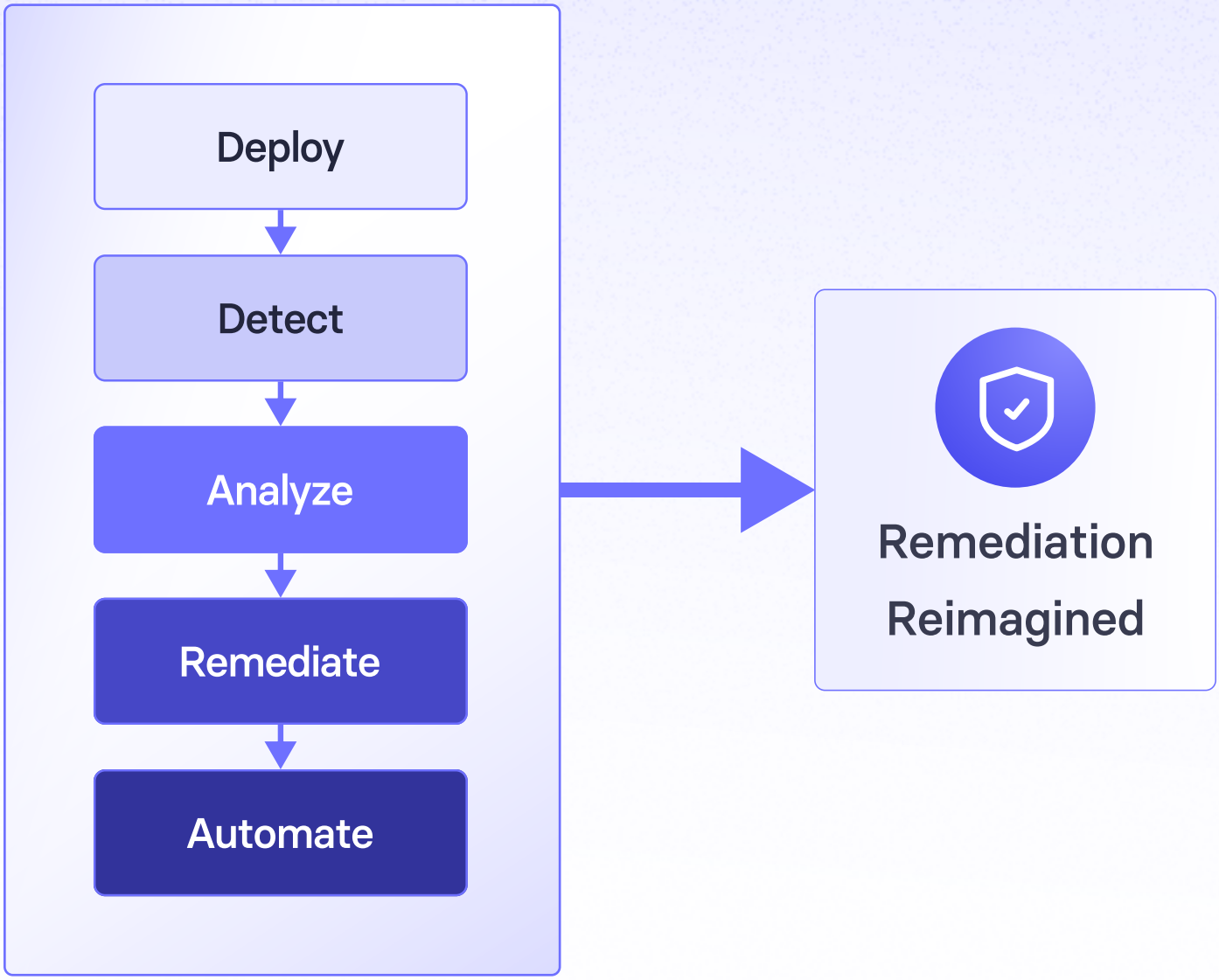
vicarius

Vicarius vRx Maturity Model



Purpose

The Vicarius Cybersecurity Maturity Model is designed to help organizations assess their current security posture and identify actionable opportunities for improvement. Rather than acting in a silo, this model positions **vRx as a mapping layer** translating operational practices into well-known frameworks such as NIST CSF 2.0, CIS Controls v8, and ISO/IEC 27001:2022. This allows organizations to benchmark progress using standards their boards, auditors, and regulators already recognize.

vRx is an advanced vulnerability remediation platform that enables real-time patching, script-based fixes, and patchless protection. The maturity model provides a structured framework to evaluate security operations across five key stages: **Deploy, Detect, Analyze, Remediate, and Automate**. Each stage maps to core security functions and can be linked to measurable controls from industry frameworks.

By understanding where your organization stands across these stages, you can prioritize investments, track maturity at both global and site levels, and coordinate improvements across teams and tools. The model supports **both self-assessment and automated scoring**, aligned with real platform usage.

This document offers:

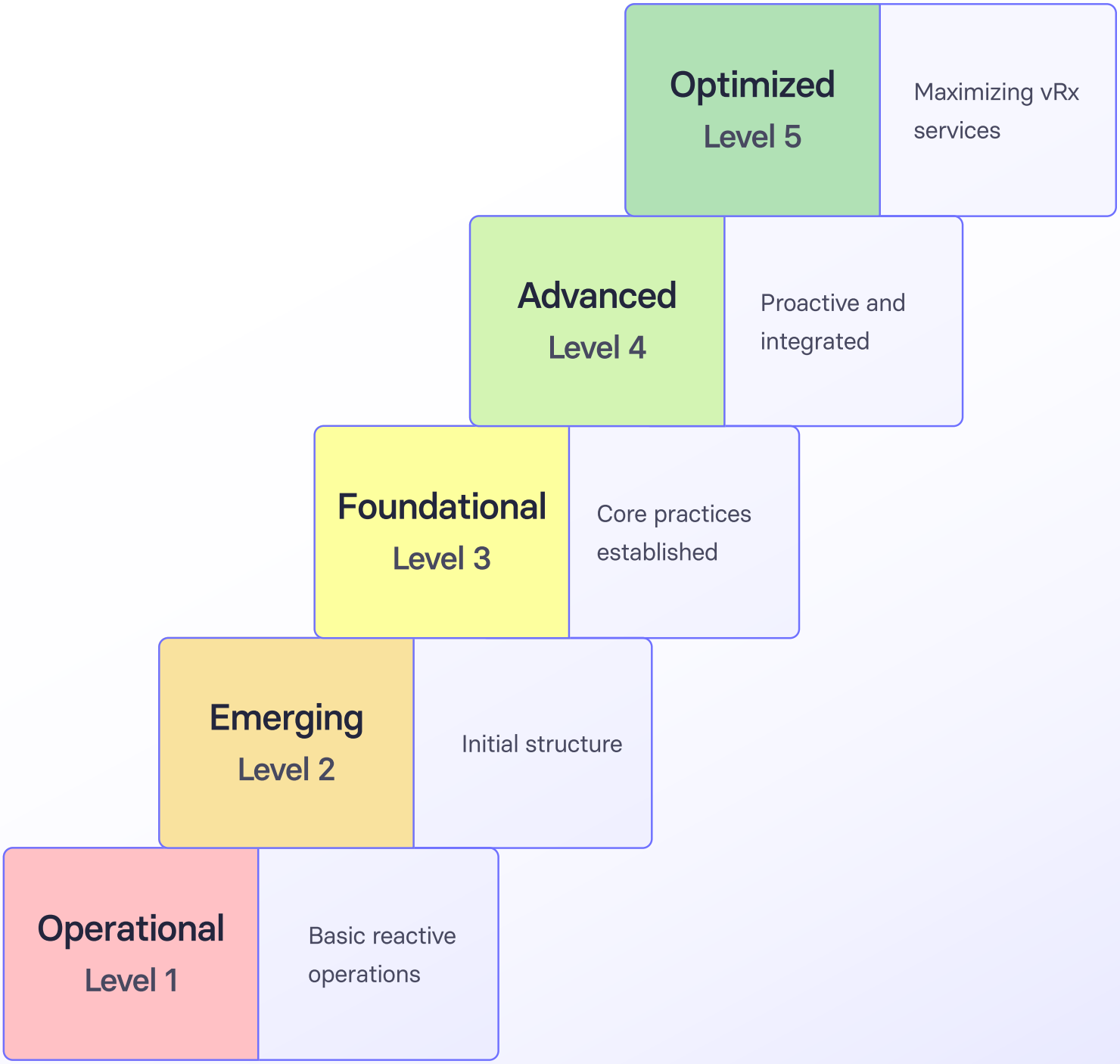
1. A structured approach to assess cybersecurity maturity across business units or environments.
2. Milestones mapped to global frameworks to guide improvement plans and audit readiness.
3. Specific guidance on how to use Vicarius to fill control gaps and orchestrate security workflows across your existing tools (e.g., XDR, RMM, ITSM, SOAR).

By leveraging this model, organizations can operationalize maturity scoring, reduce risk through automation, and improve compliance posture without replacing their current stack.

Maturity Levels Explained

- **Operational (Level 1)**: Basic, reactive operations with minimal formal processes. Organizations at this level are largely manual in their approach, focusing on essential tasks to keep things running. Use of vRx is limited to fundamental features and on an as-needed basis.
- **Emerging (Level 2)**: Initial structure and consistency are developing. The organization has started to implement repeatable processes and makes greater use of vRx capabilities, though coverage and efficiency are still improving.
- **Foundational (Level 3)**: Core practices are established and consistently executed. The organization has a solid base – using vRx across the environment – and follows routine policies for vulnerability management.
- **Advanced (Level 4)**: Proactive and well-integrated processes define this level. The organization integrations) to drive efficient, coordinated security operations.
- **Optimized (Level 5)**: Continuous improvement and automation are paramount. The organization maximizes all vRx features, with fully automated, orchestrated workflows and ongoing tuning. Processes are refined based on metrics, and the system adapts quickly to new threats with minimal human intervention.

Maturity Levels



Security Operation Stages Explained

Level 1: Deploy

Description: This stage covers how security tooling and controls are rolled out across assets. It includes deploying the vRx platform/agents, ensuring coverage of all servers, workstations, and applications, and maintaining an accurate asset inventory. Higher maturity here means broader and more automated deployment of vRx for complete environment visibility.

Key Characteristics:

- Basic setup of security tools Initial configuration across essential assets
- Limited visibility of the entire network or system
- Manual deployment of agents or software

Symptoms:

- Manual, ad-hoc deployment of security tools
- Limited or no automation for asset discovery or vulnerability scanning
- Gaps in asset visibility and inconsistent patching and vulnerability remediation practices
- Reactive security posture, only addressing vulnerabilities as they arise

Strategy Structure:

- Basic security tools are deployed, often only on critical systems
- Security practices are unstructured and inconsistent
- Vulnerability management is done on a case-by-case basis with little long-term planning.
- Deployment processes lack standardization and automation

Governance:

- Minimal formal policies or procedures in place for security operations
- No centralized oversight for vulnerability management or asset tracking
- Ad-hoc reporting and risk analysis with no formalized metrics or goals

Team Alignment:

- Teams work in silos, with minimal coordination between security, IT, and operatio
- Security teams are often reactive, with little cross-department collaboration or integration

Example Practices:

- Install vRx agents on a limited number of critical systems
- Use manual processes to track assets and deployments
- Perform basic vulnerability scans periodically
- Apply patches as needed, without a clear schedule
- Conduct one-time vulnerability assessments with limited scope

Level 2: Detect

Description : Detect refers to discovering vulnerabilities and exposures in the environment. It entails how an organization monitors for new vulnerabilities (e.g. continuous scanning, real-time alerts) using vRx. Mature detection leverages vRx's real-time scanning and multiple threat intelligence feeds to ensure no vulnerability goes unnoticed.

Key Characteristics:

- Basic monitoring for vulnerabilities, mainly using simple detection tools
- Periodic vulnerability scans or system checks with manual log analysis with little automation
- Limited incident detection outside high-profile threats
- Reactive alerting based on predefined security rules

Symptoms:

- Regular vulnerability scans, but coverage is still limited
- Inconsistent detection of new vulnerabilities or threats
- Manual log analysis with little integration of alerts
- Delayed response times to detected issues due to reactive processes
- Threat detection primarily focuses on high-profile or known vulnerabilities

Strategy Structure:

- Detection processes are becoming more structured, with scheduled vulnerability scans
- Use of basic security monitoring tools, but no real-time threat detection or correlation
- Vulnerabilities are detected reactively rather than proactively
- Some automation in alerting, but manual intervention is still common

Governance:

- Basic incident response plans are in place, but often untested
- Some security policies exist, but they are not consistently enforced
- Limited centralized oversight for security event monitoring and threat detection
- Reporting is infrequent and lacks detailed analysis of trends or root causes

Team Alignment:

- Security team collaborates more with IT, but processes are still fragmented
- Roles and responsibilities are somewhat defined, but there is still reliance on manual efforts
- Security team is reactive, with limited proactive involvement in detecting new threats
- Cross-team communication exists but is not streamlined for fast decision-making or response

Example Practices:

- Conduct vulnerability scans with vRx on a weekly or monthly basis
- Use vRx to detect and alert on known vulnerabilities
- Manually monitor systems for new threats or abnormal behaviors
- Set up basic alerting within vRx to notify teams of high-risk vulnerabilities
- Review and respond to security logs without a centralized alerting system

Level 3: Analyze

Description : This stage involves assessing and prioritizing the detected vulnerabilities. It covers how the organization uses vRx's contextual risk assessment and reporting to understand which vulnerabilities matter most. At high maturity, analysis is data-driven with vRx's AI-powered risk scoring providing insight into asset criticality and exploit likelihood.

Key Characteristics:

- Increased sophistication of threat analysis leveraging threat intel for deeper vulnerability insights.
- Risk-based vulnerability prioritization with standardized threat analysis processes.
- Use of threat intelligence to provide deeper insights into vulnerabilities
- Documentation of incidents for future reference and improvement

Symptoms:

- Analysis of vulnerabilities is consistent, but often focused on high-priority issues only
- Structured threat analysis incorporating asset criticality and limited intelligence integration • Standardized incident response processes, not yet fully data-driven

Strategy Structure:

- A more formalized approach to vulnerability prioritization using risk assessments
- Vulnerabilities are categorized based on asset value, business impact, and exploitability
- Regular analysis of threats with periodic reviews of past incidents
- The organization is beginning to use data-driven approaches to analyze risks and threats

Governance:

- Documented processes for incident response and vulnerability management
- Threat intelligence is integrated into analysis workflows, though not fully automated
- Reporting is more frequent, with established metrics for risk and vulnerability trends
- Governance is improving, with some oversight from security leadership, but still reactive in nature

Team Alignment:

- Security and IT teams work more closely to assess and respond to threats
- Clearer roles and responsibilities are defined for incident analysis and escalation
- Teams collaborate on identifying vulnerabilities, but decision-making can still be slow
- Incident response processes are more formalized, with some automation, but manual efforts are still common for complex analysis

Example Practices:

- Leverage vRx to prioritize vulnerabilities by asset value and criticality
- Analyze security incidents with a focus on root cause and business impact
- Use vRx's reporting features to document and analyze vulnerabilities in depth
- Integrate threat intelligence feeds into vRx for better understanding of emerging threats
- Use risk scoring from vRx to adjust vulnerability prioritization

Level 4: Remediate

Description : Remediation is the process of fixing or mitigating vulnerabilities. This includes applying patches, executing script-based fixes, or using virtual patching (patchless protection) via vRx. Increasing maturity denotes a shift from ad-hoc, manual patching to automated, multi-faceted remediation using vRx's full toolset.

Key Characteristics:

- Proactive patch management with automated remediation for known vulnerabilities
- Scripted fixes for vulnerabilities with no available patches
- Risk-based remediation focusing on critical systems first
- Post-remediation validation to ensure fixes are effective

Symptoms:

- Remediation is proactive and focused on high-risk vulnerabilities first
- Patch management is automated, with minimal manual intervention required
- Vulnerabilities are addressed swiftly, often before they are exploited
- Complex issues, such as zero-days, are handled with scripted fixes or virtual patching
- Remediation is streamlined, with some manual oversight for edge cases

Strategy Structure:

- A comprehensive, automated patching strategy that covers all systems and applications
- Risk-based remediation targets high-impact vulnerabilities on critical assets
- Use of virtual patching and script-based fixes for unpatchable vulnerabilities
- Structured workflows for patching, verification, and validation of fixes

Governance:

- Formalized patching and remediation policies are consistently enforced
- Continuous tracking and reporting on the status of vulnerabilities and remediation efforts
- Incident response and remediation activities are tracked with clear timelines and success metrics
- Regular remediation audits ensure effectiveness and compliance with internal standards

Team Alignment:

- Security and IT teams are closely integrated and work collaboratively on remediation tasks
- Defined roles for remediation efforts, with accountability for patching and fixing vulnerabilities
- Proactive security teams monitor threats and deploy immediate vulnerability fixes
- Teams align on priorities with strong patching communication and coordination

Example Practices:

- Use vRx's automated patch deployment for Windows, Linux, and macOS systems.
- Apply scripts or use Patchless Protection for vulnerabilities without vendor patches.
- Automate patching schedules with vRx to ensure timely remediation.
- Focus remediation efforts first on high-risk vulnerabilities based on their impact.
- Validate that vulnerabilities are fixed and no new issues arise after remediation.

Level 5: Automate

Description : The automate stage reflects the degree to which the above processes are streamlined through automation and integration. This ranges from manual workflows at low levels to fully automated vRx-driven processes (scheduled patch jobs, API-triggered actions, etc.) at the highest level

Key Characteristics:

- Full integration of security processes into the IT environment
- Continuous monitoring and automated incident response
- Reduced manual intervention for routine tasks
- Data-driven decision making with automated reporting and risk assessment
- Self-healing systems with automated remediation of common issues

Symptoms:

- vRx automates detection, analysis, and remediation with minimal manual effort
- Processes are continuously optimized based on feedback and changing threats
- Self-healing systems auto-fix vulnerabilities, preventing issues from escalating
- The organization operates with near-zero downtime and a highly resilient security posture

Strategy Structure:

- Fully automated vulnerability management: detection, prioritization, remediation, and patching
- Continuous integration enables seamless data flow and automated security responses
- AI-driven decision-making, with policies adapting to new threats based on data and analysis
- Proactive threat intelligence feeds directly inform automated workflows and security actions

Governance:

- Governance is data-driven, with real-time dashboards and reports accessible to key stakeholders
- Automated compliance monitoring enforces security policies and remediation continuously
- Metrics analyzed to improve and adapt systems to emerging threats
- Continuous audits and feedback align processes with goals and best practices

Team Alignment:

- Security focuses on oversight, refining automation, and handling exceptions
- Teams aligned via shared goals and automation, boosting efficiency
- Cross-functional collaboration integrates security into IT and business process
- Security shifts to proactive optimization, not incident-level management

Example Practices:

- Set up automated workflows in vRx to continuously detect and remediate vulnerabilities
- Use vRx's API to integrate with other tools for seamless threat detection and response
- Automatically deploy patches and updates without manual scheduling
- Implement real-time automated alerts and responses using vRx's threat intelligence features
- AI tools auto-adjust security policies through continuous threat analysis

Security Operation Stages Explained

The Vicarius vRx Maturity Model is designed to complement, not compete with globally recognized cybersecurity standards. To help security teams, auditors, and leadership teams align internal progress with external expectations, the table below maps each vRx operational stage to NIST CSF 2.0 Functions and Tiers, CIS Controls v8 Implementation Groups (IGs), and ISO/IEC 27001:2022 Annex A clauses.

This ensures that organizations can use the vRx model as a translation layer, enabling direct comparisons across different compliance and governance frameworks.

vRx Stage	Primary Purpose	NIST CSF 2.0 Function / Tier	CIS Controls v8 IGs	ISO/IEC 27001:2022 Annex A Controls
Deploy	Asset visibility and agent rollout	Identify (Tiers 1–2)	IG1 – Safeguards 1–2	A.5.7 (Inventory), A.8.1 (Responsibility)
Detect	Continuous vulnerability discovery	Detect (Tiers 1–2)	IG1 – Safeguard 7	A.8.8 (Vulnerability Management)
Analyze	Risk-based vulnerability prioritization	Govern (Tiers 2–3)	IG2 – Analytics Items	A.5.4 (Governance), A.8.2 (Classification)
Remediate	Patch, script, or virtual remediation	Respond (Tiers 2–3)	IG2–IG3 – Safeguard 7	A.12.6.1 (Patch Management)
Automate	Orchestrated, selfhealing workflows	Recover / Improve (Tiers 3–4)	IG3 – Automation Practices	A.8.16 (Monitoring & Review), A.5.31 (Automation)

This approach ensures that maturity assessments are not isolated exercises, but directly tied to recognized compliance requirements. Security leaders can use the model to track improvements by site or business unit, generate evidence for audits, and drive remediation plans based on clear control objectives.

Using vRx as the mapping and execution layer allows organizations to coordinate maturity, compliance, and operational efficiency without duplicating effort or replacing existing tools.

Remediation Gap Packs: From Gaps to Actions

vRx helps organizations close security and compliance gaps by mapping every uncovered control across CIS Controls v8, NIST CSF 2.0, and ISO/IEC 27001:2022 to an actionable fix. Each gap generates a "Gap Pack," which includes either a vRx-native remediation (patch, script, or policy) or a recommended external control (e.g., enabling MFA in your IdP).
For example:

Deploy

Control Gap	Gap Pack Action
ISO A.5.7 – Asset Inventory	Automatically deploy vRx agents, tag and scan assets on a schedule, and push coverage reports to your asset management system
CIS IG1 Safeguard 1 – Hardware Inventory	
NIST Identify Tier 1 → 2	

Detect

Control Gap	Gap Pack Action
ISO A.8.8 – Vulnerability Management	Enable continuous and scheduled scanning in vRx, route alerts, and integrate with your SIEM for unified threat visibility
CIS IG1 Safeguard 7 – Vulnerability Detection	
NIST Detect Function – Coverage Gaps	

Analyze

Control Gap	Gap Pack Action
ISO A.8.2 – Classification of Information	Use vRx risk scoring to prioritize vulnerabilities with contextual analysis and exploit
CIS IG2 – Risk Analysis	
NIST Govern Function – Threat Modeling	

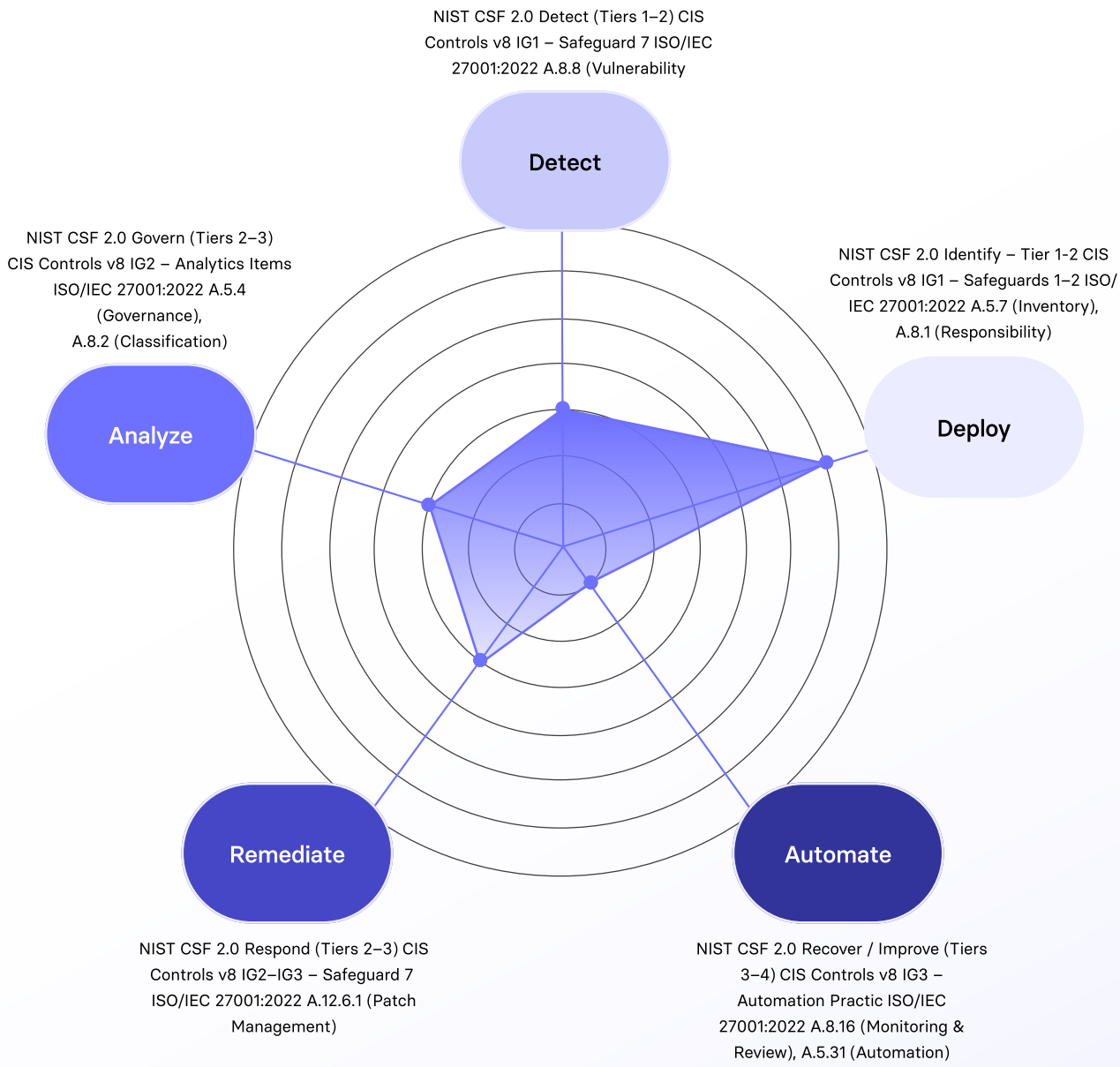
Remediate

Control Gap	Gap Pack Action
ISO A.12.6.1 – Patch Management	Automate patching in vRx based on risk level, apply remediation scripts for legacy systems, and enforce SLA-driven workflows
CIS IG2/IG3 Safeguard 7 – Patch Applications	
NIST Respond Function – Timely Fixes	

Automate

Control Gap	Gap Pack Action
ISO A.8.16 – Monitoring & Review	Leverage vRx dashboards and alerts for self-healing, integrate with RMM/ITSM for orchestration, and automate post-patch validation with rollback checks
CIS IG3 – Workflow Automation	
NIST Recover Function – Continuous Improvement	

Security Operation Stages Explained



This radar chart illustrates an organization in the Operational (Level 1) to Emerging (Level 2) stages of its vRx maturity. It shows significant gaps in the Automate and Remediate stages, indicating limited or no automation in vulnerability management processes and a reactive approach to remediation. The Deploy and Detect stages show moderate maturity, with some automation and regular scanning, but still relying on manual efforts for key actions. The Analyze stage appears slightly more developed, suggesting a growing use of risk-based prioritization but still lacking full integration and data-driven decision-making.

Importantly, this model does not operate in isolation each vRx stage maps directly to controls from NIST CSF 2.0, CIS Controls v8, and ISO/IEC 27001. This allows the organization to use vRx as a bridge between operational maturity and global security frameworks, translating platform activity into meaningful progress against widely accepted standards.

Visual Representation of the Maturity Model

Vicarius Cybersecurity Maturity Model

	Operational	Emerging	Foundational	Advanced	Optimized
Automate	• Manual scans, analysis, patching • Minimal vRx automation used • Basic external scripting • Each vulnerability handled manually end-to-end	• Some tasks scheduled in vRx • Patches auto-deployed to select systems • Basic integrations like email alerts • Semi-automated critical patching reduces workload	• Routine scans, patching, and reporting automated • Integration trigger alerts or tickets • Playbooks used for common fixes • Team focuses on analysis and strategy	• Scanning, prioritization, remediation automated • Integrates with SIEM, CI/CD tools • Custom workflows and one-click actions • Exceptions handled manually	• Self-driving security automates end-to-end • API-triggered workflows adapt to changes • Responds 24/7, including isolation • Team handles oversight and exceptions
Remediate	• Patching is ad-hoc and delayed • No regular cadence • Some use of vRx for critical fixes • Remediation is reactive	• Scheduled patching for OS and apps • High-severity issues addressed • Advanced tools rarely used • Complex cases often deferred	• Automated patching for OS and apps • Aligned with maintenance windows • Scripts used for complex cases • Exceptions tracked and reviewed	• Patching, scripting, patchless protection used fully • Reduces patch time by 80% • Handles complex cases like Log4j etc. • Patchless Protection used when no patch exists	• Near real-time remediation automated • Policies handle patches and scripts • MTTR well below industry norms • Feedback loop ensures safe deployment
Analyze	• Risk analysis is minimal • Decisions based on CVSS only • No context considered • Reporting is ad-hoc and reactive	• Basic prioritization using vRx • Asset importance considered • CVSS and spreadsheets still dominate • Contextual analysis used selectively	• Standardized risk-based analysis • Prioritization includes asset criticality • Reports highlight trends and compliance • Consistent remediation across scan cycles	• AI-driven risk scoring beyond CVSS • Factors in business impact and threat likelihood • Dashboards guide decisions • Focus on critical vulnerabilities	• Continuous, dynamic risk analysis • Real-time metrics on dashboards • Adapts using feedback • Enables proactive, data-driven decisions
Detect	• Scans run infrequently or post-incident • Vulnerabilities linger undiscovered • No zero-day monitoring • Lacks external threat intelligence integration	• Regular scans on critical systems • Known vulnerabilities detected • Detection is periodic, not continuous • Coverage not yet organization-wide	• Scheduled scans across OSs and apps • Platform feeds alerts on new vulnerabilities • Most assets covered • Real-time focus on critical systems	• Continuous monitoring across all assets • Detects zero-days with threat intel • Integrates with advance tools • Real-time alerts and correlation	• Real-time, predictive detection active • Assets report continuously • Zero-day and threat feed coverage • Filters false positives intelligently
Deploy	• vRx deployed on few systems • Many assets unmonitored • Asset inventory incomplete • Manual updates, no full visibility	• vRx covers key systems • Asset discovery is infrequent • Gaps in coverage remain • New assets added manually, not systematically	• vRx deployed on most systems • Asset inventory mostly complete • Scans detect new assets • Some onboarding steps still manual	• vRx deployed on all endpoints • Auto-enrollment for new devices • Real-time asset visibility • Continuous monitoring ensures full coverage	• Auto-enrollment via policy or script • Integrates with IT/DevOps workflows • Live asset inventory updates • Full, gap-free infrastructure coverage

The visual representation of the **Vicarius Maturity Model** showing the progression through the stages: **Deploy, Detect, Analyze, Remediate, and Automate**. This helps highlight how organizations evolve in their cybersecurity practices as they move from basic deployment to fully automated security operations.

You can use this model and the associated questionnaire to evaluate where you currently stand in you cybersecurity journey and work towards higher maturity levels with Vicarius solutions.

From Maturity to Compliance: Operationalizing Frameworks with vRx

The Vicarius vRx Maturity Model provides a structured framework for organizations to assess and improve their vulnerability and remediation management practices. The first step in evaluating your current maturity level is to complete the self-assessment questionnaire, which aligns with the stages of Deploy, Detect, Analyze, Remediate, and Automate. This will help you determine where your organization stands from Operational to Optimized and identify key areas for improvement.

What sets this model apart is its direct alignment with globally recognized cybersecurity frameworks, including NIST CSF 2.0, CIS Controls v8, and ISO/IEC 27001. vRx serves as a bridge between operational activities and formal compliance standards, allowing security and IT teams to translate daily platform usage into measurable progress against these frameworks. This mapping provides clear value not only to technical teams but also to CISOs, auditors, and boards, offering a shared language for tracking risk reduction, audit readiness, and operational maturity.

To advance through the maturity stages, organizations should focus on automating routine tasks, integrating threat intelligence, and fully utilizing Vicarius vRx's capabilities such as real-time patching, script-based remediation, and risk prioritization. Strengthening detection, analysis, and remediation processes ensures continuous improvement, reduced exposure, and a more resilient security posture.

Start by using the questionnaire to assess your current state, map your results to compliance frameworks, and take actionable steps toward a unified, standards-aligned approach to vulnerability management with Vicarius vRx.

Assess your maturity level

Identify gaps

Improve your maturity

Quick Self-Assessment Questionnaire

1. Deploy : How automated and systematic is your asset deployment process?

1. Manual installation of agents, minimal coverage.
2. Some automation, but many manual steps involved.
3. Deployment is mostly automated with some manual intervention.
4. Full automation, integrated with other IT processes.
5. Automated deployment with continuous visibility and immediate coverage of new assets.

2. Detect : How effective is your vulnerability detection process?

1. Reactive, only occasional scans or alerts for critical issues.
2. Regular vulnerability scans with limited coverage, manual log analysis.
3. Continuous scanning, with some automation for real-time alerts.
4. Real-time scanning and detection, leveraging advanced threat intelligence.
5. Fully automated, real-time detection with AI-driven insights and integrations.

3. Analyze : How do you analyze and prioritize vulnerabilities?

1. Manual analysis based on CVSS scores, no standardization.
2. Some use of risk-based prioritization, with limited integration of context.
3. Formalized processes with contextual risk assessments.
4. Advanced risk scoring and integration of business impact analysis.
5. Data-driven, continuous analysis with automated prioritization and feedback loops.

4. Remediate : How do you manage vulnerability remediation?

1. Ad-hoc remediation, manual patching with delays.
2. Scheduled patching, some script-based fixes.
3. Automated patching with regular validation and scripts for complex issues.
4. Fully automated remediation with risk-based prioritization.
5. Self-healing systems with automated remediation of all identified vulnerabilities.

5. Automate : How automated are your security operations?

1. Manual processes for most tasks, little to no automation.
2. Some automation, mostly for routine tasks.
3. Increased automation, with integrated systems for key tasks.
4. Automated workflows with AI-driven decisions and real-time responses.
5. Fully orchestrated, self-adjusting systems with continuous optimization and minimal manual intervention.

How to Score:

Total Score: Add up the scores for each of the five questions (Deploy, Detect, Analyze, Remediate, Automate).

Maturity Level:

5-7: Operational (Level 1)
8-12: Emerging (Level 2)
13-17: Foundational (Level 3)
18-22: Advanced (Level 4)
23-25: Optimized (Level 5)

The higher the score, the more mature and automated the organization's security operations are.