

Netradyne IT Patching Procedure

## V3.0

Internal and Confidential

#### Table of Contents

[Netradyne IT Patching Procedure 0](#_bookmark0)

[Document Control 2](#_bookmark1)

1. [PURPOSE 3](#_bookmark2)
2. [SCOPE 3](#_bookmark3)
3. [ROLES AND RESPONSIBILITIES 3](#_bookmark4)
4. [PROCEDURE 3](#_bookmark5)
   1. [COMMUNICATION/NOTIFICATION 4](#_bookmark6)
   2. [VULNERABILITY ASSESSMENT 4](#_bookmark7)
   3. [PATCH EVALUATION AND PRIORITIZATION 4](#_bookmark8)
   4. [PATCH TESTING 5](#_bookmark9)
   5. [PATCH DEPLOYMENT 5](#_bookmark10)
   6. [PATCH DEPLOYMENT – ROLES & RESPONSIBILITIES 5](#_bookmark11)
   7. [PLAN OF ACTION FOR PRODUCTION PATCH DEPLOYMENT 6](#_bookmark12)
   8. [PATCH DEPLOYMENT STEPS. 6](#_bookmark13)
      1. [STEPS WITH THE SCREENSHOT OF PATCH DEPLOYMENT: 7](#_bookmark14)
      2. [PATCH DOCUMENTATION 11](#_bookmark15)
   9. [COMPLIANCE AND AUDITING 12](#_bookmark16)
   10. [TRAINING AND COMMUNICATION 12](#_bookmark17)
5. [CONDUCT 12](#_bookmark18)
6. [EXCEPTION 12](#_bookmark19)
7. [TERMS/ACRONYMS 12](#_bookmark20)
8. [POLICIES 12](#_bookmark21)
9. [PROCESS/PROCEDURES 13](#_bookmark22)
10. [APPENDIX A: DOCUMENT RACI MATRIX 13](#_bookmark23)

Document Control

|  |  |
| --- | --- |
| **Document ID** | NDITPVM2024001 |
| **Document Name** | Netradyne IT Patching Procedure |
| **Document Status** | Released |
| **Document Released Date** | 30-APR-2024 |
| **Document Author** | Ramesh Babu |
| **Document Content Contributors** | Priyesh Parashar, Sudhansu Kumar, Chethan Gangaraju |
| **Document Signatory** | Saravanan Sankaran |
| **Document Owner** | Chethan Gangaraju |
| **Document Version** | V3.0 |
| **Information Classification** | Internal |

### Document Edit History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Additions/Modifications** | **Prepared/Revised By** |
| v1.0 | 30-APR-2024 | Initial Release | Ramesh Babu |
| V2.0 | 26-JUN-2024 | Major Changes | Chethan G, Ramesh Babu & Priyesh Parashar |
| V3.0 | 20-JUN-2025 | Tool replacement | Ramesh Babu |

### Document Review/Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Signatory Name** | **Organization/Signatory Title** | **Comments** |
| 30-APR-2024 | Saravanan Sankaran | Senior Director, IT & InfoSec | Approved |
| 28-JUN-2024 | Saravanan Sankaran | Senior Director, IT & InfoSec | Approved |
| 27-JUN-2025 | Saravanan Sankaran | VP, IT & Infosec | Approved |

### Distribution of Final Document

|  |  |
| --- | --- |
| **Name** | **Organization/Title** |
| Internal | Netradyne |
|  |  |
|  |  |

# Purpose

IT patching is the process of installing software updates to fix security vulnerabilities, bugs, and improve performance. Patches are typically released by software vendors after they have been discovered. It is an important part of any IT security strategy. By regularly patching systems, organizations can help to protect themselves from security vulnerabilities and improve the overall stability and performance of their systems.

# Scope

The scope of IT patching refers to Netradyne IT owned assets specifically assigned to end users which comprises of Windows OS, Mac OS and Ubuntu OS. Patching activity includes all systems, software, and 3rd party applications that are used in the organization. The scope of patching can vary depending on the organization's specific needs and requirements. It is important to note that the scope of IT patching can change over time. As new vulnerabilities are discovered and new software is released, the organization may need to update its patching scope.

Handheld devices (e.g. iPad, Tablets, Mobiles etc.) and virtual machines (VMs) are out of scope for patching activities. These devices are not considered Netradyne IT-owned assets specifically assigned to end users and are not included in the patching scope.

# Roles and Responsibilities

Roles and responsibilities specific to this document are included below:

#### Role Responsibilities

|  |  |
| --- | --- |
| *Owner* | * Team or SME responsible for the process area needs to ensure this document is up to date and compliant with governing requirements. * Is the point of contact for the document. * Responsible for initiating and managing document review and the approval process from start to finish including gathering or delegating the collection of content including diagrams, formatting etc. as well as identifying stakeholders to participate   in the peer review process. |
| *Reviewers/Stakeholders Approvers*  *Document Release* | Representations from teams that can affect or be affected by the document under review (e.g., Operation, Security, Compliance, Quality) |
| The Person(s) of authority to validate the document and sign-off on the latest version. Such Person include Document owner, Functional Team Lead, Security Lead, Product Delivery Lead. |
| Document Owner/team to work with repository administrator to make  release version available. |

# Procedure

All kinds of Operating systems (Windows, MacOS, and Ubuntu) and applications in use at NETRADYNE and ensuring they are fully patched and secured in a controlled manner is a priority. This includes all aspects of infrastructure, applications, and any other hardware and software.

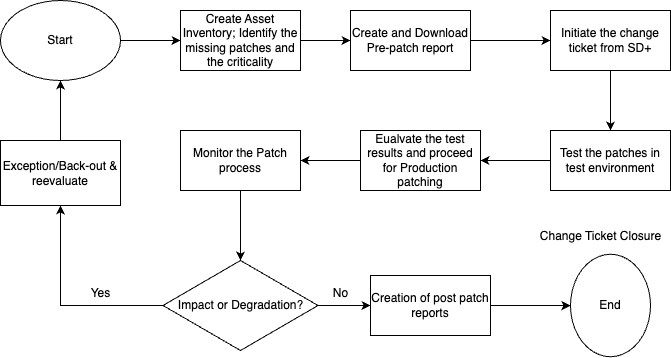
To adhere to standard software versioning practices, our goal is to maintain the software version at either level 'n' or 'n-1'.

NETRADYNE implements a packaging and configuration management system to guarantee that all systems receive up-to-date security and functional software patches and fixes. Moreover, they ensure that patches

are applied in a controlled and seamless manner using an array of tools. All patches, whether they are classified as Critical, Medium, or Low severity, are thoroughly evaluated and applied within a maximum of 30 business days.

All patches must deploy in adherence to NETRADYNE’s Change Management Policy. This includes initiate a change ticket for every month planned activity (e.g., Microsoft released OS patches comes every month on 2nd Tuesday), download & test patches before deployment to production in controlled environment.

The flow below depicts high-level patch management process followed in Netradyne for respective System Owner/Administrator:



# Communication/Notification

Before pushing patches to end users, IT team will ensure that there will be a communication sent to the users informing about the planned patching activity. All the patched that are approved by infosec team are tested and deployed to UAT users group in a controlled manner to minimize the risk of causing any issues or disruptions to the organization's systems.

Communication Template

# Vulnerability Assessment

The IT department will regularly conduct vulnerability assessments to identify systems, applications, and infrastructure that require patching. The assessment will be considered from trusted sources, such as software vendors (adobe, Microsoft, Google chrome, Cisco etc.., security bulletins from Microsoft, crowd strike, etc, and vulnerability databases such as end point central and CrowdStrike.

# Patch Evaluation and Prioritization

The IT department will evaluate patches based on severity, criticality, and potential impact on systems and infrastructure. Patches will be prioritized according to the level of risk and the potential impact on business operations.

However, the OEM level severity (for critical and high) need to be reassessed from Netradyne environment perspective.

# Patch Testing

Before deploying patches to production systems, the IT department will perform thorough testing in a UAT environment. Testing will verify patch compatibility, functionality, and potential side effects.

Test results will be documented and evaluated for potential issues or conflicts.

The UAT Patch user list is selected across various departments across Netradyne. This user list will have users using all operating system flavours. (Windows, Mac & Ubuntu).

Each month, we select different UAT users based on applicable patches for end-user machines and communicate accordingly.

# Patch Deployment

Once patches have been evaluated and tested in UAT environment, the IT department will coordinate with system owners, vendors, and stakeholders to schedule patch deployment. Deployment will be scheduled during maintenance windows to minimize disruption to business operations. Proper change management procedures will be followed, including communication with users and stakeholders regarding potential downtime or system availability.

# Patch Deployment – Roles & Responsibilities

This section maps the Roles and Responsibilities to the various steps in the workflow.

* Responsible: Those who do the work to achieve a task. There is typically one role with a participation type of Responsible.
* Accountable: Those who are ultimately accountable for the correct and thorough completion of the deliverable or task, and the one to whom Responsible is accountable. Typically, the process owner is Accountable for a process, and there must be only one Accountable specified for each task or deliverable.
* Consulted: Those who are not directly involved in the process but provide inputs and whose opinions are sought.
* Informed: Those who receive outputs from the process or are kept up to date on the progress, often only on completion of the task or deliverable

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activity** | **IT Department** | **InfoSec Department** | **Change Manager** | **Internal Stakeholders** |
| Patching Notification | R,A | R | C,I | I |
| Pre-Patch Report | R | R,A | C |  |
| Change Creation | R,A | C,I | C,I | - |
| Change Review | C,I | R,A | R | C |
| Change Approval | I | C | R,A | - |
| Change Implementation | R,A | I | C | - |
| Change Closure Post-Patch Report | R R | C R,C | A C | -  - |

\*Note – UAT users are expected to report any issue which they observe on immediate basis.

# Plan of Action for Production Patch Deployment

### Monthly Deployment Schedule:

* + Implement a standard patch deployment window during the first week of every month (Tuesday – Friday).
  + Send detailed communication emails to all users 1 week before deployment, including any changes in the schedule.

### Regional Deployment Policies:

* + A unified patch deployment policy is configured for both India and US regions.
  + The patching schedule is set to run from **12:00 AM to 11:59 PM local system time**, ensuring that all systems—regardless of region—are covered based on their respective time zones and are patched when they are online.

### Patch Reboot Enforcement Policy:

* + Once the patch installation is completed, users are encouraged to **manually reboot their systems** at their convenience.
  + If the system is not rebooted by the user, an **automatic reboot will be enforced at 7:00 PM (system local time)** on the **patch schedule end date**.

# Patch Deployment Steps.

The patch deployment process/steps are carried out using our patch management tool which is **SanerNow Secpod Tool**. It is carried out in a simple two-stage process:

* **Patch Assessment or Scanning**: This is the first stage of the patch deployment process. In this stage, SanerNow Secpod scans the network for missing patches. The scan results will show you a list of all the systems that need to be patched, along with the severity of the vulnerability.
* **Patch Download and Deployment:** This is the second stage of the patch deployment process. In this stage, SanerNow Secpod downloads the missing patches from the vendor's website and deploys them to the systems that need to be patched.

The patch deployment process in SecPod SanerNow is available both manual / Automation process. SanerNow (SecPod) automatically scans the network for missing patches on a scheduled basis. However, manual scans can also be initiated as needed to ensure the latest patch data is available before deployment. Patches identified as missing can be deployed to the respective systems.

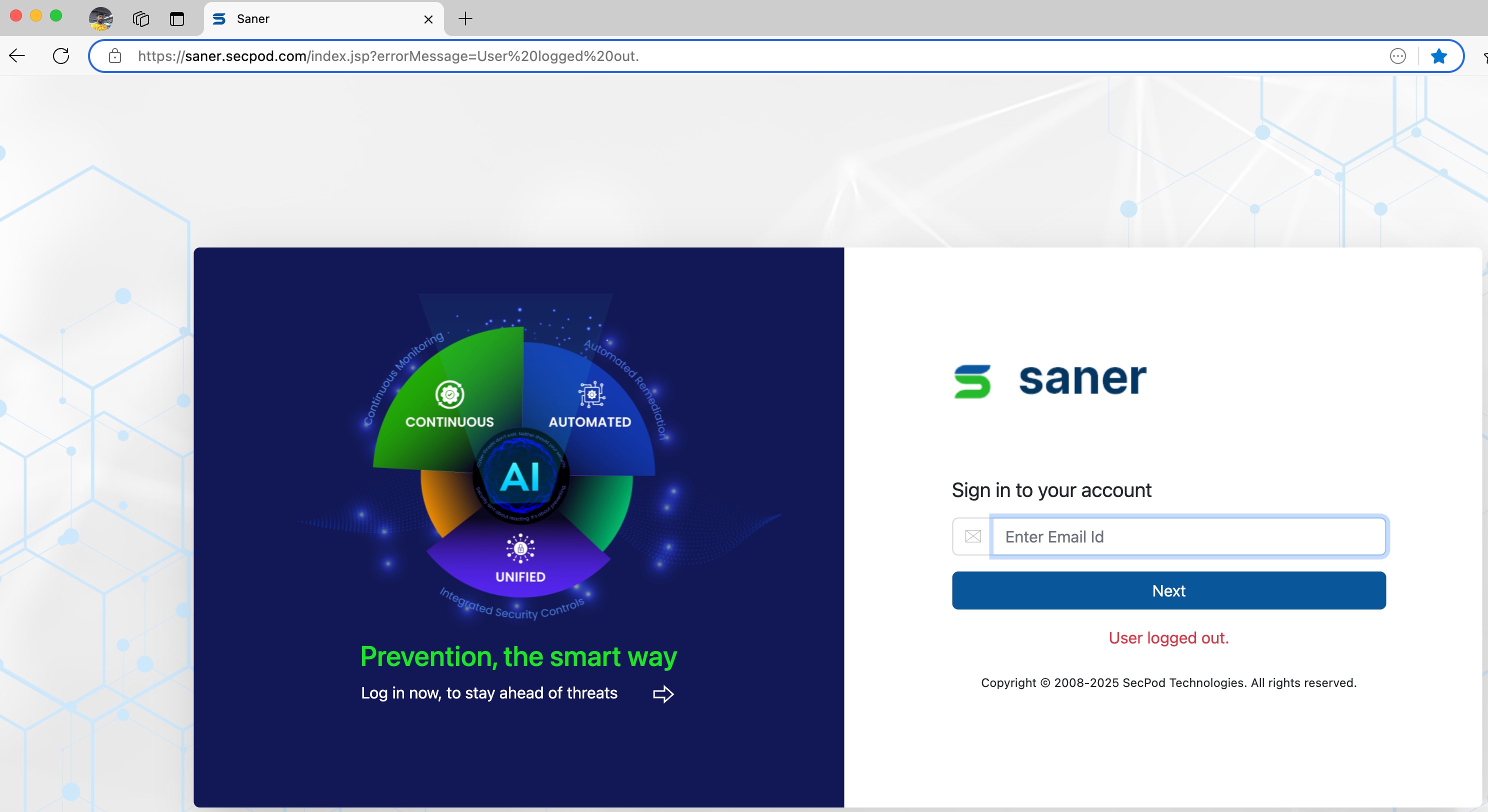
Here are the steps on how to deploy patches in SanerNow Secpod:

* Log in to the SanerNow Secpod web console.
* Click on the menu icon and select the PM Patch management.
* Click on the Missing patches.
* Select the missing patches from the list and click on Apply Selected patches.
* Next is creating the patching task by using the task controls available in the Secpod.
* Select the Task name and provide the name for patching activity.
* Next, select the Remediation Schedule, choose a custom date, and specify the Task Execution Date along with the Task Start Window timing.
* Click on Reboot Control, select the scheduled date and time, and provide the reboot date, time, and reboot message.
* Click on Remediation End Time and enter the required details accordingly.
* Click on Patching Notification and enter the Notification Start Message, Notification End Message, and Job Summary Notification details as per the on-screen instructions.
* Next, click on Remediation Script. If any scripts are available for the patch update, attach them accordingly.
* If using the Test and Deploy method, select the option, enter the required details as per the on-screen instructions, and click Next.
* Click on Apply Selected Patches.
* Once you have applied patches, by selecting the status module you can view the patching Job.

# Steps with the screenshot of patch deployment:

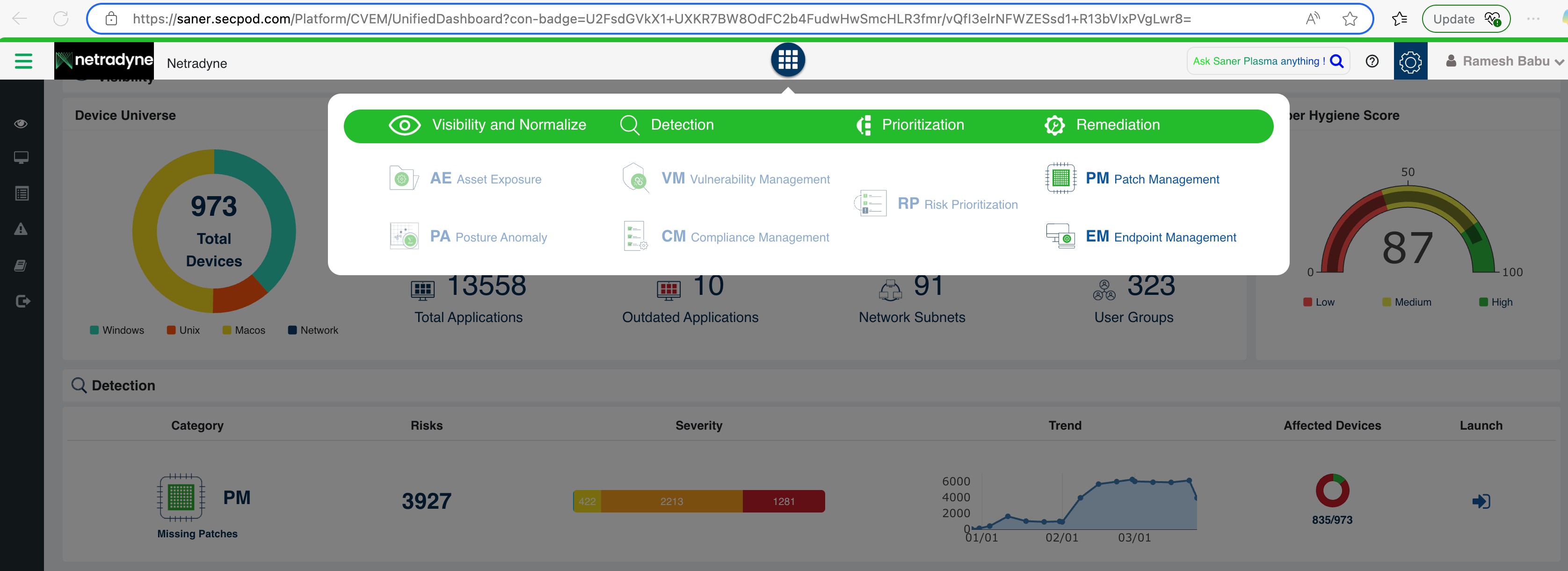
### Step 1- Log in to the SanerNow Secpod web console.

* + - * Provide the username and password to login.



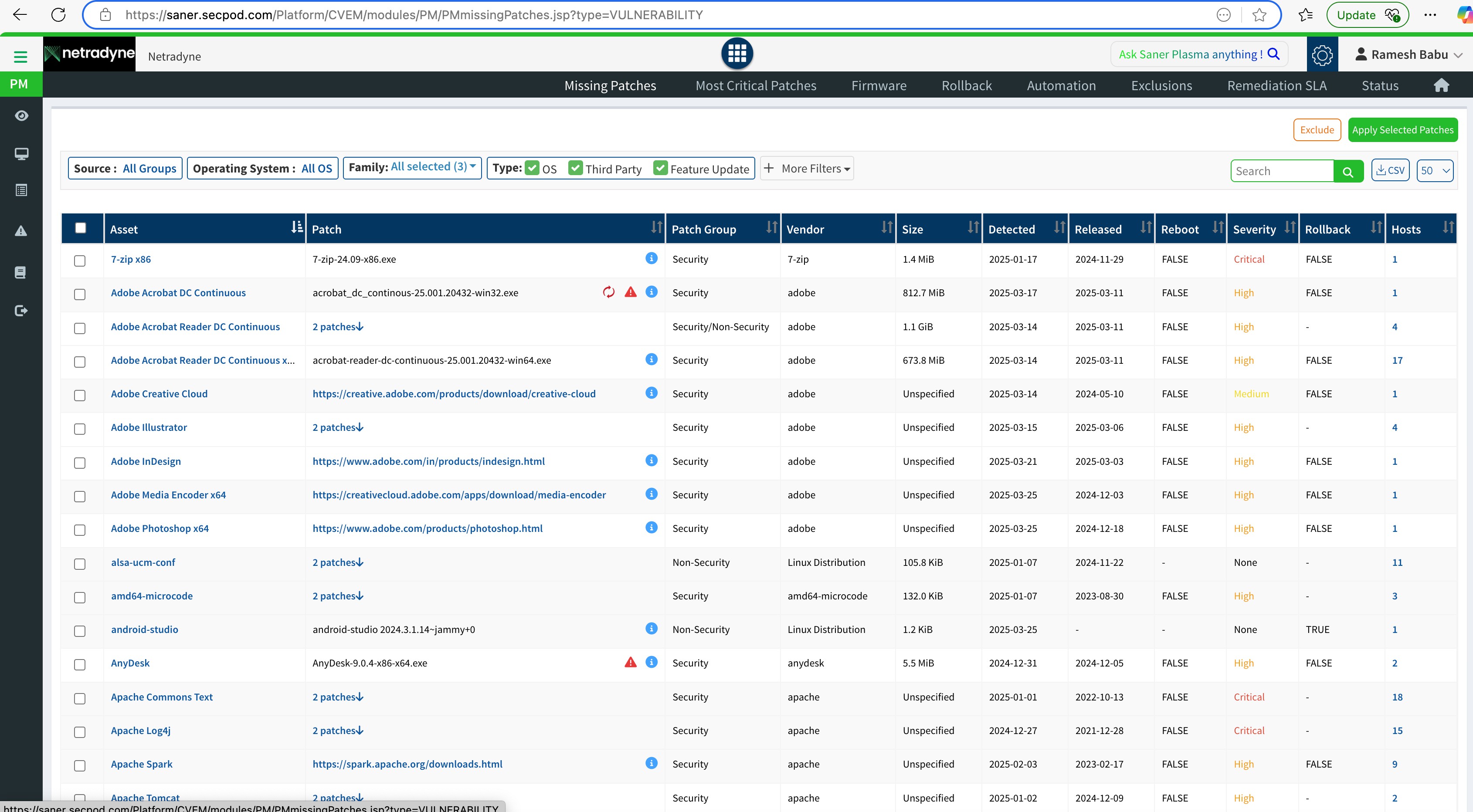
### Step 2 - Click on the menu icon.

* + - * Click on the menu icon and select the PM Patch management.



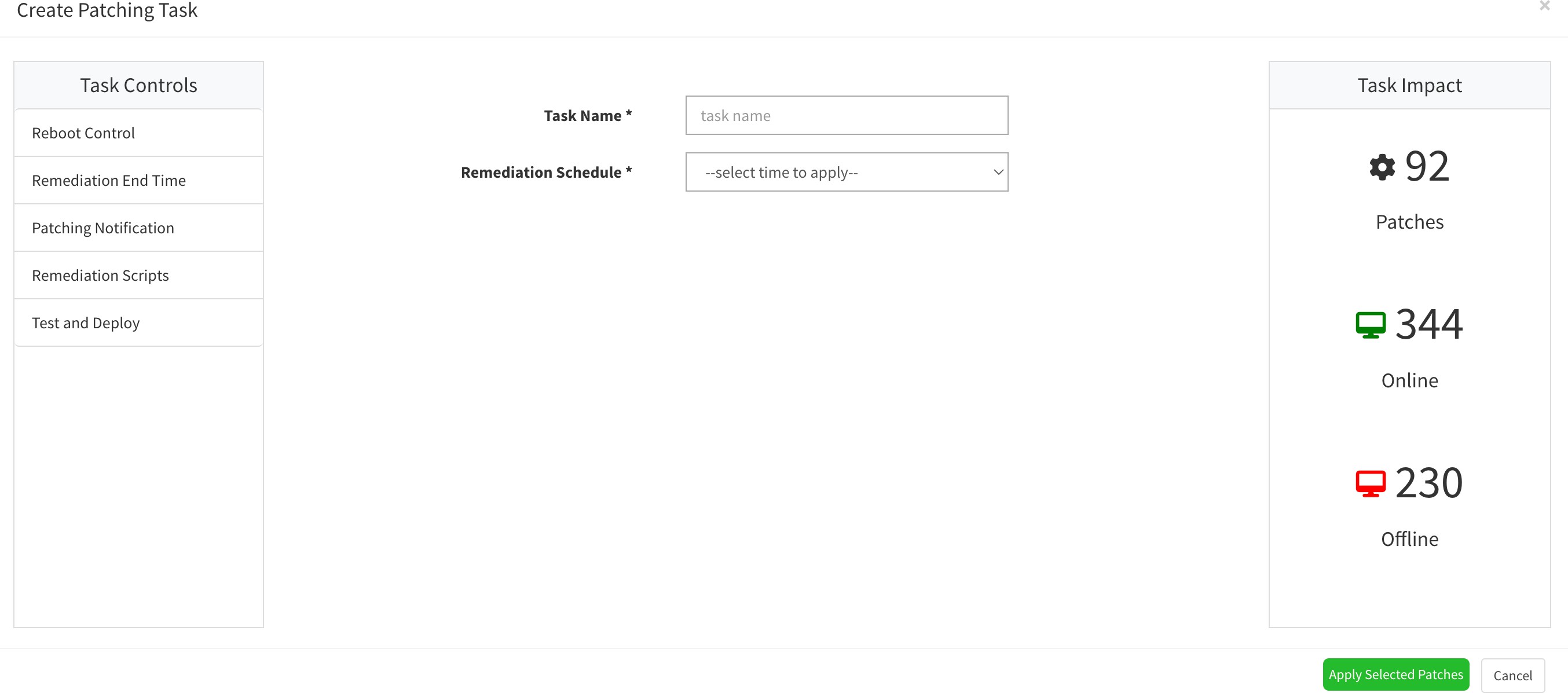
### Step 3- Click on the Missing patches.

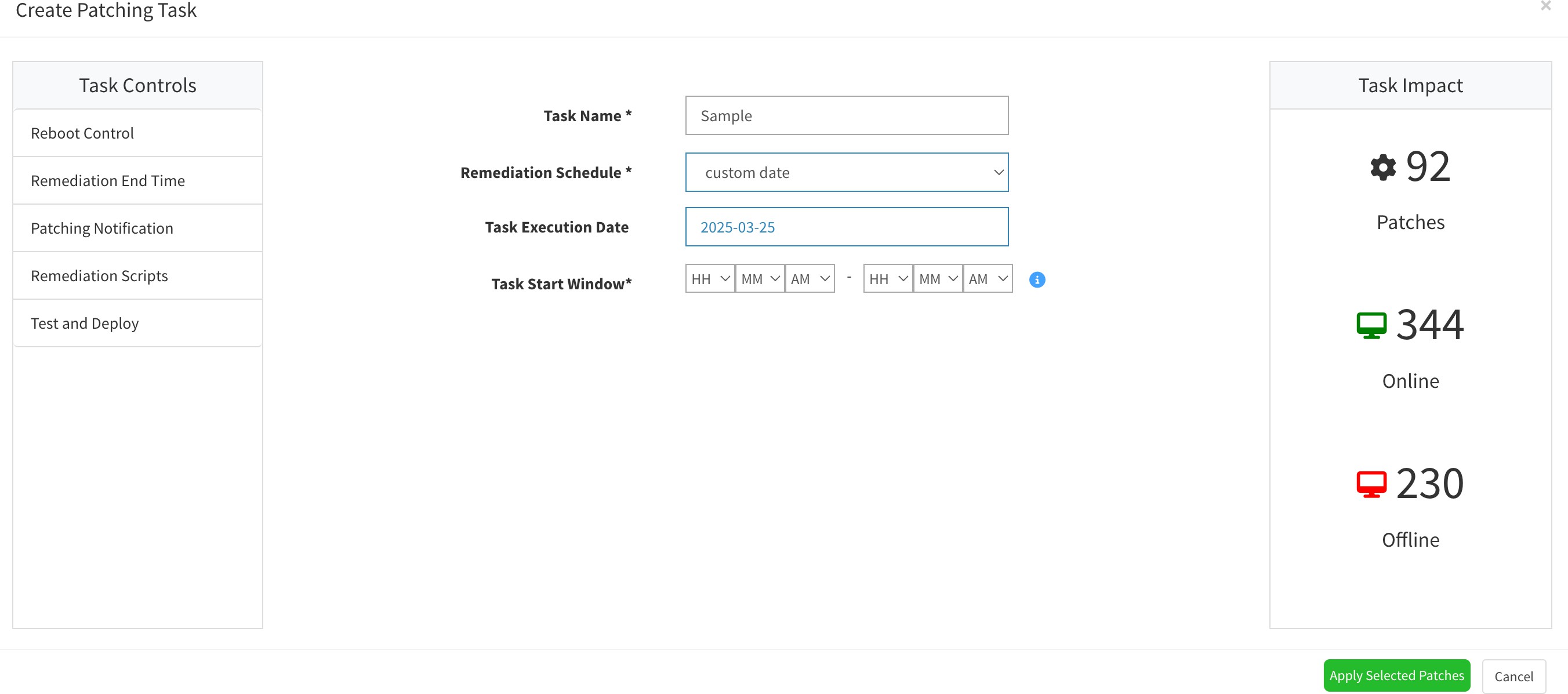
* Selected the patches and click on Apply Selected Patches.



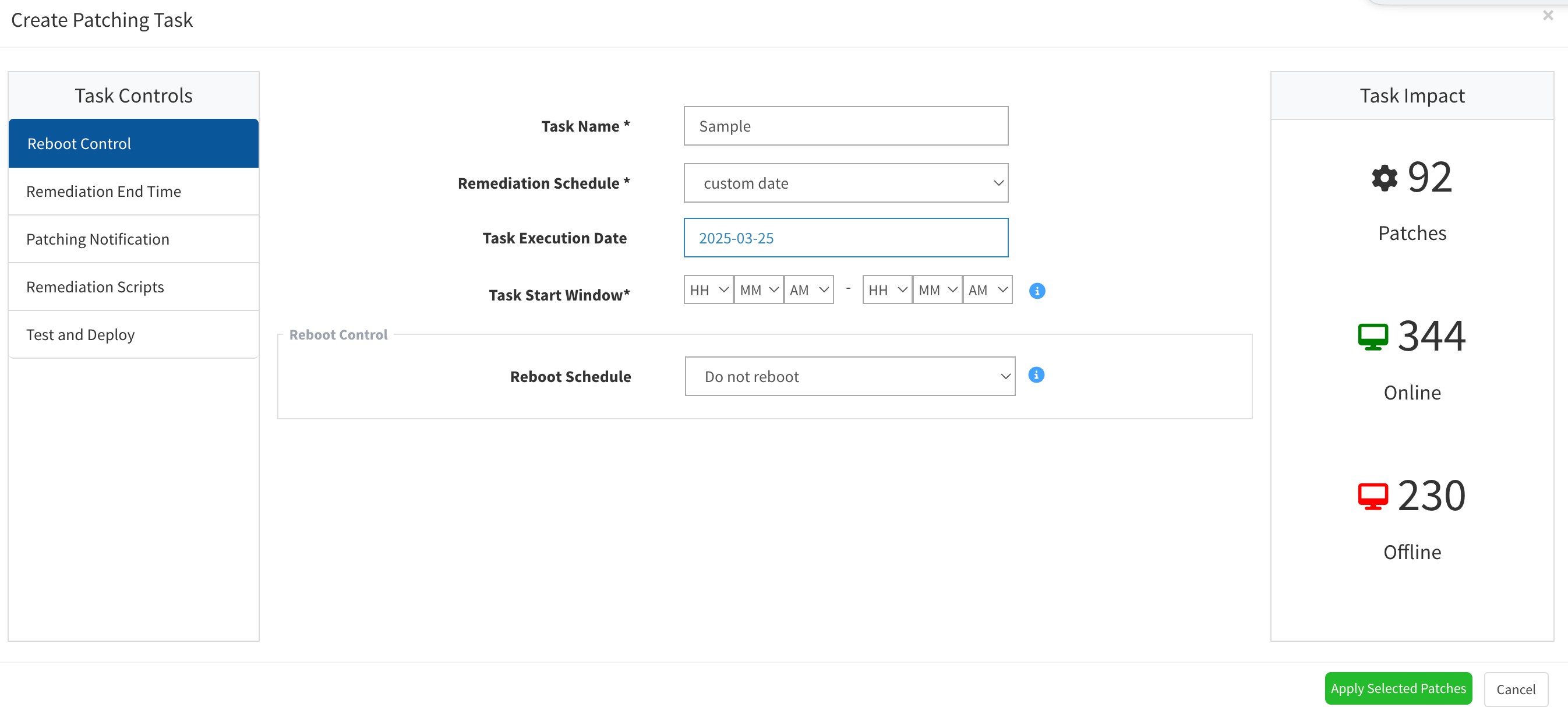
### Step 4- Next is creating the patching task by using the task controls available in the Secpod.

* The below is the reference page or home page for creating patching task.
* Select the Task name and provide the name for patching activity.
* Next, select the Remediation Schedule, choose a custom date, and specify the Task Execution Date along with the Task Start Window timing.
* ​

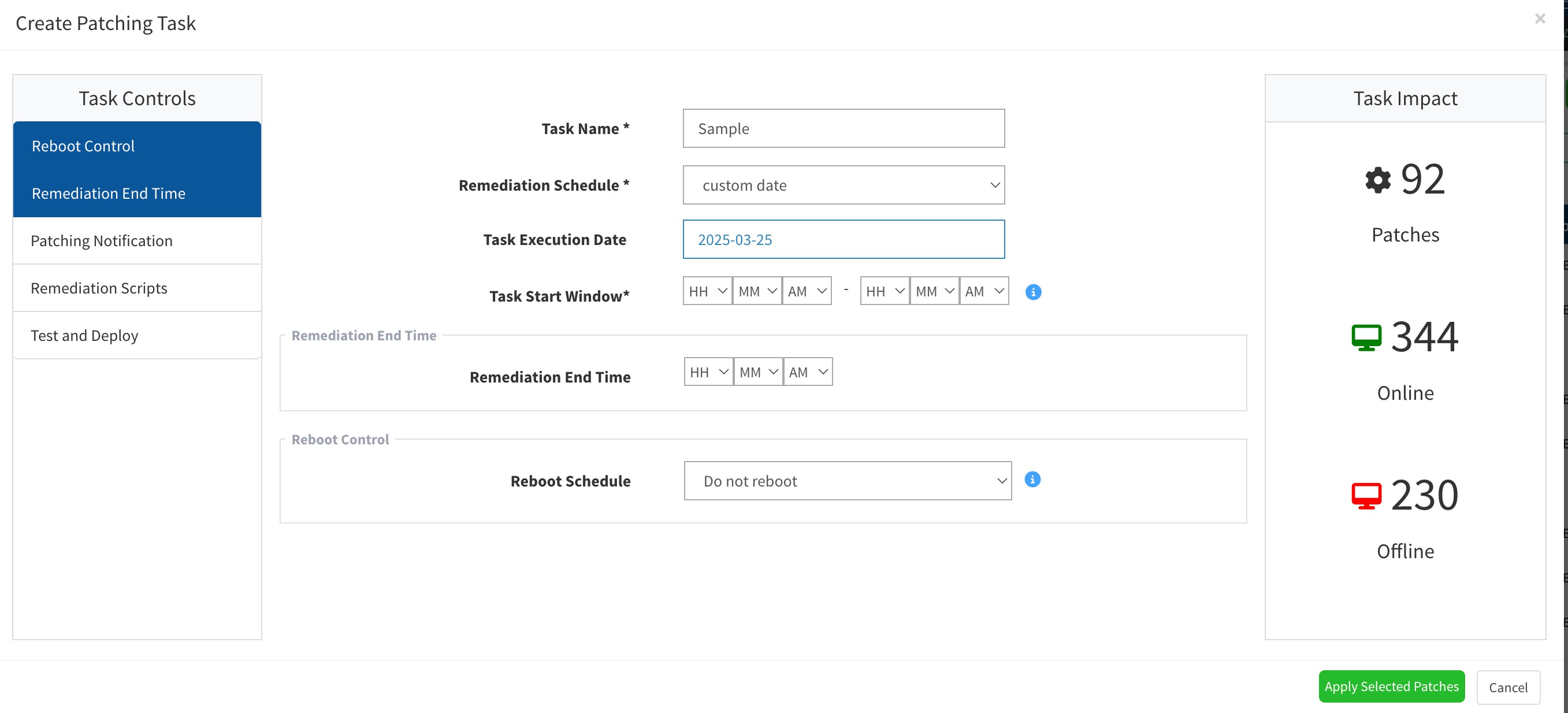




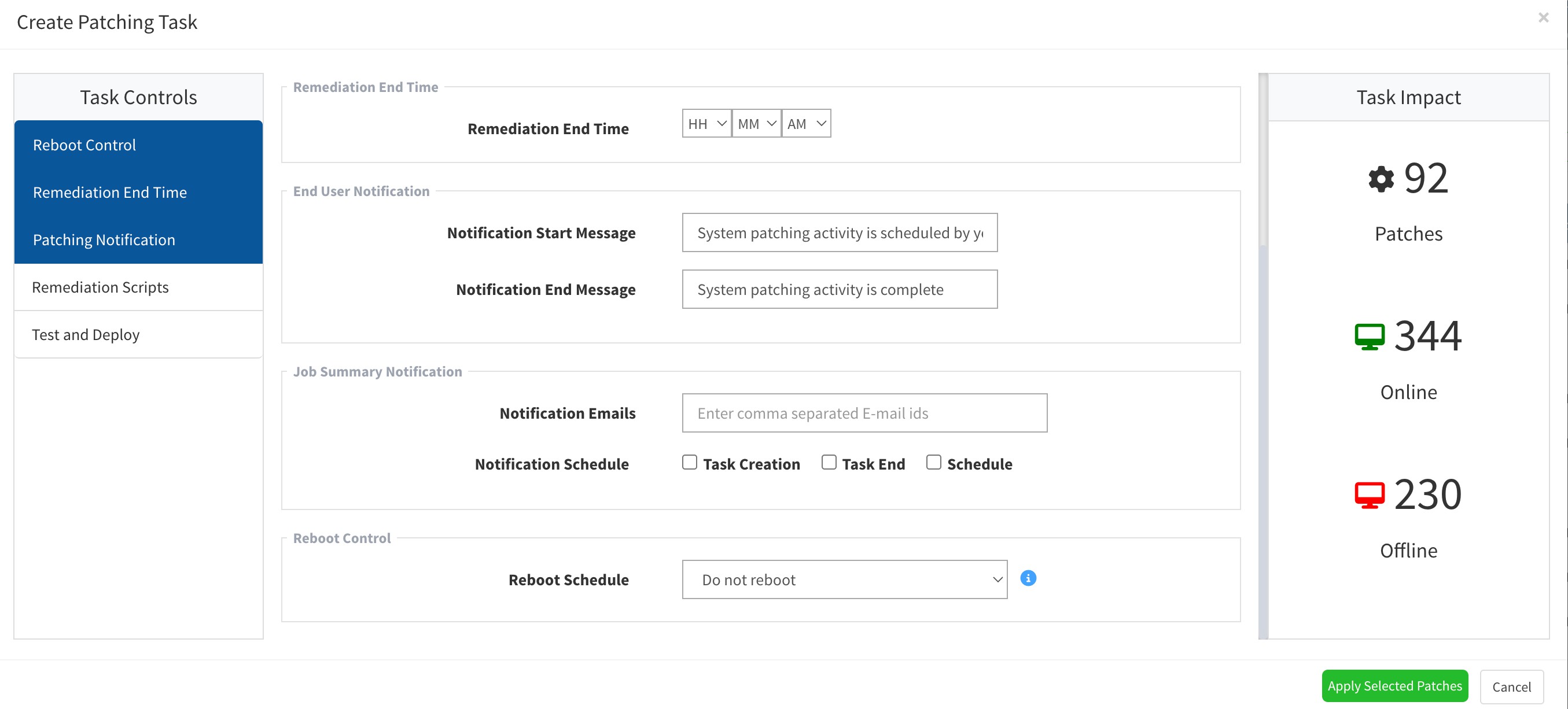
* + Click on Reboot Control, select the scheduled date and time, and provide the reboot date, time, and reboot message.



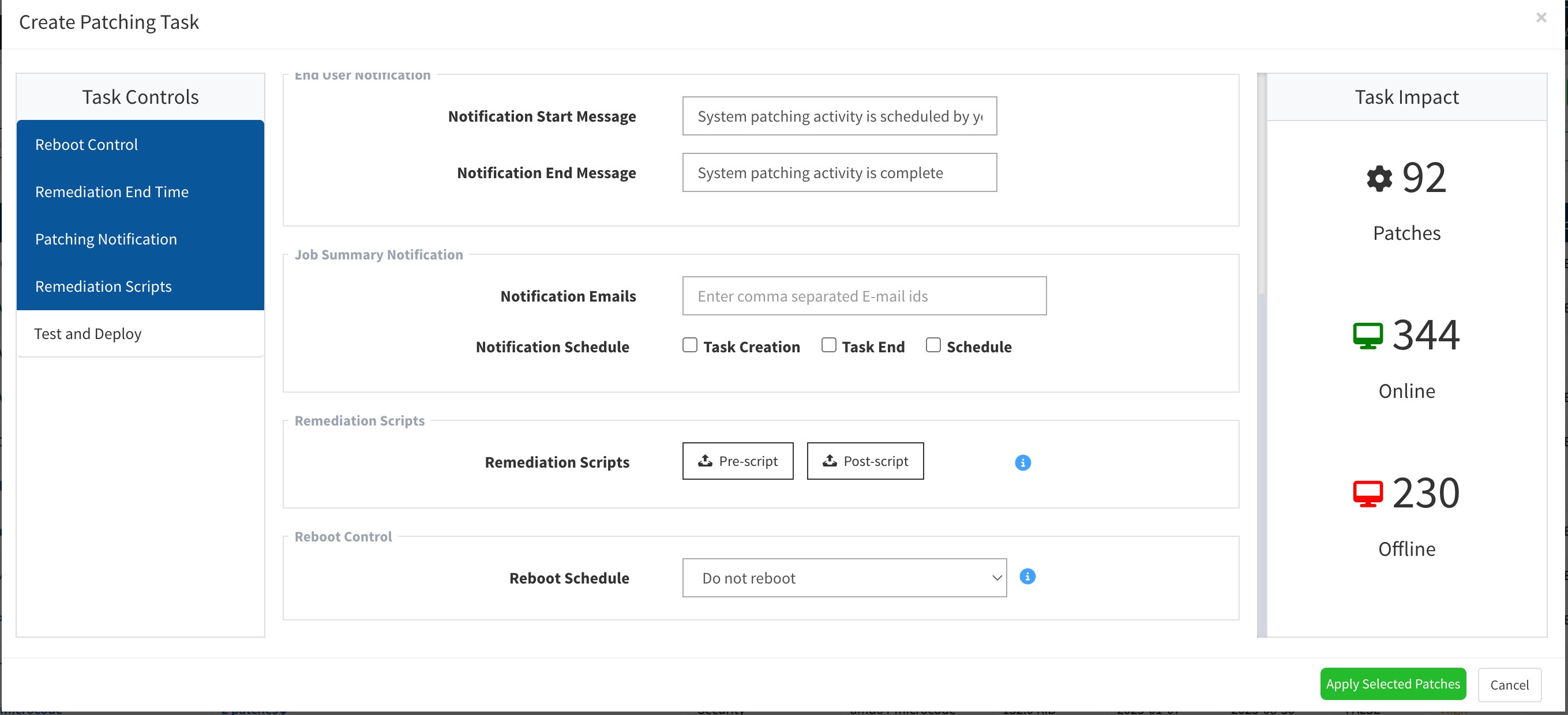
* + Click on Remediation End Time and enter the required details accordingly.



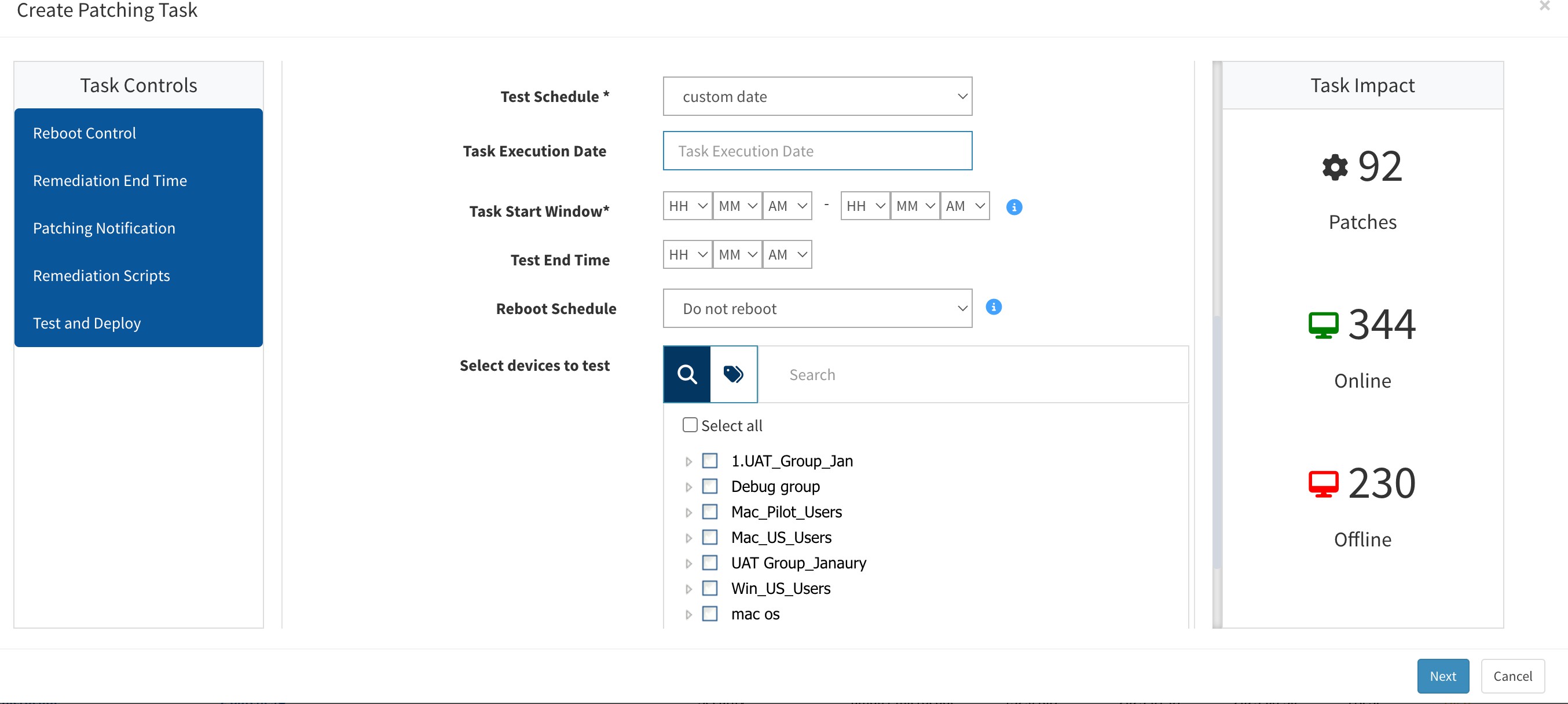
* + Click on Patching Notification and enter the Notification Start Message, Notification End Message, and Job Summary Notification details as per the on-screen instructions.



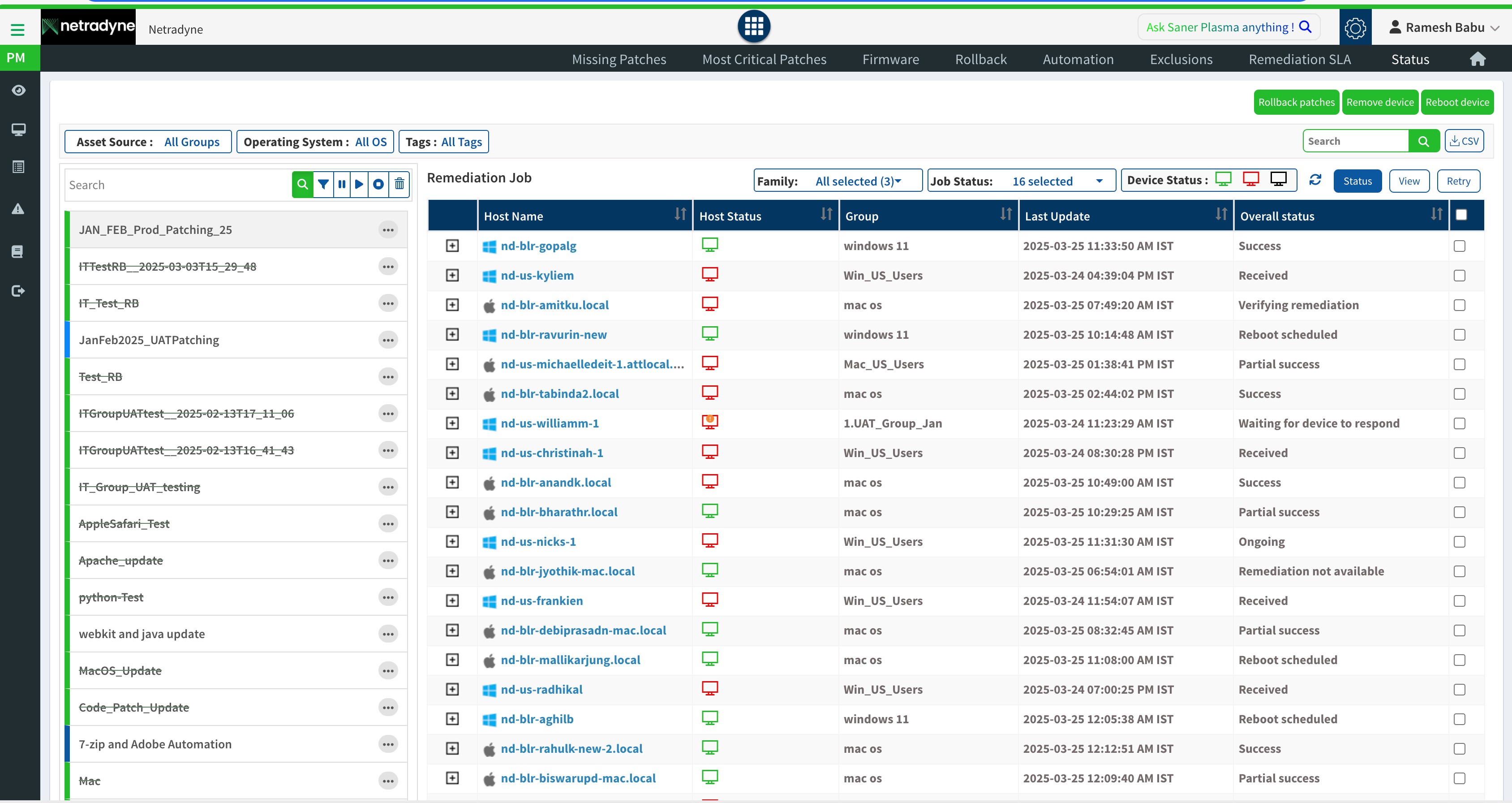
* + Next, click on Remediation Script. If any scripts are available for the patch update, attach them accordingly.



* + If using the Test and Deploy method, select the option, enter the required details as per the on-screen instructions, and click Next.



* + Click on Apply Selected Patches.
  + Once you have applied patches, by selecting the status module you can view the patching Job and monitor the status as shown in the below.



* Note: The above configuration is as per present deployment, any changes please connect with document owner.

### Execution Summary Description:

* + **Success** – the remediation task installed successfully.
  + **Received** – the device has received the patch task and yet to install.
  + **Verifying remediation-** Patching in progress.
  + **Reboot scheduled** – Installed patch reboot is required.
  + **Waiting for device to respond-** System is not connected to the network during the patch interval
  + **Partial success**- Patching remediation is not completed (example: OS update its downloaded but not installed due to restart is required)
  + **Ongoing**- Patching activity is ongoing.
  + **Fail**- Remediation failed.

# Patch Documentation

The IT department will maintain comprehensive documentation of all patching activities.

Documentation will include patch details (vendor, version, release notes), deployment dates, system owners, and any associated issues or considerations.

### Pre-Patching report:

Pre-patching involves the proactive assessment of software vulnerabilities and the identification of available patches before deployment. It includes compiling a report detailing current endpoint status, existing vulnerabilities, and recommended patching strategies. This pre-emptive approach ensures timely mitigation of security risks and enhances system reliability

### Post-Patching report:

A post-patching report summarizes the outcomes and effectiveness of the patching process after updates have been applied to endpoints. It typically includes details such as the status of patch deployment, any issues encountered during the process, and an assessment of whether the patches successfully addressed identified vulnerabilities. Additionally, the report may provide recommendations for future patch management strategies based on lessons learned from the current cycle. Overall, the post-patching report helps evaluate the efficacy of patching efforts and informs decision-making for ongoing security maintenance.

# Compliance and Auditing

The IT department will ensure compliance with relevant policies, regulations, and industry best practices regarding patch management.

There is a PVM governance call scheduled every month with Infosec team, and we review the previous months patching activity.

# Training and Communication

The IT department will provide appropriate training and guidance to system owners, stakeholders, and IT personnel on patch management processes, roles, and responsibilities.

Regular communication will be maintained with stakeholders regarding patching schedules, known issues, and system availability.

# Conduct

Compliance Checks to this process to be performed through various methods, including but not limited to reports, internal/external audits, Awareness training/assessments and feedback to the process owner. Non- compliance will be escalated to the Netradyne leadership team.

# Exception

Exception to this procedure must be approved through the Netradyne Exception Process

# Terms/Acronyms

#### Term/Acronym Definition

|  |  |
| --- | --- |
| *IT UAT*  *Infosec PVM*  *Asset* | Information Technology |
| User Acceptance Testing |
| Information Security |
| Patch Vulnerability Management  Asset means application in secpod terminology. |

# Policies

*Netradyne Information Security Policy & Procedure.pdf Netradyne Information Security Exception Process.pdf Acceptable Usage Policy.pdf*

# Process/Procedures

*NETRADYNE DISASTER RECOVERY PROCESS.pdf NETRADYNE BUSINESS CONTINUITY PLAN.pdf*

*Netradyne Vulnerability & Patch Management Process.pdf NetradyneSecurityIncidentResponsePlan.pdf*

# Appendix A: Document RACI Matrix

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Role/Activity** | **Document Owner/Functional**  **Area Lead** | **Document Contributor** | **ND**  **Leadership** | **Functional Area Team** | **InfoSec** | **All ND Member(s)** |
| **Ensure document is kept current** | A | R | I, C | R, C | C | I |
| **Ensure stakeholders are kept informed** | A | R | - | R | C | - |
| **Ensure document contains all relevant**  **information** | A | R | I, C | R, C | C | I |
| **Ensure document adheres to document governance**  **policy** | A, R | R | I | R, C | R, C | I |
| **Provide SME advice** | I, R | A, R | I | R, C | I, C | I |
| **Gathering and adding document**  **contents** | I | A, R | I, C | R, C | C | I |
| **Document Approval** | A | R | I, R | I | I, R | I |

*Key*

|  |  |
| --- | --- |
| *R* | Responsible |
| *A*  *C I* | Accountable |
| Consulted |
| Informed |