RAPID7

Guide to tracking ASD Essential Eight within InsightVM

TABLE OF CONTENTS

Executive summary

To help organisations mitigate cybersecurity incidents, the Australian Signals Directorate (ASD) published a cybersecurity baseline, “The Strategies to Mitigate Cyber Security Incidents.” This is a list of prioritised initiatives to strengthen computer security. Of these, the Essential Eight are the most fundamental elements of that list, providing a baseline cybersecurity posture.

Since the release of the ASD Essential Eight, many organisations have asked Rapid7 how they can report their position against the framework and measure the effectiveness of their program, specifically against vulnerability management guidelines such as: “Internet-facing services with exploitable vulnerabilities should be patched within 48 hours.”

This document outlines how the out-of-the-box capabilities within InsightVM can be leveraged to provide organisations with visibility into their current position, as well as measure the effectiveness of their program against the Essential Eight guidelines.

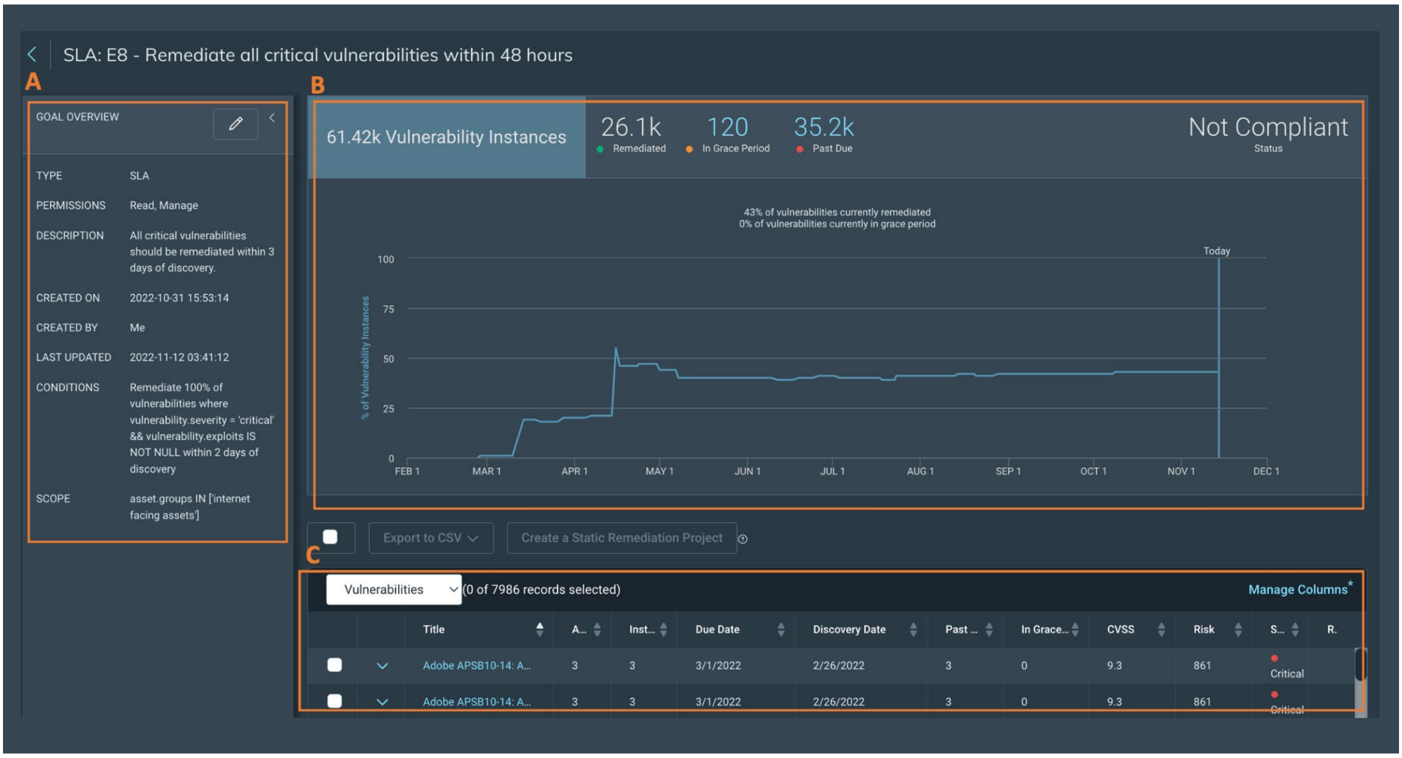
Goals and SLAs

To provide further insight into the performance of an organisation's overall vulnerability management programme of work in alignment to the Essential Eight, InsightVM enables the creation of metric-based Goals and SLAs.

There are three types of goals that can be configured within InsightVM:

- Time-Bound Goals: A time-bound goal is a one-time goal with a set deadline; e.g., to migrate all outdated operating systems to a supported operating system by a specific date.
- Continuous Goals: A continuous goal lets you monitor progress or criteria without a time limit, such as a rule or a key performance indicator; e.g., if you need to keep port 22 closed on all assets, you can create a continuous goal to monitor if any assets have an open port 22.
- Service Level Agreements: An SLA lets you track remediation over a dynamic time span; e.g., remediation of a vulnerability within a specified number of days of discovery.

To measure and track the vulnerability management programme's performance against the ASD Essential Eight (for example, Internet-facing services with exploitable vulnerabilities should be patched within 48 hours), InsightVM's SLA functionality can be leveraged to not only show how the organisation is tracking against the benchmark, but also provide detail on "why" in the event of non-compliance. The platform does this by providing a list of assets and vulnerabilities that require remediation in order to be compliant with the configured SLA. The below image provides an example of a non-compliant SLA, configured to track the Essential Eight benchmark.



SLA: E8 - Remediate all critical vulnerabilities within 48 hours

GOAL OVERVIEW

TYPE	SLA
PERMISSIONS	Read, Manage
DESCRIPTION	All critical vulnerabilities should be remediated within 3 days of discovery.
CREATED ON	2022-10-31 15:53:14
CREATED BY	Me
LAST UPDATED	2022-11-12 03:41:12
CONDITIONS	Remediate 100% of vulnerabilities where vulnerability.severity = 'critical' && vulnerability.exploits IS NOT NULL within 2 days of discovery
SCOPE	asset.groups IN ['internet facing assets']

61.42k Vulnerability Instances

26.1k Remediated · 120 In Grace Period · 35.2k Past Due

Not Compliant
Status

43% of vulnerabilities currently remediated
0% of vulnerabilities currently in grace period

(0 of 7986 records selected)

Title	A...	Inst...	Due Date	Discovery Date	Past ...	In Grace...	CVSS	Risk	S...	R.
Adobe APSB10-14: A...	3	3	3/1/2022	2/26/2022	3	0	9.3	861	● Critical	
Adobe APSB10-14: A...	3	3	3/1/2022	2/26/2022	3	0	9.3	861	● Critical	

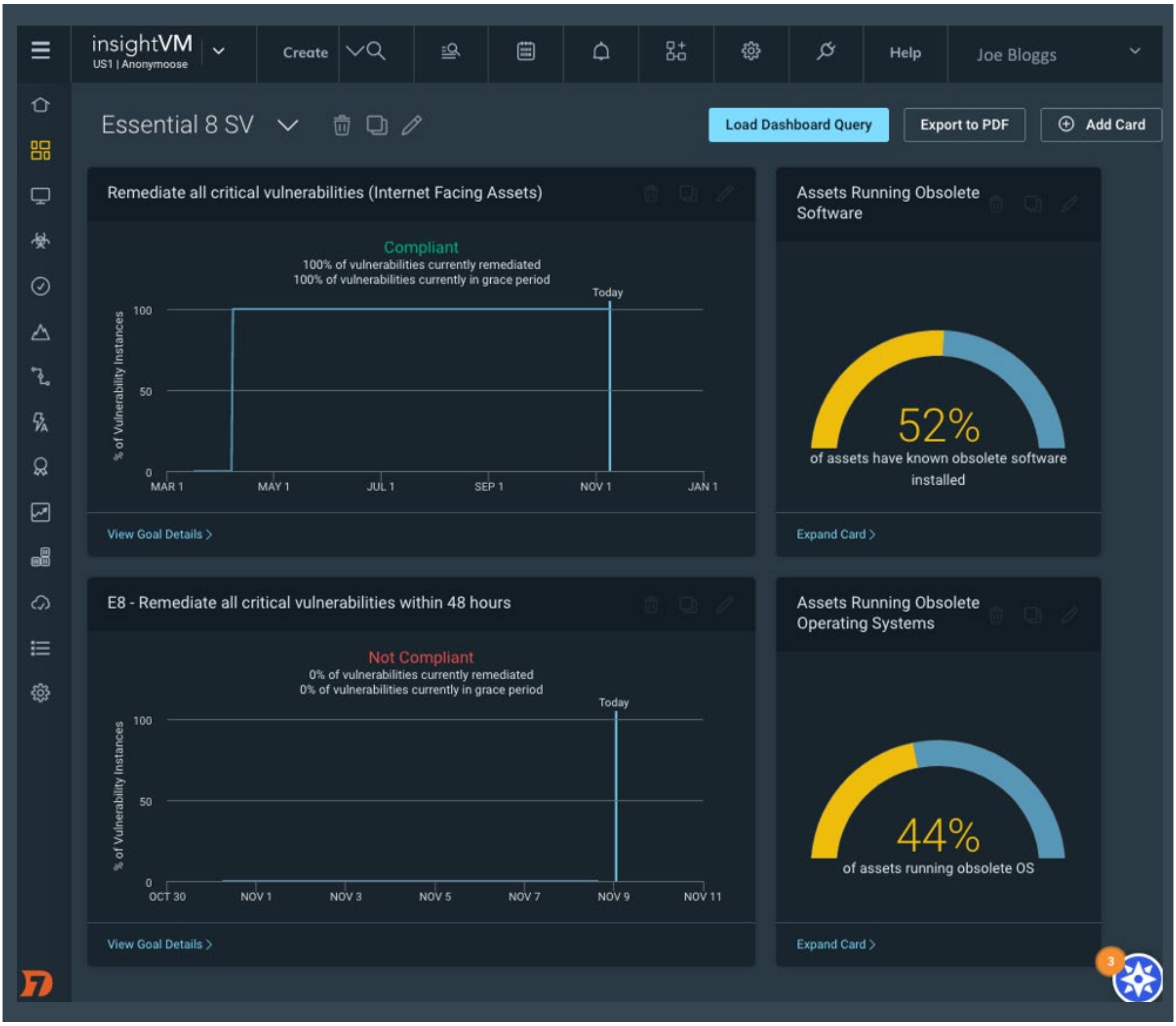
A: Detail of the SLA, including conditions of the SLA and Scope of Assets covered
B: Performance of the SLA over time
C: List of assets/vulnerabilities that require remediation inorder for the SLA to be compliant.

Instructions on how to create an Essential Eight tracking SLA can be found in Appendix A.

Dashboards and Reporting

InsightVM contains a variety of pre-built report templates designed for a wide range of audiences and purposes. This includes engineer-level Remediation Plan reports; high-level Executive Summary reports; reports documenting compliance, trend data, and overall data about the scanned environment; baseline comparisons to analyse changes over time; and more. Default reports can be customised to support risk management goals. Sections can be added and removed through new custom report templates or modification of default templates, allowing configuration and vulnerability assessment data to be included in reports in varying capacities.

Leveraging this capability, InsightVM clients can create a dashboard that shows all of the required metrics to understand the effectiveness and compliance of an organisation's vulnerability management programme against the ASD Essential Eight. This can be achieved by applying configured goals and SLAs to a dashboard, providing a single pane of glass from which to gain visibility. The below image shows an example of a dashboard configured to track and measure progress and overall performance against the ASD Essential Eight benchmarks.



Remediate all critical vulnerabilities (Internet Facing Assets)

Compliant
100% of vulnerabilities currently remediated
100% of vulnerabilities currently in grace period

Assets Running Obsolete Software

52%
of assets have known obsolete software installed

E8 - Remediate all critical vulnerabilities within 48 hours

Not Compliant
0% of vulnerabilities currently remediated
0% of vulnerabilities currently in grace period

Assets Running Obsolete Operating Systems

44%
of assets running obsolete OS

Instructions on how to create an Essential Eight tracking dashboard can be found in Appendix B.

Policy Scanning

The ASD Essential Eight includes other areas for which InsightVM's policy scanning capability can be leveraged to understand an organisation's current compliance. For example:

- Configure Microsoft Office Macro Settings Controls, such as:
    - Microsoft Office is configured to prevent activation of OLE packages
    - Microsoft Office has been configured to block Microsoft Office macros from running in Microsoft Office files from the internet
- User Application Hardening Controls, such as (for Maturity level One):
    - Web browsers do not process Java from the internet
    - Internet Explorer 11 is disabled or removed

InsightVM's built-in policy manager allows configuration policy customization and provides a dashboard for drilling down into compliance by policy, asset group, asset, and individual policy element. InsightVM can assess for specific settings such as macro enforcement options, measure compliance based on a multitude of built-in CIS benchmarks, and leverage a framework for creating complex vulnerability checks using a simple XML format. Below are some examples of proof that Essential Eight assessors would be looking for to ensure adherence to the example controls above, all of which can be checked for compliance by the InsightVM policy manager.

E8 Control	Assessor Test	Proof Assessors Are Looking For
Microsoft Office is configured to prevent activation of OLE packages.	Microsoft Office files do not execute OLE packages.	Check if the required registry key exists: Get-ItemProperty -Path "HKCU\SOFTWARE\Microsoft\office\<version>\<application>\security\" | Select-Object -property "PackagerPrompt" Example: Get-ItemProperty -Path "HKCU\SOFTWARE\Microsoft\office\16.0\excel\security\" | Select-Object -property "PackagerPrompt"
Microsoft Office macros in files originating from the internet are blocked.	Microsoft Office has been configured to block Microsoft Office macros from running in Microsoft Office files from the internet.	Check if the following registry value exists and is set to 1. Do this for all installed Microsoft Office applications: Computer\HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\office\<version>\<Application>\security\blockcontentexecutionfromInternet
Web browsers do not process Java from the internet.	Java content does not execute in Microsoft Edge.	Check the registry keys at: HKLM\SOFTWARE\Oracle\JavaDeploy\WebDeployJava And HKLM\SOFTWARE\JavaSoft\Java Plug-in\
Internet Explorer 11 is disabled or removed	Internet Explorer 11 is not able to be opened due to an application control policy, group policy setting, or another mechanism.	Check the group policy setting for the "NotifyDisableIEOptions" key to confirm if the group policy setting has been configured in the registry key: (HKCU/HKLM)\Software\Policies\Microsoft\Internet Explorer\Main\

The ACSC (Australian Cyber Security Center) provides some information which organisations can use to guide their Essential Eight compliance processes. This includes guidance around Microsoft Office macros and application hardening, as well as guidance for the assessment of an organisation's maturity level. The below links are articles published by the ACSC for these specific areas:

- Configure Microsoft Office Macro Settings: https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-365-office-2021-office-2019-and-office-2016
- User Application Hardening: https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control
- Essential Eight Assessment Process Guide: https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-assessment-process-guide

Using this information, organisations can create their own custom policy scan templates to measure compliance to these standards across their environment. The below link provides guidance in how to create custom policy scan templates:

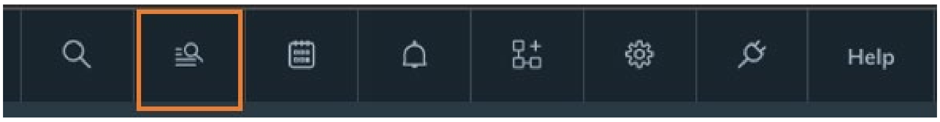
Custom Policy Check Builder Guidance: https://docs.rapid7.com/insightvm/custom-policy-builder/

Appendix A:
How to Create an Essential Eight Vulnerability Remediation Tracking SLA

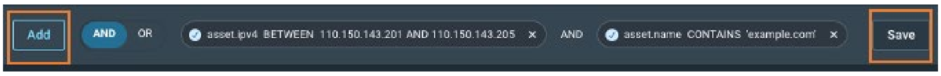
The below steps show how to create an SLA to track compliance to the ASD Essential Eight requirement of "Internet-facing services with exploitable vulnerabilities should be patched within 48 hours."

The first step for the creation of this SLA is to identify and group together the internet-facing assets. This can be easily achieved by using the platform's query functionality (skip to step 4 for the creation of the SLA):

1. At the top of the portal select the **"Query builder"** icon

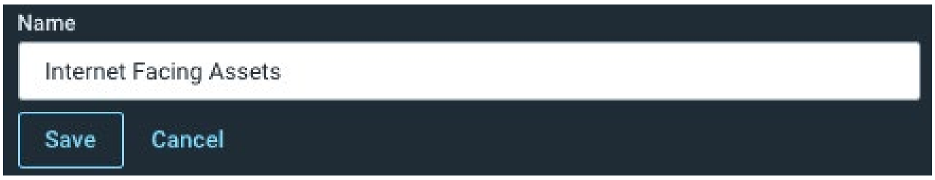


2. Create a **filtered asset search** based on specific criteria (e.g., IP Range) by clicking **"Add"**, then select **"Save"**.



asset.ipv4 BETWEEN 110.150.143.201 AND 110.150.143.205 × AND asset.name CONTAINS 'example.com' ×

3. Add a **name to the query**, then select **"Save"** to create the query.



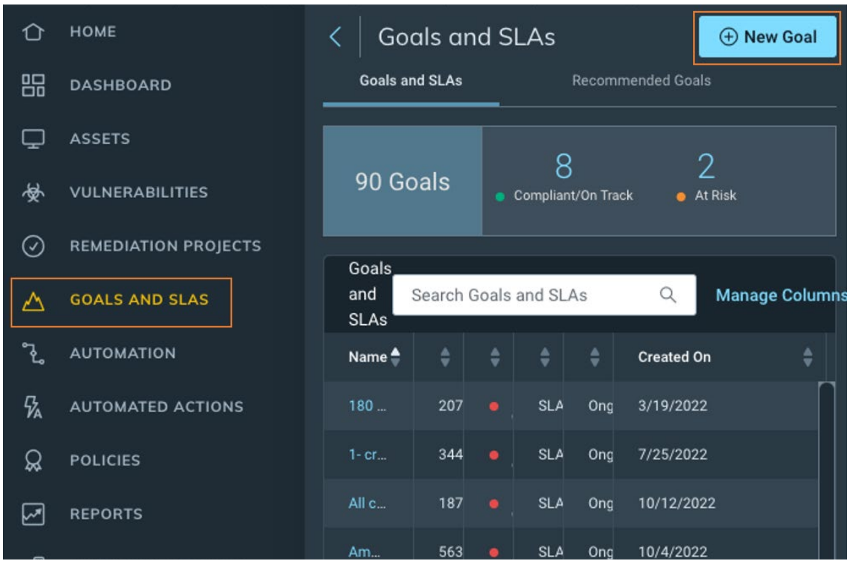
Name: Internet Facing Assets

Queries can be leveraged across a range of functionality in the platform, from filtering dashboards by showing only data pertaining to the filter of the query to the creation of goals, SLAs, and remediations projects.

Now that the internet-facing assets have been identified and grouped, the SLA can be created:

4. Go to the **"Goals and SLAs"** page and select **"New Goal"**.

   This will start the "New Goal" wizard to create the SLA.



90 Goals | 8 Compliant/On Track | 2 At Risk

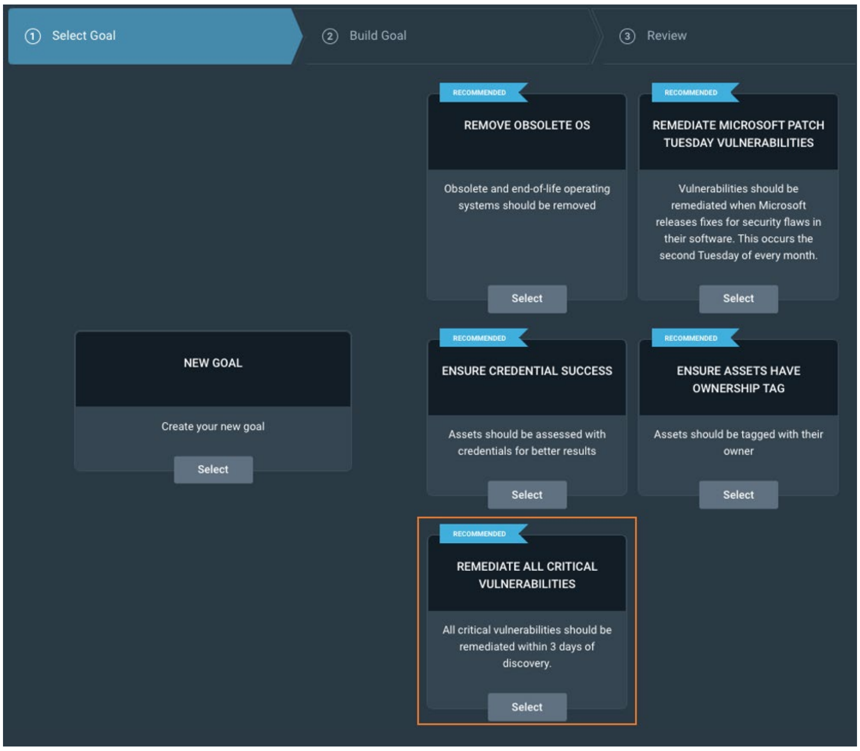
Goals and SLAs

Name					Created On
180 ...	207	●	SLA	Ong	3/19/2022
1- cr...	344	●	SLA	Ong	7/25/2022
All c...	187	●	SLA	Ong	10/12/2022
Am...	563	●	SLA	Ong	10/4/2022

5. The “New Goal” wizard provides options to either create an entirely new goal, or select from a premade template which can be modified.

For ease of creation, select the premade template **“Remediate All Critical Vulnerabilities”**.

This will provide a starting point for the SLA, of which the criteria is: 100% of Vulnerabilities with a severity of “Critical” are to be remediated within 3 days. This can then be modified to track against the ASD Essential Eight requirement.



NEW GOAL
Create your new goal

RECOMMENDED
REMOVE OBSOLETE OS
Obsolete and end-of-life operating systems should be removed

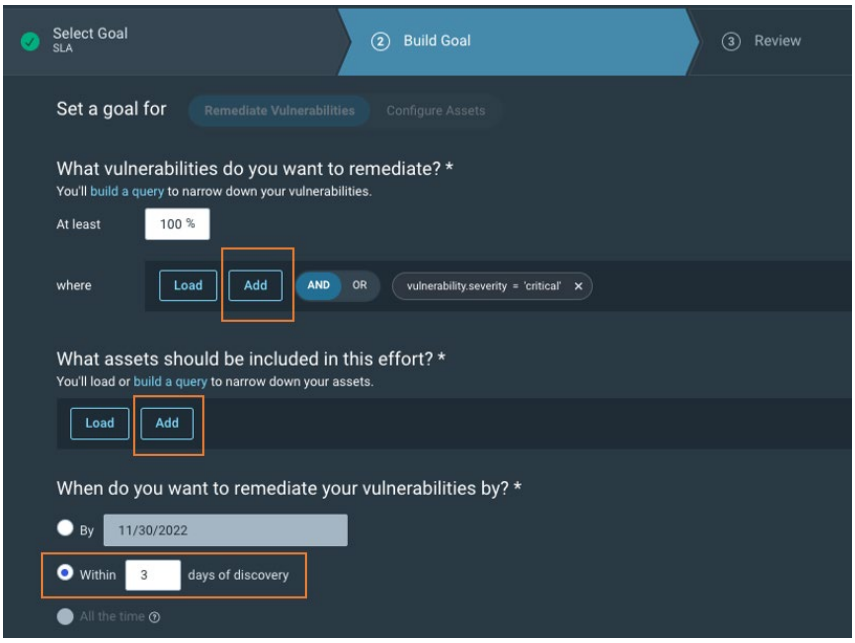
RECOMMENDED
REMEDIATE MICROSOFT PATCH TUESDAY VULNERABILITIES
Vulnerabilities should be remediated when Microsoft releases fixes for security flaws in their software. This occurs the second Tuesday of every month.

RECOMMENDED
ENSURE CREDENTIAL SUCCESS
Assets should be assessed with credentials for better results

RECOMMENDED
ENSURE ASSETS HAVE OWNERSHIP TAG
Assets should be tagged with their owner

RECOMMENDED
REMEDIATE ALL CRITICAL VULNERABILITIES
All critical vulnerabilities should be remediated within 3 days of discovery.

6. **Modify the conditions** of the SLA to meet the ASD Essential Eight requirement, as well as the assets to which the SLA will be applied.



Set a goal for

What vulnerabilities do you want to remediate? *
You'll build a query to narrow down your vulnerabilities.

At least 100 %

where vulnerability.severity = 'critical' ×

What assets should be included in this effort? *
You'll load or build a query to narrow down your assets.

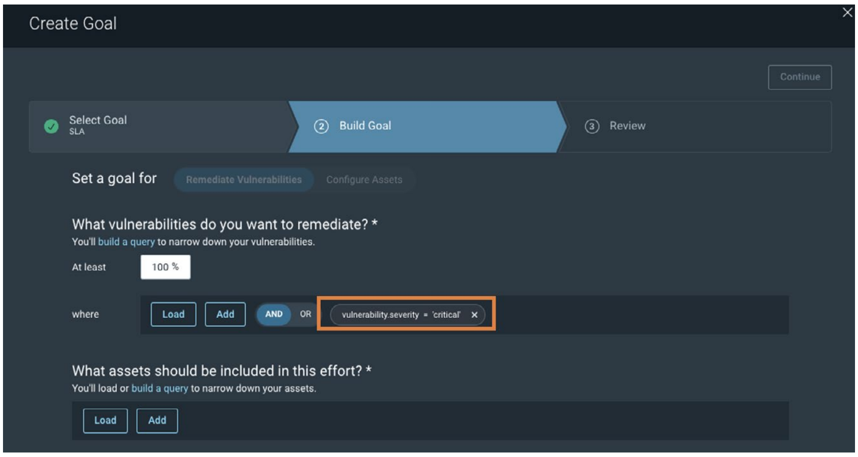
When do you want to remediate your vulnerabilities by? *

○ By 11/30/2022

● Within 3 days of discovery

○ All the time

6a. **Remove** the “Vulnerability Severity=Critical” condition.



Create Goal

Set a goal for

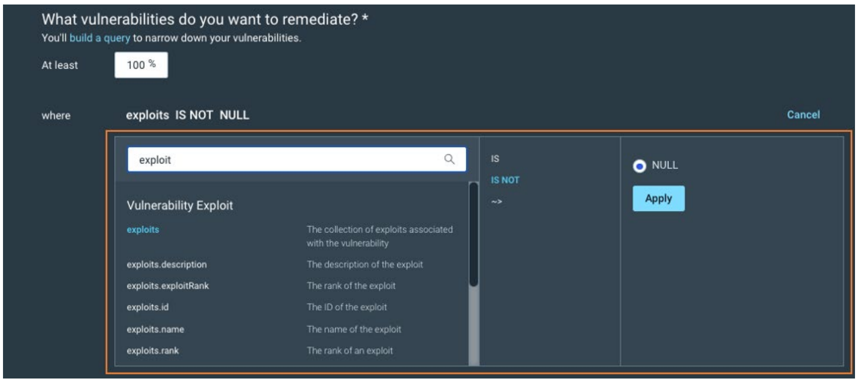
What vulnerabilities do you want to remediate? *
You'll build a query to narrow down your vulnerabilities.

At least 100 %

where vulnerability.severity = 'critical' ×

What assets should be included in this effort? *
You'll load or build a query to narrow down your assets.

6b. Add **“Exploit is not Null”** Condition to the SLA.



What vulnerabilities do you want to remediate? *
You'll build a query to narrow down your vulnerabilities.

At least 100 %

where exploits IS NOT NULL

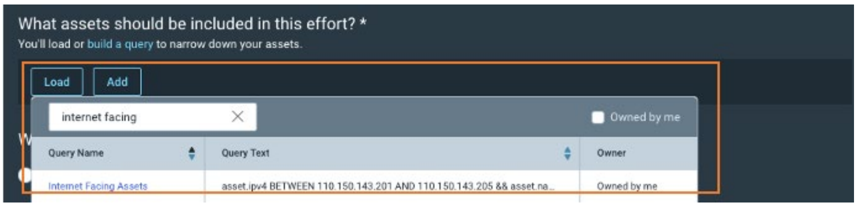
Cancel

exploit

Vulnerability Exploit

exploits	The collection of exploits associated with the vulnerability
exploits.description	The description of the exploit
exploits.exploitRank	The rank of the exploit
exploits.id	The ID of the exploit
exploits.name	The name of the exploit
exploits.rank	The rank of an exploit

6c. Add the newly created **“Internet-Facing Assets”** Query to the “**What assets should be included in the effort”** section by selecting “Load” then searching and selecting the required query.

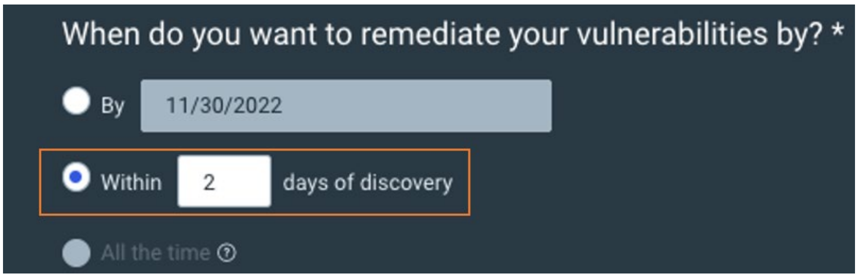


What assets should be included in this effort? *
You'll load or build a query to narrow down your assets.

internet facing

Query Name	Query Text	Owner
Internet Facing Assets	asset.ipv4 BETWEEN 110.150.143.201 AND 110.150.143.205 && asset.na...	Owned by me

6d. Adjust **“When do you want to remediate your vulnerabilities by”** to within **2 days** to meet ASD Essential Eight requirements.



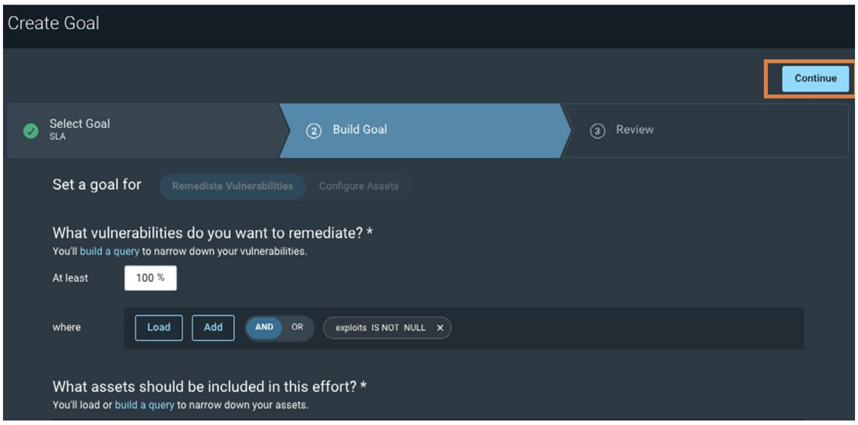
When do you want to remediate your vulnerabilities by? *

○ By 11/30/2022

● Within 2 days of discovery

○ All the time

6e. Click **“Continue”**



Create Goal

Set a goal for Remediate Vulnerabilities Configure Assets

What vulnerabilities do you want to remediate? *
You'll build a query to narrow down your vulnerabilities.

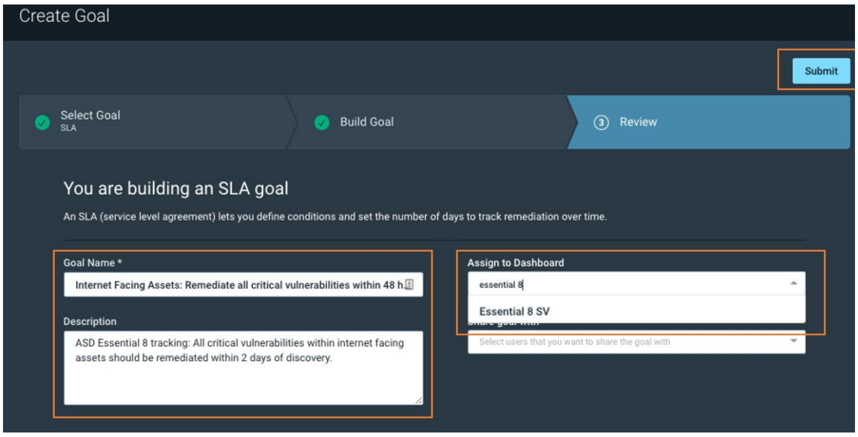
At least 100 %

where Load Add AND OR exploits IS NOT NULL ×

What assets should be included in this effort? *
You'll load or build a query to narrow down your assets.

7. Make changes to the **“Goal Name”** and **“Description”** (these are pre-filled from the template). Select a **dashboard** to add the SLA to (if a dashboard is already created).

Select **“Submit”** to create the SLA.



Create Goal

You are building an SLA goal

An SLA (service level agreement) lets you define conditions and set the number of days to track remediation over time.

Goal Name *
Internet Facing Assets: Remediate all critical vulnerabilities within 48 h

Description
ASD Essential 8 tracking: All critical vulnerabilities within internet facing assets should be remediated within 2 days of discovery.

Assign to Dashboard
essential 8
Essential 8 SV

Select users that you want to share the goal with

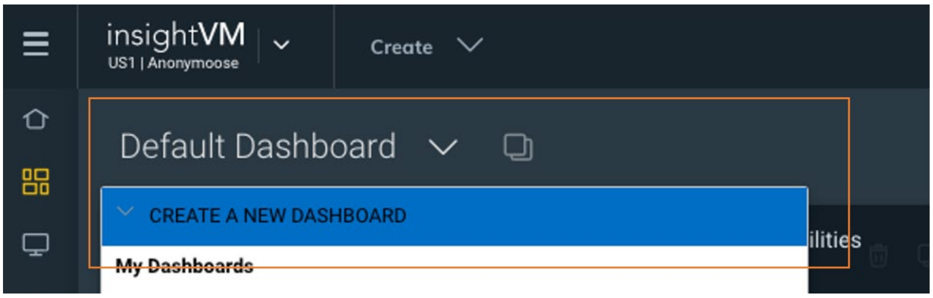
Appendix B:
How to Create an Essential Eight Remediation SLA Tracking Dashboard

The below steps show how to create a dashboard from which to track the performance of a vulnerability management programme against the ASD Essential Eight guidelines. The below provides steps in adding the following reports to the dashboard:

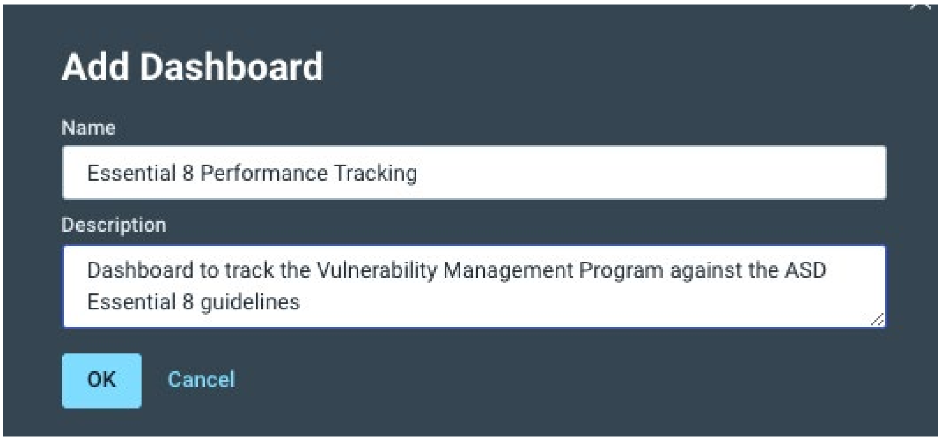
- SLA (specifically tracking the remediation of vulnerabilities where an exploit exists on a internet-facing asset within 48 hours)
- % Assets running obsolete operating systems
- % Assets running obsolete software

1. Create a Dashboard.

   To do so expand the selection menu from the dashboard title bar, then select **"Create New Dashboard"**.



2. **Name** and add a description for the dashboard. Then **select "OK"**.



Add Dashboard

Name

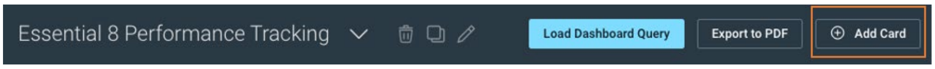
Essential 8 Performance Tracking

Description

Dashboard to track the Vulnerability Management Program against the ASD Essential 8 guidelines

3. Add a SLA report card to the dashboard.

   To do so select **"Add Card"**.

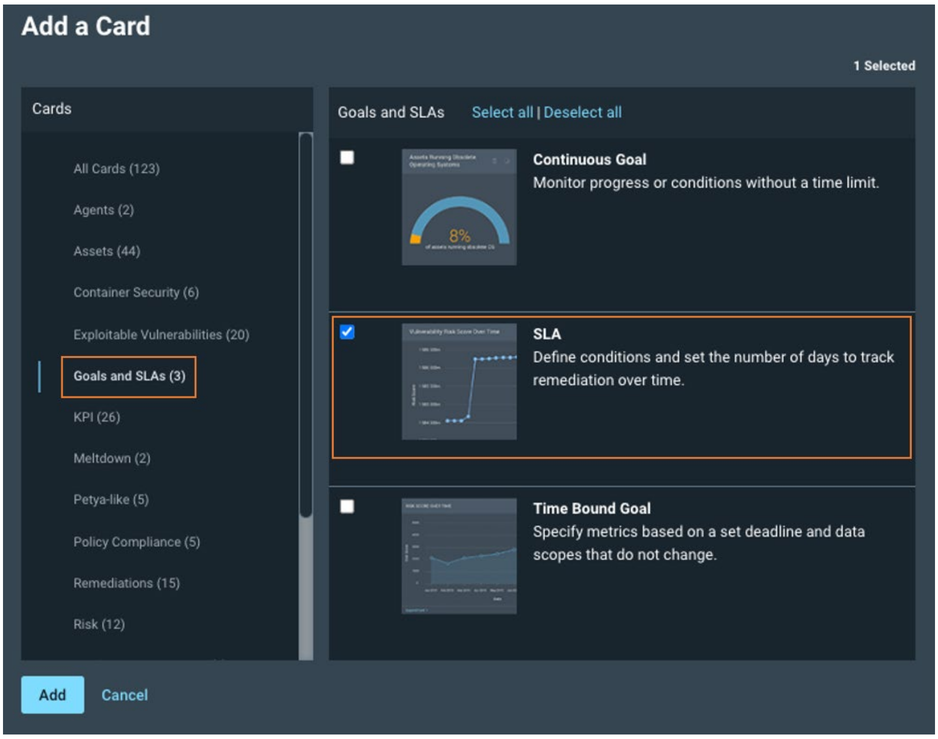


3a. Add a SLA report card to the dashboard.

Select **"Goals and SLAs"** from the category pain, then select **"SLA"**.

Select **Add**.

This will now add the reporting card to the dashboard.



Add a Card

1 Selected

Cards

All Cards (123)

Agents (2)

Assets (44)

Container Security (6)

Exploitable Vulnerabilities (20)

Goals and SLAs (3)

KPI (26)

Meltdown (2)

Petya-like (5)

Policy Compliance (5)

Remediations (15)

Risk (12)

Goals and SLAs Select all | Deselect all

□ **Continuous Goal**
Monitor progress or conditions without a time limit.

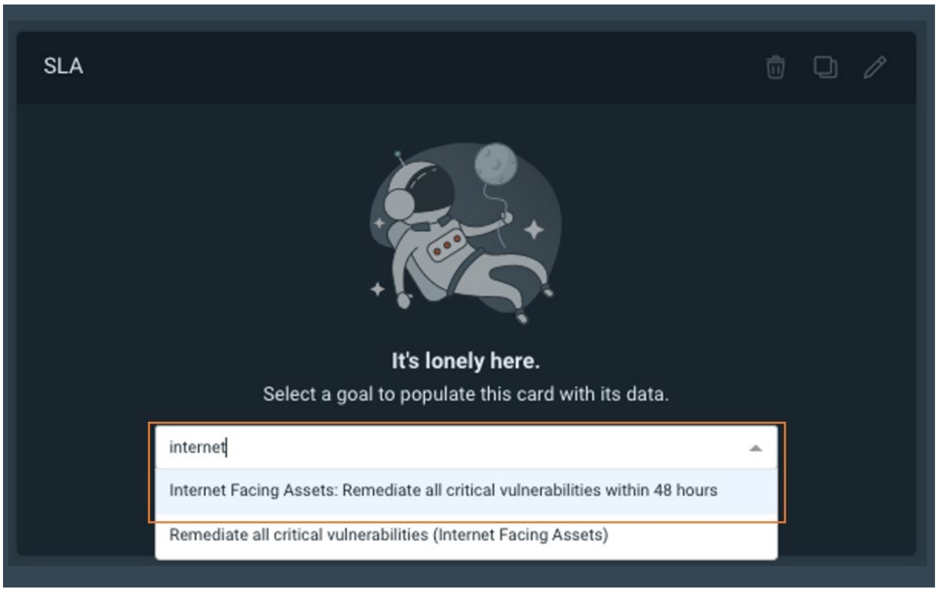
☑ **SLA**
Define conditions and set the number of days to track remediation over time.

□ **Time Bound Goal**
Specify metrics based on a set deadline and data scopes that do not change.

Add Cancel

3b. **Select an SLA goal to track** in the reporting card.

To do so, use the drop-down menu with the card to search for the created Essential Eight SLA, then select it.



SLA

It's lonely here.

Select a goal to populate this card with its data.

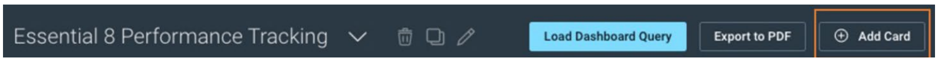
internet

Internet Facing Assets: Remediate all critical vulnerabilities within 48 hours

Remediate all critical vulnerabilities (Internet Facing Assets)

4. Add reporting cards to track obsolete operating systems and software.

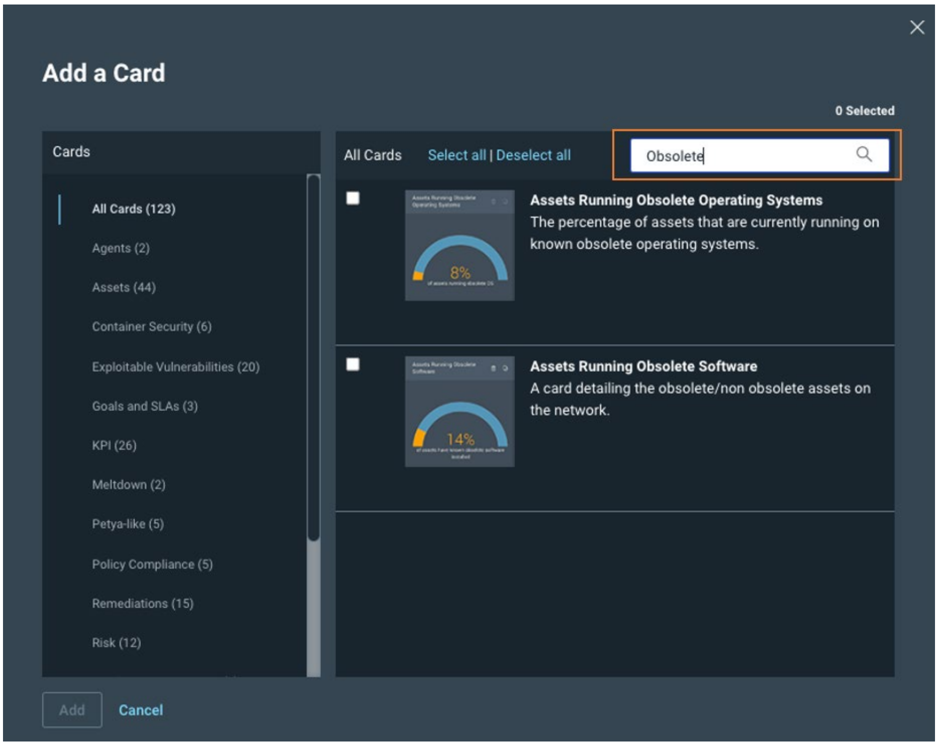
To do so select **"Add Card".**



Essential 8 Performance Tracking

Load Dashboard Query Export to PDF Add Card

4a. Within search type **“Obsolete”.**



□ **Assets Running Obsolete Operating Systems**
The percentage of assets that are currently running on known obsolete operating systems.

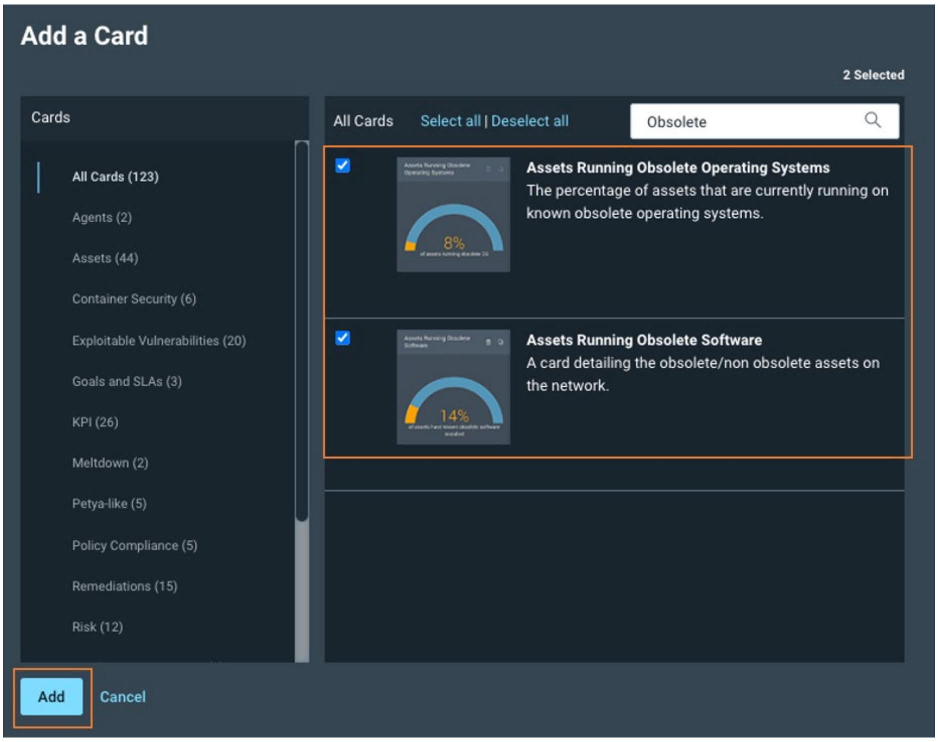
□ **Assets Running Obsolete Software**
A card detailing the obsolete/non obsolete assets on the network.

4b. Select the 2 report cards:

- Assets Running Obsolete Operating Systems
- Assets Running Obsolete Software

Select **Add**.

This will now add these additional reporting cards to the dashboard.



☑ **Assets Running Obsolete Operating Systems**
The percentage of assets that are currently running on known obsolete operating systems.

☑ **Assets Running Obsolete Software**
A card detailing the obsolete/non obsolete assets on the network.

Additional reporting cards can be added to the dashboard to provide visibility as required by following the same steps.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organisations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimise our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

www.rapid7.com