Threat Modeling Report

Created on 11/10/2019 2:54:27 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	15
Not Applicable	0

Needs Investigation	0
Mitigation Implemented	1
Total	16
Total Migrated	0

Diagram: Diagram 1

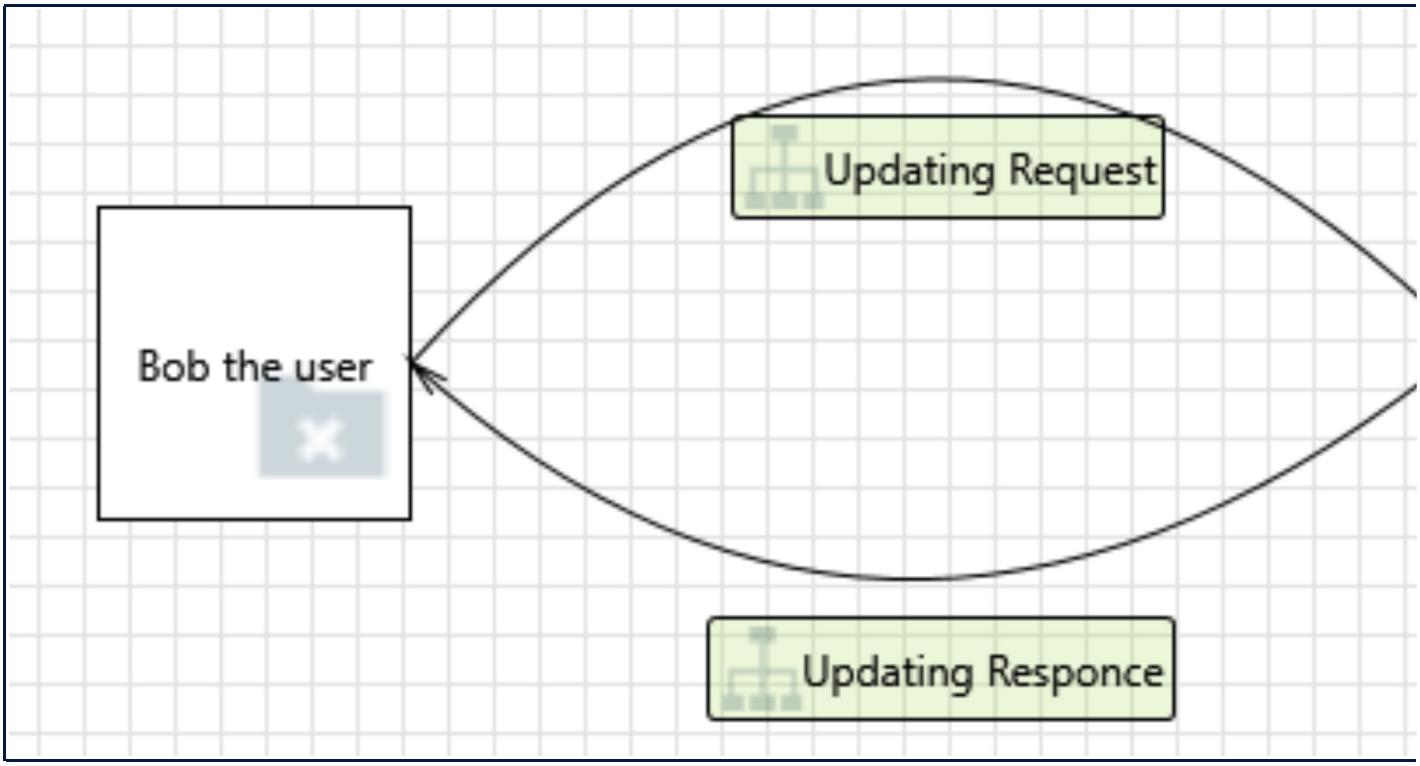
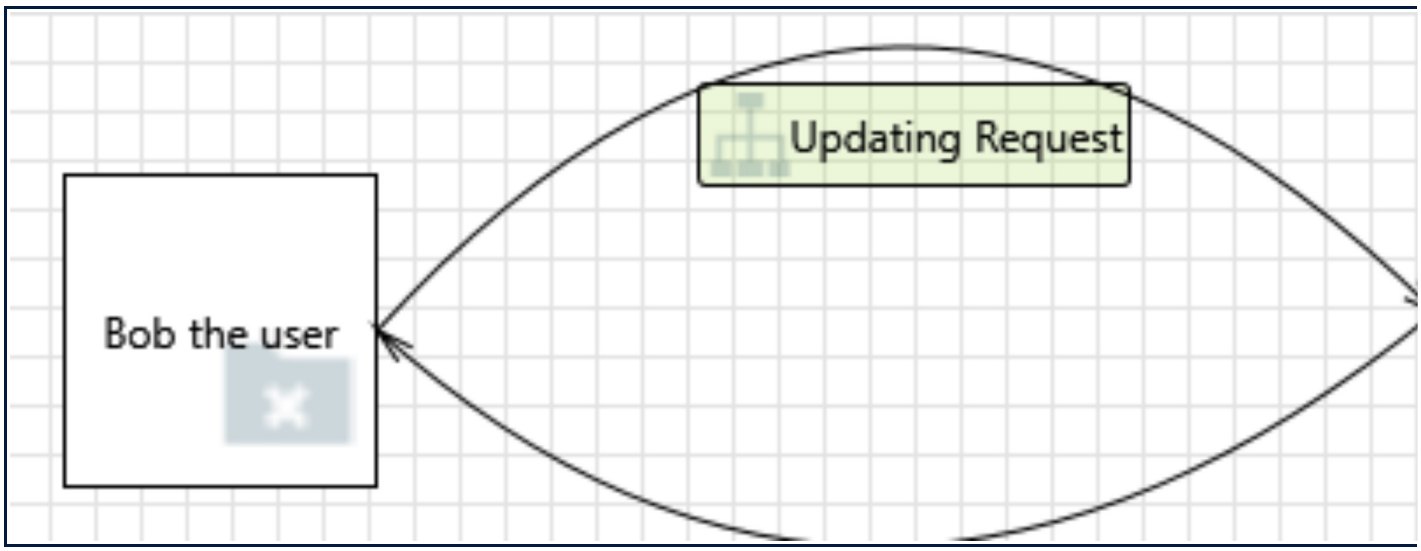


Diagram 1 Diagram Summary:

Not Started	1
Not Applicable	0

Needs Investigation	0
Mitigation Implemented	1
Total	2
Total Migrated	0

Interaction: Updating Request



1. Spoofing the User External Entity [State: Mitigation Implemented] [Priority: High]

Category:	Spoofing
Description:	Bob the user may be spoofed by an attacker and this may lead to unauthorized access to Kodi Add-ons. Consider using a standard authentication mechanism to identify the

external entity.

Justification: <no mitigation provided>

2. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Kodi Add-ons may be able to impersonate the context of Bob the user in order to gain additional privilege.

Justification: <no mitigation provided>

Diagram: Diagram 2

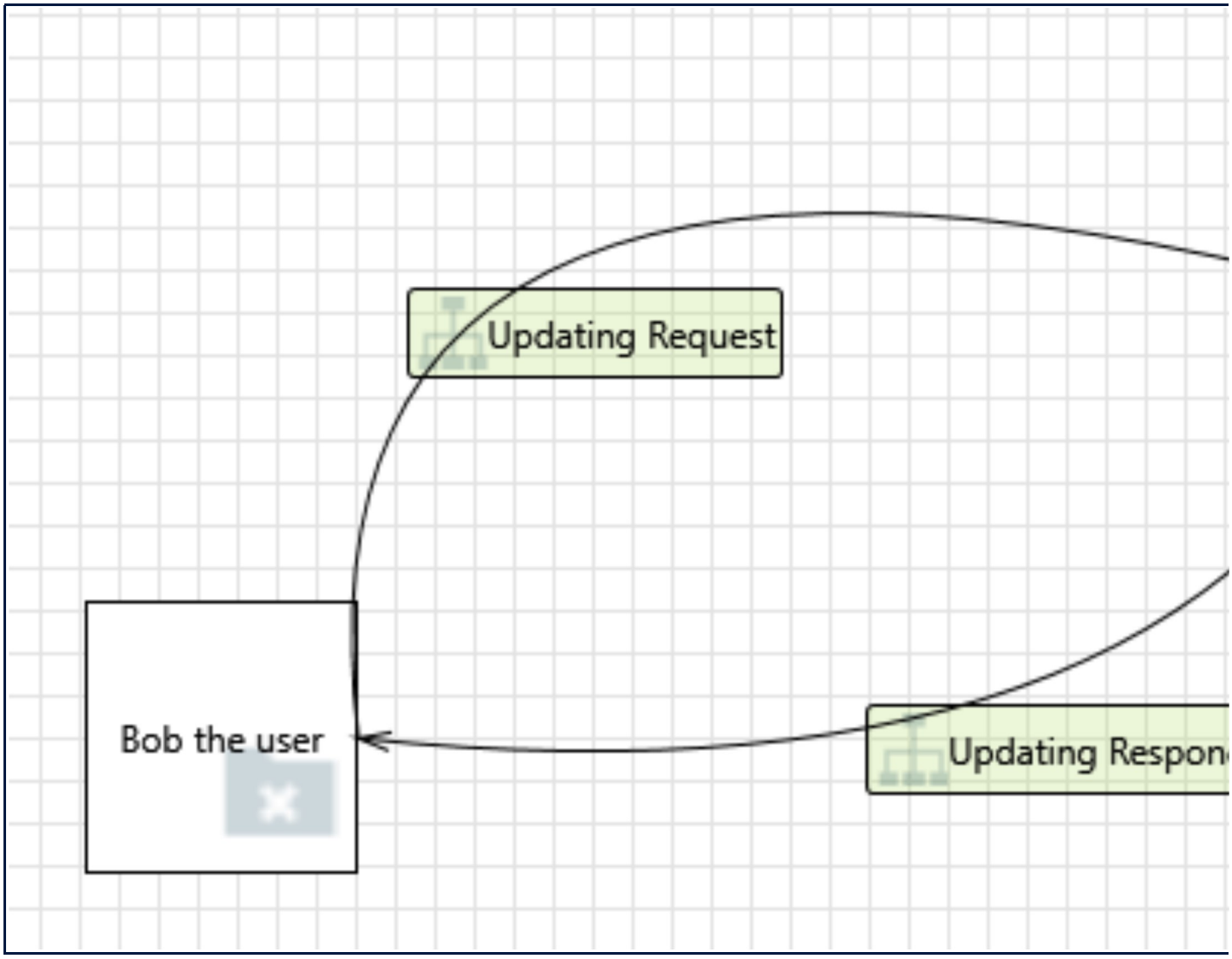
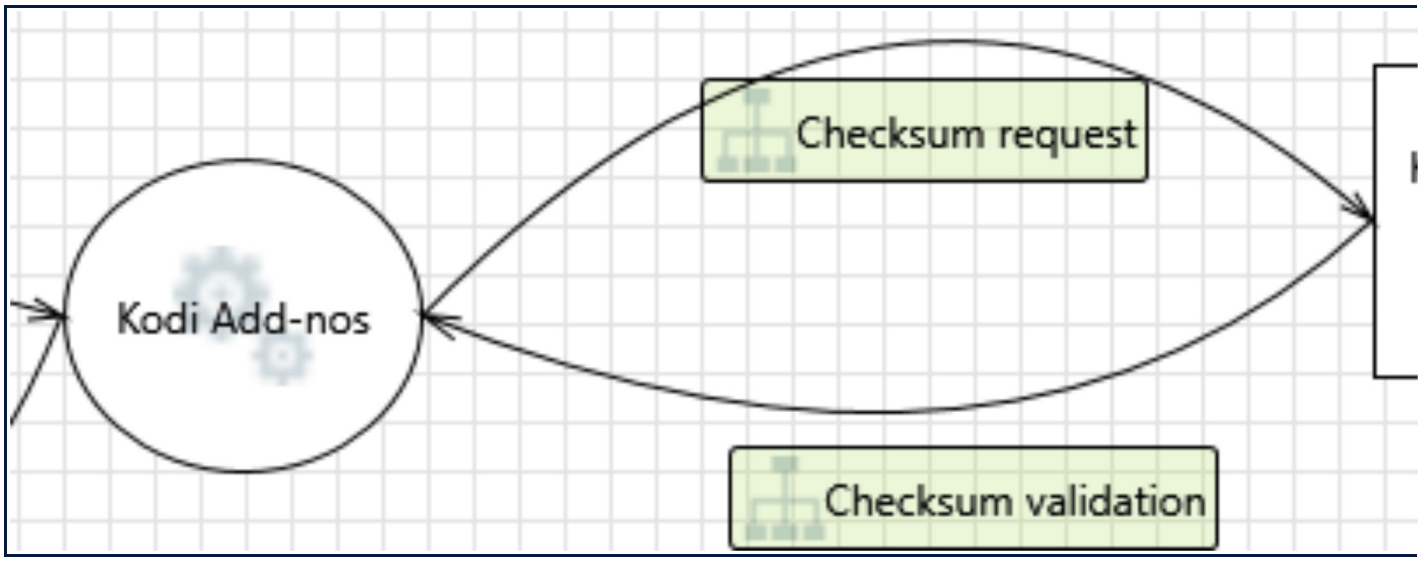


Diagram 2 Diagram Summary:

Not Started	4
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	4
Total Migrated	0

Interaction: Checksum validation



3. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Kodi Add-nos may be able to impersonate the context of Kodis tursted Add-on repositiory in order to gain additional privilege.
Justification:	<no mitigation provided>

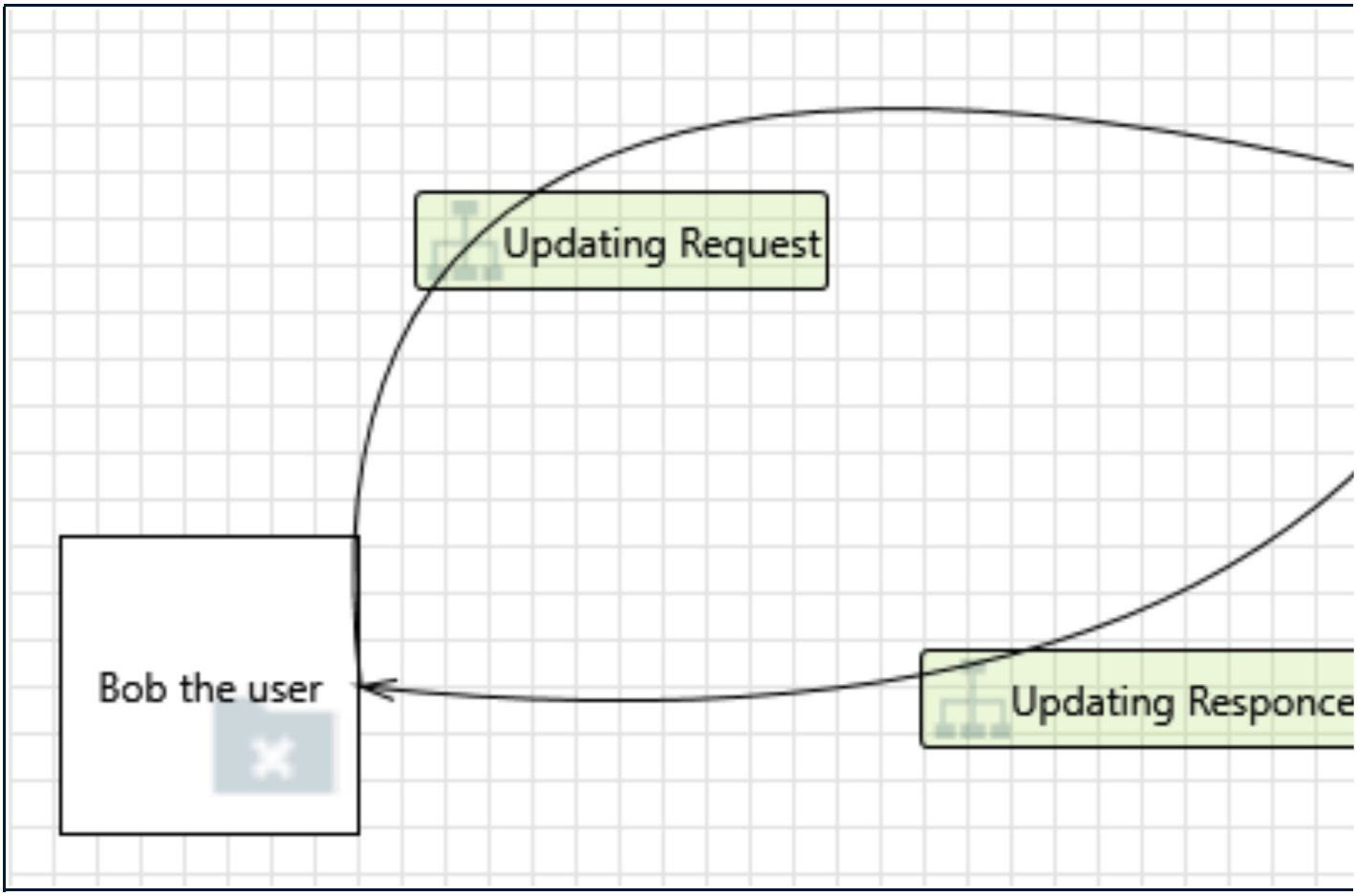
4. Spoofing the Kodis tursted Add-on repositiory External Entity [State: Not Started] [Priority: High]

Category: Spoofing

Description: Kodis tursted Add-on repositiory may be spoofed by an attacker and this may lead to unauthorized access to Kodi Add-nos. Consider using a standard authentication mechanism to identify the external entity.

Justification: <no mitigation provided>

Interaction: Updating Request



5. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category:	Elevation Of Privilege
Description:	Kodi Add-nos may be able to impersonate the context of Bob the user in order to gain additional privilege.
Justification:	<no mitigation provided>

6. Spoofing the Bob the user External Entity [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Bob the user may be spoofed by an attacker and this may lead to unauthorized access to Kodi Add-nos. Consider using a standard authentication mechanism to identify the external entity.
Justification:	<no mitigation provided>

Diagram: Diagram 3

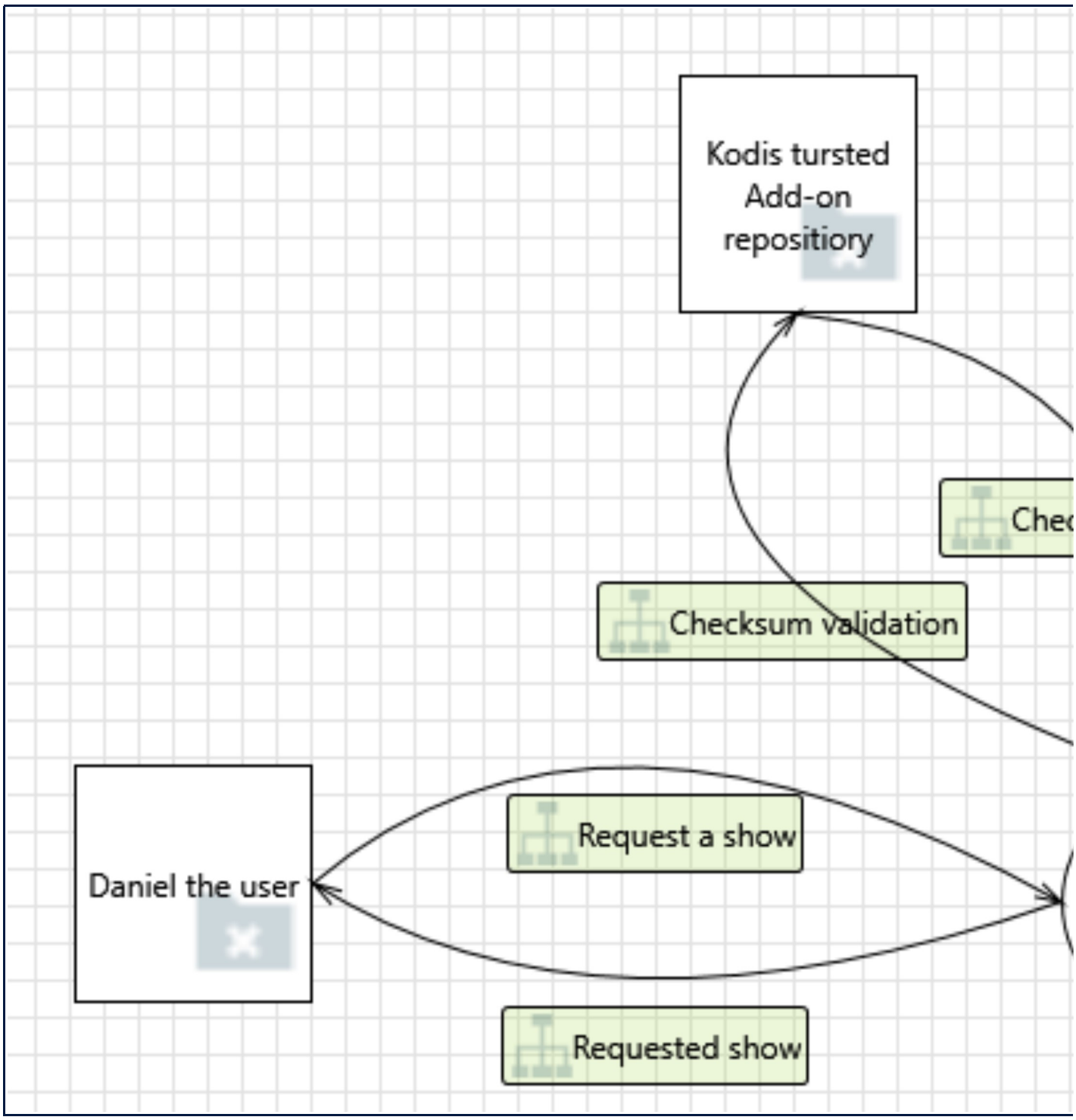
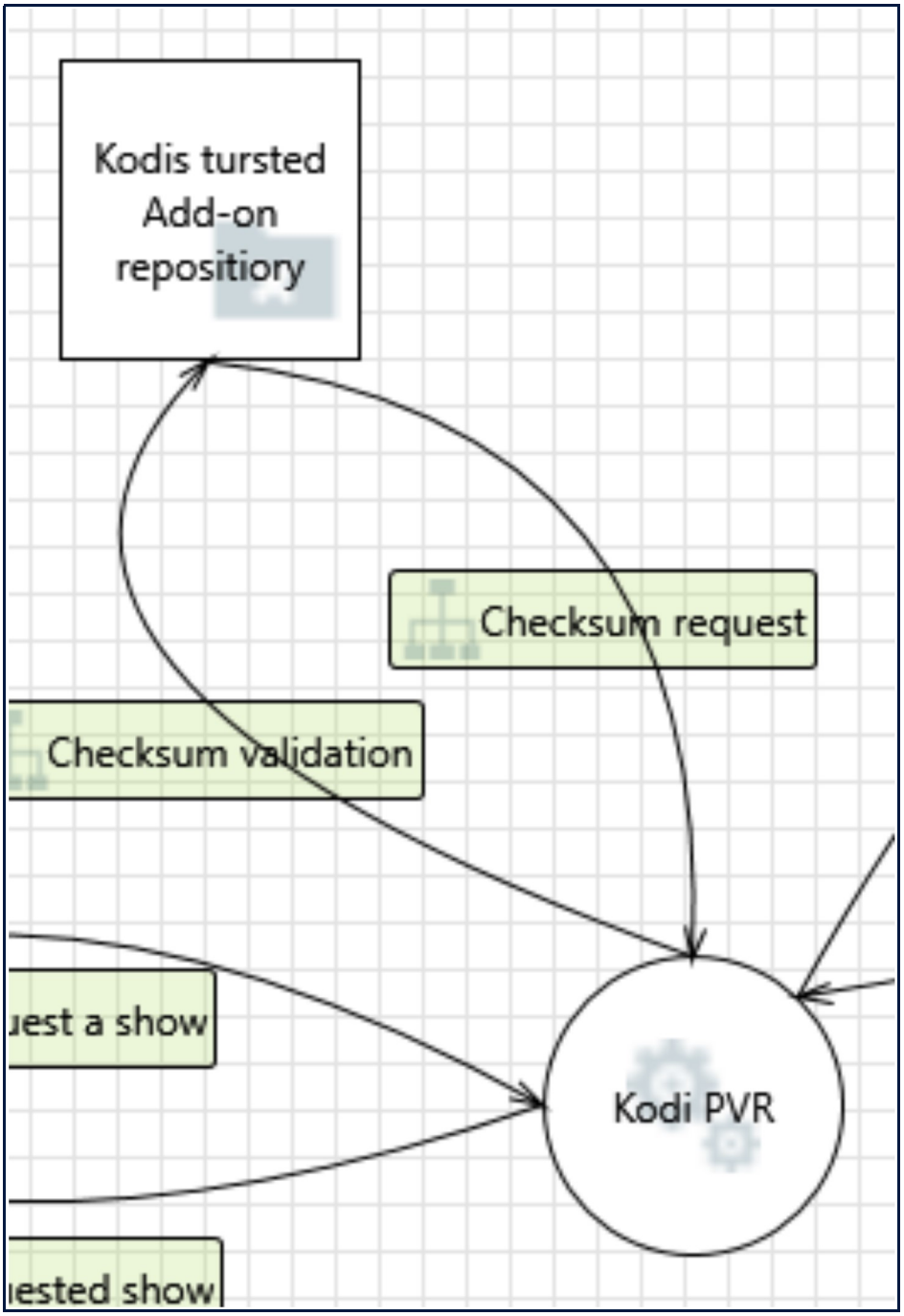


Diagram 3 Diagram Summary:

Not Started	8
Not Applicable	0

Needs Investigation	0
Mitigation Implemented	0
Total	8
Total Migrated	0

Interaction: Checksum request



7. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Kodi PVR may be able to impersonate the context of Kodis tursted Add-on repositiory in order to gain additional privilege.

Justification: <no mitigation provided>

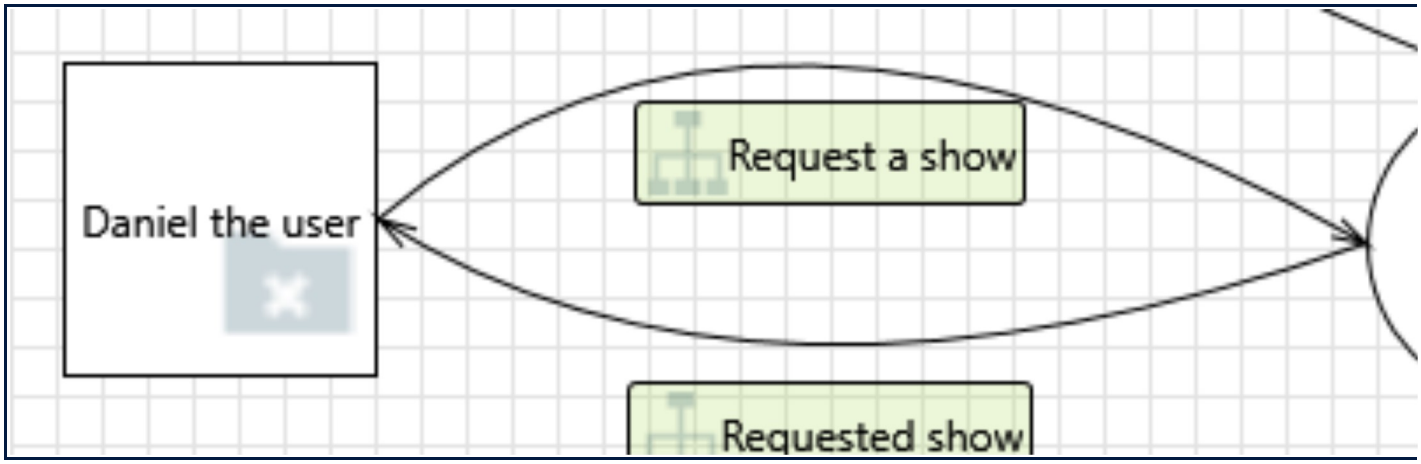
8. Spoofing the Kodis tursted Add-on repositiory
External Entity [State: Not Started] [Priority: High]

Category: Spoofing

Description: Kodis tursted Add-on repositiory may be spoofed by an attacker and this may lead to unauthorized access to Kodi PVR. Consider using a standard authentication mechanism to identify the external entity.

Justification: <no mitigation provided>

Interaction: Request a show



9. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Kodi PVR may be able to impersonate the context of Daniel the user in order to gain additional privilege.

Justification: <no mitigation provided>

10. Spoofing the Bob the user External Entity [State: Not Started] [Priority: High]

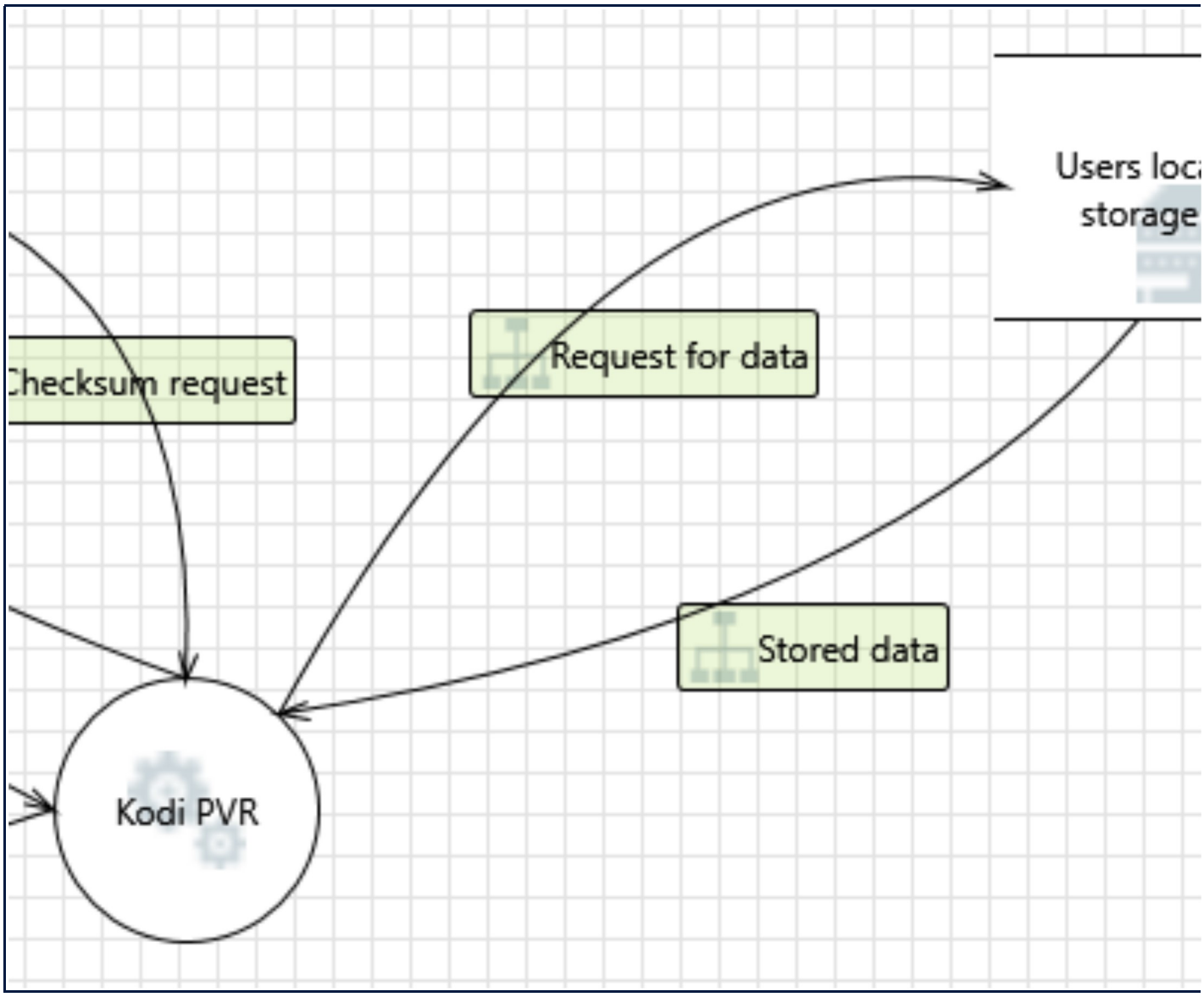
Category: Spoofing

Description: Daniel the user may be spoofed by an attacker and this may lead to unauthorized access to Kodi PVR. Consider using a

standard authentication mechanism to identify the external entity.

Justification: <no mitigation provided>

Interaction: Request for data



11. Potential Excessive Resource Consumption for

Using PVR or Users local storage [State: Not Started] [Priority: High]

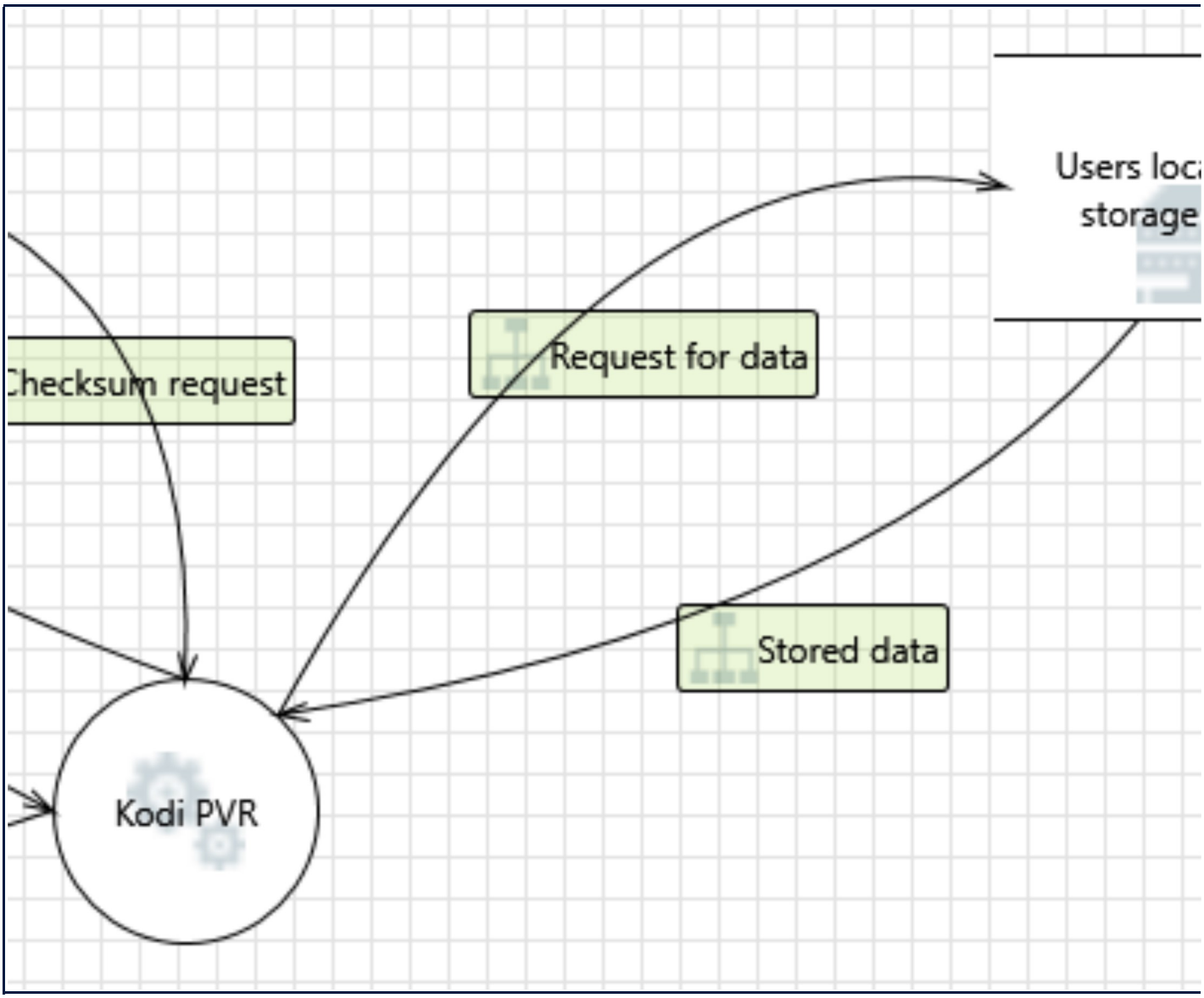
Category:	Denial Of Service
Description:	Does Kodi PVR or Users local storage take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Justification:	<no mitigation provided>

12. Spoofing of Destination Data Store Users local storage [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Users local storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Users local storage. Consider using a standard authentication mechanism to identify the destination data store.

Justification: <no mitigation provided>

Interaction: Stored data



13. Weak Access Control for a Resource [State: Not Started] [Priority: High]

Category:	Information Disclosure
Description:	Improper data protection of Users local storage can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification:	<no mitigation provided>

14. Spoofing of Source Data Store Users local storage [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	Users local storage may be spoofed by an attacker and this may lead to incorrect data delivered to Kodi PVR. Consider using a standard authentication mechanism to identify the source data store.
Justification:	<no mitigation provided>

Diagram: Diagram 4

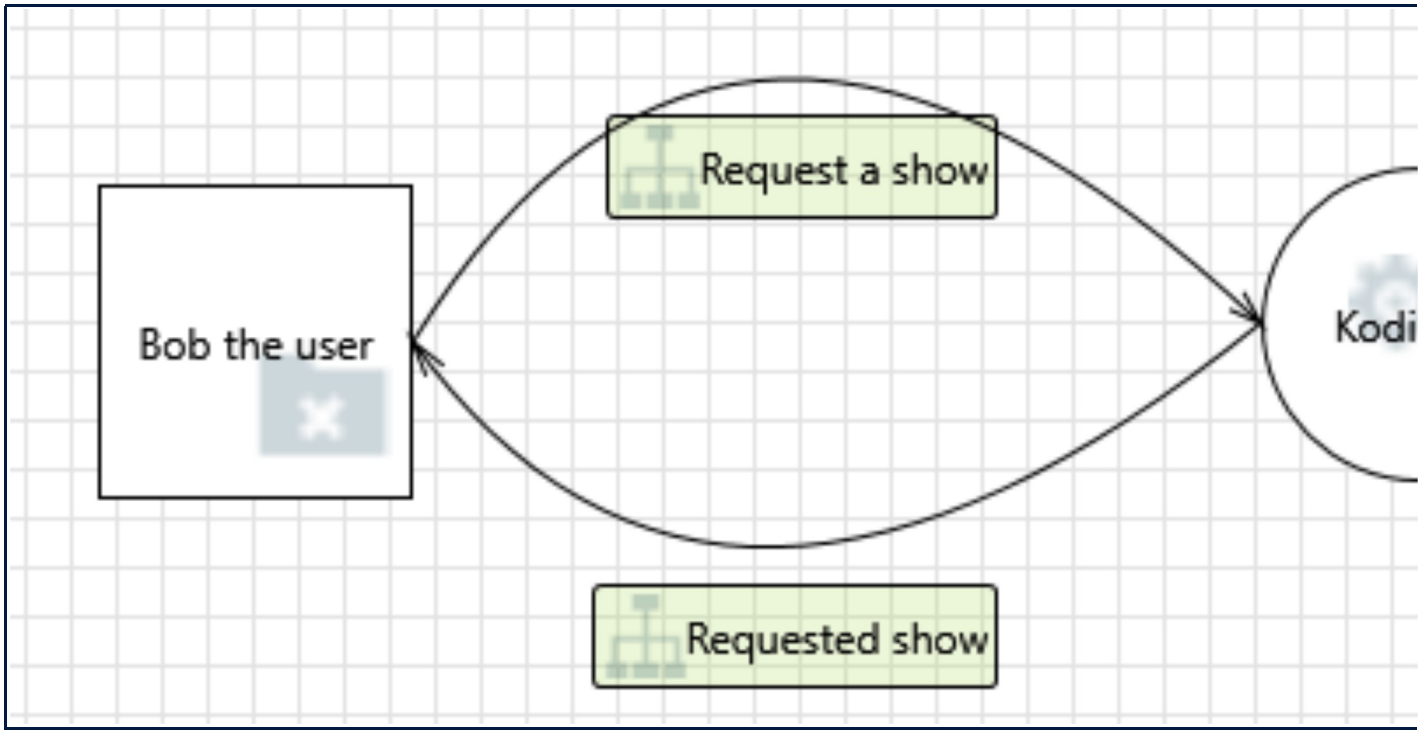
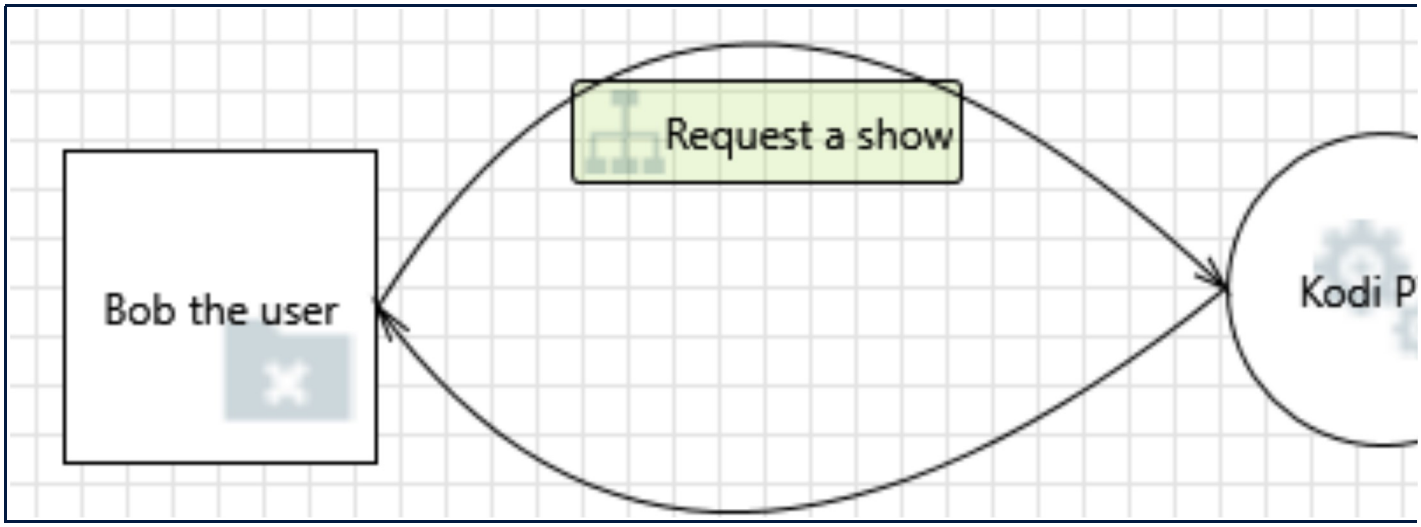


Diagram 4 Diagram Summary:

Not Started	2
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	2
Total Migrated	0

Interaction: Request a show



15. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Kodi PVR may be able to impersonate the context of Bob the user in order to gain additional privilege.

Justification: <no mitigation provided>

16. Spoofing the Bob the user External Entity [State: Not Started] [Priority: High]

Category: Spoofing

Description: Bob the user may be spoofed by an attacker and this may lead to unauthorized access to Kodi PVR. Consider using a standard

authentication mechanism to identify the external entity.

Justification: <no mitigation provided>