



# 第三方元件檢測及管理系統建置案 Sonatype IQ Server 管理者教育訓練

精誠資訊

# 大綱

- 軟體簡介
- Proxy Server設定
- 使用者管理
- 政策管理
- 預設合規政策
- Legacy Violation
- 持續監控與通知管理
- 使用豁免(Waiver)功能
- 弱點處理流程

The background features a series of concentric circles and a spiral pattern in various shades of blue and teal. The spiral starts from the center and expands outwards, creating a dynamic, swirling effect. The colors transition from a deep blue in the center to lighter, more vibrant teal and cyan towards the edges.

# Sonatype軟體簡介

# Sonatype Platform



- Sonatype Lifecycle

- 自動檢測和提供修復建議，在DevOps中實踐安全開發並避免攻擊。

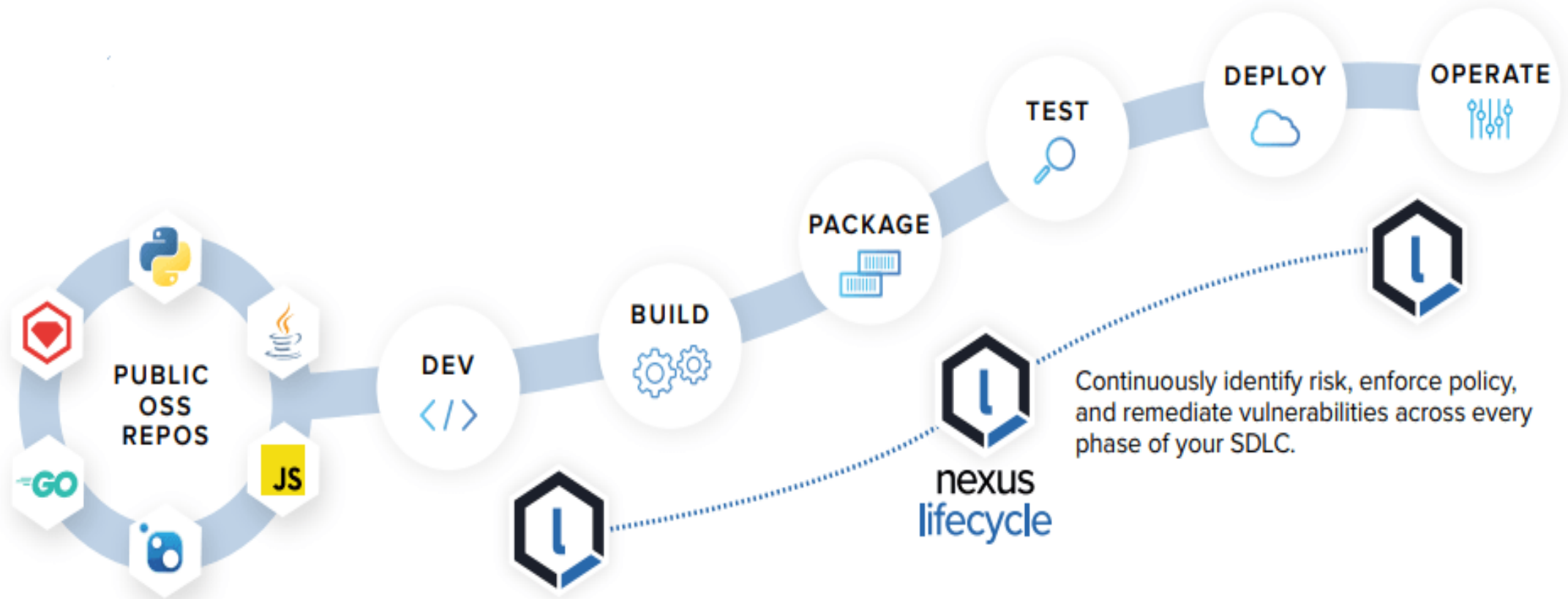
- Sonatype Nexus Repository

- 提供單一安全套件來源；支援多達18種主流套件儲存庫。

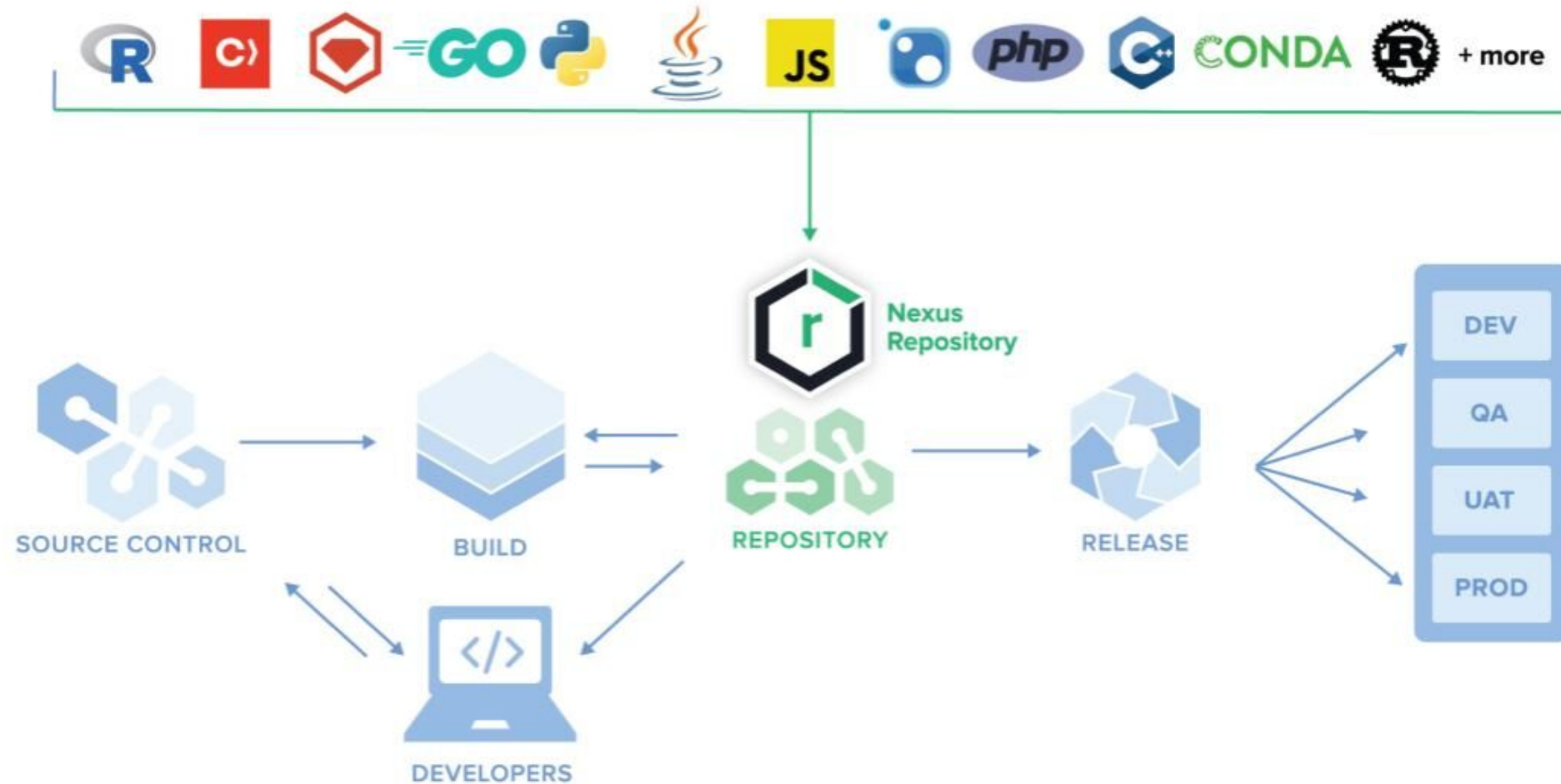
- Sonatype Repository Firewall

- 早期識別和預警，自動阻止已知漏洞和有害的套件版本以降低風險。

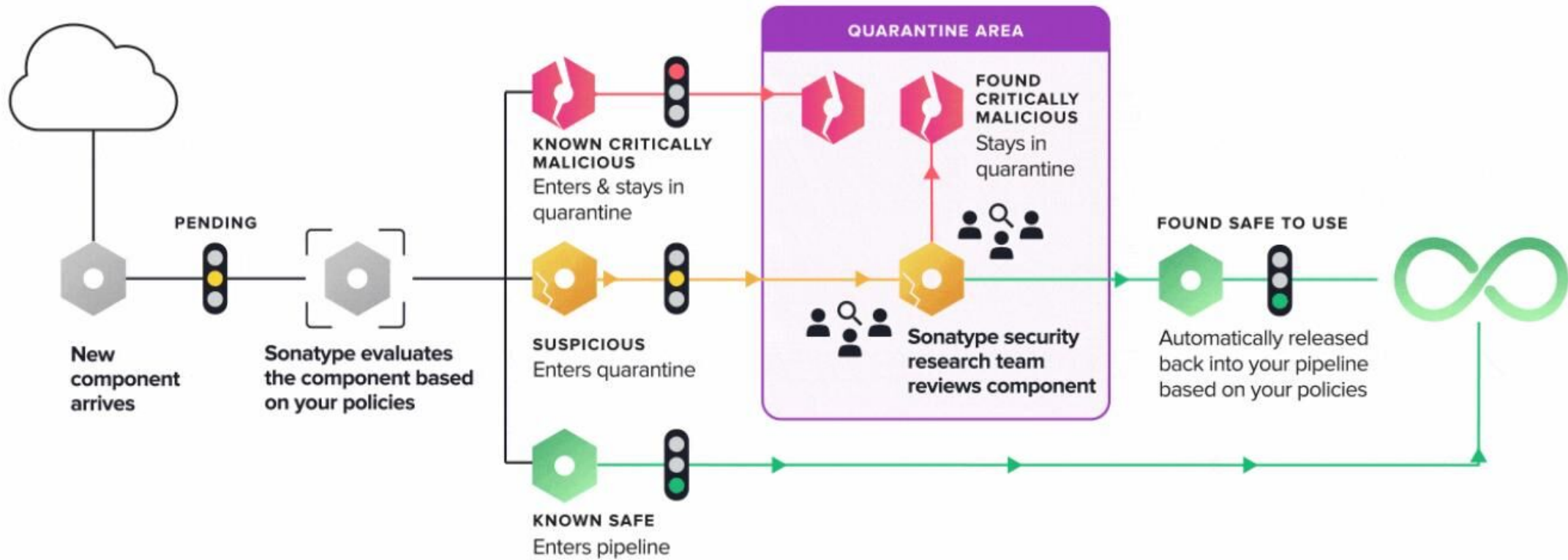
# Sonatype Lifecycle



# Sonatype Nexus Repository



# Sonatype Repository Firewall





# Proxy Server設定



# Proxy Server Configuration

## Proxy

### Configure Proxy

To use a Proxy Server for outbound requests, configure it here.

**Hostname**

**Port**

**Username** Optional

**Password** Optional

**Exclude Hosts** Optional  
Must be comma delimited.

Delete Configuration

Cancel

Save

Hostname :

\*\*\*.\*\*\*.\*\*\*.\*\*\*

Port :

8080



# 使用者管理

# LDAP 整合

The image displays two screenshots of the Nexus Lifecycle web interface, illustrating the steps to access the LDAP configuration page.

**Top Screenshot:** Shows the main dashboard with a sidebar on the left containing navigation links: Dashboard, Orgs and Policies, Reports, Success Metrics, Vulnerability Search, Advanced Search, and Firewall. The main content area is titled "Results" and includes tabs for Violations (0), Components, and Applications. Below these are filters for THREAT, POLICY, APPLICATION, and COMPONENT. A message states: "No data available in the last 30 days given the applied filters and permissions." In the top right corner, a settings gear icon is highlighted with an orange box. A red arrow points from this icon to the "LDAP" option in the "System Preferences" dropdown menu, which is also highlighted with an orange box.

**Bottom Screenshot:** Shows the "LDAP" configuration page. The sidebar is identical to the top screenshot. The main content area is titled "LDAP" and contains a section "Configure LDAP" with the text "LDAP Servers will be queried in the order listed below". Below this text is a list area that currently displays "No LDAP servers are defined". In the top right corner of the "Configure LDAP" section, there are two buttons: "Reorder List" and a blue button labeled "+ Add a Server", which is highlighted with an orange box.

# LDAP 設定

Server Name	名稱
LDAP server address	ldap://***.***.***.***:389
Search base DN	ou=XXX,dc=YYYY,dc=corp
Authentication method	Simple Authentication
Username or DN	用於查詢LDAP的帳號
Password	*****
User relative DN	用於指定使用者的組織 例：ou=資訊部
Object class	Person
User ID attribute	sAMAccountName
Real name attribute	用於顯示使用者名稱的欄位 例：cn
Email attribute	用於帶入使用者郵件的欄位 例：mail

# Roles - 角色階層

- 授予角色的權限範圍取決於該角色在系統階層結構中的位置。
  - Root Organization：授予所有組織、應用程式和儲存庫的權限。
  - Organization：授予該單個組織及其附加的任何應用程序的權限。
  - Application：僅向單個應用程式授予權限。

# Roles – 預設角色

Configure Roles		<a href="#">+ Create Role</a>
Built-In		
System Administrator	Manages system configuration and users.	>
Policy Administrator	Manages all organizations, applications, policies, and policy violations.	>
Owner	Manages assigned organizations, applications, policies, and policy violations.	>
Developer	Views all information for their assigned organization or application.	>
Application Evaluator	Evaluates applications and views policy violation summary results.	>
Component Evaluator	Evaluates individual components and views policy violation results for a specified application.	>
Legal Reviewer	Reviews legal obligations for component licenses.	>

# Roles – 預設角色 (2)

- 系統管理角色：
  - System Administrator：管理系統設定和使用者的使用者，其中包括 LDAP 和產品授權管理，以及將其他使用者設定為系統管理員角色的能力。
  - Policy Administrator：提供對組織、應用程式、策略、策略違規和自定義角色的完全控制。
- 組織管理角色：
  - Owner：管理分配的組織、應用程式、策略和違反策略的情況。
  - Developer：查看為其設定的組織或應用程式的所有資訊。
  - Application Evaluator：通過 CI 整合掃描應用程式的最低權限。評估應用程式並查看 CI 中的策略違規摘要結果。
  - Component Evaluator：評估單個組件並查看 IDE 整合中指定應用程式的策略違規結果。
  - Legal Reviewer：審查套件許可的法律義務。

# Roles - Permissions

## Permissions

### Administrator

☒ View all roles

### IQ

☒ Edit proprietary components

☒ Claim components

☒ Edit iq elements

☒ View iq elements

☒ Edit access control

☒ Evaluate applications

☒ Evaluate individual components

☒ Add applications

☒ Manage automatic application creation

☒ Manage automatic source control configuration

### Remediation

☒ Waive policy violations

☒ Change licenses

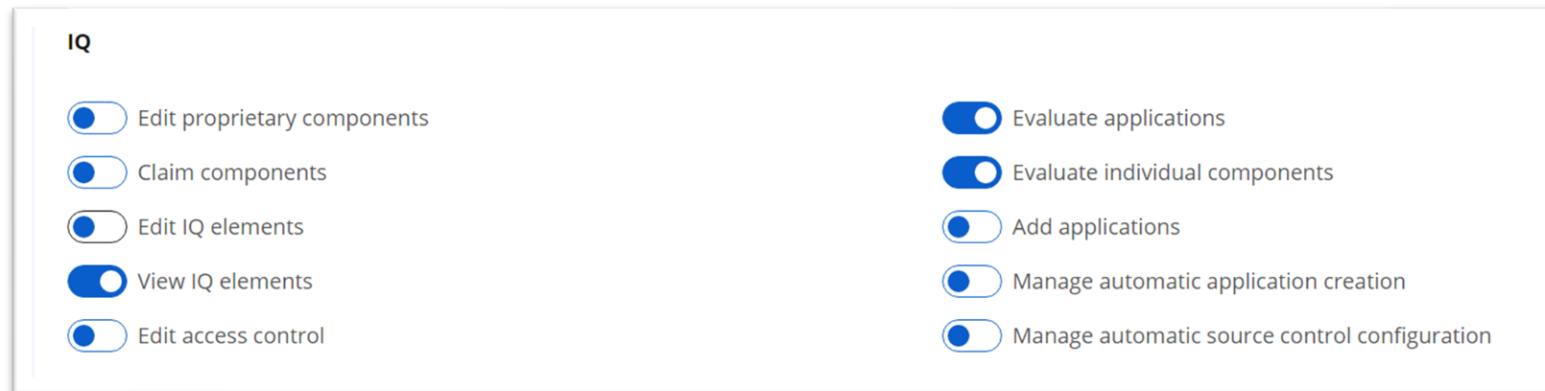
☒ Change security vulnerabilities

☒ Review legal obligations for components licenses



# Roles – Permissions (2)

- 舉例：開發人員角色權限
  - Evaluate Application：允許使用者評估應用程式的套件狀態。
  - Evaluate Individual Components：允許使用者評估單個套件，應用在IDE插件及Chrome擴充元件的評估功能。
  - View IQ Elements：允許使用者可瀏覽被授予權限的組織、應用程式及掃描報告。



The image shows a configuration panel titled "IQ" with two columns of toggle switches. The left column contains five switches, and the right column contains five switches. The switches are labeled as follows:

Left Column	Right Column
<input type="checkbox"/> Edit proprietary components	<input checked="" type="checkbox"/> Evaluate applications
<input type="checkbox"/> Claim components	<input checked="" type="checkbox"/> Evaluate individual components
<input type="checkbox"/> Edit IQ elements	<input type="checkbox"/> Add applications
<input checked="" type="checkbox"/> View IQ elements	<input type="checkbox"/> Manage automatic application creation
<input type="checkbox"/> Edit access control	<input type="checkbox"/> Manage automatic source control configuration



# 政策管理

# Policy Management 簡介

- 靈活管理風險
- 依企業風險承受度設定政策
- 選擇更好的套件

# Sonatype風險分類

- Security
  - 此安全漏洞可能有被利用的風險。
- License
  - 來自授權義務的法律風險，例如GPL授權將要求揭露源始碼。
- Quality
  - 來自低品質的套件風險，例如發佈時間的遠近、熱門程度。
- Other
  - 其他各類型的風險，例如套件匹配程度、套件類別。

# Policy - 合規政策

在 Lifecycle 中的 Policy 是用來自動識別整個企業中套件風險的規則。在您閱讀的掃描報告中，以及整個開發生命週期的各個階段提供您套件風險程度，並可依賴其執行強制合規。在首次啟動 Nexus Lifecycle 時，會自動載入一套已包括安全、套件類別、授權等的規則。可以在後續的應用中，因地制宜的調整它。

Policies					
	NAME	PROXY	DEVEL...	SOURCE	BUILD
Local to Root Organization					
10	Security-Namespace Conflict	Fail	—	—	—
10	Security-Malicious	—	—	—	—
10	Security-Critical	—	—	—	—
10	License-Banned	—	—	—	—
9	Security-High	—	—	—	—
9	License-None	—	—	—	—
9	Integrity-Rating	Fail	—	—	—
8	License-Copyleft	—	—	—	—
7	Security-Medium	—	—	—	—

# Policy - Summary

Policy 名稱應描述您嘗試檢測的風險或違規行為。您輸入的名稱用於標識 IQ Server 報告中的策略。為避免系統層次結構混亂，建議您為每個策略設定一個專有名稱；盡量不要在不同組織中建立相同的策略名稱。

SUMMARY

Policy Name

License-Banned

Threat Level

10

Policy Violation Grandfathering

☐ Allow this policy to be grandfathered

威脅級別 (Threat Level) 是對違反政策所帶來風險的主觀價值。其主要目的是對 IQ Server 報告中的策略違規進行排序；威脅級別最高的違規行為會首先出現，然後是威脅級別較低的違規行為。威脅級別值按嚴重性分組並由特定顏色標識。

Critical	紅色	8-10	10
Severe	橘色	4-7	9
Moderate	黃色	2-3	8
Low	深藍色	1	7
None	淺藍色	0	6

# Policy - Inheritance

當有多個應用程式  
( Application ) 附加到某個組織  
( Organization ) 時如何實施策  
略呢？

## INHERITANCE

### This Policy Inherits to

- ☒ All Applications and Repositories
- ☐ Applications of the specified Application Categories in Root Organization

以下有兩種選擇：

- **All Applications and Repositories**
  - 該策略應用於此層次結構級別以下的每個應用程式和儲存庫。
- **Applications of the specified Application Categories in Root Organization**
  - 該策略僅適用於分配了特定類別的應用程式。通過此設置，您可以選擇要使用的類別。

第二種選擇可以讓您藉由使用應用程式類別，對具有相似特徵的應用程式定製策略的實施。

## Application Categories

available to apps in Root Organization

### LOCAL

#### Distributed

Applications that are provided for consumption outside the company

#### Hosted

Applications that are hosted such as services or software as a service.

#### Internal

Applications that are used only by your employees

# Policy - Constraint

定義您要檢測的違規行為。如果 any (任一) 或 all (所有) 條件為真，則滿足此項目的規則。在策略中可以多個條件以 OR 來結合使用，因此如果違反該策略中的任何一個項目，則違反該策略。

※未知套件只有 Match State, Proprietary 及 Data Source 三種條件可以比對，其他條件因為套件不存在任何資訊，所以條件永遠不會成立。

### CONSTRAINTS

**Constraint Name**  
License not approved in any s

**Conditions**  
This constraint is in violation if  
any of the following are true:  
License Threat Group is Banned  
[+ Add Condition](#)

[+ Add Constraint](#)



# Policy - Constraint - Condition - Security

Condition	Type	Description
Security Vulnerability Severity	Security	驗證套件如有安全漏洞，且其嚴重性級別值是否 = 、< 、<= 、> 或 >= 指定的數值。
Security Vulnerability Status	Security	驗證套件的安全漏洞狀態是否為以下值之一： Open, Acknowledged, Not Applicable, Confirmed.
Proprietary Name Conflict	Security	確定 Proxy Repository 中的套件名稱是否與 Hosted 中任何企業內部獨有的套件名稱相同。請注意，此策略條件僅與 Nexus Firewall 和 Proxy 階段相關。
Security Vulnerability Category	Security	驗證安全漏洞類別是否為指定類別。 Data - 該漏洞利用涉及攻擊者發送受污染的請求。 Operational - 該套件參與網路服務器的操作。 Functional - 影響套件的特定部分，該部分不是套件操作的組成部分。 Configuration - 取決於套件實現的特定配置。 Test Code - 該漏洞位於產品不需要的測試代碼中。 Sample Code - 該漏洞位於套件隨附的範例中。 Privileged - 攻擊者需要提升特權級別才能利用。 Malicious Code - 套件嵌入了惡意代碼。 Other - 不在上述類別中。

# Policy - Constraint - Condition - License

Condition	Type	Description
License	License	驗證套件是否為指定的授權方式。
License Status	License	驗證使用者定義的授權狀態是否為以下值之一： Open - 預設狀態； Acknowledged - 表示該套件的授權方式正在研究中； Overridden - 允許您選擇另一種授權方式，將覆蓋原有設定； Selected - 允許新增您觀察到此套件的其他授權方式； Confirmed - 表示確認目前的授權方式是正確的
License Threat Group	License	驗證套件的授權方式是否在已定義的授權威脅組別中。特殊值 [unassigned] 可用於檢查是否不屬於任何授權威脅組別，即表示未知風險。
License Threat Group Level	License	驗證套件在授權威脅組別的級別是否 $\leq$ 、或 $\geq$ 指定的威脅級別值。

# Policy - Constraint - Condition - Quality

Condition	Type	Description
Age	Quality	驗證套件是否為 older than 、younger than 指定的值 (年、月、週、日)
Hygiene Rating	Quality	開源項目的品質等級是否為以下之一： Laggard - 落後 Exemplar - 典範
Integrity Rating	Quality	驗證套件的完整性(可疑程度)等級是否為以下之一： Normal - 正常 Suspicious - 可疑的 Malicious - 含有惡意代碼
Relative Popularity (Percentage)	Quality	驗證套件版本的相對流行度（與同一套件的其他版本相比）是否為 = 、< 、<= 、> 或 >= 到指定的百分比值。



# Policy - Constraint - Condition - Other

Condition	Type	Description
Label	Other	驗證套件標籤是否已被設定。
Match State	Other	驗證套件與已知套件是否匹配，驗證值如下： Exact、Similar、Unknown。
Format	Other	驗證套件是否為指定格式。例如：npm、maven 等
Coordinates	Other	驗證套件是否匹配 Maven、A-Name 或 PyPI 坐標。對於每種類型的坐標，您可以輸入特定的屬性。您可以在屬性末尾使用萬用字元 (*) 來擴大搜索範圍。
Package URL	Other	驗證套件是否與指定的套件 URL 匹配。您可以在可選屬性的末尾使用萬用字元 (*) 來擴大搜索範圍。
Proprietary	Other	驗證套件是否為企業內部獨有的套件。

# Policy - Constraint - Condition - Other (2)

Condition	Type	Description
Identification Source	Other	驗證套件的標識是否為以下之一： Sonatype - 當辨識資料來自於 IQ Server 時 Manual - 當辨識資料來自於自行定義的套件時 Clair - 根據 Clair Scanner 的辨識結果 *Container scan tool Package Manifest -當辨識資料來自於清單文件掃描時
Component Category	Other	驗證套件類別是否為指定類別值。 例如：Console、File Utilities、Gaming、GUI等。
Data Source	Other	驗證找到套件資訊內容是否支援以下項目之一： Identify、License
Dependency Type	Other	驗證套件相依類型是否如下： Direct - 當確定在應用程式或專案中形成依賴關係時； Transitive - 當從另一個套件加入依賴關係時； InnerSource - 當直接依賴項被確定為內部開發的模組。

# Policy Action

Actions							
	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
 Warn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 Fail	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

允許您指定在開發生命週期的特定階段發生違規時要採取的操作。

- No Action - 預設，無任何處理動作。
- Warn - 違反此策略時會出現警示訊息。
- Fail - 違反此策略的嚴重程度須停止該階段的開發動作。

如果您使用外部工具連接了 IQ Server，則該操作會直接影響該工具。當外部工具請求（應用程式、儲存庫或套件的）策略評估時，IQ Server 會提供策略違規信息以及該工具可能（或可能不）實施的操作。例如，如果您在策略中將 Build 階段設置為 Fail，則 CI 工具可能會在違反該策略時停止應用程序的構建。同樣，在不同的工具中，如果您將階段設置為警告，則在發生策略違規時，可能會顯示警告消息或將警告消息記錄在文件中。有關使用操作的更多詳細信息，請參閱每個階段的使用建議。

# Policy - Notification

NOTIFICATIONS									
RECIPIENT	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE	CONTINUO... MONITORING	
✉ nxrm.admin@sonatype.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	🗑
✉ developer@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	🗑
✉ repo.owner@sonatype.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	🗑
✉ release.mgr@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	🗑
✉ app.owner@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	🗑

Recipient Type

Email

Email Address

+ Add

發送通知時，它只會顯示在最新評估中發現的新違規行為。如果您發現自己沒有收到通知，請確認是否存在新的違規行為。

# Policy Management 簡介

- 靈活管理風險
- 依企業風險承受度設定政策
- 選擇更好的套件



# Sonatype風險分類

- Security
  - 此安全漏洞可能有被利用的風險。
- License
  - 來自授權義務的法律風險，例如GPL授權將要求揭露源始碼。
- Quality
  - 來自低品質的套件風險，例如發佈時間的遠近、熱門程度。
- Other
  - 其他各類型的風險，例如套件匹配程度、套件類別。

# Policy - 合規政策

在 Lifecycle 中的 Policy 是用來自動識別整個企業中套件風險的規則。在您閱讀的掃描報告中，以及整個開發生命週期的各個階段提供您套件風險程度，並可依賴其執行強制合規。在首次啟動 Nexus Lifecycle 時，會自動載入一套已包括安全、套件類別、授權等的規則。可以在後續的應用中，因地制宜的調整它。

Policies					
	NAME	PROXY	DEVEL...	SOURCE	BUILD
Local to Root Organization					
10	Security-Namespace Conflict	Fail	—	—	—
10	Security-Malicious	—	—	—	—
10	Security-Critical	—	—	—	—
10	License-Banned	—	—	—	—
9	Security-High	—	—	—	—
9	License-None	—	—	—	—
9	Integrity-Rating	Fail	—	—	—
8	License-Copyleft	—	—	—	—
7	Security-Medium	—	—	—	—

# Policy - Summary

Policy 名稱應描述您嘗試檢測的風險或違規行為。您輸入的名稱用於標識 IQ Server 報告中的策略。為避免系統層次結構混亂，建議您為每個策略設定一個專有名稱；盡量不要在不同組織中建立相同的策略名稱。

SUMMARY

Policy Name

License-Banned

Threat Level

10

Policy Violation Grandfathering

☐ Allow this policy to be grandfathered

威脅級別 (Threat Level) 是對違反政策所帶來風險的主觀價值。其主要目的是對 IQ Server 報告中的策略違規進行排序；威脅級別最高的違規行為會首先出現，然後是威脅級別較低的違規行為。威脅級別值按嚴重性分組並由特定顏色標識。

Critical	紅色	8-10	10
Severe	橘色	4-7	9
Moderate	黃色	2-3	8
Low	深藍色	1	7
None	淺藍色	0	6
			5
			4
			3
			2
			1
			0

# Policy - Inheritance

當有多個應用程式  
( Application ) 附加到某個組織  
( Organization ) 時如何實施策略呢？

## INHERITANCE

### This Policy Inherits to

- ☒ All Applications and Repositories
- ☐ Applications of the specified Application Categories in Root Organization

以下有兩種選擇：

- **All Applications and Repositories**
  - 該策略應用於此層次結構級別以下的每個應用程式和儲存庫。
- **Applications of the specified Application Categories in Root Organization**
  - 該策略僅適用於分配了特定類別的應用程式。通過此設置，您可以選擇要使用的類別。

第二種選擇可以讓您藉由使用應用程式類別，對具有相似特徵的應用程式定製策略的實施。

## Application Categories

available to apps in Root Organization

### LOCAL

#### Distributed

Applications that are provided for consumption outside the company

#### Hosted

Applications that are hosted such as services or software as a service.

#### Internal

Applications that are used only by your employees

# Policy - Constraint

定義您要檢測的違規行為。如果 any (任一) 或 all (所有) 條件為真，則滿足此項目的規則。在策略中可以多個條件以 OR 來結合使用，因此如果違反該策略中的任何一個項目，則違反該策略。

※未知套件只有 Match State, Proprietary 及 Data Source 三種條件可以比對，其他條件因為套件不存在任何資訊，所以條件永遠不會成立。

### CONSTRAINTS

**Constraint Name**  
License not approved in any s

**Conditions**  
This constraint is in violation if  
any of the following are true:  
License Threat Group is Banned  
[+ Add Condition](#)

[+ Add Constraint](#)

# Policy - Constraint - Condition - Security

Condition	Type	Description
Security Vulnerability Severity	Security	驗證套件如有安全漏洞，且其嚴重性級別值是否 = 、< 、<= 、> 或 >= 指定的數值。
Security Vulnerability Status	Security	驗證套件的安全漏洞狀態是否為以下值之一： Open, Acknowledged, Not Applicable, Confirmed.
Proprietary Name Conflict	Security	確定 Proxy Repository 中的套件名稱是否與 Hosted 中任何企業內部獨有的套件名稱相同。請注意，此策略條件僅與 Nexus Firewall 和 Proxy 階段相關。
Security Vulnerability Category	Security	驗證安全漏洞類別是否為指定類別。 Data - 該漏洞利用涉及攻擊者發送受污染的請求。 Operational - 該套件參與網路服務器的操作。 Functional - 影響套件的特定部分，該部分不是套件操作的組成部分。 Configuration - 取決於套件實現的特定配置。 Test Code - 該漏洞位於產品不需要的測試代碼中。 Sample Code - 該漏洞位於套件隨附的範例中。 Privileged - 攻擊者需要提升特權級別才能利用。 Malicious Code - 套件嵌入了惡意代碼。 Other - 不在上述類別中。

# Policy - Constraint - Condition - License

Condition	Type	Description
License	License	驗證套件是否為指定的授權方式。
License Status	License	驗證使用者定義的授權狀態是否為以下值之一： Open - 預設狀態； Acknowledged - 表示該套件的授權方式正在研究中； Overridden - 允許您選擇另一種授權方式，將覆蓋原有設定； Selected - 允許新增您觀察到此套件的其他授權方式； Confirmed - 表示確認目前的授權方式是正確的
License Threat Group	License	驗證套件的授權方式是否在已定義的授權威脅組別中。特殊值 [unassigned] 可用於檢查是否不屬於任何授權威脅組別，即表示未知風險。
License Threat Group Level	License	驗證套件在授權威脅組別的級別是否 $\leq$ 、或 $\geq$ 指定的威脅級別值。

# Policy - Constraint - Condition - Quality

Condition	Type	Description
Age	Quality	驗證套件是否為 older than 、younger than 指定的值 (年、月、週、日)
Hygiene Rating	Quality	開源項目的品質等級是否為以下之一： Laggard - 落後 Exemplar - 典範
Integrity Rating	Quality	驗證套件的完整性(可疑程度)等級是否為以下之一： Normal - 正常 Suspicious - 可疑的 Malicious - 含有惡意代碼
Relative Popularity (Percentage)	Quality	驗證套件版本的相對流行度（與同一套件的其他版本相比）是否為 = 、< 、<= 、> 或 >= 到指定的百分比值。





# Policy - Constraint - Condition - Other

Condition	Type	Description
Label	Other	驗證套件標籤是否已被設定。
Match State	Other	驗證套件與已知套件是否匹配，驗證值如下： Exact、Similar、Unknown。
Format	Other	驗證套件是否為指定格式。例如：npm、maven 等
Coordinates	Other	驗證套件是否匹配 Maven、A-Name 或 PyPI 坐標。對於每種類型的坐標，您可以輸入特定的屬性。您可以在屬性末尾使用萬用字元 (*) 來擴大搜索範圍。
Package URL	Other	驗證套件是否與指定的套件 URL 匹配。您可以在可選屬性的末尾使用萬用字元 (*) 來擴大搜索範圍。
Proprietary	Other	驗證套件是否為企業內部獨有的套件。

# Policy - Constraint - Condition - Other (2)

Condition	Type	Description
Identification Source	Other	驗證套件的標識是否為以下之一： Sonatype - 當辨識資料來自於 IQ Server 時 Manual - 當辨識資料來自於自行定義的套件時 Clair - 根據 Clair Scanner 的辨識結果 *Container scan tool Package Manifest -當辨識資料來自於清單文件掃描時
Component Category	Other	驗證套件類別是否為指定類別值。 例如：Console、File Utilities、Gaming、GUI等。
Data Source	Other	驗證找到套件資訊內容是否支援以下項目之一： Identify、License
Dependency Type	Other	驗證套件相依類型是否如下： Direct - 當確定在應用程式或專案中形成依賴關係時； Transitive - 當從另一個套件加入依賴關係時； InnerSource - 當直接依賴項被確定為內部開發的模組。

# Policy Action

Actions							
	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
 Warn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 Fail	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

允許您指定在開發生命週期的特定階段發生違規時要採取的操作。

- No Action - 預設，無任何處理動作。
- Warn - 違反此策略時會出現警示訊息。
- Fail - 違反此策略的嚴重程度須停止該階段的開發動作。

如果您使用外部工具連接了 IQ Server，則該操作會直接影響該工具。當外部工具請求（應用程式、儲存庫或套件的）策略評估時，IQ Server 會提供策略違規信息以及該工具可能（或可能不）實施的操作。例如，如果您在策略中將 Build 階段設置為 Fail，則 CI 工具可能會在違反該策略時停止應用程序的構建。同樣，在不同的工具中，如果您將階段設置為警告，則在發生策略違規時，可能會顯示警告消息或將警告消息記錄在文件中。有關使用操作的更多詳細信息，請參閱每個階段的使用建議。

# Policy - Notification

NOTIFICATIONS									
RECIPIENT	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE	CONTINUO... MONITORING	
✉ nxrm.admin@sonatype.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	🗑
✉ developer@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	🗑
✉ repo.owner@sonatype.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	🗑
✉ release.mgr@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	🗑
✉ app.owner@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	🗑

Recipient Type

Email ▼

Email Address

+ Add

發送通知時，它只會顯示在最新評估中發現的新違規行為。如果您發現自己沒有收到通知，請確認是否存在新的違規行為。



# 預設合規政策

# Default Policies - Security

Threat Level	Name	Constraints	Description
10	Security-Critical	Critical risk CVSS score ( $9 \leq n$ )	CVSS 評分 $\geq 9$
10	Security-Malicious	Malicious vulnerability category	該套件被嵌入了惡意代碼。
10	Security-Namespace Conflict	3rd-party component name conflicts with proprietary component name	第三方套件名稱與企業內部開發的套件名稱衝突。
9	Security-High	High risk CVSS score ( $7 \leq n < 9$ )	CVSS 評分 $7 \leq n < 9$
7	Security-Medium	Medium risk CVSS score ( $4 \leq n < 7$ )	CVSS 評分 $4 \leq n < 7$
3	Security-Low	Low risk CVSS score ( $0 \leq n < 4$ )	CVSS 評分 $0 \leq n < 4$

# Default Policies - License

Threat Level	Name	Constraints	Description
10	License-Banned	License not approved in any situation	任何情況下不應允許的授權方式。
9	License-None	1.No source available; nothing declared	Sonatype 找不到套件的來源，且套件的作者/開發人員未聲明任何內容
		2.No licenses in supplied source; nothing declared	在來源中找不到授權資訊，且套件的作者/開發人員未聲明任何內容
		3. Contact Sonatype Support - observed license issue: Not Provided	授權方式為空，且套件的作者/開發人員未聲明任何內容
		4. Contact Sonatype Support - declared license issue: Not Provided NS	Sonatype 找不到套件的來源，且套件的作者/開發人員未聲明任何內容
		5. Contact Sonatype Support - declared license issue: Not Provided NSL	在來源中找不到授權資訊，且授權方式為空
		6. Source license not available; no declaration available	Sonatype 或目標生態系統目前不支援這種型式，且套件的作者/開發人員未聲明任何內容
		7. Contact Sonatype Support - declared license issue: Not Provided	授權方式為空，且Sonatype 或目標生態系統目前不支援這種型式

# Default Policies - License (2)

Threat Level	Name	Constraints	Description
8	License-Copyleft	License containing Copyleft terms detected	檢測到包含 Copyleft 條款的授權方式。
7	License-AI-ML	License Threat Group is AI-ML	檢測到包含 AI/ML 工具相關的授權方式。
7	License-Commercial	License containing commercial terms detected	檢測到包含商業條款的授權方式。
7	License-Threat Not Assigned	License threat group has not been assigned	檢測到不屬於任何授權威脅組別，即表示未知風險。
5	License-Modified Weak Copyleft	Modified source code & license containing Weak Copyleft terms detected...	檢測到包含弱 Copyleft 條款的授權方式，以及源代碼已被修改。
5	License-Non Standard	License containing non standard terms detected. Legal review required.	檢測到包含非標準條款的授權方式。需要進行法務審查。



# Default Policy - Quality

Threat Level	Name	Constraints	Description
9	Integrity-Rating	1.Pending integrity rating	由Sonatype Intelligence判定該版本的可疑程度為-暫無結果。
		2.Suspicious integrity rating	由Sonatype Intelligence判定該版本的可疑程度為-可疑的。
1	Architecture-Quality	Version age older than 5 Years	套件發佈已超過 5 年。

# Default Policies - Other

Threat Level	Name	Constraints	Description
7	Component-Similar	Unknown modification to component	在已知的套件上進行未知的修改。
2	Component-Unknown	Unknown 3rd party component	未知的第三方套件。
1	Architecture-Cleanup	Test components	檢測到屬於測試階段的套件。

# Default Policies - Application Category

Threat Level	Name	Type	Application Categories		
			Distributed	Hosted	Internal
10	License-Banned	License	⊙	⊙	⊙
10	Security-Critical	Security	⊙	⊙	⊙
10	Security-Malicious	Security	⊙	⊙	⊙
10	Security-Namespace Conflict	Security	⊙	⊙	⊙
9	Integrity-Rating	Quality	⊙	⊙	⊙
9	License-None	License	⊙	⊙	
9	Security-High	Security	⊙	⊙	⊙
8	License-Copyleft	License	⊙		
7	Component-Similar	Other	⊙	⊙	⊙
7	License-AI-ML	License	⊙		

# Default Policies - Application Category (2)

Threat Level	Name	Type	Application Categories		
			Distributed	Hosted	Internal
7	License-Commercial	License	⊙	⊙	
7	License-Threat Not Assigned	License	⊙	⊙	⊙
7	Security-Medium	Security	⊙	⊙	⊙
5	License-Modified Weak Copyleft	License	⊙	⊙	⊙
5	License-Non Standard	License	⊙		
3	Security-Low	Security	⊙	⊙	⊙
2	Component-Unknown	Other	⊙	⊙	⊙
1	Architecture-Cleanup	Other	⊙	⊙	⊙
1	Architecture-Quality	Quality	⊙	⊙	⊙

The background features a series of concentric circles and a spiral pattern in various shades of blue and teal. The spiral starts from the center and expands outwards, creating a sense of depth and movement. The text is positioned on the right side of the image, overlaid on the background.

# 不溯及既往機制 Legacy Violation

# Legacy Violations

- 針對既有的應用程式，在導入初期可能面對大量違反策略的情形，可以針對某些政策違規的項目設定 Legacy Violation 機制，將不會被視為主動違規，也不會顯示威脅級別，如有需要，還可以撤銷 Legacy Violation 機制，恢復為正常的違反策略行為。

※預設情況下，在啟用Legacy Violation時，不會開啟Policy嚴重程度為8到10的項目。

# Legacy violation enabled

The image displays two screenshots of the 'webgoat Build Report' interface, illustrating the impact of enabling legacy violations.

**Left Screenshot (2024-09-06):**

- Report Title: webgoat Build Report
- Triggered by: Web UI (Re-evaluation) on 2024-09-06 11:00:48 UTC+0800
- Summary: 49 (red), 83 (orange), 3 (yellow) icons. 135 VIOLATIONS Affecting 34 components. 183 COMPONENTS 99% of all components identified. 0 LEGACY VIOLATIONS.
- Aggregate by component: ☒
- Table Headers: THREAT, POLICY, COMPONENT
- Table Content (highlighted row):

THREAT	POLICY	COMPONENT
7	Security-Medium	jquery 3.5.1

**Right Screenshot (2024-09-17):**

- Report Title: webgoat Build Report
- Triggered by: Web UI (Re-evaluation) on 2024-09-17 22:15:58 UTC+0800
- Summary: 54 (red), 83 (orange), 3 (yellow) icons. 54 VIOLATIONS Affecting 20 components. 183 COMPONENTS 99% of all components identified. 132 LEGACY VIOLATIONS.
- Aggregate by component: ☒
- Table Headers: THREAT, POLICY, COMPONENT
- Table Content (highlighted row):

THREAT	POLICY	COMPONENT
0	None	jquery 3.4.1
- Legacy Violation Detail: A yellow box highlights the 'Legacy' link and icon for the 'jquery 3.4.1' component.

Yellow arrows indicate the flow of information: from the summary section of the first report to the summary of the second, and from the specific component row in the first report to the detailed legacy violation view in the second.

# Legacy violation 設定與啟用

## Edit Policy

### Summary

**Policy Name \***

Security-Medium

7 - Severe

### Legacy Violations

Eligible violations will be reported but will not trigger actions

☒ Allow violations of this policy to be granted legacy status

### Inheritance

**This Policy Inherits to: \***

☒ All Applications and Repositories

☐ Applications of the specified Application Categories in Root Organization

**Inheritance Overrides**

☐ Allow action overrides at organization, application and repositories levels

## webgoat (webgoat)

App Categories Policies Legacy Violations Continuous monitoring Proprietary Co

### Application Categories

assigned to webgoat

**Assigned**

No application categories assigned

### Policies

N... PROXY DEVE... SOUR... BUILD STAGE

Local to webgoat

No local policies defined

Actions

- App ID to Clipboard
- Select Contact
- Edit App Name / Icon
- Change App ID
- Move webgoat
- Delete webgoat
- Legacy existing violations
- Revoke legacy status
- Evaluate a File
- View source report
- View build report
- View stage report
- View release report
- View operate report





# 持續監控與通知管理

# 通知設定 - baseUrl

## Base URL

### Configure Base URL

This setting is required for features such as email, SCM, and Jira integration

**Base URL \***

*Example `http://nexus-iq-server.example.com/`*

 Delete Configuration

Cancel

Save Configuration

# 通知設定 - SMTP

## Email

To receive email notifications for events enter the details of your SMTP Server here. For further details see the [documentation](#).

### Hostname

### Port

### Username Optional

### Password Optional

### System Email

Hostname :

\*\*\*.\*\*\*.\*\*\*.\*\*\*

Port :

25

System Email :

nexus@sonatype

# 持續監控

- 持續監控是 Lifecycle 的一項強大功能，可定期檢查應用程式是否存在新的違規行為。
- 此功能主要是保持對已發布或部署且未處於編譯階段的應用程式的能見度。
- 您可以設定 Notification 功能以提醒特定個人或角色，但是只會在違規是新發生的情況下發出通知。
- 可以安排在特定時間執行。如果大量應用程式正在使用連續監控，則此功能需要更長的時間來完成工作（有時超過 24 小時）。

# 持續監控 – 設定通知對像

NOTIFICATIONS

RECIPIENT	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE	CONTINUO... MONITORING	
✉ nxrm.admin@sonatype.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✖
✉ developer@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✖
✉ repo.owner@sonatype.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✖
✉ release.mgr@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	✖
✉ app.owner@sonatype.com	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	✖

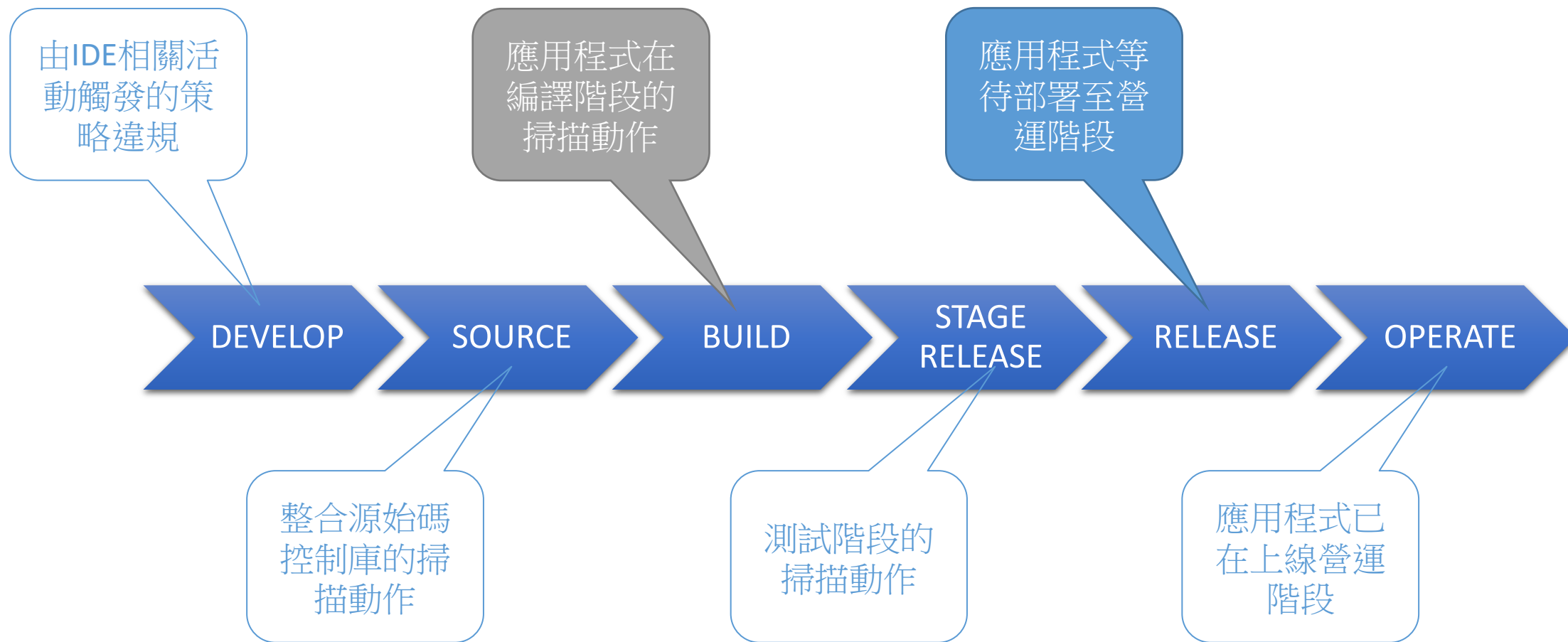
Recipient Type

Email


Email Address


+ Add


# 持續監控- 選擇監控目標





# 持續監控 – 設定監控目標


 nexus lifecycle





 Dashboard


 Orgs and Policies

 Reports


 Success Metrics


 Vulnerability Search

 Advanced Search


 Firewall


< Sandbox Organization


▶  Application Categories


▼  Policies


+ New Policy


 Policy Violation Grandfather...


 Continuous Monitoring


 Proprietary Components

▶  Component Labels

▶  License Threat Groups

 Source Control

▶  Access

 Continuous Monitoring

Each day the latest scan from this stage will be evaluated. Notifications for new violations can be configured per policy.

Monitoring Stage

☐ Inherit from Root Organization (Operate)

☐ Develop

☐ Source

☐ Build

☐ Stage Release

☒ Release

☐ Operate

Update



# 使用豁免功能 Waiver





# 決定接受不合規套件帶來的風險


- 如果不合規的套件無法更新、替換或是修復，則接受風險也可能是必要的。例如，修復可能超出預算，或者該應用程式不會再用進一步的開發動作 (legacy app)
- 以下幾種情境可適用：
  - 應用程式違反了license policy，但該應用程式僅在內部使用，因此license問題不適用
  - 應用程式違反了architectural policy，但它是legacy app，並且不合規套件無法刪除
  - 應用程式違反了security policy，但您已在應用程式的其他地方解決了該漏洞
- 最後，當您打算補救或以其他方式處理不合規套件時，但需要更多時間時，可以利用豁免功能。例如，開發人員可能估計將不合規組件替換為合規套件需要兩週時間。在這種情況下，可以設定此套件有兩週的豁免時效。


# Manage Waivers


- 在 Violation 的詳細資訊網頁，點擊 Manage Waivers

 **Violation of *Security-Critical***

 Sandbox Organization

 webgoat-server-8.2.2

 com.thoughtworks.x...

 0 Active Waivers

Threat Level

10

Policy Type

Security


First Reported


2 minutes ago


Last Reported


2 minutes ago


Stages

 Source


 Build

 Stage

 Release 2min

 Operate

Policy Owner

 Root Organization

Manage Waivers

# Waivers for Violation

## Waivers for Violation Security-Critical

### Violation Details

#### Constraint Name

Critical risk CVSS score

#### Conditions

Found security vulnerability CVE-2013-7285 with severity >= 9 (severity = 9.8)

#### Component Name

com.thoughtworks.xstream : xstream : 1.4.5

### Applicable Waivers

[Request Waiver](#)[+ Add Waiver](#)

DATE CREATED	SCOPE	COMPONENTS	WAIVER EXPIRATION	CREATED BY	COMMENTS
You don't have any waivers: to learn more about waivers you can check our <a href="#">help documentation</a> .					

- 檢視目前是否有設定任何 Waiver 項目
- 點擊 Request Waiver 可取得申請資訊
- 點擊 Add Waiver 設定豁免此漏洞

# Request Waiver

在申請豁免的網頁，會顯示豁免此漏洞的相關資訊，請將 Policy Violation ID、Policy Violation Detail Page 及 Curl Example 提供給管理人員。

請特別留意，Request Waiver 的動作並不會自動發送請求。

## Request Waiver

**i** To request a waiver, please share the Policy Violation ID and sample curl command (found below) with the approver. [Learn about automating waiver requests.](#)

### Component

com.thoughtworks.xstream : xstream : 1.4.5

### Policy

Security-Critical

### Constraint Name

Critical risk CVSS score

### Conditions

Found security vulnerability CVE-2013-7285 with severity >= 9 (severity = 9.8)

### Policy Violation ID

Copy to Clipboard

77fc5bbe47434684b06bbb84172c61fa

### Policy Violation Details Page

Copy to Clipboard

<http://localhost:8070/assets/#/violation/77fc5bbe47434684b06bbb84172c61fa>

### Curl Example

Copy to Clipboard

```
curl -X POST -u user:pass -H "Content-Type: text/plain; charset=UTF-8"
http://localhost:8070/api/v2/policyWaiver/77fc5bbe47434684b06bbb84172c61fa/applicati
on --data-binary 'waiver comment (optional)'
```

# Add Waiver

**Scope:** 選擇此 Waiver 僅影響當前的 application，或是要擴大範圍至整個組織，或是根組織(全系統)。

**Components:** 選擇此 Waiver 僅影響當前的套件版本，或是適用於全部套件(範圍依 Scope 所定)。

**Waiver Expiration:** 選擇此 Waiver 的到期時間。

需要Re-Evaluation才能生效

## Add Waiver

### Waiver Configuration

 **xstream**

com.thoughtworks.xstream : xstream : 1.4.5

### Policy

 **Security-Critical**

### Constraint Name

Critical risk CVSS score

### Conditions

Found security vulnerability CVE-2013-7285 with severity  $\geq 9$  (severity = 9.8)

[See Security Vulnerability Details](#)

### Scope

- ☒ Application - webgoat-server-8.2.2
- ☐ Organization - Sandbox Organization
- ☐ Organization - Root Organization

### Components

- ☒ com.thoughtworks.xstream : xstream : 1.4.5
- ☐ All Components

### Waiver Expiration

Never 

# Viewing Waivers

可使用 Filter 設定顯示 Waived 項目。

The image shows a 'Filter' panel with a list of filterable categories and their counts. The 'Violation State' category is expanded, showing several options. The 'Waived' option is selected and highlighted with a red rectangular box.

Filter	Count
Proprietary	2
InnerSource	2
Component Match State	3
Violation State	1 of 4
<input type="checkbox"/> all/none	
<input type="checkbox"/> Not Violating	
<input type="checkbox"/> Open	
<input checked="" type="checkbox"/> Waived	
<input type="checkbox"/> Grandfathered	
Dependency Type	3
Policy Types	4
Policy Threat Level	0 - 10

# Removing Waiver

## Waivers for Violation Security-Critical

### Violation Details

#### Constraint Name

Critical risk CVSS score

#### Conditions

Found security vulnerability CVE-2013-7285 with severity >= 9 (severity = 9.8)


#### Component Name

com.thoughtworks.xstream : xstream : 1.4.5

### Applicable Waivers

Request Waiver

+ Add Waiver

DATE CREATED	SCOPE	COMPONENTS	WAIVER EXPIRATION	CREATED BY	COMMENTS	
10/04/2022	Application - webgoat-server-8.2.2	com.thoughtworks.xstream : xstream : 1.4.5	in 3 months	Admin BuiltIn	--	

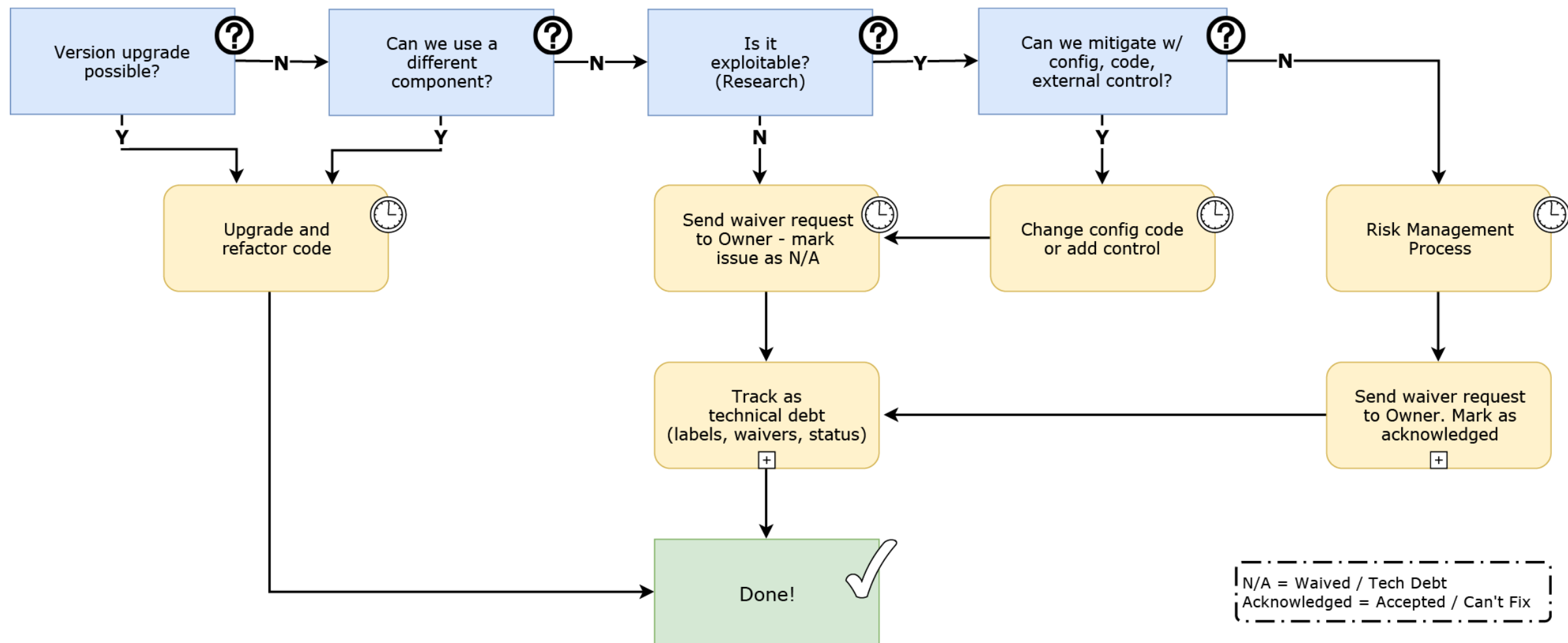
- 可在 Manage Waivers 畫面中，點擊垃圾桶圖示，將已設定的 Waiver 項目刪除。



# 弱點處理流程



# 流程範例



# Vulnerable vs. Exploitable

- 漏洞(vulnerability)是應用系統中的一個弱點。漏洞利用(exploit)是指利用該漏洞的攻擊。易受攻擊(vulnerable)意味著理論上存在一種利用(exploit)某些東西的方法（即存在漏洞）；攻擊者希望找到實際上可以利用的弱點。作為一名防守者，易受攻擊(vulnerable)並不好，但是更應該擔心被利用(exploitable)。
- 理論上易受攻擊(vulnerable)的弱點實際上無法利用(exploitable)的主要原因有幾個：
  - 可能沒有足夠的公共資訊使攻擊者能夠利用該漏洞。
  - 攻擊者可能沒有可利用的身份驗證或本地系統存取權限。
  - 現有的安全控制可能使其難以攻擊。
- 參考資料
  - [Vulnerable vs. Exploitable](#)

# Thank You

Contact Us



[www.systemx.com](http://www.systemx.com)

**SYSTEMX** 精誠集團