Galaxy Software Services

應用系統安全把關
從流程考量做起

主講人　資訊安全事業處
資安經理 郭俐佳

GSS 叡揚資訊
Galaxy Software Services

國家產業創新獎
卓越中堅企業

2018

大綱

AGENDA

- 應用系統的威脅
- 開發人員資安意識提升
- 第三方元件管控
- 傳統應用系統 VS 行動化應用系統
- 持續整合與部署平台
- 結論

國家產業創新獎

卓越中堅企業

Chapter

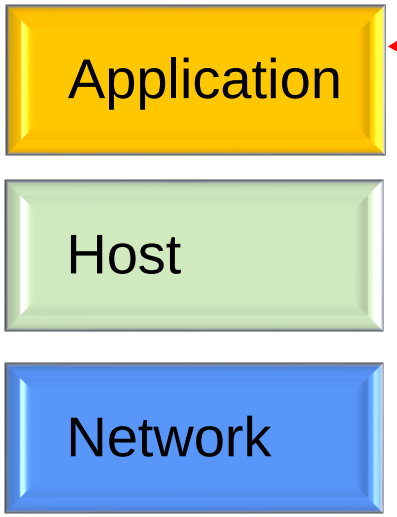
1

應用系統的威脅

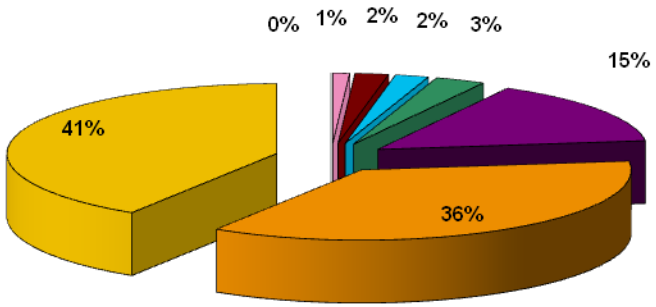
GSS 叡揚資訊
Galaxy Software Services
2018
UX
Cloud services
AI Bot DevOps
Big data SaaS
IOT Blockchain

應用系統的安全問題層出不窮

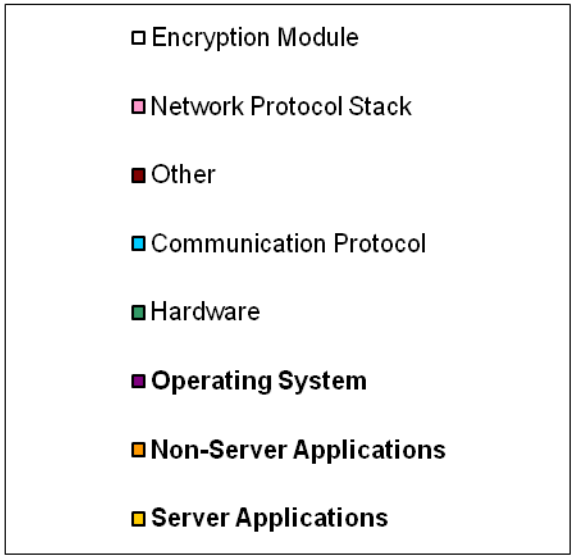
- Gartner
  - 75% of hacks occur at the application level
- NIST
  - 92% of reported vulnerabilities are in apps, not networks



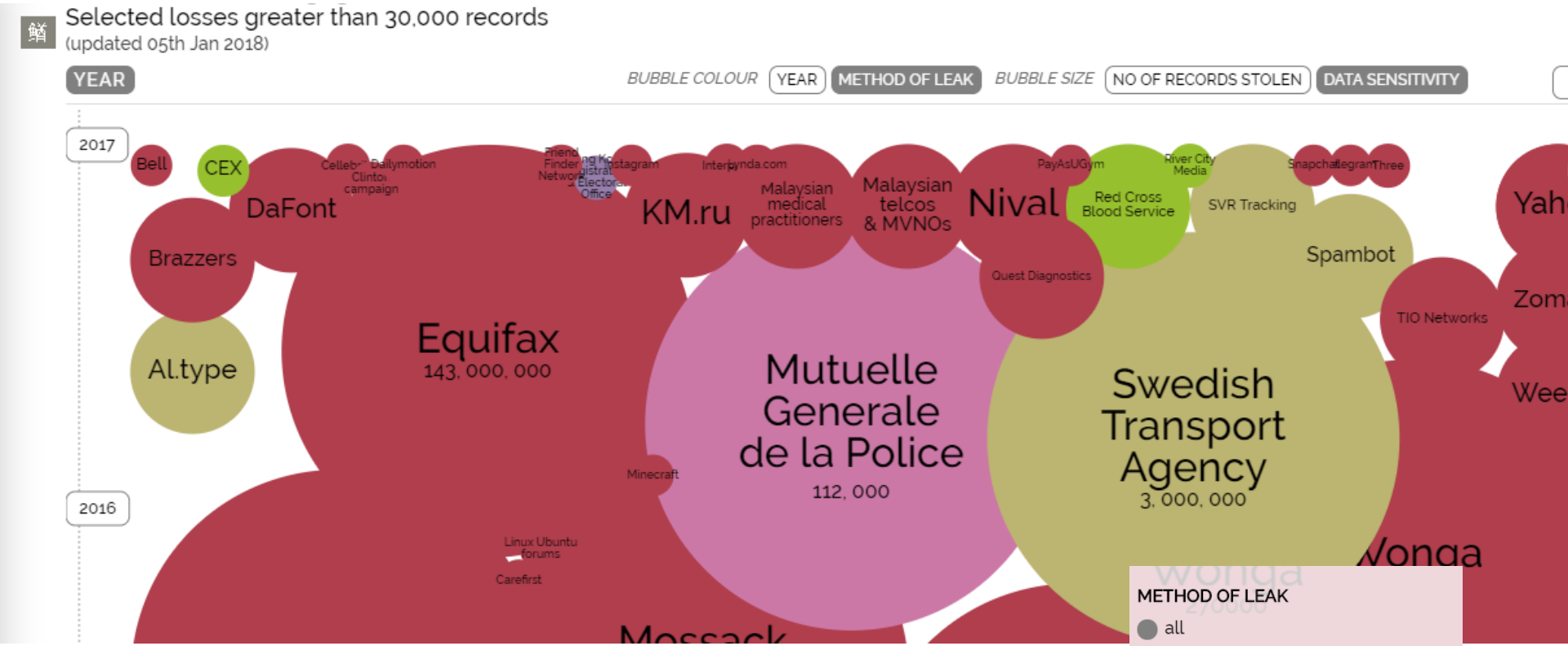
75% of hacks occur at the application level



Source: NIST

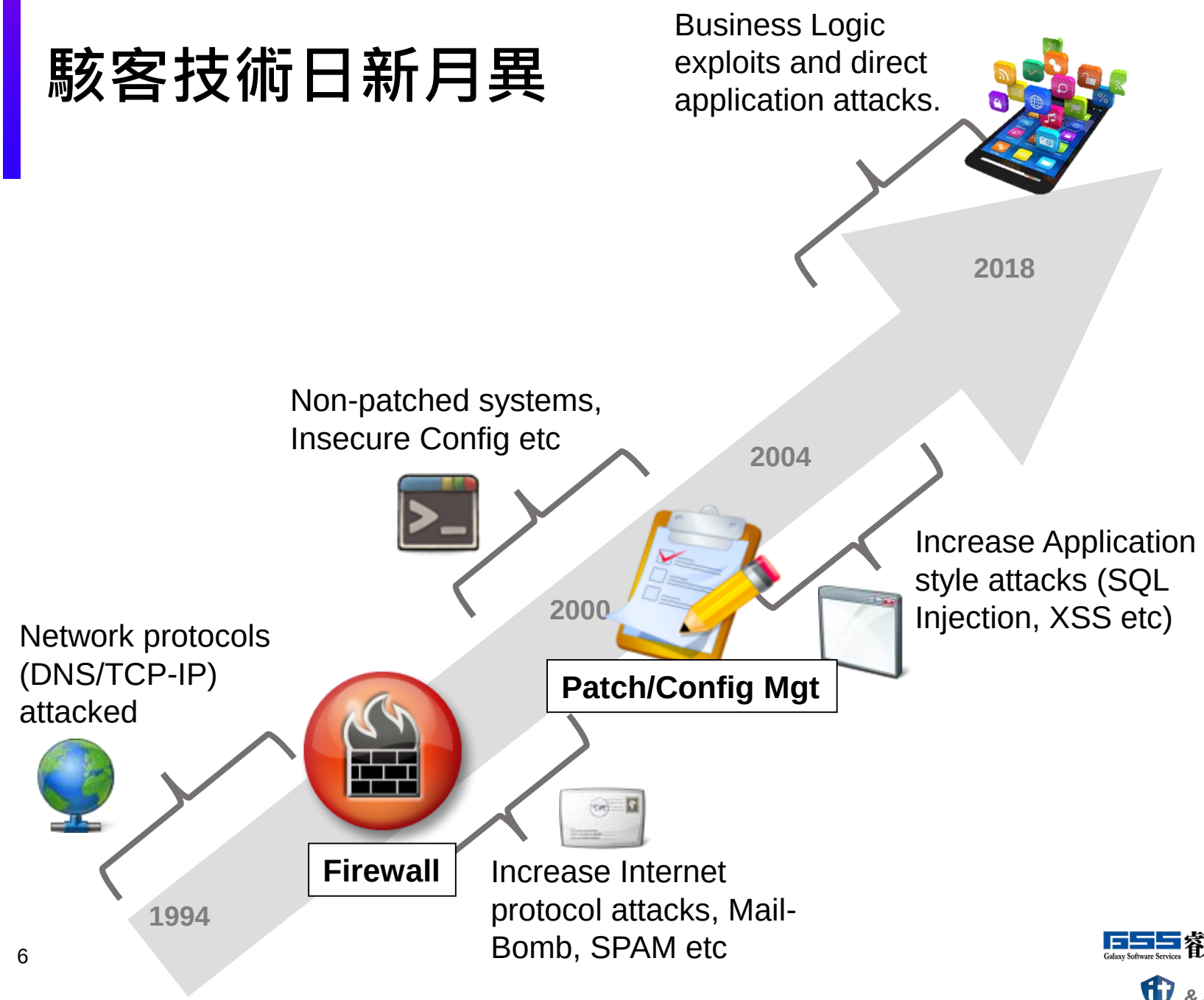


資安大數據



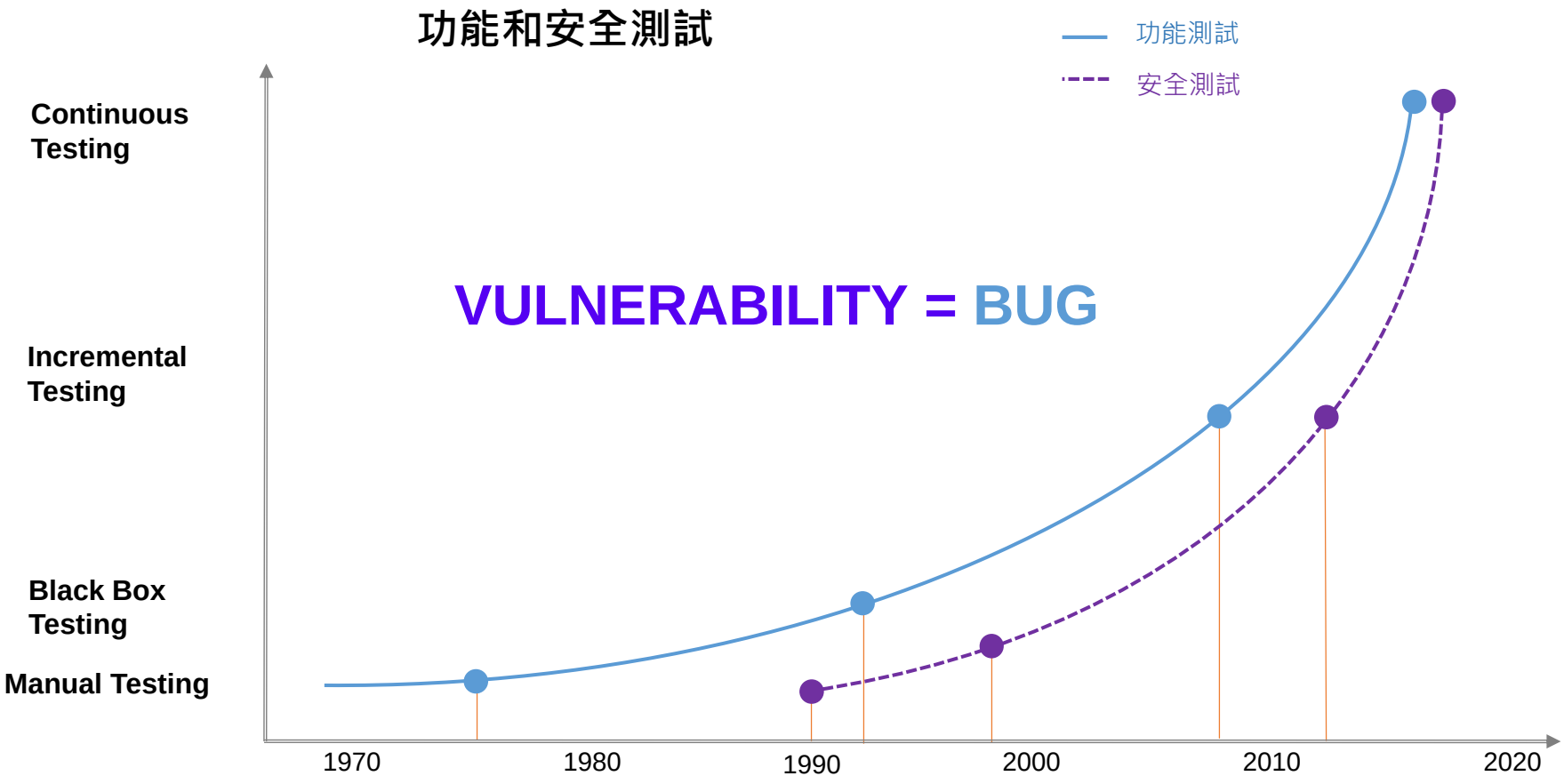
Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

駭客技術日新月異



GSS 叡揚資訊 Galaxy Software Services
& Security

測試方式的演進



GSS 叡揚資訊 Galaxy Software Services
& Security

OWASP Top 10 2017

- A1: Injection
- A2: Broken Authentication
- A3: Sensitive Data Exposure
- A4:XML External Entites (XXE)
- A5:Broken Access Control (As it was in 2004)
- A6:Security Mis-configuration
- A7: Cross-Site Scripting (XSS)
- A8: Insecure Deserialization
- A9: Using Components with Known Vulnerabilities
- A10: Insufficient Logging & Monitoring

GSS 叡揚資訊 Galaxy Software Services
IT & Security

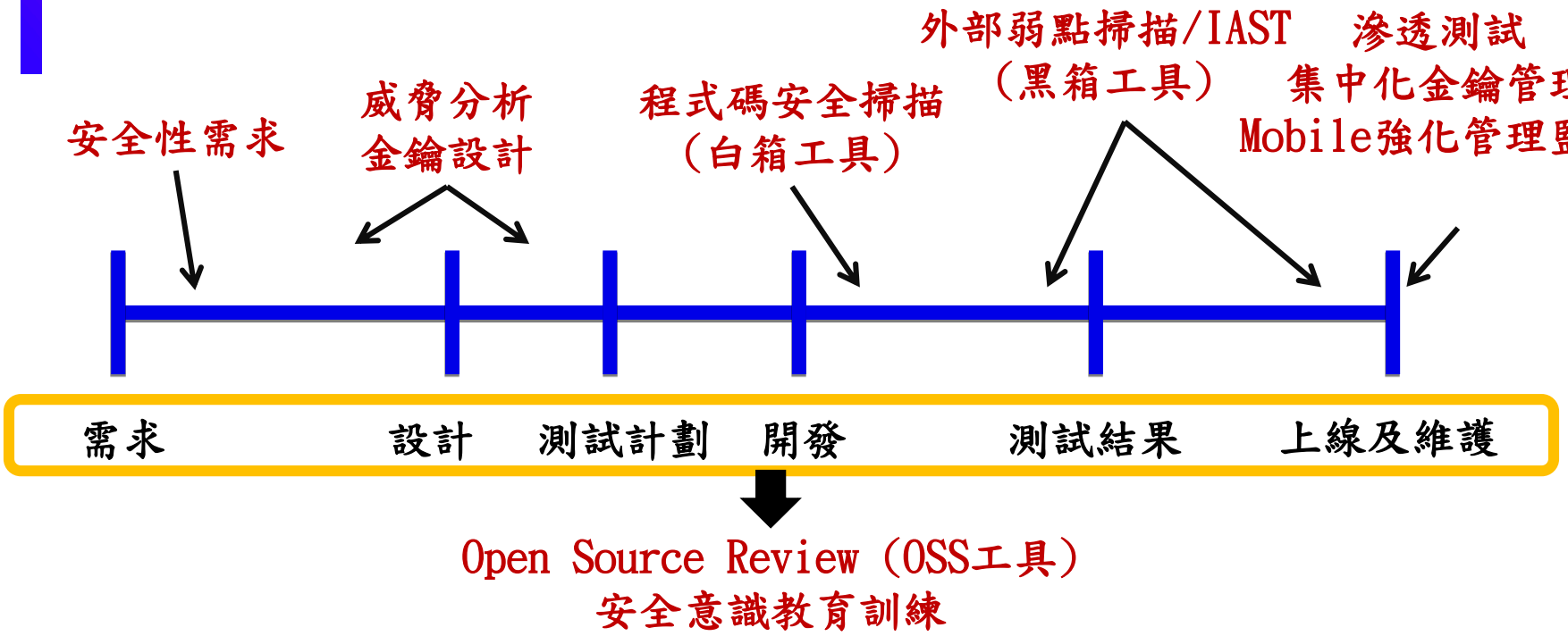
Mobile OWASP Top 10 Risk 2016

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M9: Reverse Engineering
- M10: Extraneous Functionality

How/When to fix?

GSS 叡揚資訊 Galaxy Software Services
IT & Security

遵循軟體開發生命週期之作業流程



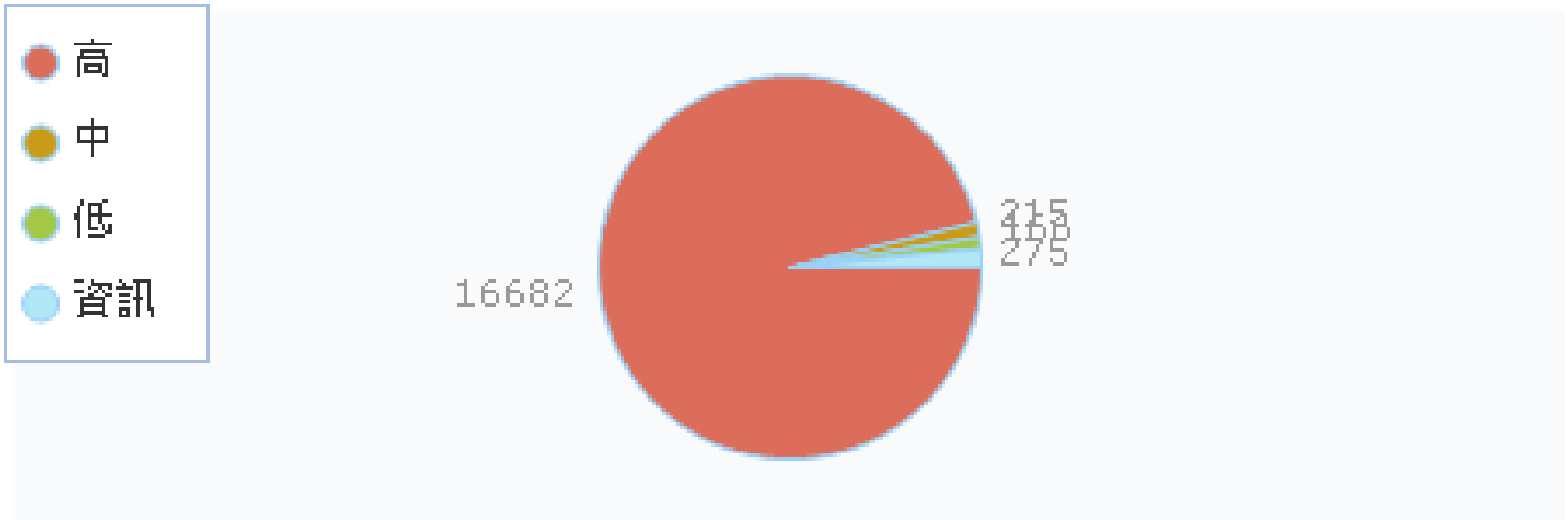
- 應針對應用系統進行整合性測試，包含原碼審查/弱點掃瞄，如發現弱點，並安排修復確保應用系統安全
- 針對應用系統所檢測之弱點應定期產生管理性報表，以進行分析追蹤

GSS Galaxy Software Services 叡揚資訊
& Security

實際狀況

驗收前因為客戶要求所以進行安全掃描

	問題總和	高	中	低	資訊
結果	17338	16682	215	166	275



*第一次進行測試結果通常很可觀

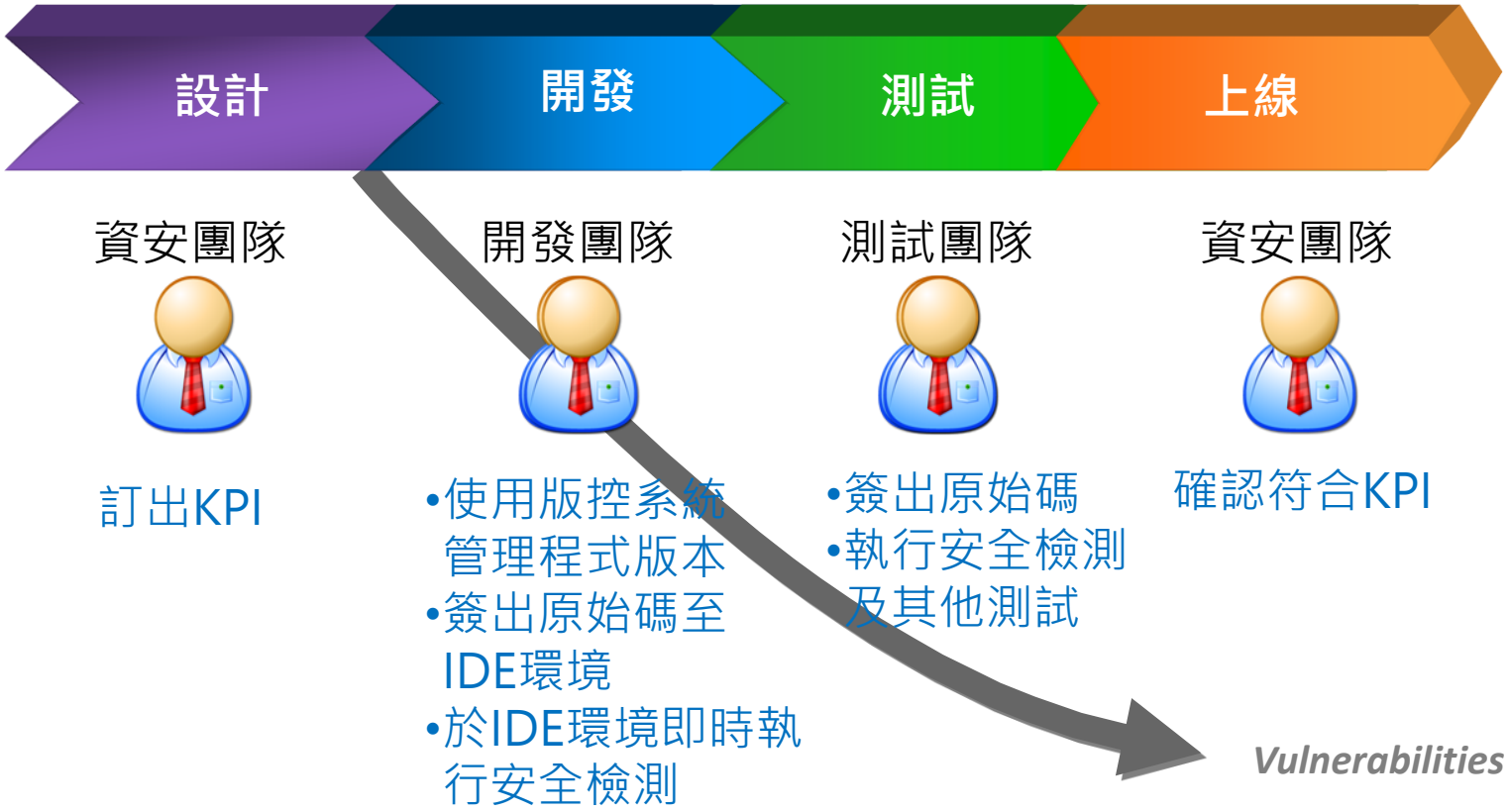
GSS 叡揚資訊 Galaxy Software Services
& Security

資安官的挑戰

- 開發團弱缺乏安全知識和意識。
- 資安團隊缺乏開發經驗
- 傳統的開發課程注重功能開發
- AppSec團隊缺少有效的把關機制

叡揚資訊
Security

遊戲規則制定

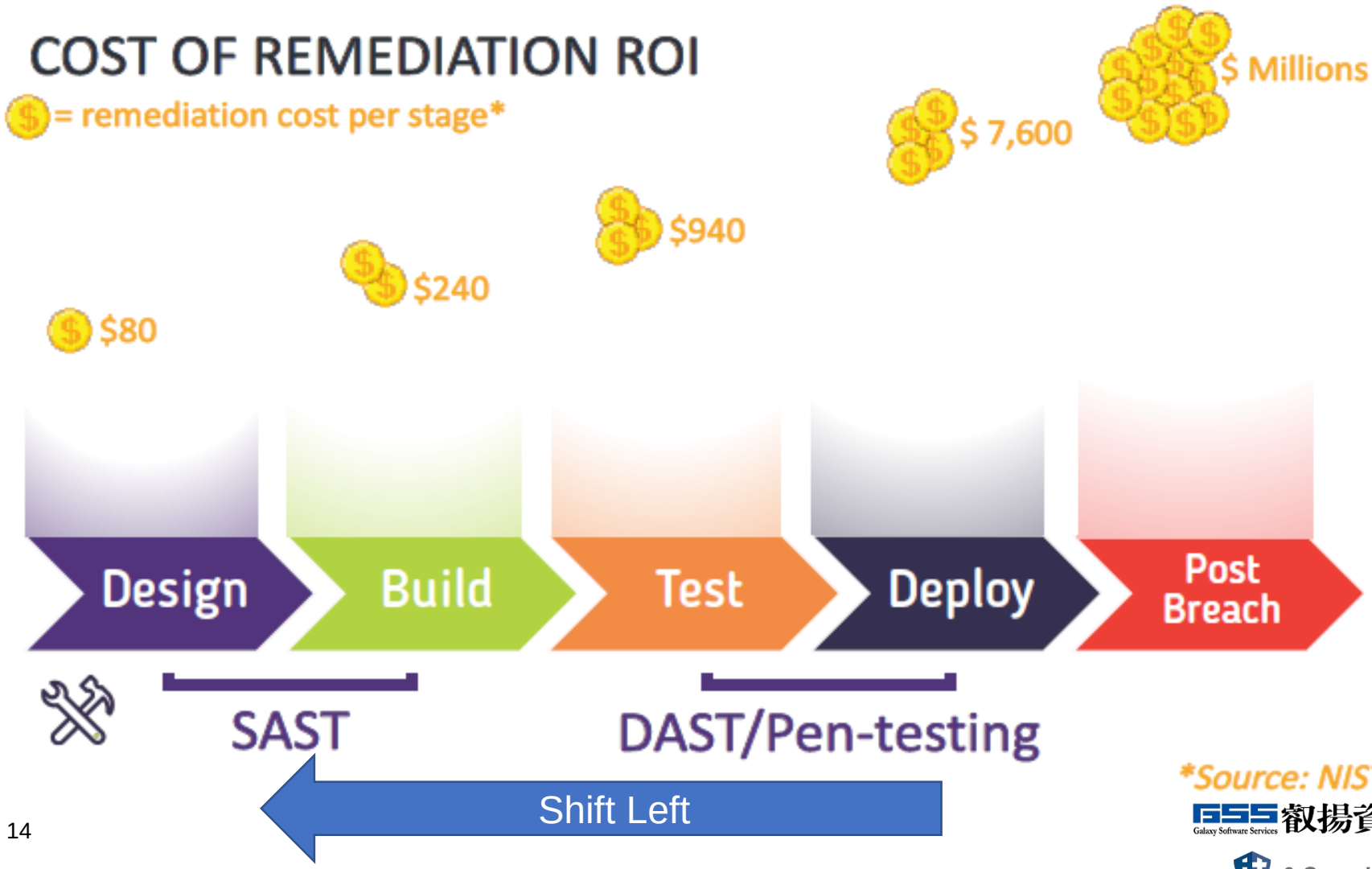


範例:源始碼檢測-Checkmarx 檢測要求

1. 不能有高風險OWASP TOP 10
2. 不能有 Injection HIGH issues

GSS 叡揚資訊 Galaxy Software Services
& Security

問題修復成本



*Source: NIST

GSS Galaxy Software Services 叡揚資訊
& Security

Chapter

2

開發人員資安意識提升

GSS 叡揚資訊 Galaxy Software Services
2018
UX
Cloud services
AI Bot DevOps
Big data SaaS
IOT Blockchain

資安修復隱藏成本

耗費成本

無法傳承

Know-How

企業

規格未列

- ●登入
- ●購物車
- ●公佈欄
- ●...
- ~~○SQL Injection~~
- ~~○XSS~~

GSS Galaxy Software Services 叡揚資訊
& Security

了解漏洞、風險

GSS 叡揚資訊 Galaxy Software Services
IT & Security

一般弱點解說

Reflected XSS All Clients

風險

可能發生什麼問題

攻擊者可能利用社交工程攻擊來導致使用者發送網站設計的輸入，重寫網頁並插入惡意腳本。
然後，攻擊者可以偽裝成原來的網站，這將使攻擊者可以竊取使用者的密碼，要求使用者的信用卡資訊，提供偽造訊息，或執行惡意軟體。
但從受害者的角度來看，這是原來的網站，受害人會責怪網站所產生的損害。

靜態文字，無法讓開發人員有深刻印象

原因

如何發生

'從使用者輸入的資料
如果資料包含HTML片
該漏洞主因為未先對

一般建議

如何避免

1.
驗證所有輸入，無論其來源為何。驗證應基於白名單：僅接受資料擬合一個指定的結構，而不是拒絕不良 patterns. 應確認: ● 資料類型 ● 大小 ● 範圍 ● 格式 ● 期望值 2. 在輸出嵌入之前完全編碼所有動態資料。
3. 編碼應該是上下文相關的。例如：● HTML內容使用HTML的編碼方式
●HTML編碼特性是將資料輸出到特性的值 ● JavaScript的編碼方式為伺服器產生的Javascript 4.
考慮使用ESAPI的編碼庫，或它的內置功能。對於舊版的ASP.NET，請考慮使用AntiXSS。5.
在HTTP類型對應的表頭，明確定義整個頁面的字元編碼。6. 設置 httpOnly
標誌於會期資訊，以防止利用XSS來竊取資訊。

程式碼範例

CSharp

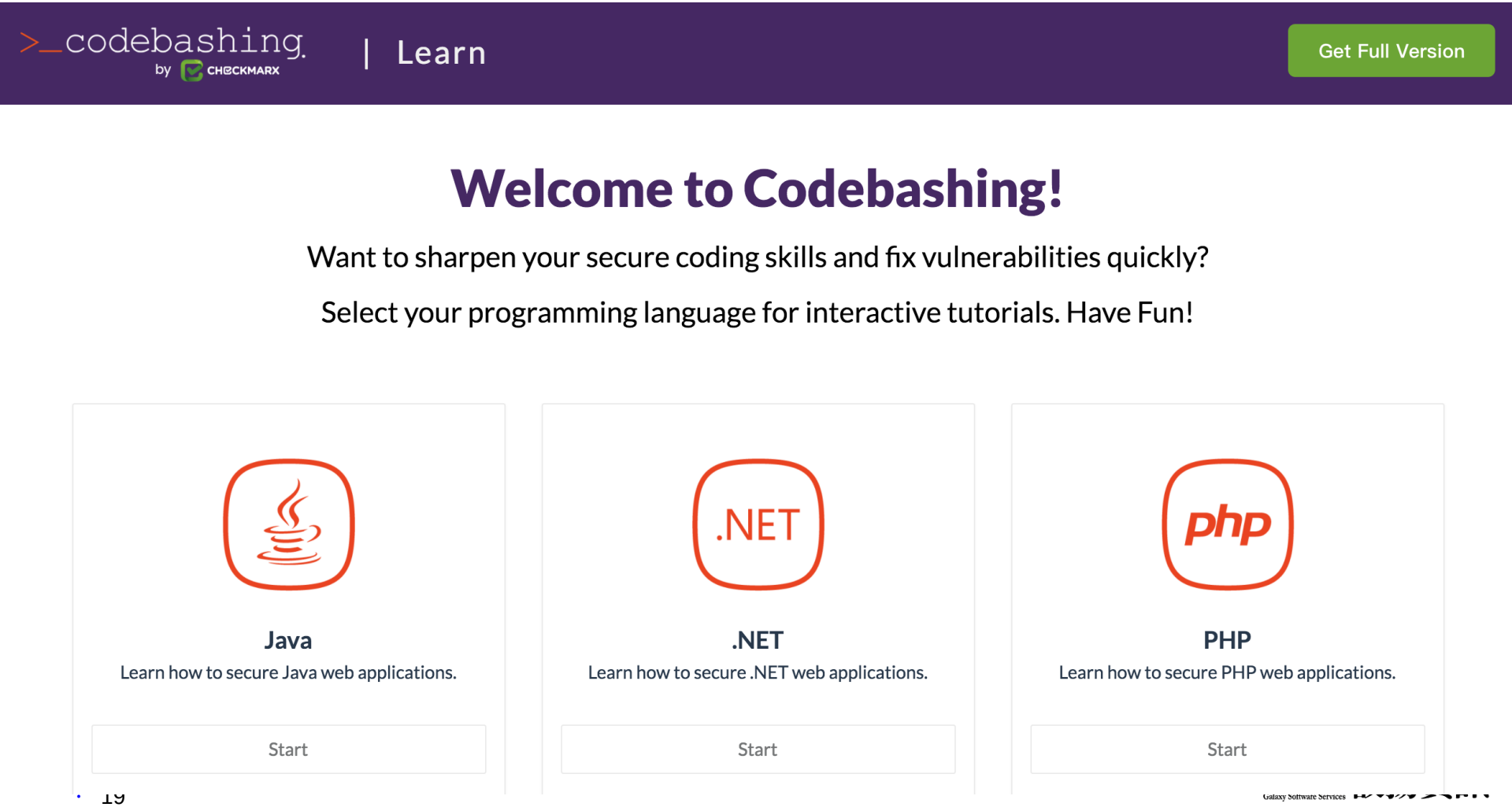
應用程式是使用「Referer」欄位字串來建立 HttpResponse

```
public class ReflectedXssAllClients
{
        public static void foo(HttpRequest Request, HttpResponse Response)
        {
                string Referer = Request.QueryString["Referer"];
                Response.BinaryWrite(Referer);
        }
}
```


SSS 叡揚資訊 Galaxy Software Services
& Security

線上弱點學習平台

Learning from CodeBashing



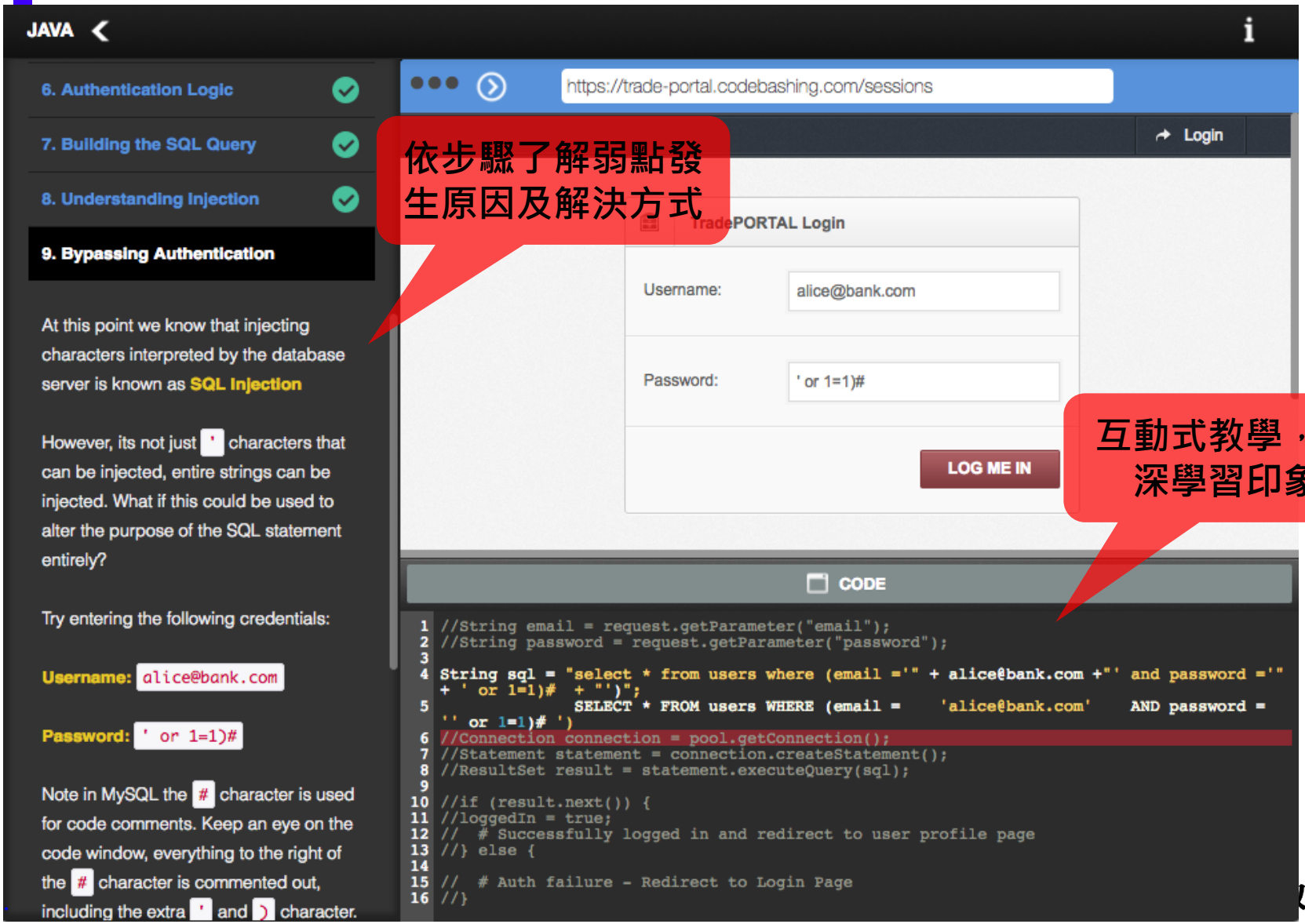
Galaxy Software Services
& Security

線上弱點學習平台

Learning from CodeBashing

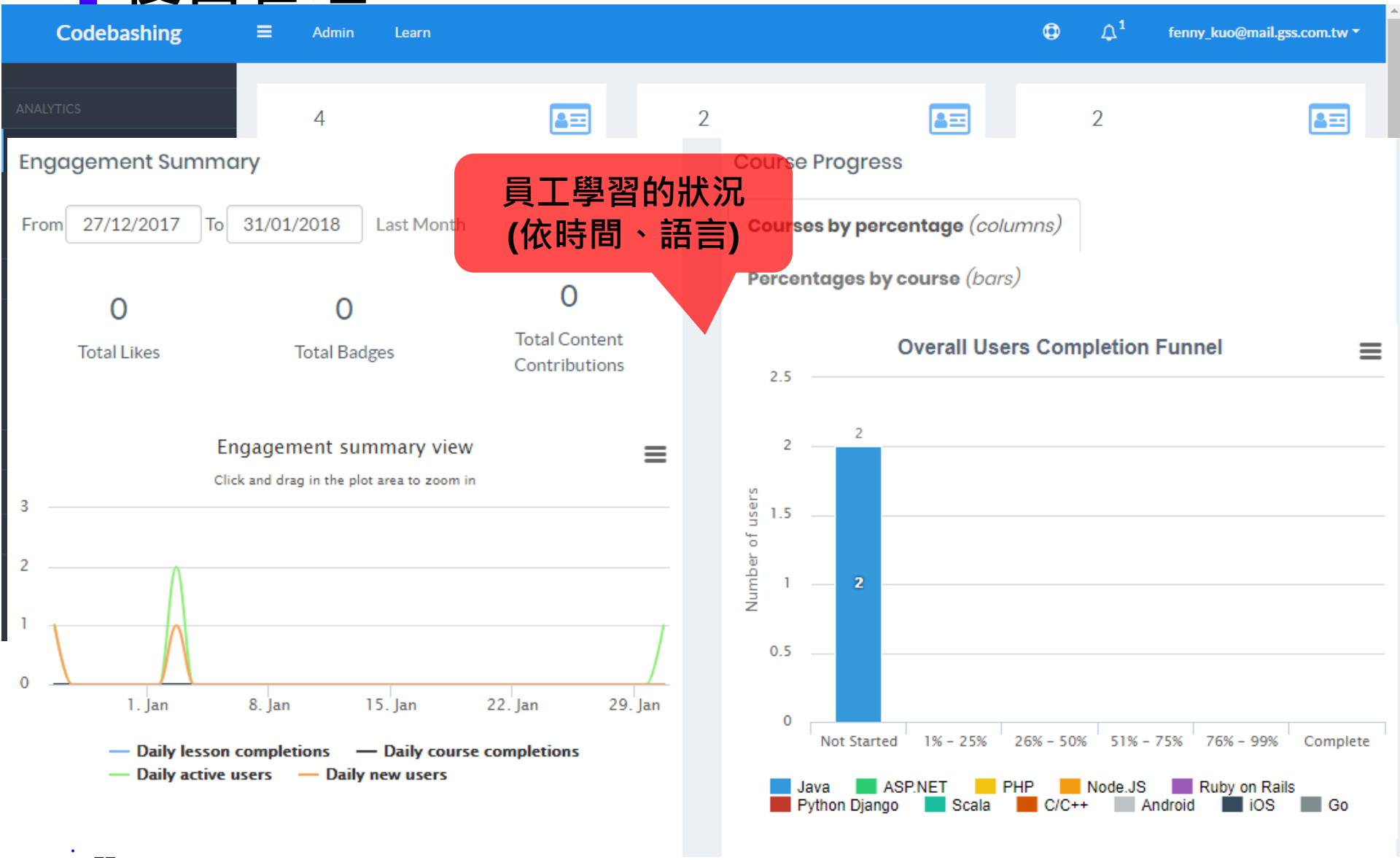
GSS 叡揚資訊 Galaxy Software Services
& Security

線上弱點學習平台



揚資訊
& Security

後台管理



& Security

Chapter

3

第三方元件管控

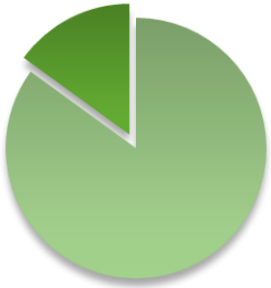
OSS

GSS 叡揚資訊 Galaxy Software Services
2018
UX
Cloud services
AI Bot DevOps
Big data SaaS
IOT Blockchain

OSS使用率增長

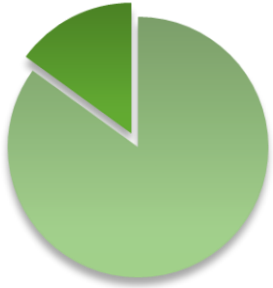
Gartner

85%



of commercial software vendors rely on open source

FORRESTER®



80%

of developers used open source in their applications in the past year

Gartner User Survey Analysis: Open-Source Software, 2015

Forrester developer survey 2015

GSS Galaxy Software Services 叡揚資訊 & Security

潛在的資安問題

我們到底有使用多少OSS?
我所使用的OSS合規嗎？
我所使用的OSS安全嗎？

GSS Galaxy Software Services 叡揚資訊
& Security

風險 - OWASP Top 10 2017

- A1: Injection
- A2: Broken Authentication
- A3: Sensitive Data Exposure
- A4:XML External Entites (XXE)
- A5:Broken Access Control (As it was in 2004)
- A6:Security Mis-configuration
- A7: Cross-Site Scripting (XSS)
- A8: Insecure Deserialization
- A9: Using Components with Known Vulnerabilities
- A10: Insufficient Logging & Monitoring

GSS 叡揚資訊 Galaxy Software Services
IT & Security

OSS風險

資安趨勢部落格 > 漏洞攻擊 > CVE-2017-5638：Apache Struts 2 漏洞可能讓駭客從遠端執行程式

CVE-2017-5638：Apache Struts 2 漏洞可能讓駭客從遠端執行程式

POSTED ON 2017 年 03 月 15 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

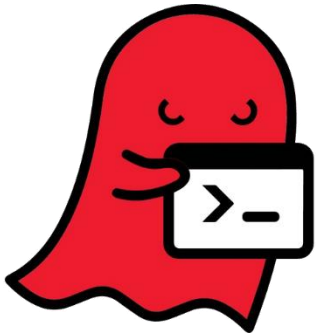
Like 8 Share G+

Apache Struts 是一個免費的開放原始碼程式開發架構，用來開發 Java 網站應用程式。我們仔細研究了過去 Apache Struts 被發現的幾個遠端程式碼執行 (Remote Code Execution，簡稱 RCE) 漏洞之後發現，歹徒大多使用 Object Graph Navigation Language (OGNL) 這個程式語言。OGNL 之所以很容易讓駭客從遠端執行任意的程式碼，是因為 Apache Struts 在大多數的流程當中都用到這個語言。

叡揚資訊 & Security

重大OSS議題

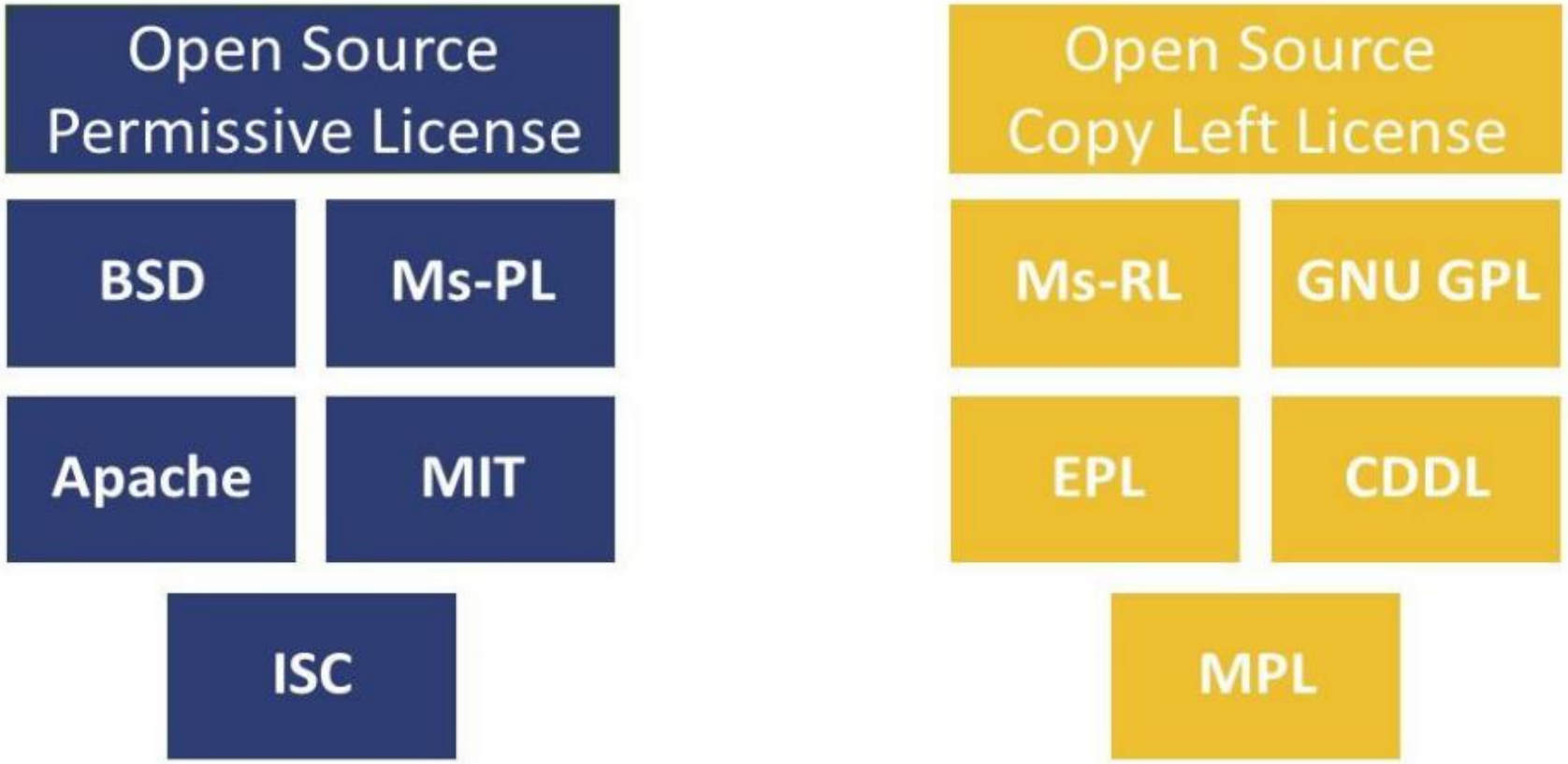
EQUIFAX



GSS 叡揚資訊 Galaxy Software Services

& Security

Permissive vs Copy Left



GSS 叡揚資訊 Galaxy Software Services
& Security

OSS應加強的管理

Use WhiteSource Get Better

雙重使用方式

發現：結合CI工具，早期發現風險

Know Where You Stand

報告：多面向資訊，全面了解現況

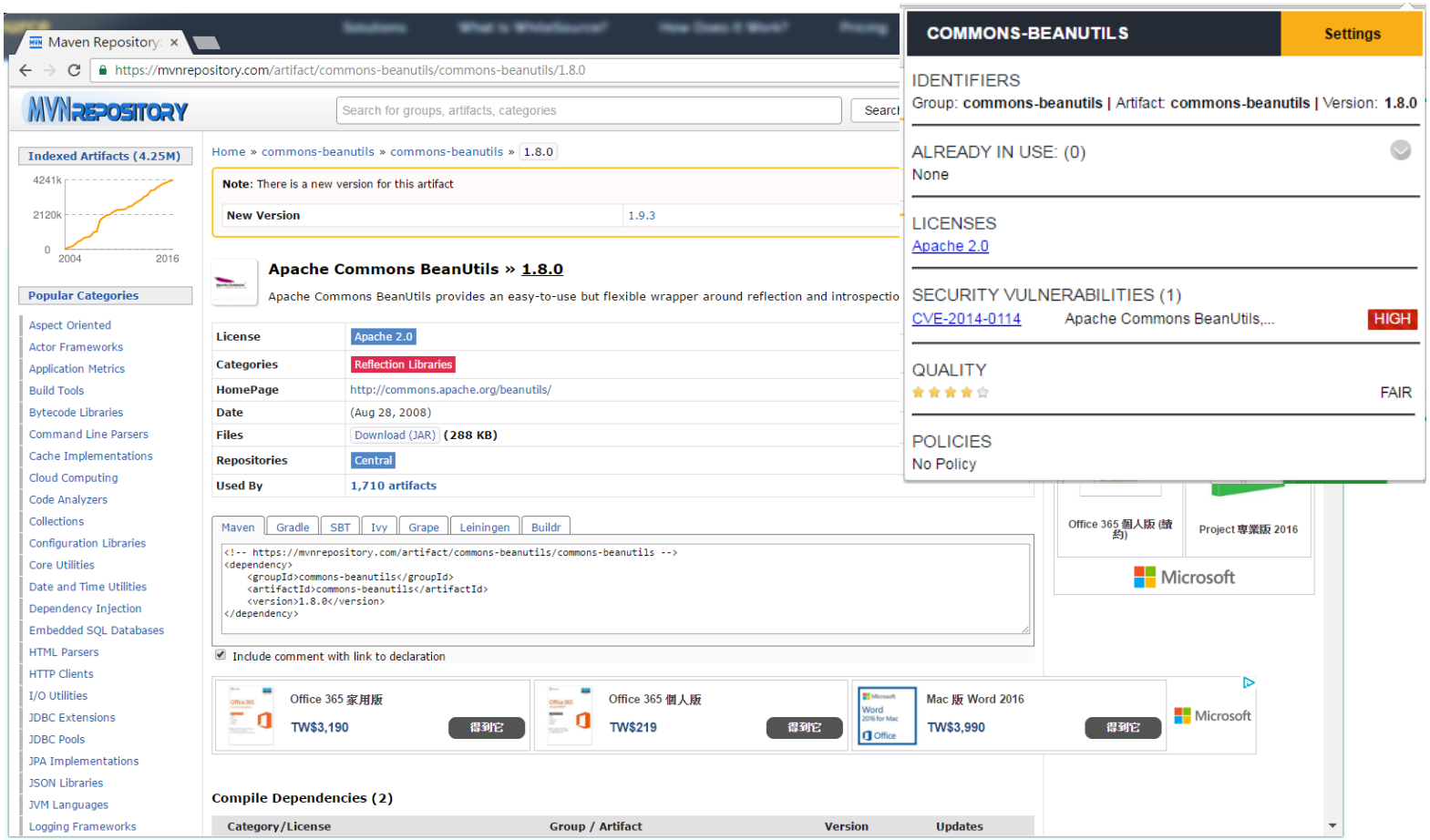
選擇：列出多項版本，選擇最適合您的

警示：依公司政策，建立預警機制

Continuous Management

選擇適合的OSS

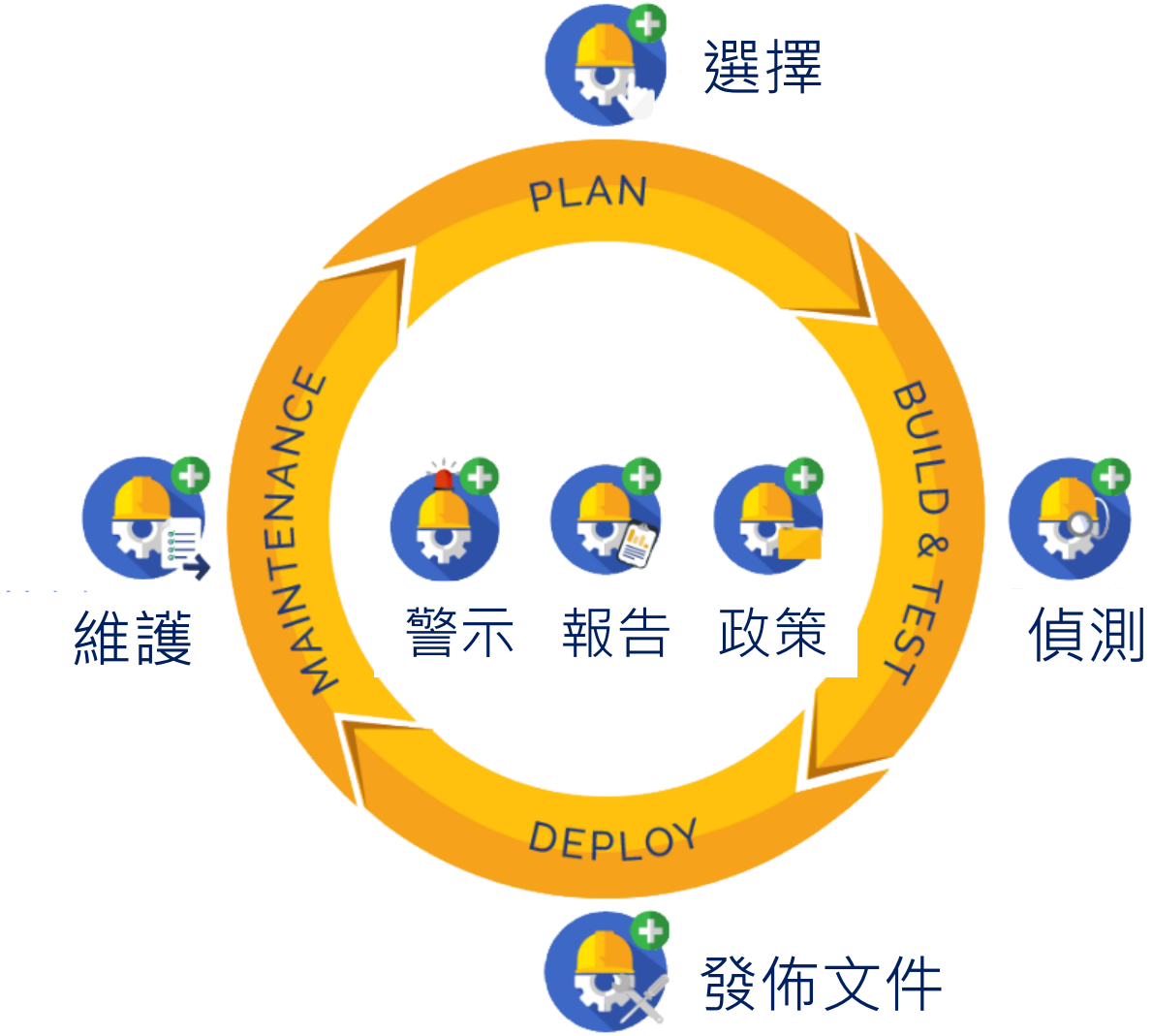
Use WhiteSource Get Better



GSS 叡揚資訊 Galaxy Software Services & Security

OSS SDLC 觀點

Use WhiteSource Get Better



GSS 叡揚資訊 Galaxy Software Services
& Security

Chapter

4

傳統應用系統 VS 行動化應用系統

GSS 叡揚資訊 Galaxy Software Services
2018
UX
Cloud services
AI Bot DevOps
Big data SaaS
IOT Blockchain

網頁與App資訊安全概觀

集中化信任的環境

APPs 在未受信任裝置環境

- Web Apps
- Data Center Applications

攻擊者不容易存取應用程式Binary file

防護-

+ Perimeter Security & Application Security Testing

- Mobile Apps
- Internet of Things
- Packaged Software

攻擊者容易存取應用程式 **Binary file**

防護-

+ Application Self-Protection

GSS Galaxy Software Services 叡揚資訊
& Security

破解後影響

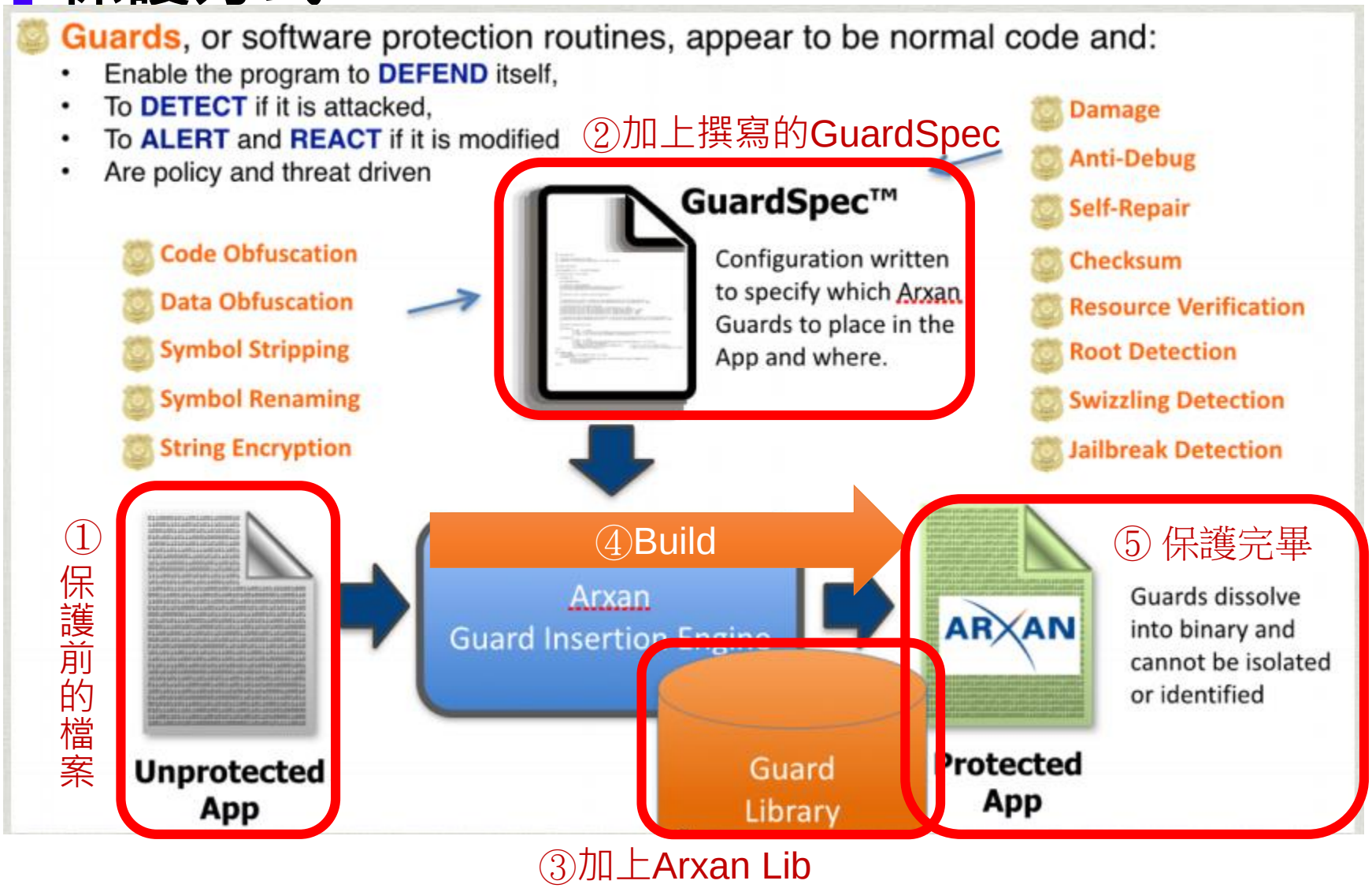
駭客想要做的事情

數位資產
Treasure Trove
&
Monetary Gains

- **Piracy and unauthorized distribution**
- **IP theft (如.重要演算法) 透過反組譯逆向工程**
- **Sensitive information (如. 帳號,密碼,keys,憑證)**
- **Bypass security controls (如. 授權, 加密破解, licensing, DRM, root/jailbreak detection, ads)**
- **Insertion of malware or exploits in the application and repackaging**

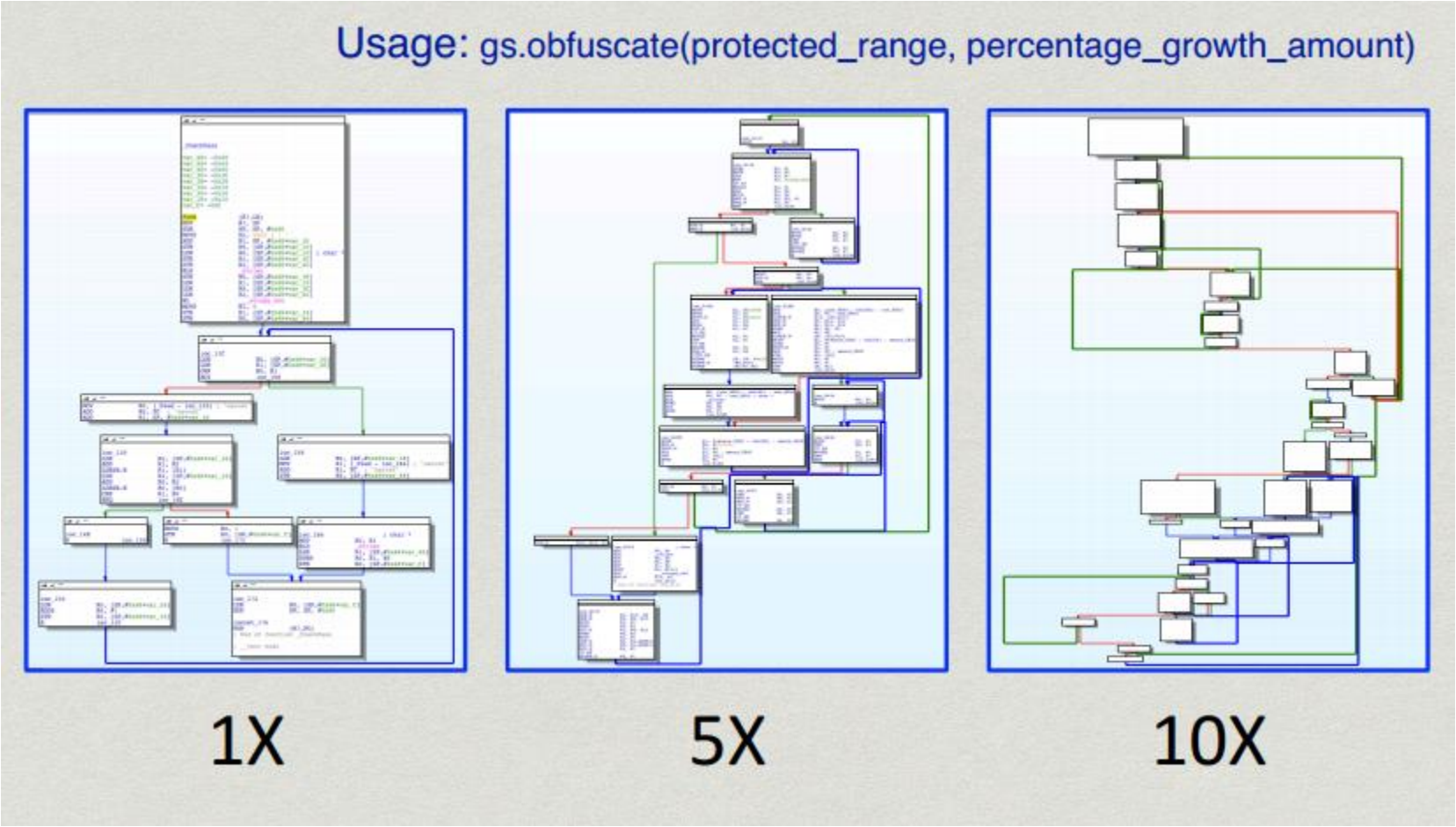
GSS 叡揚資訊 Galaxy Software Services
& Security

保護方式



GSS 叡揚資訊 Galaxy Software Services
& Security

Arxan 可彈性設計混淆程度



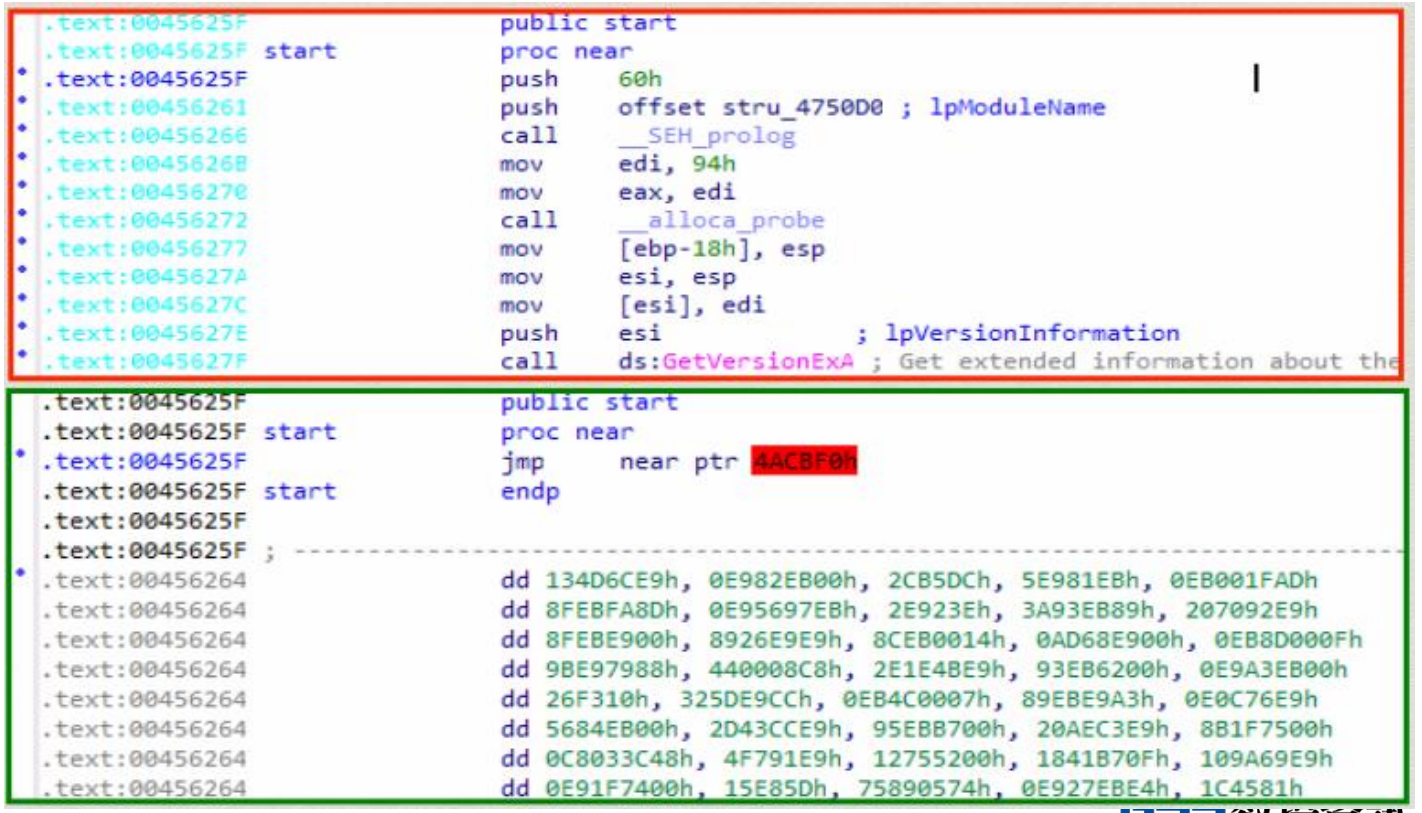
GSS 叡揚資訊 Galaxy Software Services
& Security

主要Guard介紹-Obfuscation

- Increases code complexity
- Protects against static analysis
- Obfuscating transformations

Before

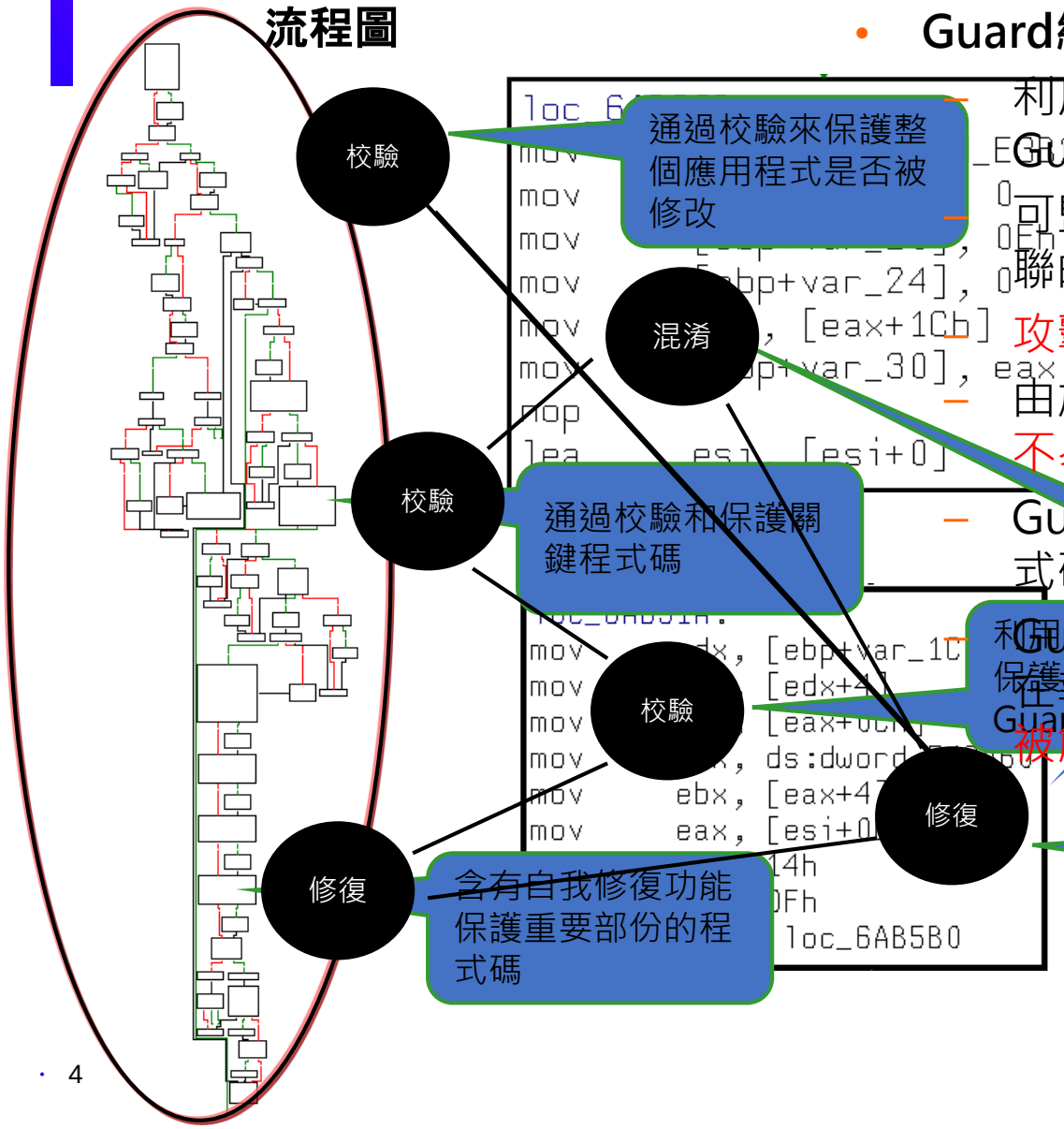
After



Galaxy Software Services 叡揚資訊
& Security

獨家Guards網路式防護

流程圖



- **Guard網路保護機制**
  - 利用交叉防護來全面確保各種功能的Guards
  - 可監測APP受到攻擊時,即時相關聯的Guards網路同步啟動保護
  - 攻擊者需同時破解所有監控位置
  - 由於Guards相互保護之下,攻擊者不易找到有關Guards的痕跡
  - Guard可調整設定保護特定範圍程式碼,或整個應用程式
  - Guard網路能有效防止利用程式碼在執行階段動態分析後通過反組譯被解

未受保護Key外漏案例

```
137   public static void init(String paramString)
138     throws Exception
139   {
140     try
141     {
142       cipher = Cipher.getInstance("AES/CBC/PKCS7Padding", "BC");
143       skeySpec = new SecretKeySpec(paramString.getBytes("UTF8"), "AES");
144       return;
145     }
146     catch (Exception localException)
147     {
148       Debuk.WriteLine("encrypt failed", localException);
149       throw localException;
150     }
151   }
152
153   public static void main(String[] paramArrayOfString)
154   {
155     try
156     {
157       encrypt(String.valueOf(new Date().getTime()), "[redacted]@@86136982");
158       return;
159     }
160     catch (Exception localException) {}
161   }
162 }
```


GSS Galaxy Software Services 叡揚資訊
& Security

Whitebox Cryptography?

Use TransformIT Ensure Security

- 白箱加密(White-box Cryptography)是一種用於混淆加密演算法的縝密方法，使得金鑰可充分隱藏、防止窺探，其目的在於防止加密運算中的關鍵資訊(比如私鑰)洩露，以免潛在攻擊者完全存取系統。
- 白箱定義在於因App是在行動裝置端執行，可透過反組譯察看到內容，攻擊者可進行記憶體偵查分析出私鑰內容，資訊都可透明看到，因此稱之為白箱。

GSS 叡揚資訊 Galaxy Software Services
& Security

使用Hybrid開發背景

- 減少開發時間以及學習雙平台開發成本
- 使用Javascript開發模式+HTML5方式
- Web/Hybrid應用
  - 只要使用一種方式就可以雙平台(iOS/Android)開發
  - 不需要多花時間學習Object-C/Swift,Android
  - 學習門檻低

- Web應用(RWD Responsive Web Design響應式網頁)
  - 直接透過行動裝置瀏覽器執行
  - 依照設備螢幕大小自動調整畫面
  - 不需要上架App store/Google Play

GSS Galaxy Software Services 叡揚資訊
& Security

保護後的結果確認-靜態反組譯

加強混淆Javascript程式碼

保護前:原始的Javascript程式碼

```
var passwordField;
var secretsArea;
var correctColor = "#e0ffe0";
var wrongColor = "#ffe0e0";
var secretsRevealed = false;

function startSimon()
{
    passwordField = document.getElementById("password");
    secretsArea = document.getElementById("secrets");
    passwordField.focus();
    checkPassword();
}

function checkPassword()
{
    var password = passwordField.value;
    if (password == "secret")
    {
        passwordField.style.backgroundColor = correctColor;
        revealSecrets();
    }
    else
    {
        passwordField.style.backgroundColor = wrongColor;
        if (secretsRevealed) clearSecrets();
    }
}

function revealSecrets()
{
    secretsArea.value = "Baked in credentials are never a good idea.";
    secretsRevealed = true;
}

function clearSecrets()
{
    secretsArea.value = "";
    secretsRevealed = false;
}
```

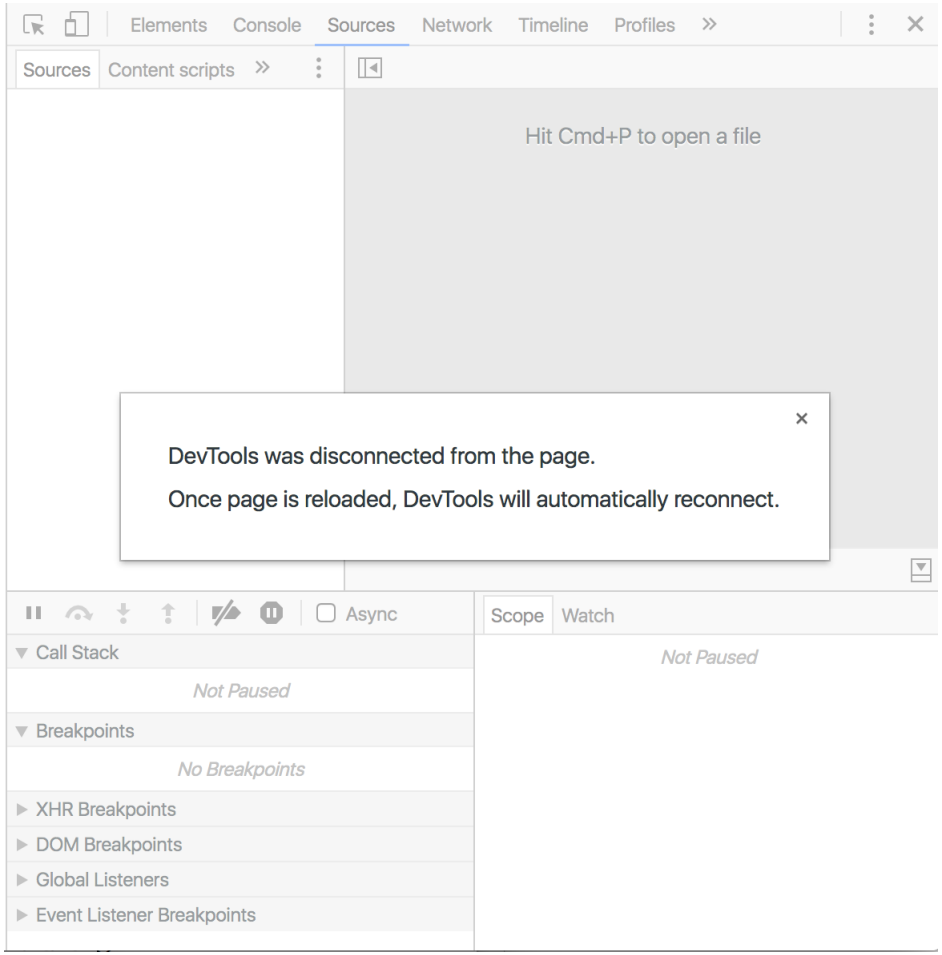
保護後:混淆後難以閱讀理解

```
var !>ij>--i-=+ ! +[]+! +[]+! +[]+! +[]+! +[]+! +[]+! +[],j*j!ii*!-=! +[]+!
    +[],<ijj>>i*-=+ ! +[]+! +[]+! +[],*jij--ij>=[+ ! +[]]+[+[]],-<j<--!-j=! +[]+!
    +[]+! +[]+! +[],>j:-ij>*>=[+ ! +[]]+[+[]]-+ ! +[],-j-i-ii>>=+ ! +[]+! +[]+!
    +[]+! +[]+! +[],ji<!!ij->=+ ! +[],jj!!i:-ij=[+ ! +[]]+[+[]]-2,ij-j:i-!-=+ ! +[]+!
    +[]+! +[]+! +[]+! +[]+! +[],>jj>ji:j=+[];var
    -<i:-ij>-=>jj>ji:j+-<j<--!-j*jij--ij>+!>ij>--i-*(
    *jij--ij>*jij--ij>),:j*j-i-->=j*j!ii*!-+ji<!!ij->*jij--ij>+ji<!!ij->*(
    *jij--ij>*jij--ij>),i->>--j!-=-j-i-ii>>+ji<!!ij->*jij--ij>+!>ij>--i-*(
    *jij--ij>*jij--ij>),>j*-j:>*-=ij-j:i-!-+<ijj>>i*-*jij--ij>+-j-i-ii>>*(
    *jij--ij>*jij--ij>)+-j-i-ii>>*(*jij--ij>*(*jij--ij>*jij--ij>))+ij-j:i-!-*(
    *jij--ij>*(*jij--ij>*(
    *jij--ij>*jij--ij>))),*<i-j!<<-=ji<!!ij->+-<j<--!-j*jij--ij>+-<j<--!-j*(
    *jij--ij>*jij--ij>),-!-!::j-=!>ij>--i-+j*j!ii*!-*jij--ij>+jj!!i:-ij*(
    *jij--ij>*jij--ij>),:-iiij:j=>jj>ji:j+j*j!ii*!-*jij--ij>+<ijj>>i*-*(
    *jij--ij>*jij--ij>)+ij-j:i-!-*(*jij--ij>*(*jij--ij>*jij--ij>))+-j-i-ii>>*(
    *jij--ij>*(*jij--ij>*(
    *jij--ij>*jij--ij>))),i!-:jj:i-=>j:-ij>*>+ij-j:i-!-*jij--ij>+>j:-ij>*>*(
    *jij--ij>*jij--ij>),-j:jjj:-=ij-j:i-!-+>j:-ij>*>*jij--ij>+j*j!ii*!-*(
    *jij--ij>*jij--ij>)+-j-i-ii>>*(*jij--ij>*(*jij--ij>*jij--ij>))+-j-i-ii>>*(
    *jij--ij>*(*jij--ij>*(
    *jij--ij>*jij--ij>))),ijjj<>j*-=-<j<--!-j+>j:-ij>*>*jij--ij>+-j-i-ii>>*(
```

```
    !>jjij!<>,>j*---j-,i*-iiiijj,j!-!:j><>))][(-:ij:->>-(
    !>jjij!<>,!j<-j*!j>,--:i>*j*-,>i:i-:**))]=-jji-*i<j;if(*:j-i:ji)-:ij:->>-.call(
    this,*jij*ii<-,i*-<::ij>,-j!-j-i!j[>ij:i!ij-])};}return;}break;case jii>>ij*j:{var
    *ij!--jjj=Array.prototype.slice.call(arguments,1);var >---jiii-=*ij!--jjj[0];var
    >:i<-*i!j=*ij!--jjj[1];return >---jiii-*>:i<-*i!j;}break;}}}-:ij:->>-.call(
    this,i-<<>-:j-);function i*-<::ij>(){var <i<--<:--=[j---j<-ij];for(var
    i-!jj-*j-=0;i-!jj-*j-<arguments.length;++i-!jj-*j-){<i<--<:--.push(arguments[
    i-!jj-*j-]);}return -:ij:->>-.apply(this,<i<--<:--);}function j>iij<i>-(){var
    *i-!i:--j=[*<i-j!<<-];for(var :*ijj<ij-=0;:*ijj<ij-<
    arguments.length;++:*ijj<ij-){*i-!i:--j.push(arguments[:*ijj<ij-]);}return
    -:ij:->>-.apply(this,*i-!i:--j);}function ji:j-:i:>(){var i<:<j>j:=[-!-<j-j!-];for(
    var :ji-j-jj-=0;:ji-j-jj-<arguments.length;++:ji-j-jj-){i<:<j>j:.push(arguments[
    :ji-j-jj-]);}return -:ij:->>-.apply(this,i<:<j>j:);}function jj<:-i>:j(){var
    jj-i<j:-=[!j<i-:<<];for(var :j>--*j-=0;:j>--*j-<
    arguments.length;++:j>--*j-){jj-i<j:-.push(arguments[:j>--*j-]);}return
    -:ij:->>-.apply(this,jj-i<j:-);}function jj>j:-ji-(){var jj-ii!-j>=[-!-!::j-];for(
    var i-ji:>>i>=0;i-ji:>>i><arguments.length;++i-ji:>>i>){jj-ii!-j>.push(arguments
    [i-ji:>>i>]);}return -:ij:->>-.apply(this,jj-ii!-j>);}function <<>->><:(){var
    i:iii>!*=[*i*<j--<];for(var :ii-j:ji>=0;:ii-j:ji><
    arguments.length;++:ii-j:ji>){i:iii>!*.push(arguments[:ii-j:ji>]);}return
    -:ij:->>-.apply(this,i:iii>!*);}
```

保護後的結果確認-動態攻擊

Debug偵測啟動,防止動態分析



無法進行Debug

GSS 叡揚資訊 Galaxy Software Services
& Security

Chapter

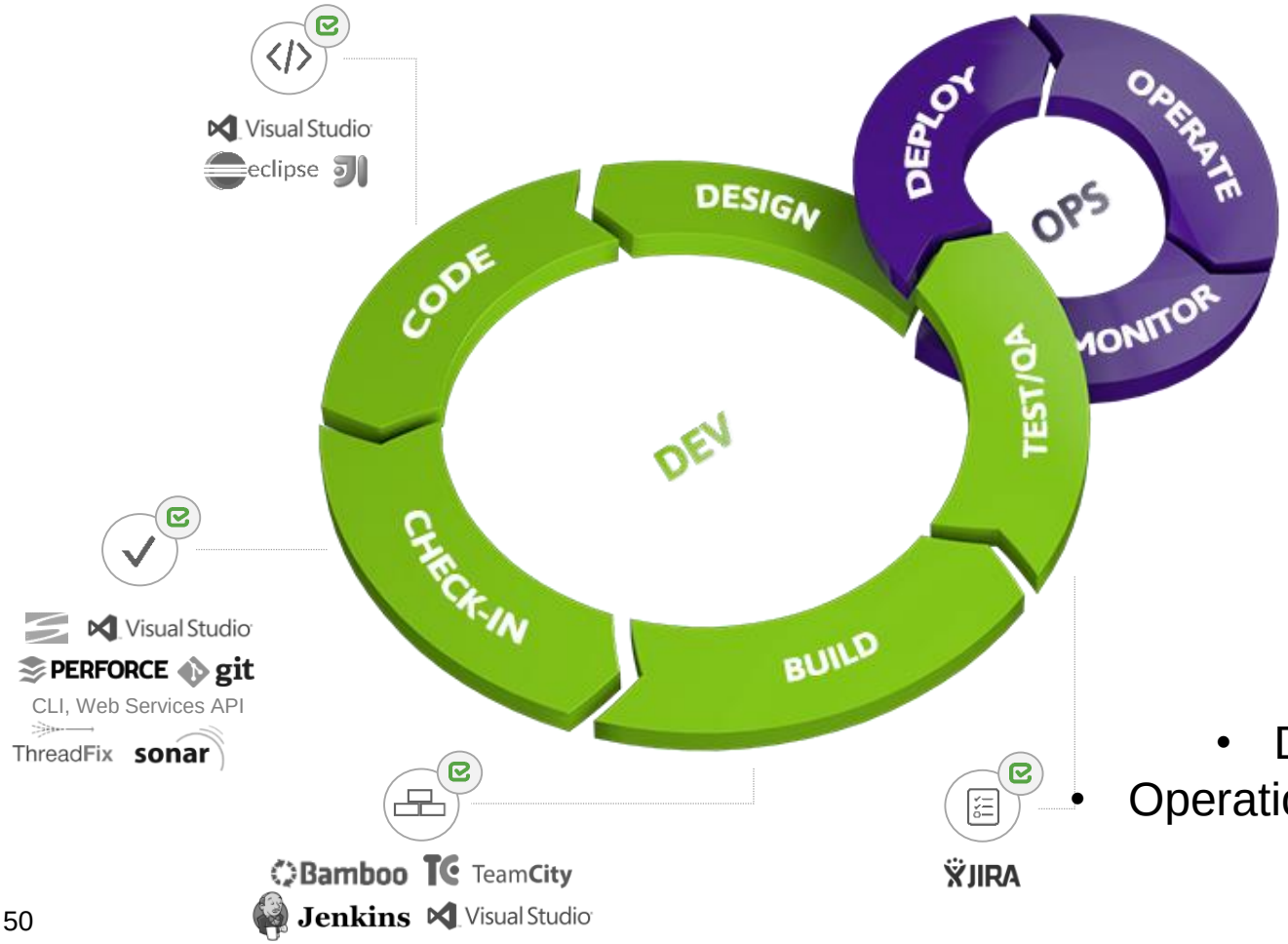
5

持續整合與部署平台

GSS 叡揚資訊 Galaxy Software Services
2018
UX
Cloud services
AI Bot DevOps
Big data SaaS
IOT Blockchain

Secure SDLC Integration and Automation

(CI/CD, DevSecOps)

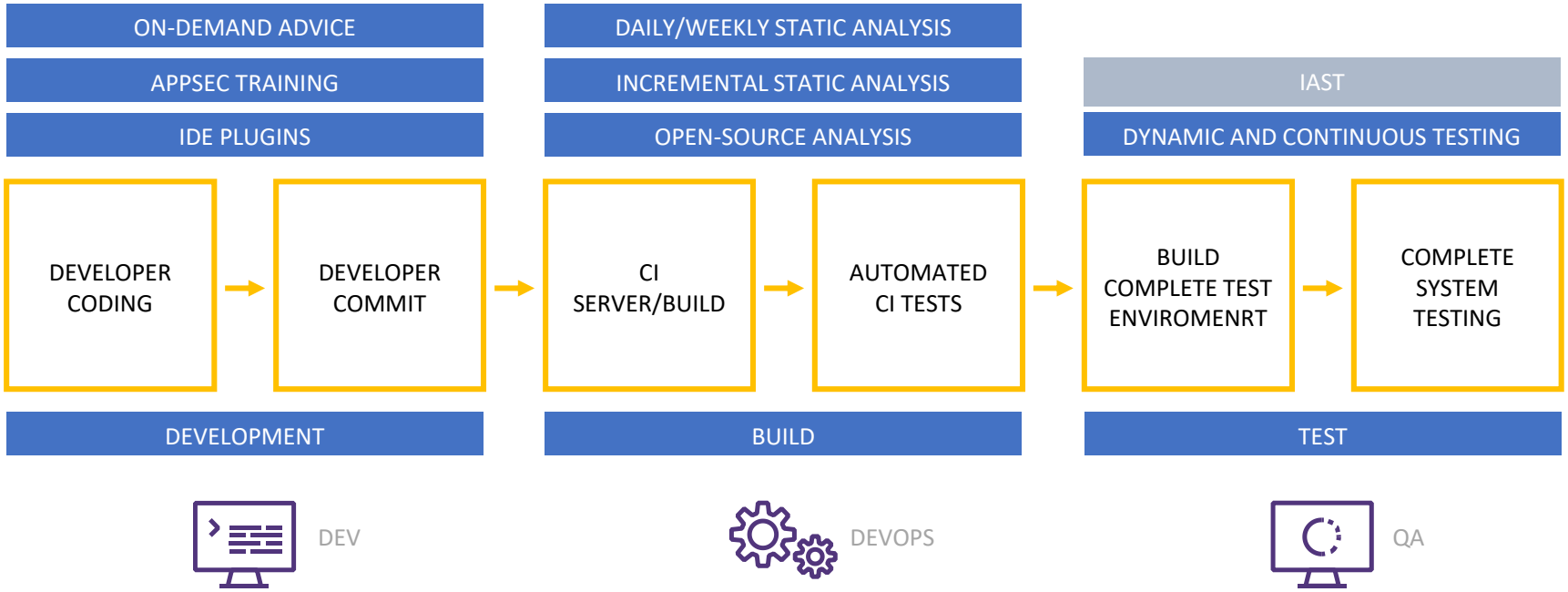


APIs and CLI

- Data extraction
- Operations and Management

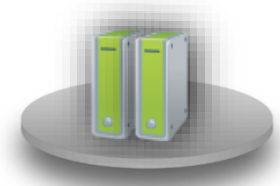
GSS 叡揚資訊 Galaxy Software Services
& Security

SEAMLESSLY EMBED APPSEC TESTING INTO DEVOPS PROCESSES



GSS 叡揚資訊 Galaxy Software Services
& Security

GSSDLC for Application & APP



自動上版平台

Jenkins自動整合平台

APACHE JMeter™

需求變更系統

nunit

JUnit

MS Build

<APACHE ANT>

Maven™

GSS-CIA Compare

衝擊分析

黑/白箱檢測

開源碼檢測

發布前後自動程序

CHECKMARX

AppScan

IBM Security

WhiteSource

ARXAN

APPERIAN MOBILE APP MANAGEMENT

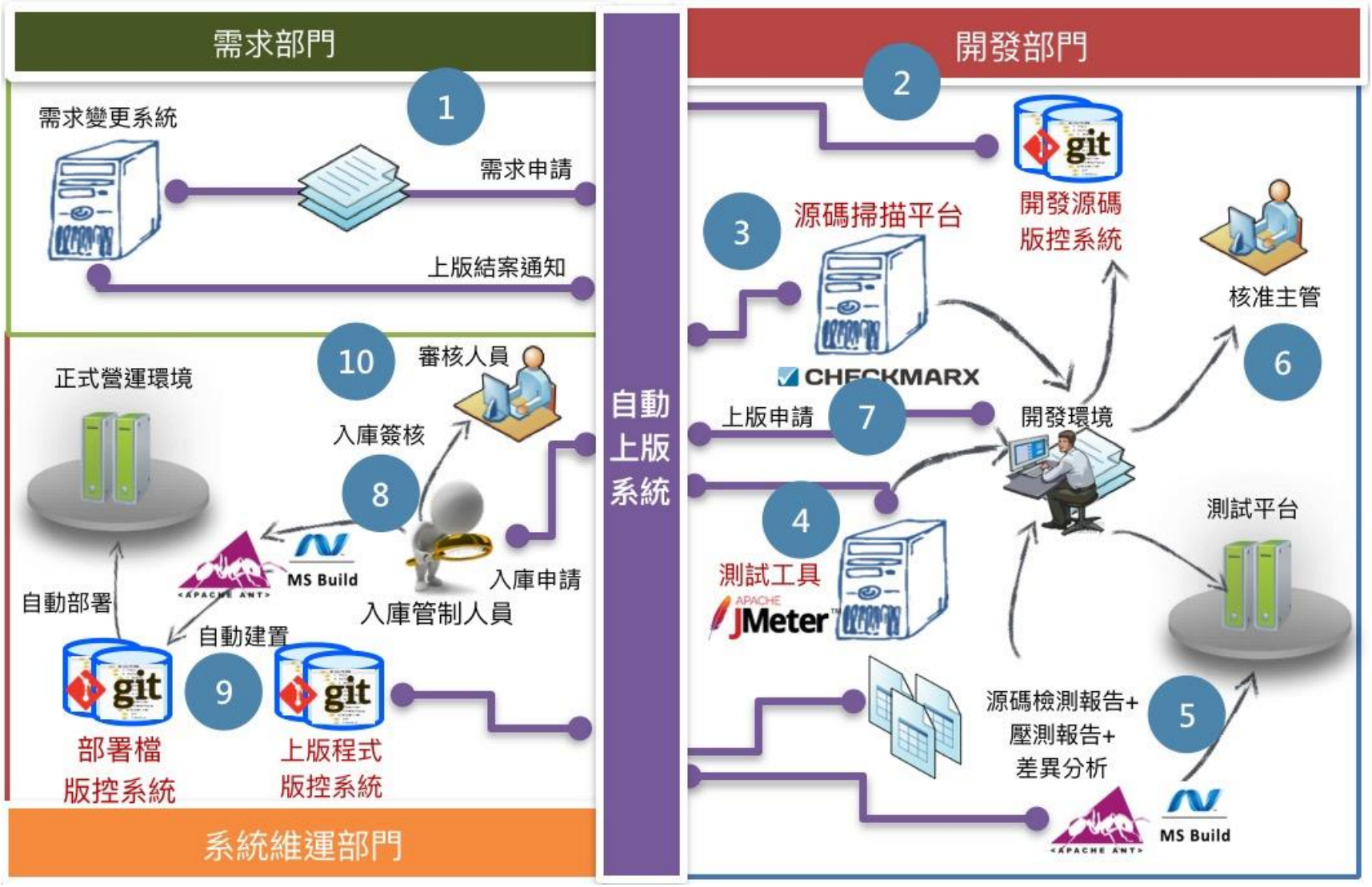
git

SUBVERSION

需求變更介接 → 差異分析 → 源碼檢測 → 自動測試 → 自動建置 → 自動部署

GSS Galaxy Software Services 叡揚資訊
& Security

GSSDLC 案例



GSS Galaxy Software Services 叡揚資訊
& Security

Chapter

6

結論

GSS 叡揚資訊 Galaxy Software Services
2018
UX
Cloud services
AI Bot DevOps
Big data SaaS
IOT Blockchain

結論

- 對於企業
  - 可整合**企業資安規範**，依需求客製化檢測規則
  - 提升應用系統之**安全強度**
  - 整合現有 SDLC 早期發現應用系統弱點，**降低修復成本**
  - 結合自動化程式碼安全檢測機制，能大量**節省人力**成本
  - 提供**定期的更新**機制， 符合安全現況趨勢
  - 設計獨一無二的APP防護，**強化APP安全**
- 對於使用者(開發者)
  - 互動式的學習平台，**增加開發人員資安意識**
  - 安全程式開發指引，**減少重工情境**
  - 提供圖形化檢測結果，方便進行修復程式碼弱點
  - 明確指出第三方元件適用與否便利選擇

GSS Galaxy Software Services 叡揚資訊
& Security

請填寫問卷 會後抽出問卷禮

GSS 叡揚資訊
Galaxy Software Services

Thank You

感謝您的聆聽，敬請指教

IT & Security

國家產業創新獎
卓越中堅企業

GSS 叡揚資訊

Vital 雲端服務家族

GSS 技術部落格