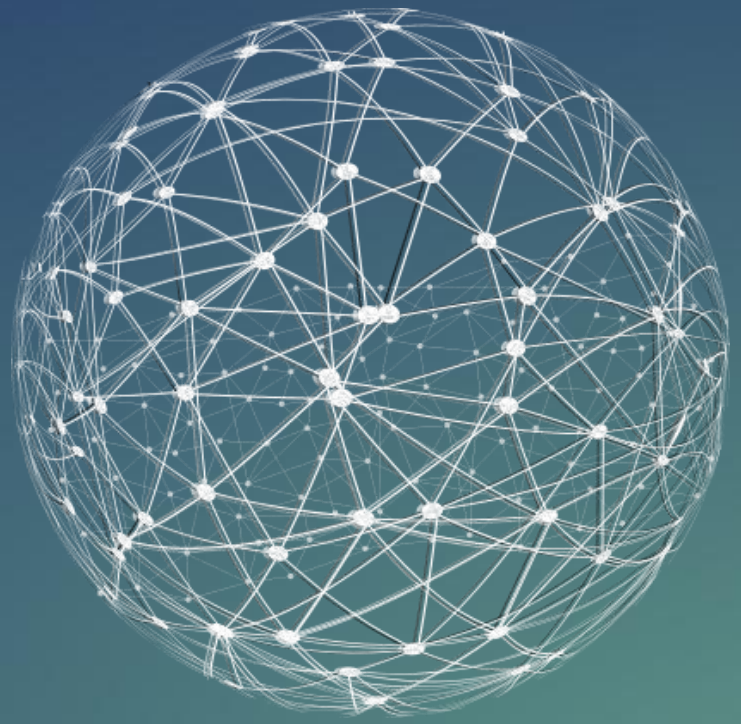
OSSEC与webshell实时监控探索

易果生鲜 涂宏伟

2017携程信息安全沙龙



关于我

挖土

一号店/平安/飞牛

安全技术在企业落地

企业安全人员现状

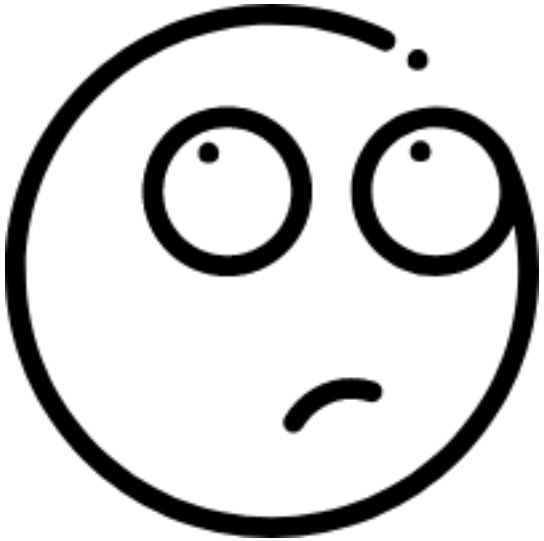
1 : 50?

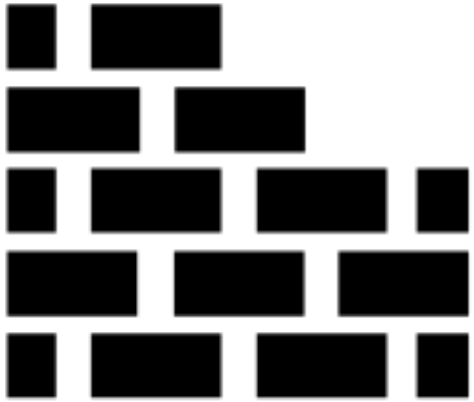
1 : 100?

1 : 200?

1 : n^n

企业安全建设的思考

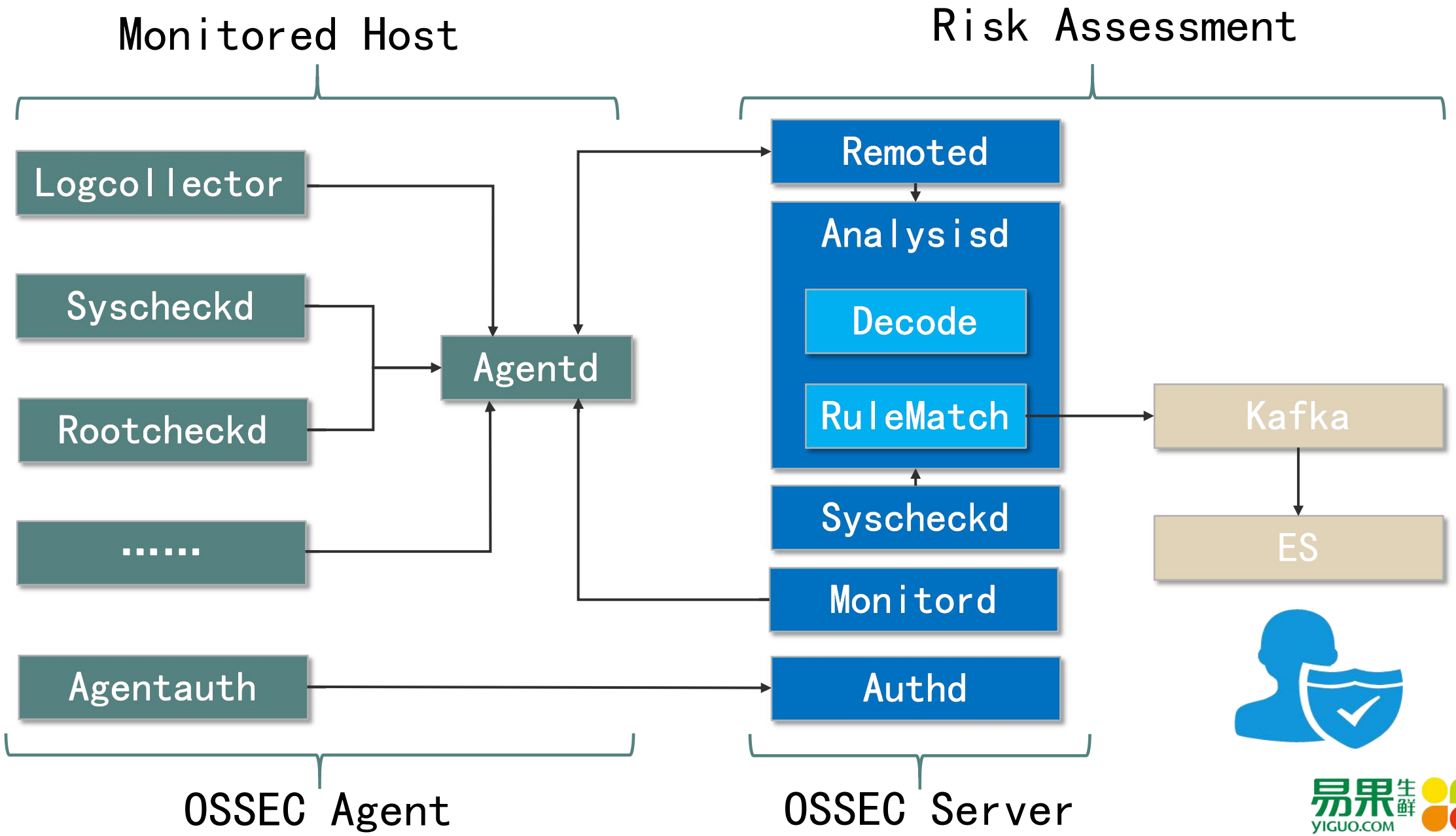




- 开源、免费，可方便的修改、定制

- 系统资源占用低，运维容易接受

OSSEC 架构



- 文件大小
- 文件hash
- 文件拥有者
- 文件权限

Syscheckd是OSSEC实现的文件完整性检查模块名称

可以定期运行以检查任何已配置的文件(Windows的注册表项)是否已更改

能够在Windows和Linux上实时检查文件的完整性

WebShell

可执行文件修改

可执行文件上传/创建

Agent

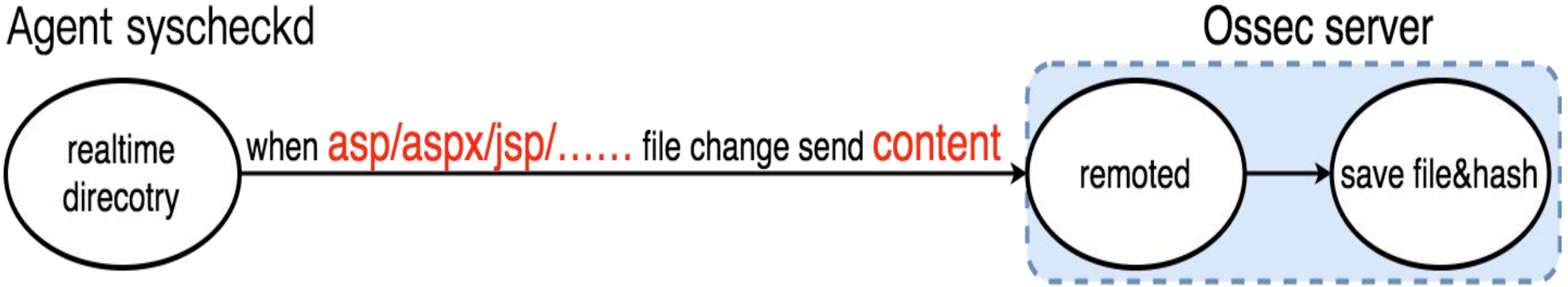
- 本地化检测
- 无大量文件上传
- 代码保护(公有云)

- 存在绕过、漏报
- 资源消耗会增加

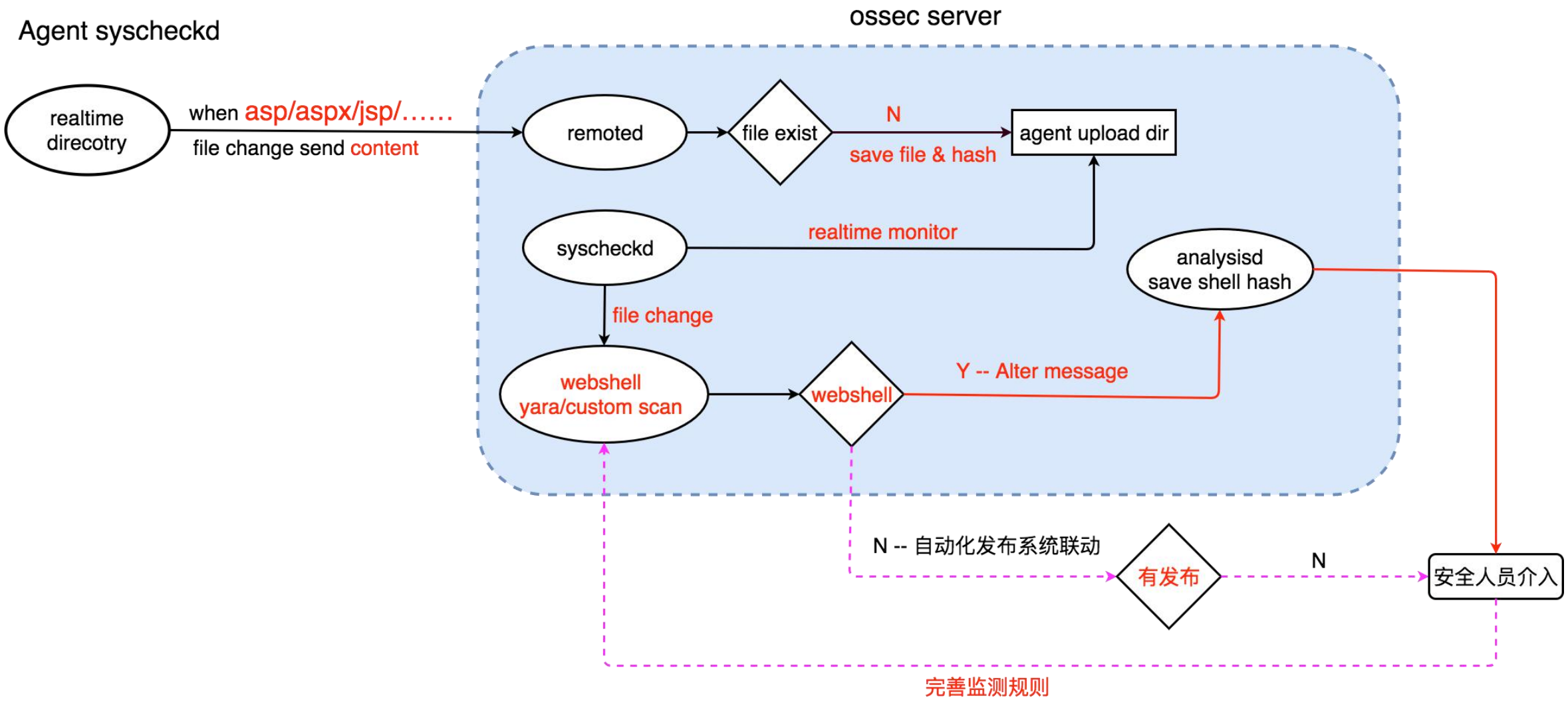
Server

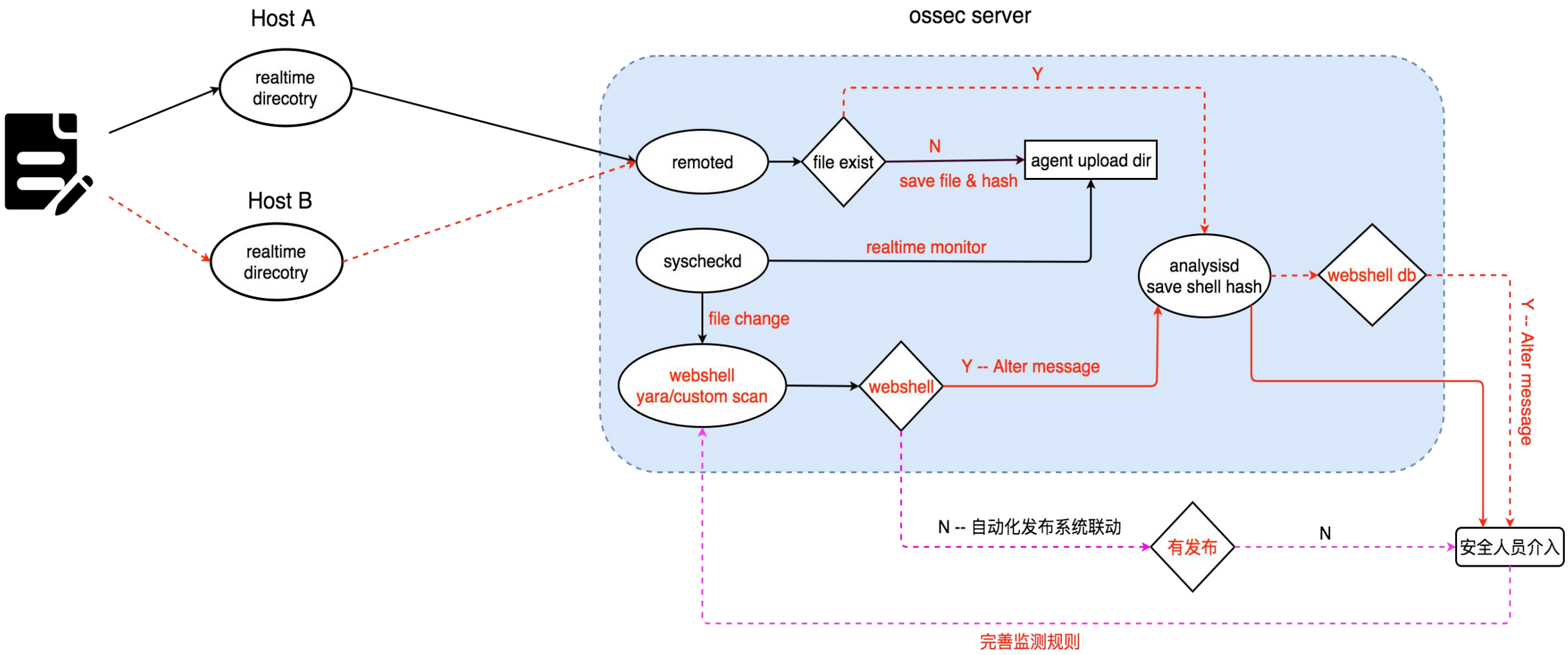
- 检测规则透明化
- 检测方法多样化
- 安全控制颗粒化

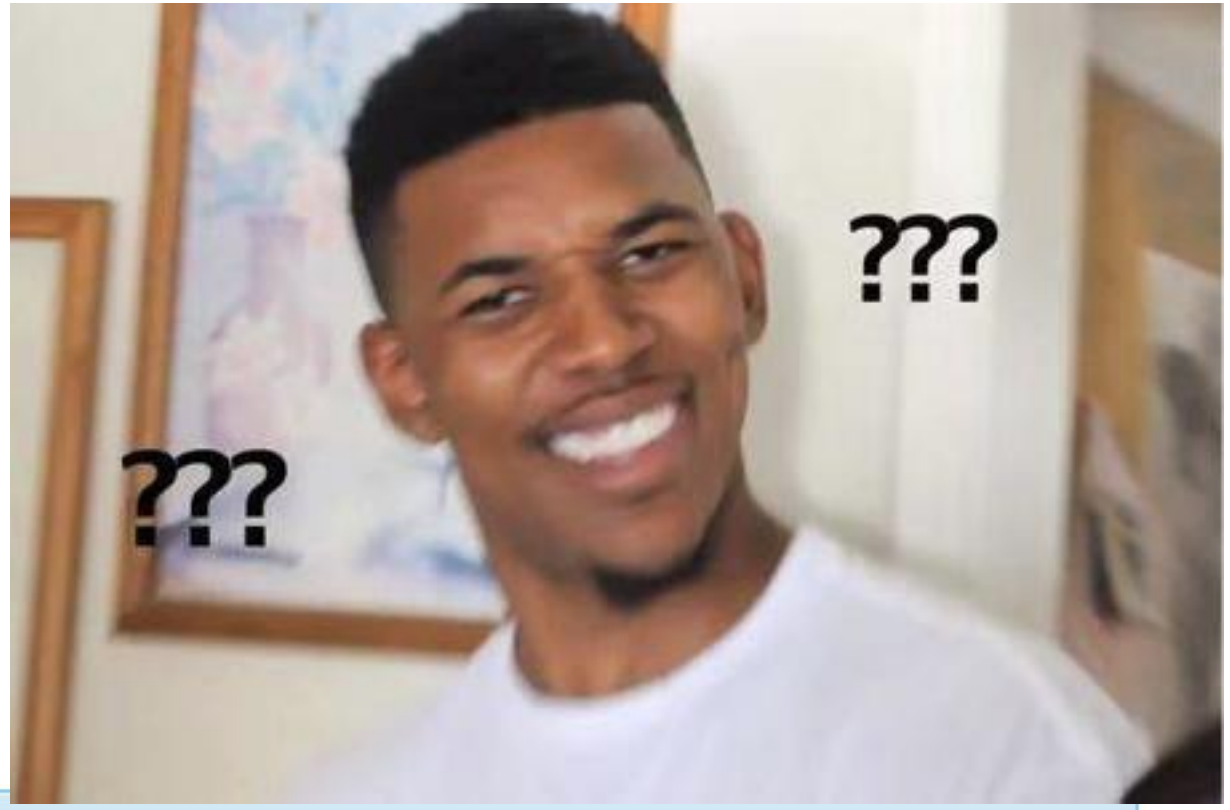
- 需要文件上传



注：Linux下可以发送文件变更内容，agent需要对文件进行备份且发送变更内容长度受限


Agent syscheckd
ossec server
realtime direcotry
when asp/aspx/jsp/……
file change send content
remoted
file exist
N
save file & hash
agent upload dir
syscheckd
realtime monitor
analysisd
save shell hash
file change
webshell
yara/custom scan
webshell
Y -- Alter message
N -- 自动化发布系统联动
有发布
N
安全人员介入
完善监测规则





alert_new_files

Specifies if syscheck should alert on new files created.

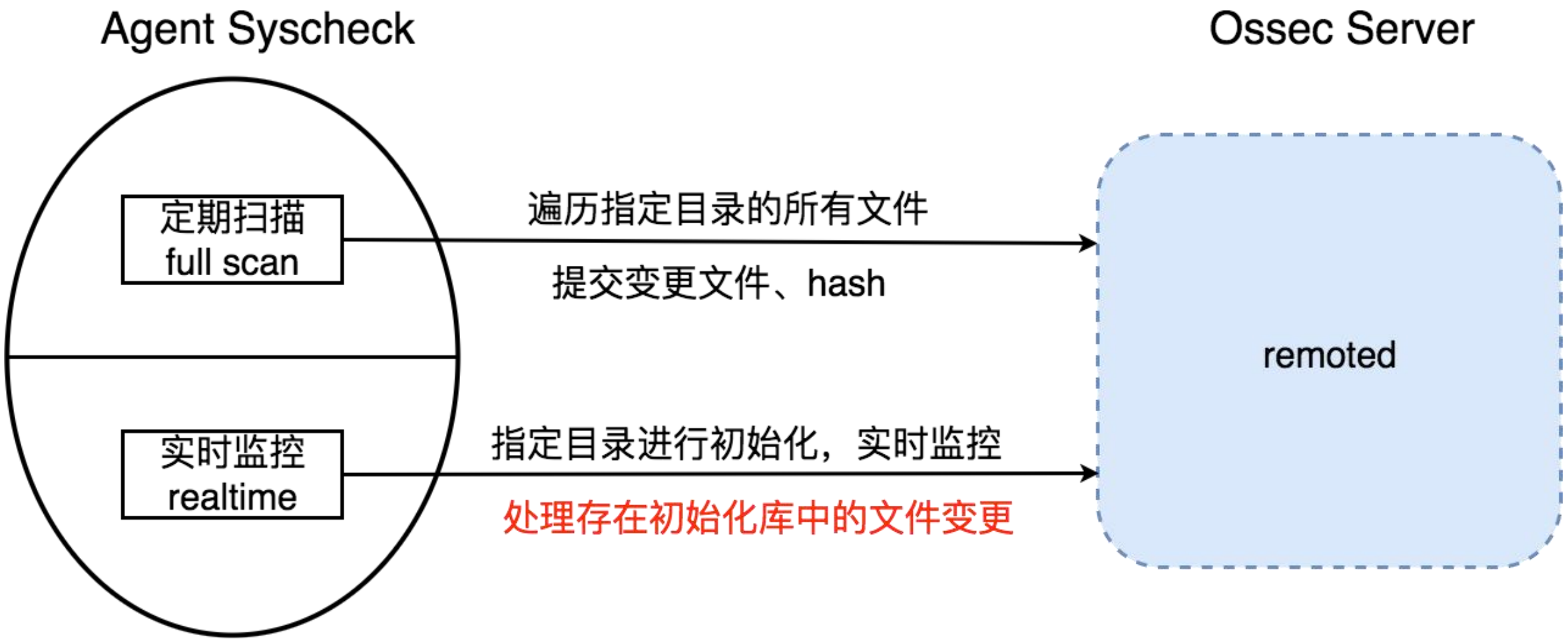
Default: no

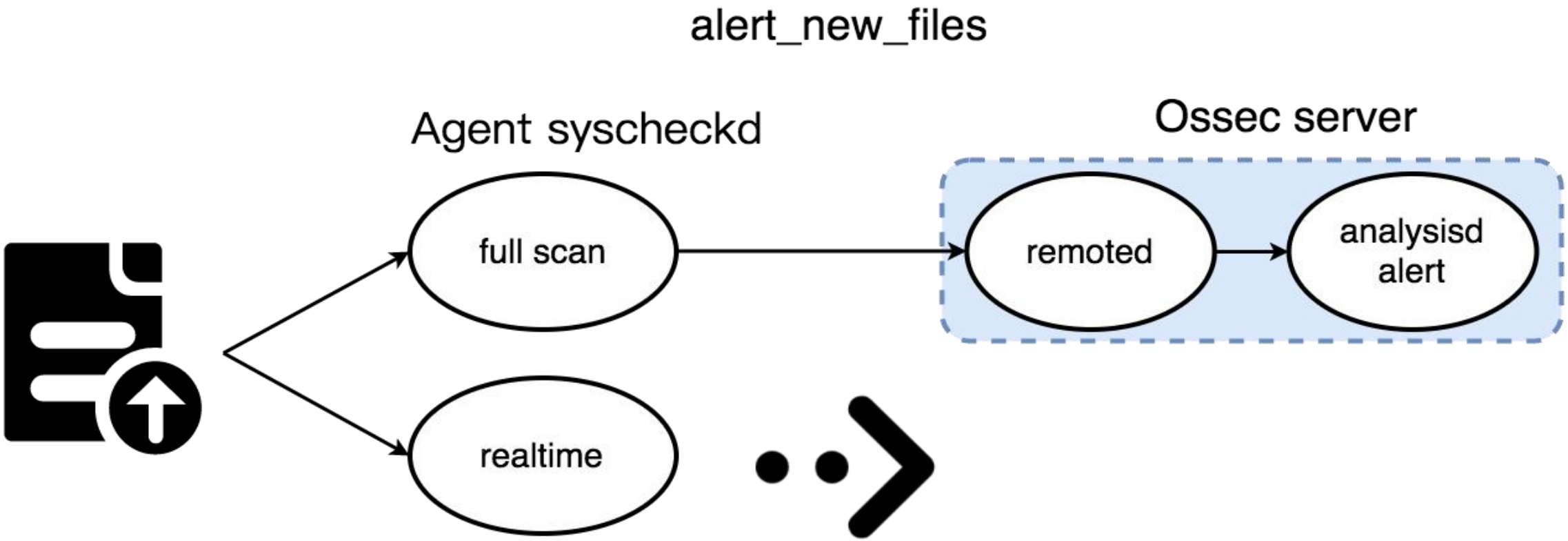
Allowed: yes/no

Valid: server, local

Note

New files will only be detected on a full scan, this option does not work in realtime.

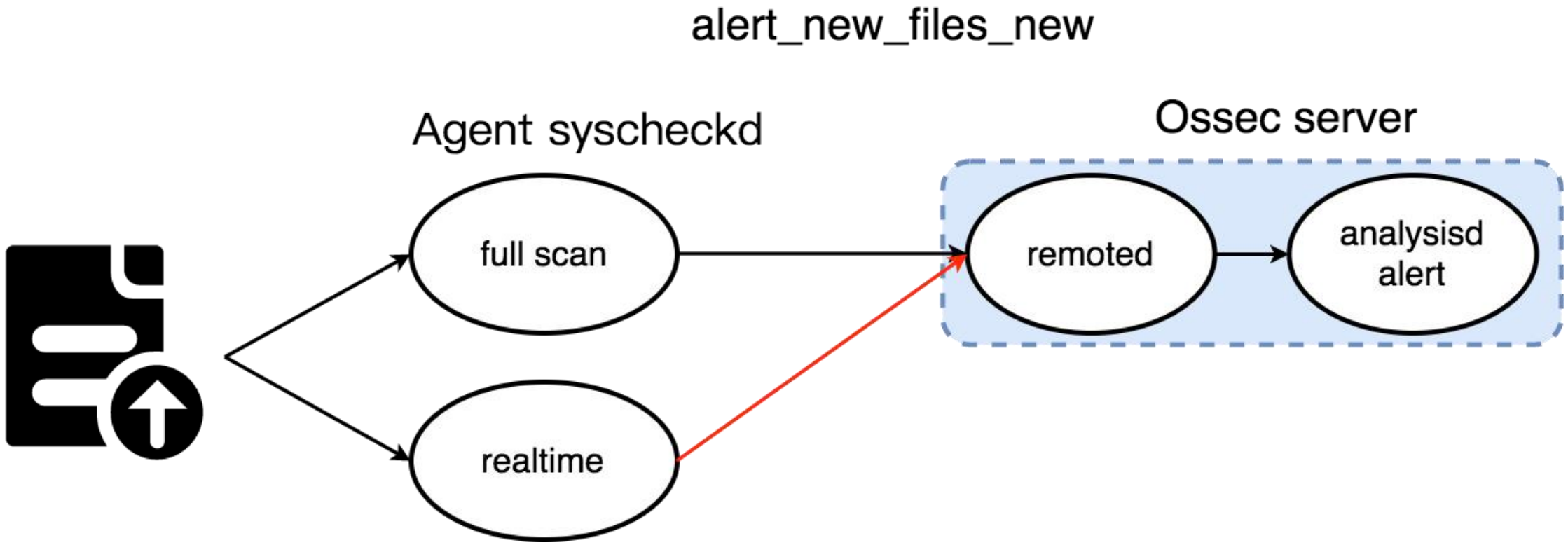


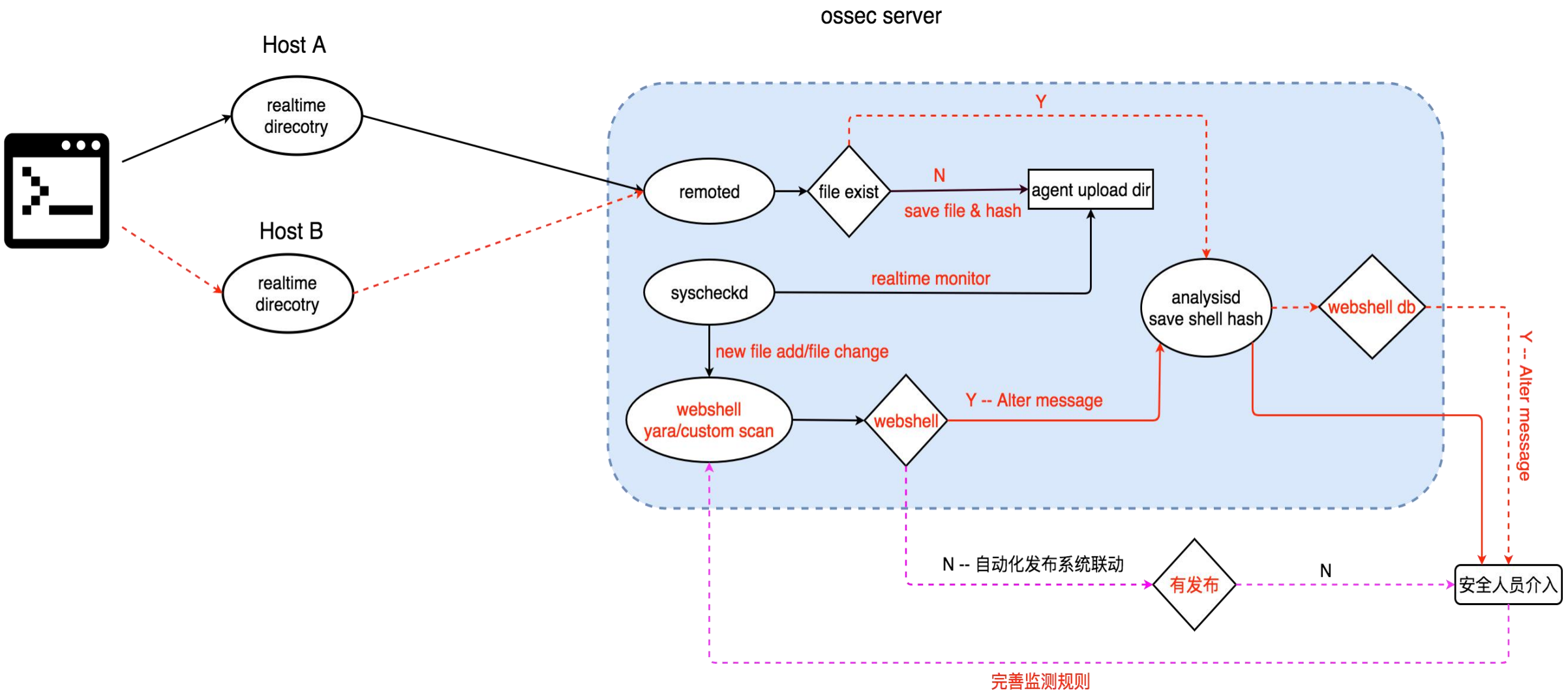


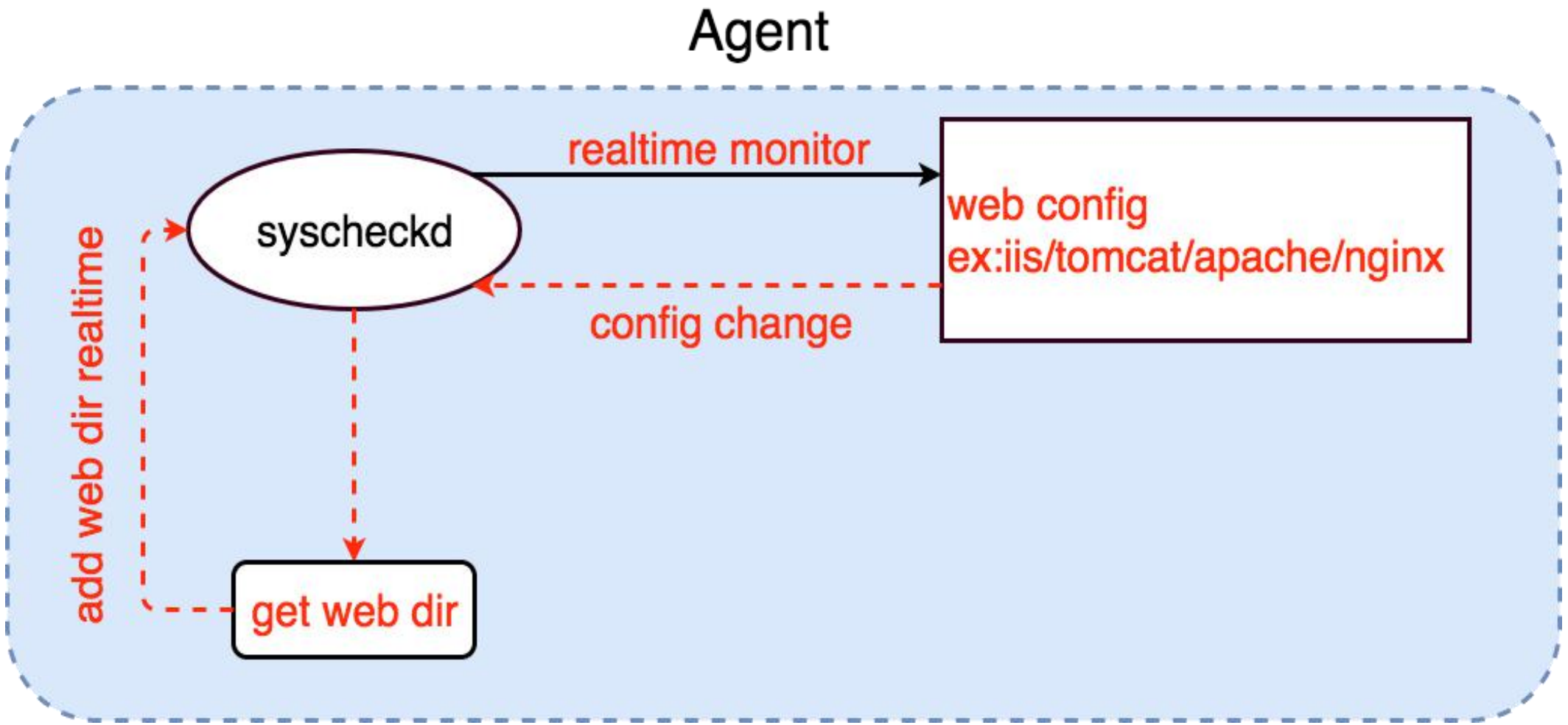
WindowsOs:ReadDirectoryChangesW

LinuxOs:inotify

- ✓IN_CREATE
- ✓IN_ATTRIB
- ✓IN_DELETE
- ✓IN_MODIFY
- ✓.....




ossec server
Host A
realtime direcotry
Host B
realtime direcotry
remoted
file exist
N
save file & hash
agent upload dir
Y
syscheckd
realtime monitor
new file add/file change
webshell yara/custom scan
webshell
Y -- Alter message
analysisd save shell hash
webshell db
Y -- Alter message
N -- 自动化发布系统联动
有发布
N
安全人员介入
完善监测规则



帐户已成功登录
帐户登录失败
用户权限已分配
用户帐户已被更改
策略已经更改
试图重置帐户密码
用户帐户已删除
用户被添加到本地安全组
用户帐户被锁定
审计日志被清除
……

自实现的正则

非标准XML解析

Decode/Rule字段

Windows 32 on 64

cJson中文内存泄露

官方文档不完善

希望有更多的人关注、使用、回馈社区

Agent优化：

将安全基线等检查整合进去

融合类sysmon功能，可以更全方位的掌握主机状态

.....

服务端性能优化

目前服务端太过于依赖文件，希望可以用缓存等替换

analysisd增加多线程，发挥服务器性能，增加处理能力

.....

THANKS
Q&A

应用安全、安全管理
tuhongwei@yiguo.com