云享家 | 基于AWS云平台的IDS联合监控分析

原创：沈晓卿 BespinGlobal 10月29日

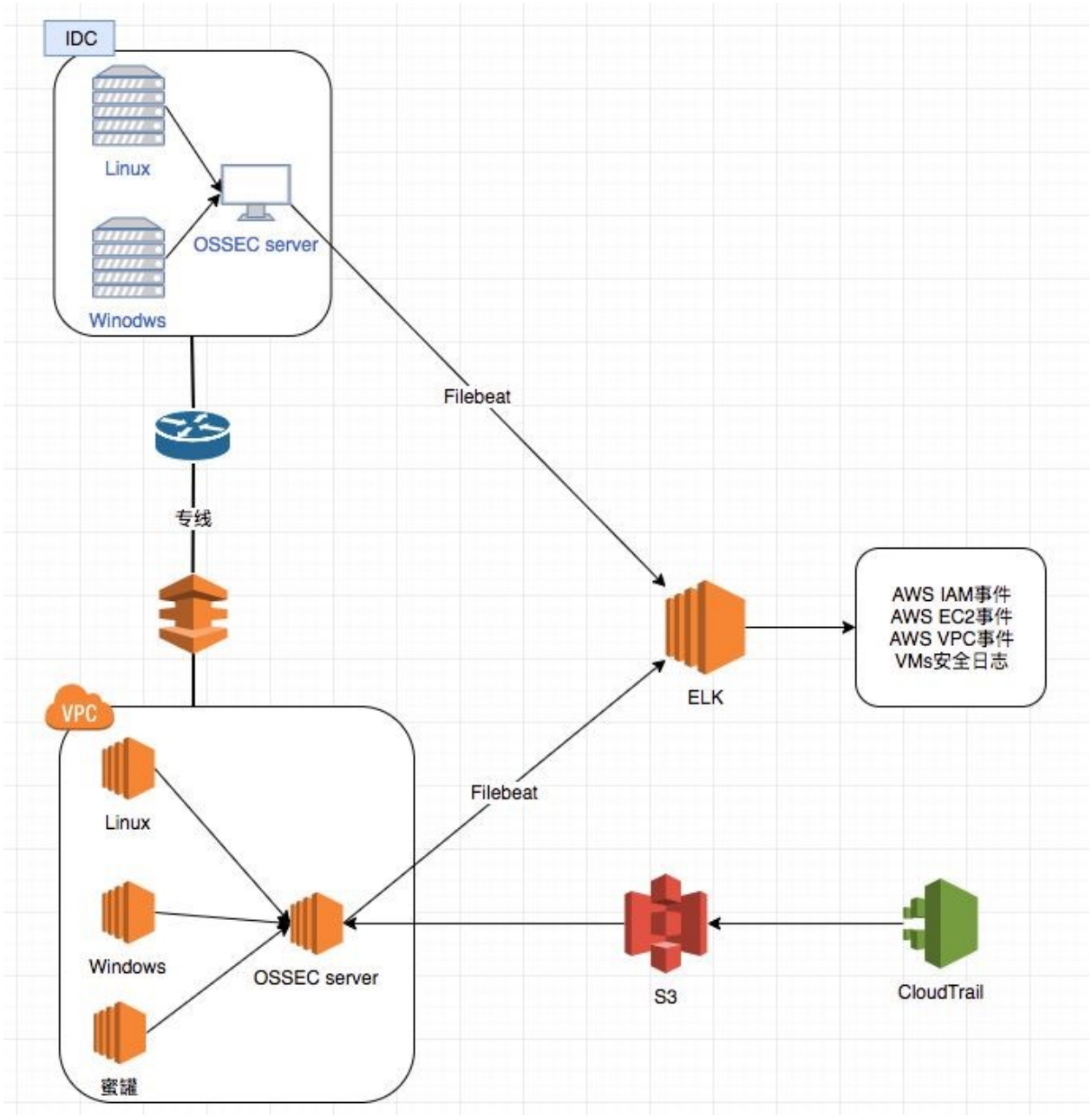
入侵检测（Intrusion Detection）是对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、其它网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。因此被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测。本期“云享家”要和大家分享的是“**基于AWS云平台的IDS联合监控分析**”。

为什么要做IDS联合监控?

- 安全日志过大、误报过多、难以很好的展示。
- 系统是否存在rootkit？系统基线是否符合标准?
- 如何持续性对系统做合规检查，PCI-DSS、GDPR等?
- 混合云环境如何集中收集安全日志?

方案介绍

2.1 基于OSSEC+ELK+AWS S3+多蜜罐架构



2.2 架构说明

- OSSEC是一个可扩展的，可移植的开源入侵检测系统（HIDS）。OSSEC负责给PCI-DSS提供的服务包括日志分析，文件完整性检查，监控策略，入侵检测，实时报警和及时响应。日常情况下，该系统作为日志分析工具，实时监控并分析网络的活跃情况，服务器和用户身份认证。OSSEC是由两部分组成，一个是中央管理部分(manager)，用于接收并监控传入的日志数据;另一个是采集器(wazuh-agents)用于采集数据，并将信息发送给中央管理器(manager)。
- 以wazuh-manger为服务核心，通过Flilebeat将日志数据传输到ELK做集中展示。
- 通过S3存储读取AWS CloudTrail日志，使ELK分析AWS CloudTrail日志。
- Wazuh为OSSEC的日志管理平台集成开发了一个模块。为了使OSSEC入侵检测系统可以支持ELK，我们将用Wazuh HIDS模块
- 通过大量部署蜜罐，来增大内网捕获黑客的几率。

2.3 使用的服务

- ossec: 基于主机的HIDS，用于安全检测，合规性监控。此外ossec还支持通过syslog收集防火墙、交换机、路由器等事件日志。
- ELK: 软件套件（Filebeat，Logstash，Elasticsearch，Kibana），用于收集，解析，索引，存储，搜索和显示日志数据。它提供了一个Web前端，提供事件的高级仪表板视图，允许对事件数据存储进行深入分析和数据挖掘。
- S3: 存储CloudTrail的事件。
- 蜜罐: 欺骗黑客，收集黑客行为。

2.4 实现功能

- 文件完整性监控: 在修改文件时触发警报；
- 日志收集：监控重要系统日志、防火墙日志、WAF日志；
- 异常检测：检测系统上的恶意软件，如：rootkit。通过，文件完整性行、运行进程、隐藏文件、网络接口多维度检测。
- PCI DSS合规检测：通过执行日志分析，文件完整性检查，策略监控，入侵检测，实时警报和主动响应来帮助实施PCI DSS。
- 蜜罐：多蜜罐部署，SSH中交互式蜜罐，针对windows SMB蜜罐、Struts2漏洞等。支持样本分析，重现。
- 外部API集成：通过集成VirusTotal API可以聚合多个防病毒产品以及在线扫描引擎。

使用方式

3.1 使用流程简单介绍

1) 部署wazuh-manger；
2) 开启AWS CloudTrail, S3；
3) 创建AWS CloudTrail key，给wazuh-manger调用；
4) 部署ELK整套套件；
5) 在相关实例上部署ossec wazuh-agent；
6) 登入ELK查看日志；
7) 部署多蜜罐加强防御；

3.2 对于已有系统的影响

操作系统需要安装ossec wazuh-agent，ossec wazuh-agent的系统消耗非常小。

3.3 联合安全日志处理

规则会进行不同的分组处理，以防止误报。

联合安全日志展示

- 所有安全日志的分类展示

- AWS事件展示

- PCI DSS事件展示

使用ossec联动蜜罐

- 公网的蜜罐
- 直接暴露在公网的蜜罐
- 收集不同的webshell，rootkit，暴力破解词典等，以便将来针对性的做安全加固。
- 内网的蜜罐
- 不暴露在公网，只能内网访问
- 当黑客攻入防火墙后，对内网进行扫描时，可以通过内网的蜜罐，引诱黑客，且通过wazuh-manger第一时间告警，防止黑客对正式业务造成损坏。

5.1 蜜罐日志展示

- 漏洞利用

- 黑客行为记录

5.2 部署方式

安装cowrie

- Cowrie是一款中度交互的SSH与Telnet蜜罐，用于记录攻击者的暴力破解攻击和shell交互。

安装方式参考https://github.com/cowrie/cowrie.git

1. 在cowrie上安装wazuh-wazuh-agent
2. 在wazuh-manger上使用分组功能集中管理wazuh-wazuh-agent，下图将cowire加入sec分组

3. 配置/var/ossec/etc/shared/sec/wazuh-agent.conf ，添加cowire的日志文件目录以及payload目录

4. 在wazuh新增cowire的rules，vim /var/ossec/ruleset/rules/0900-cowrie_rules.xml

5. 重启wazuh-manger

6. 先等30分钟，让公网上黑客来扫描，之后登入ELK查看

7. 同样的部署方式可以在内网中部署别的蜜罐如下：

- Cowrie：中交互ssh蜜罐
- Glastopf：低交互型Web应用蜜罐

- Elasticpot：模拟elastcisearch RCE漏洞的蜜罐
- Honeytrap：观察针对TCP或UDP服务的攻击

ossec实战

6.1 SQL Injection

通过部署部署sql靶机环境，来看下OSSEC是如何帮助我们识别SQL注入。

- 通过docker部署dvwa靶机环境，并将apache的日志文件挂在到本地

- 在dvwa上部署wazuh-agent
- 在wazuh-manger创建apache分组，并将sqli-lab注册到该分组下
- 修改/var/ossec/etc/shared/apache/wazuh-agent.conf

使用sqlmap对dvwa中sql injection模块进行注入，通过ossec的log测试模块看ossec是如何对sql注入进行识别的。

当收到一条log后，会使用/var/ossec/ruleset/decoders 中的0375-web-accesslog_decoders.xm解码模块进行解码，并且匹配/var/ossec/ruleset/rules中的0245-web_rules.xml进行告警。

通过登入ELK可以看到已经收到这些告警。

通过在云平台部署ossec集成到elk中可以很好的帮助企业监控自己所需要监控的安全项，上述例子中使用了AWS和linux，ossec同时也支持windows，openBSD，Azure，Aliyun等。同时也可以根据不同的log格式定制不同的decode模块，告警类型。

END

往 期 精 彩

云享家 | 多面手完善AWS CloudWatch监控图表
云享家 | AWS CloudWatch如何集成微信报警

阅读原文