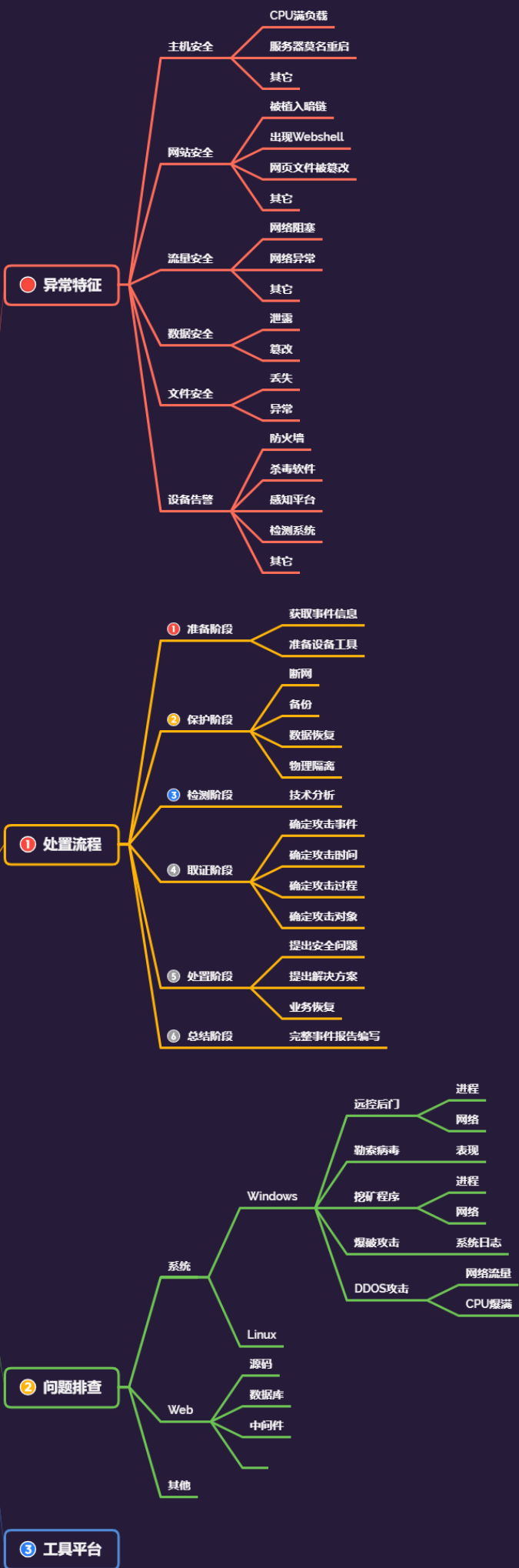


Day167 应急响应-日志自动 提取分析项目 &ELK&Logkit&LogonTrace r&Anolog等



蓝队应急-小迪安全



1.知识点

- 1、日志自动提取项目
- 2、日志自动分析项目
- 3、大型日志分析项目

2.内容点



- 1 应急响应：
- 2 1、抗拒绝服务攻击防范应对指南
- 3 2、勒索软件防范应对指南
- 4 3、钓鱼邮件攻击防范应对指南
- 5 4、网页篡改与后门攻击防范应对指南
- 6 5、网络安全漏洞防范应对指南
- 7 6、大规模数据泄露防范应对指南
- 8 7、僵尸网络感染防范应对指南
- 9 8、APT攻击入侵防范应对指南
- 10 9、各种辅助类分析工具项目使用



- 1 溯源反制：
- 2 威胁情报，信息库追踪，设备反制，IDS&IPS等反制，工具漏洞反制，蜜罐钓鱼反制等



- 1 威胁情报相关平台:
- 2 **virustotal**
- 3 深信服威胁情报中心
- 4 微步在线
- 5 **venuseye**
- 6 安恒威胁情报中心
- 7 **360**威胁情报中心
- 8 绿盟威胁情报中心
- 9 **AlienVault**
- 10 **RedQueen**安全智能服务平台
- 11 **IBM X-Force Exchange**
- 12 **ThreatMiner**

3.演示案例

3.1 日志分析商业工具项目-推荐十款




- 1 **1、Solarwinds Log&Event Manager:** windows的日志分析工具，可提供集中的日志监控体验和事件时间检测，拥有超强的响应能力，能够快速找出问题所在。检测到问题之后，自动响应阻止**IP**，关闭应用，改变访问权限，禁用帐户，**USB**设备等，将风险降至最低。该工具适合需要高度合规性的大型企业，提供一个**30**天的免费试用。
- 2 **2、PRTG Network Monitor:** 是一个网络监控平台，它提供的通知系统具有高度可定制性，这意味着几乎可以在任何设备上从**PRTG**接收网络性能更新。它的免费版本最多支持**100**个传感器，之后就必须使用付费版本，此外，它也提供**30**天的免费试用。

- 3 **3、Papertrail:** 是windows的日志分析器,可自动扫描日志数据,还可以选择希望扫描结果显示的信息,能够更快地找到安全事件的原因,可以按时间,来源或选择的自定义字段筛选日志事件,消除最重要的不相关数据。此外,它还可以通过另一种类似过滤选项允许你检测日志数据的趋势。可以按源,数据,严重性级别,工具或消息内容过滤事件。过滤后的搜索完成后,能够在屏幕底部查看结果图表。该工具是易于部署的日志分析器的理想选择。它提供免费的计划,允许每月监控多达**100 MB**的数据。
- 4 **4、Splunk:** 使用最广泛的日志管理平台之一,能够实时监控日志和数据。它的多功能性使其能够从网络中的几乎任何设备或应用中获取日志数据,轻松搜索栏查看实时和历史数据,更快找到所需信息。实时警报,能够让你不错过任何问题,有效缩短事件解决时间。**Splunk Free**是免费提供的,每位用户最多可以支持**500 MB**的数据。
- 5 **5、Xpolog:** 可以通过网络收集和分析来自设备的日志,通过实时监控日志,迅速发现问题,发出警报。最突出的一个特点是它的**AI**驱动的错误检测,及时把控安全风险,并区分表明性能不佳的日志模式。**Xpolog**的价格取决于你需要的用户数、保留数和数据量。**Basic**版本是免费的,每天支持**1GB**,**5**天数据保留。
- 6 **6、ManageEngine EventLog Analyzer:**提供简化的用户体验,能够从各种安全解决方案中收集日志。它的警报系统可以帮助你导航日志数据。该工具适用于**32**位和**64**位的**windows**和**Linux**,可以下载两个版本:免费版和高级版。免费版最多支持五个日志源,而高级版支持多达**1000**个日志源。
- 7 **7、LOGalyze:** 是一款面向企业用户的开源日志分析器和网络监控工具,支持具有实时事件检测功能的设备、**windows**主机和**Linux / Unix**服务器。可以使用搜索功能查找所需的日志数据,用户可以自定义相关警报,创建故障,记录问题。这种工具是一种低成本替代方案,特别适合寻求经济实惠的日志管理解决方案的小型企业。

- 8 8、**Datadog**: 可以记录和搜索来自各种设备和应用程序的日志数据, 以图形的形式显示日志数据, 随时看到网络性能的变化情况, 并通过过滤器来确定列出的信息。“集中存储”的方法可以更好地防止日志泄露。**Datadog**提供14天免费试用版。
- 9 9、**EventTracker**: 可以收集和分析**windows**事件、**syslog**和**w3C/IIS**日志文件中的日志数据, 实时检测安全事件, 提供数百种不同的警报外的开箱与**EventTracker**。
- 10 10、**LogDNA**: 可以实时监控日志数据, 在云的基础上, 可以在不到两分钟的时间内配置为从**AWS**, **Heroku**, **Elastic**, **Docker**和其他供应商收集日志, 并立即使用带宽聚合来自网络中应用程序和服务器的日志, 以处理每秒一百万个日志事件。该工具适用于需要基于云的可扩展日志管理解决方案的企, 免费版支持单个用户。

3.2 日志自动提取-七牛Logkit&观星应急工具

- 
- 1 1、七牛**Logkit**: (**windows&Linux&Mac**等)
 - 2 <https://github.com/qiniu/logkit/>
 - 3 支持的数据源 (各类日志, 各个系统, 各个应用等)
 - 4 **File**: 读取文件中的日志数据, 包括**csv**格式的文件, **kafka-rest**日志文件, **nginx**日志文件等, 并支持以**grok**的方式解析日志。
 - 5 **Elasticsearch**: 读取**ElasticSearch**中的数据。
 - 6 **MongoDB**: 读取**MongoDB**中的数据。
 - 7 **MySQL**: 读取**MySQL**中的数据。
 - 8 **Microsoft SQL Server**: 读取**Microsoft SQL Server**中的数据。
 - 9 **Postgre SQL**: 读取 **PostgreSQL** 中的数据。
 - 10 **Kafka**: 读取**Kafka**中的数据。
 - 11 **Redis**: 读取**Redis**中的数据。
 - 12 **Socket**: 读取**tcp\udp\unixsocket**协议中的数据。
 - 13 **Http**: 作为 **http** 服务端, 接受 **POST** 请求发送过来的数据。
 - 14 **Script**: 支持执行脚本, 并获得执行结果中的数据。

- 15 Snmp: 主动抓取 Snmp 服务中的数据。
- 16 2、观星应急工具: (windows系统日志)
- 17 SglabIr_Collector是qax旗下的一款应急响应日志收集工具, 能够快速收集服务器日志,
- 18 并自动打包, 将收集的文件上传观心平台即可自动分析。

3.3 日志自动分析-操作系统-Gscan&LogonTracer

- 1 1、Linux 系统 - GScan
- 2 <https://github.com/grayddq/GScan>
- 3 2、windows 系统 -LogonTracer
- 4 <https://github.com/ffffff0x/f8x>(自动搭建项目)
- 5 <https://github.com/JPCERTCC/LogonTracer> (建议手工安装不要docker安装)
- 6 如何安装使用:
- 7 <https://github.com/JPCERTCC/LogonTracer/wiki/>
- 8 不建议Docker安装:
- 9 <https://www.freebuf.com/sectool/219786.html>
- 10 docker pull jpcertcc/docker-logontracer
- 11 docker run \
- 12 --detach \
- 13 --publish=7474:7474 --publish=7687:7687 --publish=8080:8080 \
- 14 -e LTHOSTNAME=你的ip \
- 15 jpcertcc/docker-logontracer
- 16 建议手工安装:
- 17 1.下载并解压neo4j: tar -zxvf neo4j-community-4.2.1-unix.tar
- 18 2.安装java11环境: sudo yum install java-11-openjdk -y
- 19 3.修改neo4j配置保证外部访问:
- 20 dbms.connector.bolt.listen_address=0.0.0.0:7687

```
21 dbms.connector.http.listen_address=0.0.0.0:7474
22 ./bin/neo4j console &
23 4. 下载LogonTracer并安装库:
24 git clone
    https://github.com/JPCERTCC/LogonTracer.git
25 pip3 install -r requirements.txt
26 5. 启动LogonTracer并导入日志文件分析
27 python3 logontracer.py -r -o [PORT] -u
    [USERNAME] -p [PASSWORD] -s [IP地址]
28 python3 logontracer.py -r -o 8080 -u neo4j -p
    xiaodi -s 47.98.99.126
29 python3 logontracer.py -e [EVTX文件] -z [时区] -u
    [用户名] -p [密码] -s [IP地址]
30 python3 logontracer.py -e Security.evtx -z -13 -
    u neo4j -p xiaodi -s 127.0.0.1
31 6. 刷新访问LogonTracer-web_gui查看分析结果
32 踩坑: 1、上传按钮不能上传 2. 上传失败记得上传选模式对应值
```

3.4 日志自动分析-Web-360星图&Goaccess&ALB&Anolog



```
1 1、web - 360星图 (IIS/Apache/Nginx)
2 2、web - GoAccess (任何自定义日志格式字符串)
3 https://github.com/allinurl/goaccess
4 使用手册:
5 https://goaccess.io/man
6 输出报告:
7 goaccess -f /home/wwwlogs/access.log --log-
    format=COMBINED > /root/aa.html
8 实时监控:
9 goaccess -f /home/wwwlogs/access.log --log-
    format=COMBINED --real-time-html >
    /home/wwwroot/default/x.html
```



```
10 3、web - 自写脚本（任何自定义日志格式字符串）
11 参考: https://github.com/Lucifer1993/ALB
12 python ALB.py -f F:\access.log -t 200
13 参考: 机器语言
14 4、web -机器语言（任何自定义日志格式字符串）
15 https://github.com/Testzero-wz/analog
16 https://analog.testzero-wz.com/
```

3.5 日志综合平台-

Elasticsearch+Filebeat+Redis+Logstash+Kibana