



态势感知平台分析培训

绿盟科技版权所有

2019护网专项培训





工作原理

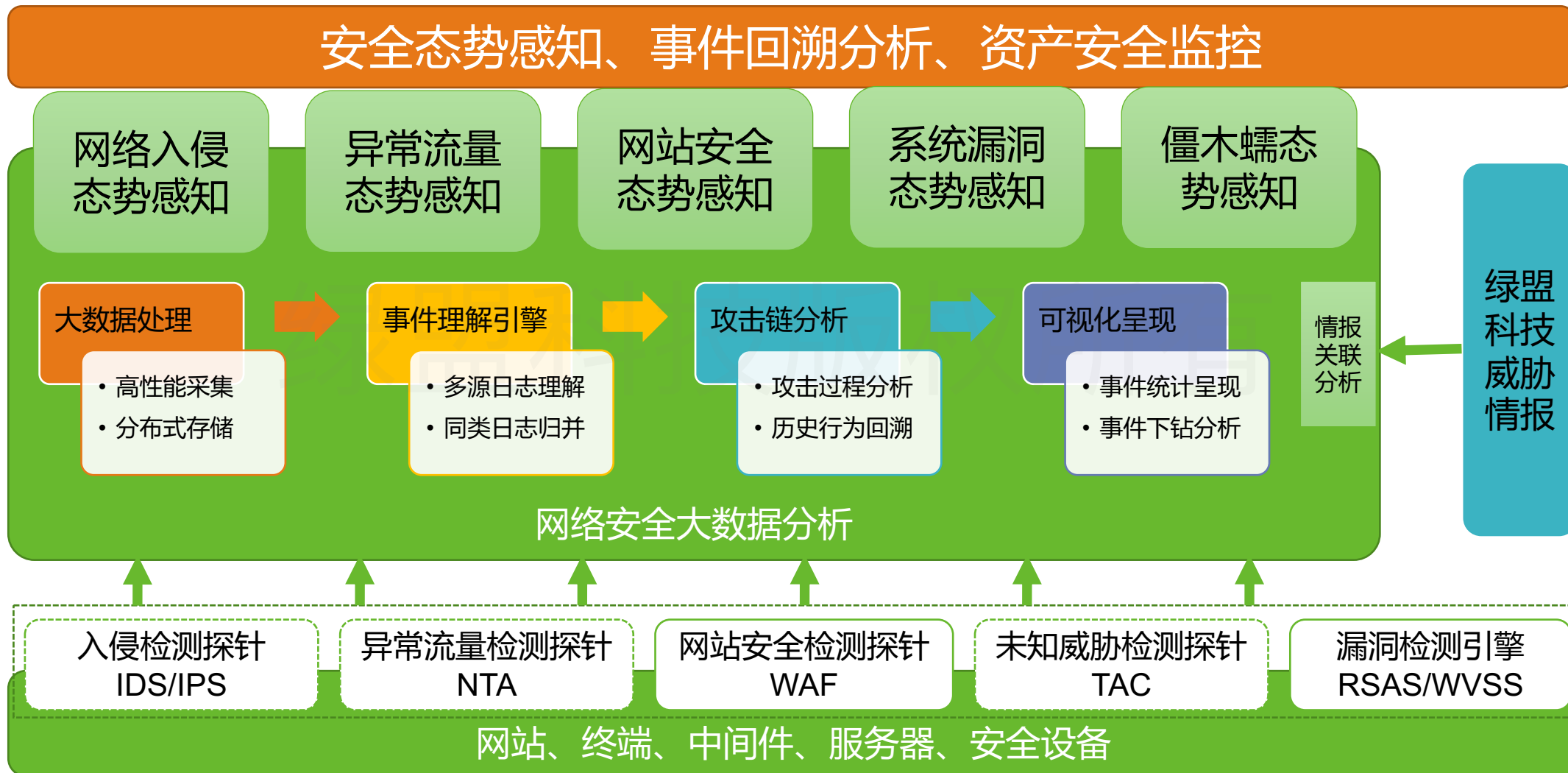
部署方式

查询分析

01

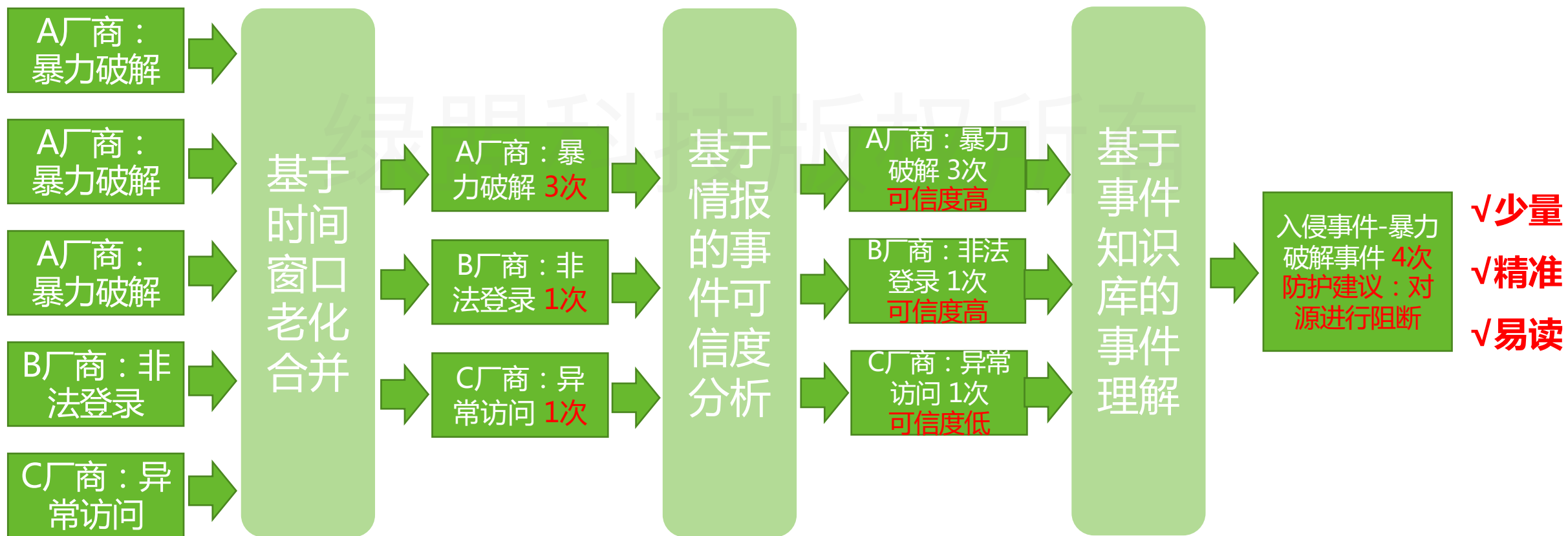
工作原理

绿盟安全态势感知平台



▶▶ 事件理解模型

事件理解模型可智能化的将时间窗口的多厂商同类型安全设备日志，进行理解、压缩、过滤，理解成同类型少量、精准、易读的安全事件，为后续关联分析提供支撑。



▶▶ 基于攻击链的安全分析

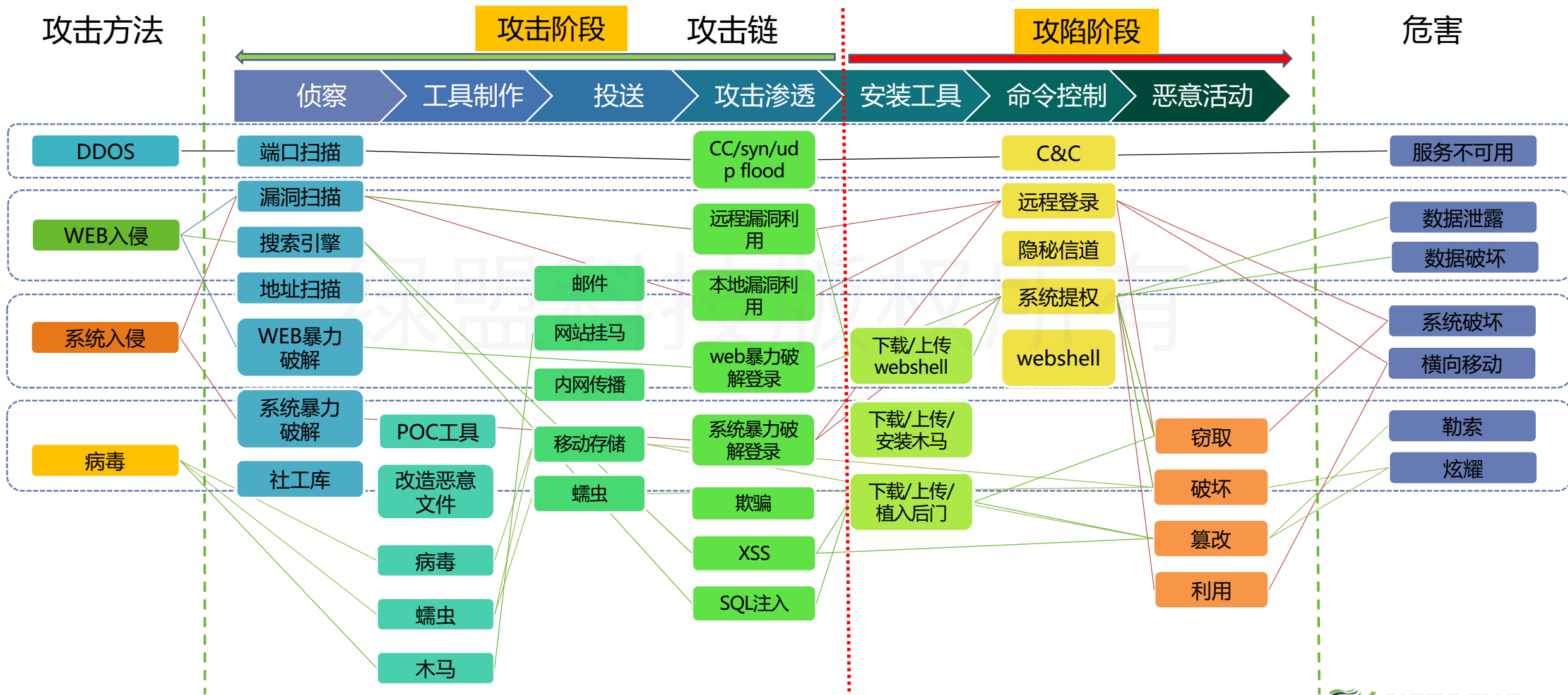
网络攻击是分阶段发生，并可以通过在每个阶段建立有效的防御机制中断攻击行为。

----洛克希德·马丁



攻击链为黑客攻击行为的分析，提供了有效的理论支撑。

机器学习实践—攻击过程归纳

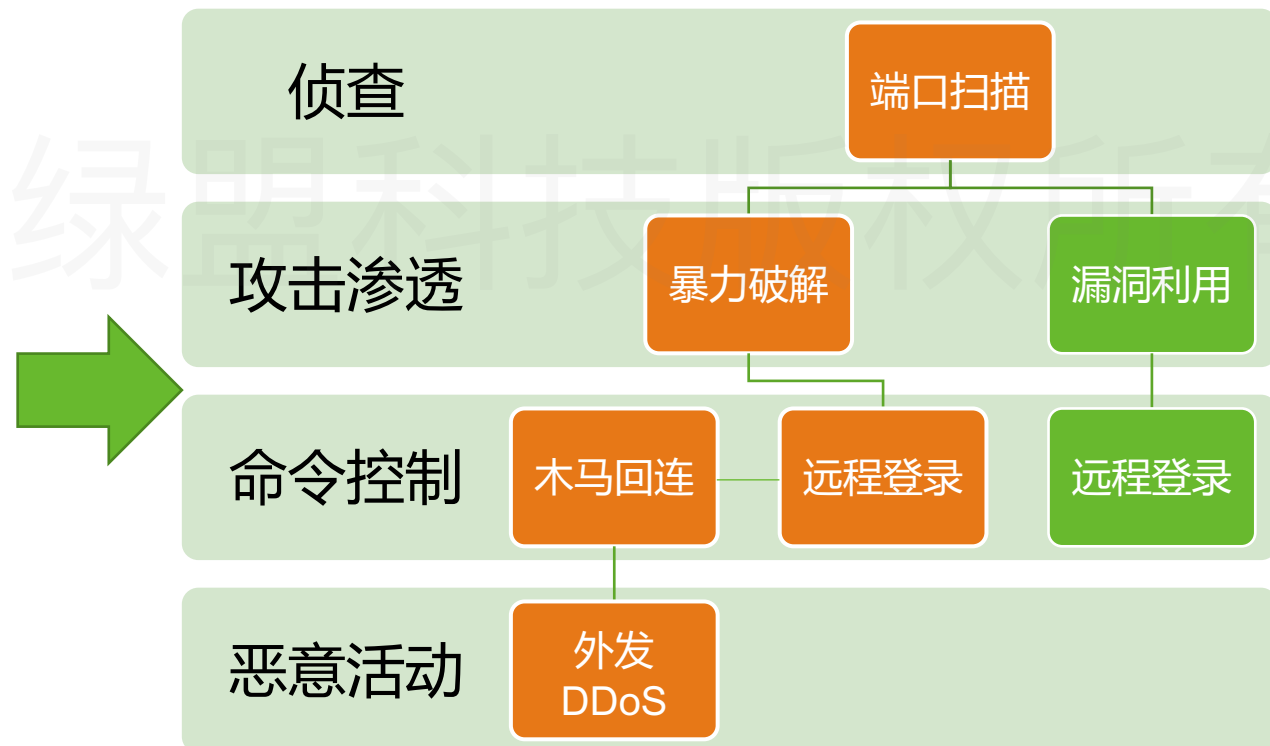


攻击分析过程

传统告警

告警事件列表
2017.5.3-端口扫描
2017.5.6-暴力破解
2017.5.7-提权
2017.5.7-漏洞利用
2017.5.8-远程登录
2017.5.8-木马回连
2017.5.9-外发DDoS

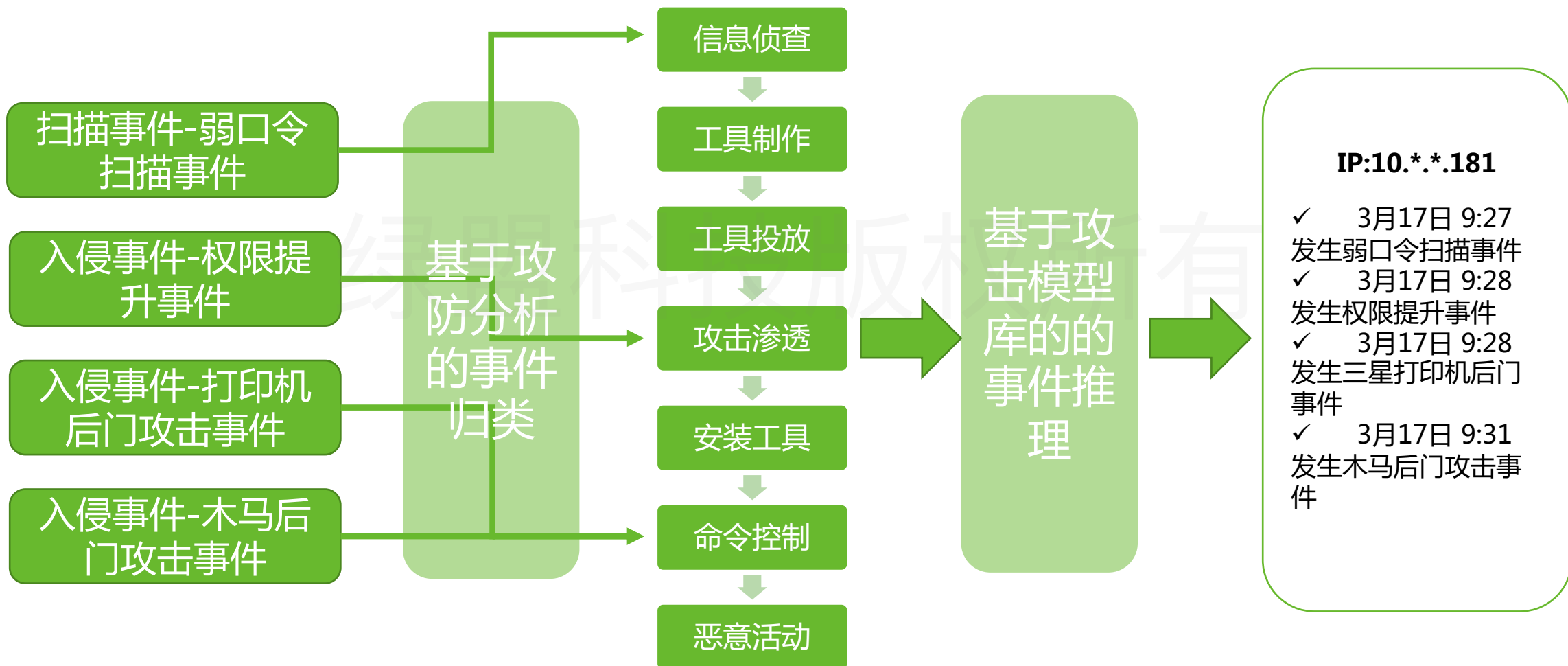
攻击过程分析



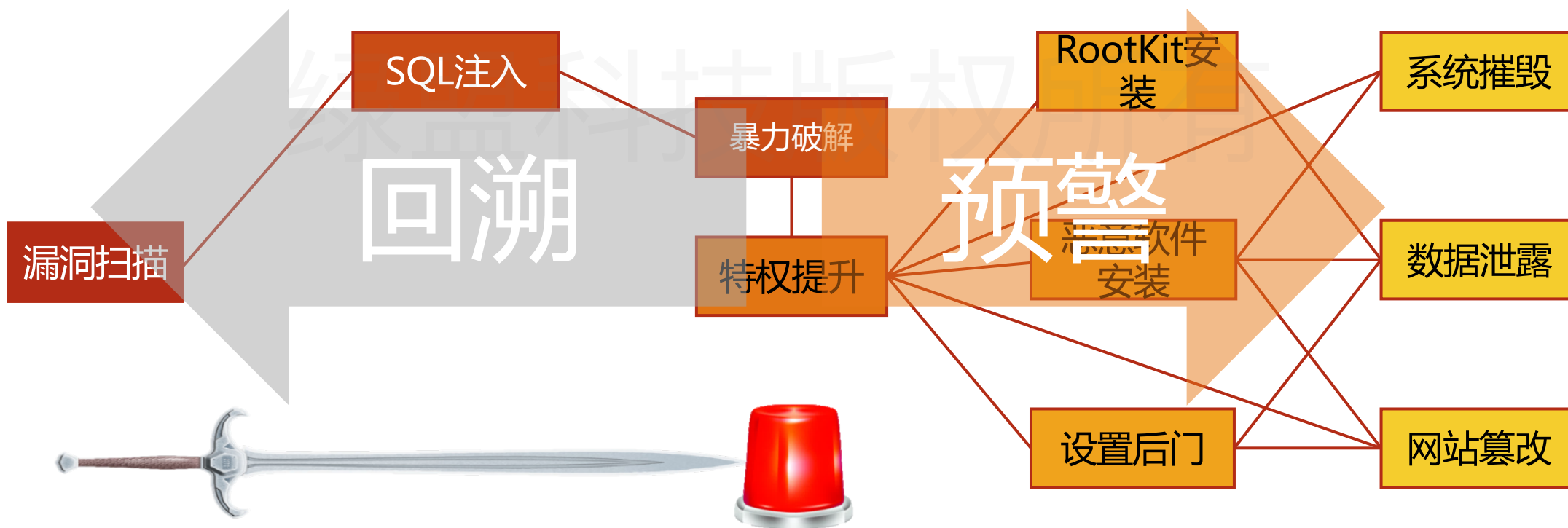
态势告警



安全场景分析



攻防场景预警及回溯



02

部署方式

▶▶ BSA安装部署流程

一.和商务申请证书

1.1申请加密狗，只能识别无驱，如何判断有驱无驱参考WIKI

所有材料请必须从工程ftp获取

二. 安装及部署

2.1操作系统centos7.3，参考操作系统安装手册和BSA安装部署手册中的要求

2.2获取BSA和APP安装包，推荐BSA F05，TSA F02，TAM F00SP03

2.3后台配置及安装BSA，参考BSA安装部署手册

2.4前台倒入证书，初始化BSA，分盘及部署组件等，参考BSA安装部署手册

2.5安装TSA,TAM APP

三.数据接入

3.1设备端安装部署及配置联动，数据接入，详情咨询设备端技术支持

3.2老A接口接入需部署BSA转发器，通过设备—转发器—BSA方式接入

3.3三方数据接入，需要配置Grok解析规则及自定义事件规则

四.数据查看

4.1查看TAM首页面及挖掘检索下的重点事件、告警，原始日志是否正常；
查看TSA首页面及风险态势下的子态势事件，数据分析下的原始日志是否正常；

4.2查看集群管理的状态，Hadoop的资源及Job状态等

和商务申请证书

绿盟科技版权所有

▶▶ BSA证书

- 集群可以给单机用，单机不可以给集群用
- 更换加密狗会有问题，因为安装时识别的hash是来自于加密狗内产生的hash



加密狗有驱无驱问题

- <http://192.168.255.65/iaes/search/viewsolution/5676>
- <http://192.168.255.65/iaes/search/viewsolution/7990>

BSA 加密狗使用、证书制作 [BSA的证书是使用加密狗hash制作的]

分类: BSA

BSA使用的是“深思洛克-精锐4型USB Key，支持U盘版和普通版：

- 1) U盘版都是无驱的，可以直接插在安装有BSA的服务器上使用。
- 2) 普通版分为：有驱动和无驱动两种，BSA只支持无驱型的。

注：如果从生产中心拿到的usb key是有驱动型的，需要通过工具转换为无驱动型的。详见知识点：11448

另外：

RSAS和BSA的加密狗，硬件相同，软件不同，不能混用。

1. 如何判断BSA使用的【普通版】加密狗是“有驱”还是“无驱”型的？ [加密狗有驱和无驱型识别和转换方法] ✓

2. 如何获取BSA加密狗的hash，供做证书使用？ [获取加密狗hash的方法] ✓

3. 如何查看BSA的证书信息？ [BSA证书查看方法] ✓

请前往工程**FTP**获取材料

▶▶ 材料获取

BSA系列产品安装包路径在install中，SP包及部分手册及漏洞修复方案均在upgrade中

The image shows two screenshots of a file explorer window. The top screenshot shows the directory /product_install/ with a table of files and folders. The bottom screenshot shows the directory /product_install/BSA/ with a table of files and folders.

名称	大小	修改时间	属性
上级目录			
1.安装平台所需操作系统	4 KB	2018/8/22 10:40:00	drwxr-xr-x
AAS-M	4 KB	2017/2/9	drwxr-xr-x
BSA	4 KB	2018/8/14 13:55:00	drwxr-xr-x

名称	大小	修改时间	属性
上级目录			
BSA	4 KB	2019/3/5 22:36:00	drwxr-xr-x
TAM	4 KB	2018/8/14	drwxr-xr-x
TAT	4 KB	2018/9/10	drwxr-xr-x
TSA	4 KB	2019/3/26 21:38:00	drwxr-xr-x
操作系统安装包及说明	4 KB	2019/4/2 22:40:00	drwxr-xr-x

材料获取

Windows Explorer window showing the directory structure of /upgrade/BSA/.

名称	大小	修改时间	属性
上级目录			
A.工程武道会	4 KB	2018/10/15 13:25:00	drwxr-xr-x
BSA	4 KB	2018/6/8	drwxr-xr-x
TAM	4 KB	2018/9/10 11:37:00	drwxr-xr-x
TAT	4 KB	2018/6/7	drwxr-xr-x
TSA	4 KB	2018/6/7	drwxr-xr-x
安装部署快速指南(一本通)	4 KB	2018/6/8	drwxr-xr-x
系统漏洞修复方案	4 KB	2018/8/21 11:01:00	drwxr-xr-x

Windows Explorer window showing the contents of /upgrade/BSA/BSA/4.技术文档/培训手册/.

名称	大小	修改时间	属性
上级目录			
2.BSA进阶培训.pptx	4.33 MB	2017/11/10	-n
4.第三方日志数据源接入BSA培训.pptx	1.32 MB	2017/5/3	-n
2018-12-27-《BSA运维介绍》.avi	252.08 MB	2018/12/28 13:55:00	-n
2019-03-12-《BSA F05产品培训》.mp4	53.03 MB	2019/3/20 10:00:00	-n
BSA F04培训.pptx	3.98 MB	2018/6/29	-n
BSA F05培训.pptx	2.55 MB	2019/3/11 17:52:00	-n
BSA运维介绍.pptx	6.46 MB	2018/12/27 16:06:00	-n
SOP-BSA售后培训.pptx	6.69 MB	2018/7/19	-n
北京培训-BSA.pptx	9.66 MB	2018/8/16	-n
西安培训-BSA.pptx	3.83 MB	2018/5/26	-n
重庆培训-BSA.pptx	10.77 MB	2018/8/17	-n

Windows Explorer window showing the contents of /upgrade/BSA/TAM/3.技术文档/常用配置手册/.



名称	大小	修改时间	属性
上级目录			
全流量的安装部署checklist(2019.4.2)	4 KB	2019/4/4 21:25:00	drwxr-xr-x
PVD-TAM-V2.0R00F00-ReleaseNotes版本更新说明.doc	231 KB	2018/7/23	-rw-r--r--
PVD-TAM-V2.0R00F00SP01-ReleaseNotes版本更新说明.doc	249 KB	2018/9/5	-rw-r--r--
PVD-TAM-V2.0R00F00SP02-ReleaseNotes版本更新说明.doc	211 KB	2018/12/11 15:33:00	-rw-r--r--
PVD-TAM-V2.0R00F00SP03-ReleaseNotes版本更新说明.doc	165 KB	2019/3/7 10:32:00	-rw-r--r--
绿盟全流量威胁分析系统安装配置手册-V2.0R00F00.pdf	1.33 MB	2018/7/23	-rw-r--r--
绿盟全流量威胁分析系统安装配置手册-V2.0R00F00SP01.pdf	1.11 MB	2018/9/4	-rw-r--r--
绿盟全流量威胁分析系统安装配置手册-V2.0R00F00SP02.pdf	1.06 MB	2018/11/23 15:17:00	-rw-r--r--
绿盟全流量威胁分析系统用户手册-V2.0R00F00.pdf	5.82 MB	2018/7/23	-rw-r--r--
绿盟全流量威胁分析系统用户手册-V2.0R00F00SP01.pdf	6.07 MB	2018/9/4	-rw-r--r--
绿盟全流量威胁分析系统用户手册-V2.0R00F00SP02.pdf	6.26 MB	2018/11/23 15:28:00	-rw-r--r--
绿盟全流量威胁分析系统证书制作说明-V2.0R00F00SP02.pdf	965 KB	2018/11/23 15:20:00	-rw-r--r--
全流量安装部署checklist(公司白牌服务器版本).xlsx	15 KB	2019/4/2 16:32:00	-rw-r--r--
全流量部署-服务器数量评估文档.xlsx	20 KB	2018/7/24	-rw-r--r--

部署操作系统

绿盟科技版权所有

配置要求

需求类型	推荐配置	
硬件	CPU	2 个 E5-2640 v3 2.60GHz 8 Core 及以上
	内存	128GB ECC DDR3
	硬盘	<ul style="list-style-type: none"> 2 块 1T 的 ssd 盘：建议配置 raid1，用来部署操作系统和 BSA 管理服务。集群部署时只需要管理节点部署两块 ssd 盘，工作节点不需要。 8~24 块 1.2T 的硬盘：建议每一块均配置成 raid0 盘或 no-raid 盘，用来部署 BSA 的组件，例如 hadoop 或 kafka 等。 <p> 说明 服务器磁盘不能配置为 raid5 格式或者 LVM 方式。</p>
	光驱	内置光驱
	网卡	1 块 Broadcom 5720 QP 1Gb 网络子卡、1 块 Broadcom 5719 PCIE Gb 网卡
	Raid 卡	推荐使用带有读写缓存的 raid 卡：例如 PERC H710p
	电源	热插拔冗余电源（1+1）1100 瓦

软件	操作系统	仅支持 64 位操作系统： <ul style="list-style-type: none"> Red Hat Enterprise Linux 6.5（注册过的） CentOS 6.5/7.x 推荐使用操作系统： <ul style="list-style-type: none"> CentOS 7.3 <p> 说明</p> <ul style="list-style-type: none"> ✓ 在安装前，请确认主机中只有新的操作系统、未安装多余软件，否则会导致 BSA 安装失败。 ✓ 安装操作系统时，需要选择安装 software development workstation 版本，否则会由于缺少依赖库，导致 BSA 安装失败。
	依赖库	已经安装如下库： <ul style="list-style-type: none"> cyrus-sasl
		<ul style="list-style-type: none"> cyrus-sasl-plain libxml2 libxslt fontconfig python2.6 或者 python2.7 java1.7 及其以上版本 <p> 说明</p> <ul style="list-style-type: none"> 若未安装依赖库，BSA 在安装管理节点时，会给出提示。在操作系统中可以执行 <code>yum install cyrus-sasl</code>，安装 cyrus-sasl 库。其他依赖库的安装与 cyrus-sasl 库类似，这里不重复介绍了。

配置要求

【基础功能模块】

- 1.数据接入和存储。包括流量日志，uts告警日志以及uts还原出来的文件。对应后台的高性能解析器，普通解析器，session日志入库，http日志入库，dns日志入库，普通入库job。
- 2.流量统计分析。对应后台的实时统计引擎。
- 3.内置场景检测。对应后台的恶意样本检测，uts告警日志检测，告警增强，告警入库，事件归并引擎。
- 4.重点事件、失陷资产、攻击者画像检测、查询和展示。对应后台的失陷资产、攻击者画像检测进程。
- 5.挖掘检索。包括事件、告警、流量日志的查询和展示。对应后台的thrift server进程。

【全部功能模块】

- 1、增加威胁情报联动功能。包括情报实时关联分析和回溯检测分析。
- 2、增加机器学习检测功能。包括蠕虫传播、dns隐蔽信道、僵尸网络、webshell访问检测模型。
- 3、自定义检测场景。包括自定义的实时和离线检测场景。

【单机场景】

单机场景只支持40核，128G内存，12*4TB的服务器，只支持跑基础功能模块，只能保留30天的数据。

用户输入区(黄色区域)	
功能场景	基础功能模块
带宽大小(Gbps)	5
数据保留时间(天)	30
服务器配置	
CPU(线程数)	40
内存(GB)	128 最低128GB，大于>=5Gbps的流量，建议使用256G内存的服务器。
磁盘(TB,可用空间):	4
数据盘数量(块):	12
计算结果	
需要的服务器的数量(台)	4 《集群规模》=7台时，单独拿一台机器作为集群管理节点。

操作系统分区

UEFI模式分区

The screenshot shows the 'MANUAL PARTITIONING' screen for CentOS Linux 7. On the left, a tree view shows the partition layout: DATA (/home/sdb sdb1, 3725.5 GiB), SYSTEM (/boot sda2, 10 GiB), and /boot/efi sda1, 10 GiB. The main area shows settings for partition sdb1: Mount Point is /home/sdb, Device(s) is DELL PERC H730 Mini (sdb), and File System is ext4. A red box highlights the File System dropdown (set to ext4) and the Label input field (containing 'gpt').

BIOS模式分区

The screenshot shows the 'MANUAL PARTITIONING' screen for CentOS Linux 7. On the left, a tree view shows the partition layout: DATA (/home/sdb sdb1, 3725.5 GiB), SYSTEM (/boot sda1, 10 GiB), and / sda2, 3587.5 GiB. The main area shows settings for partition sda3: Mount Point is /, Device(s) is DELL PERC H730 Mini (sda), and File System is ext4. A red box highlights the File System dropdown (set to ext4) and the Label input field (which is empty).

具体详情请参考手册

▶▶ 操作系统分区

错误的

```
[root@bsa204 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda5        46G   8.0G   36G  19% /
devtmpfs        126G   0    126G   0% /dev
tmpfs           126G  104K   126G   1% /dev/shm
tmpfs           126G   4.1G   122G   4% /run
tmpfs           126G   0    126G   0% /sys/fs/cgroup
/dev/sda1        9.2G  160M   8.6G   2% /boot
/dev/sda2        82G   71G   7.3G  91% /home
/dev/sdd1        1.5T   1.9G   1.4T   1% /home/sdd
/dev/sdc1        15T   1.7G   14T   1% /home/sdc
/dev/sda6        46G   65M   44G   1% /tmp
/dev/sdb1        15T   6.0G   14T   1% /home/sdb
/dev/sde         7.2G   62M   6.8G   1% /run/media/nsfocus/1678bbd1-c429-462e-af45-d
tmpfs           26G   16K   26G   1% /run/user/42
tmpfs           26G   0    26G   0% /run/user/0
tmpfs           26G   0    26G   0% /run/user/987
tmpfs           26G   0    26G   0% /run/user/986
```

正确的

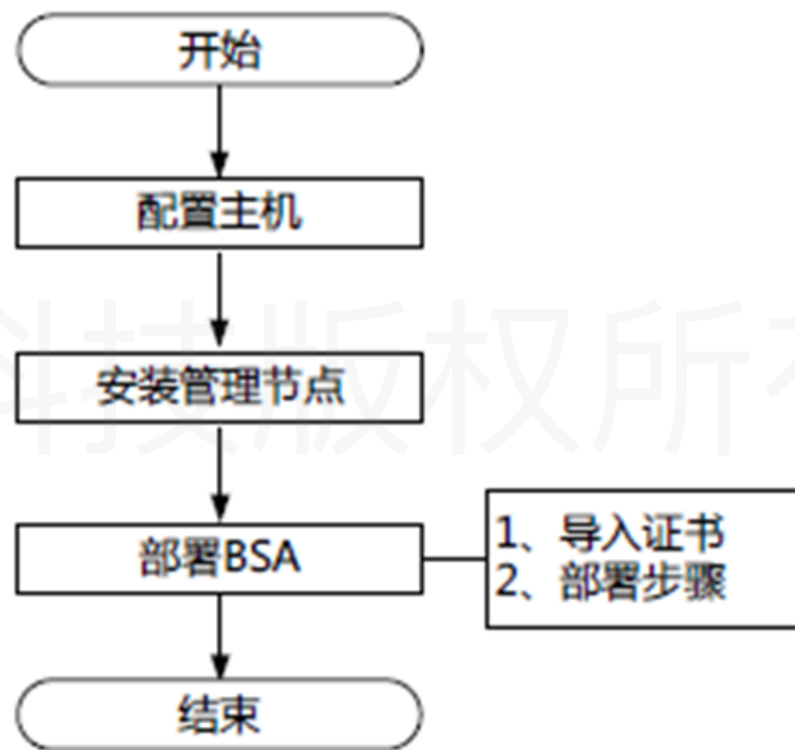
```
[root@bsa211 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda4        3.4T   3.9G   3.2T   1% /
devtmpfs        63G   0    63G   0% /dev
tmpfs           63G   80K   63G   1% /dev/shm
tmpfs           63G   11M   63G   1% /run
tmpfs           63G   0    63G   0% /sys/fs/cgroup
/dev/sda2        9.8G  154M   9.1G   2% /boot
/dev/sda1        10G   9.6M   10G   1% /boot/efi
/dev/sde1        3.6T   89M   3.4T   1% /home/sde
/dev/sdl1        3.6T   89M   3.4T   1% /home/sdl
/dev/sdf1        3.6T   89M   3.4T   1% /home/sdf
/dev/sdh1        3.6T   89M   3.4T   1% /home/sdh
/dev/sdk1        3.6T   89M   3.4T   1% /home/sdk
/dev/sdg1        3.6T   89M   3.4T   1% /home/sdg
/dev/sdb1        3.6T   89M   3.4T   1% /home/sdb
/dev/sdd1        3.6T   89M   3.4T   1% /home/sdd
/dev/sdi1        3.6T   89M   3.4T   1% /home/sdi
/dev/sdc1        3.6T   89M   3.4T   1% /home/sdc
/dev/sdj1        3.6T   89M   3.4T   1% /home/sdj
tmpfs           13G   16K   13G   1% /run/user/988
tmpfs           13G   0    13G   0% /run/user/0
```

▶▶ 安装前注意事项

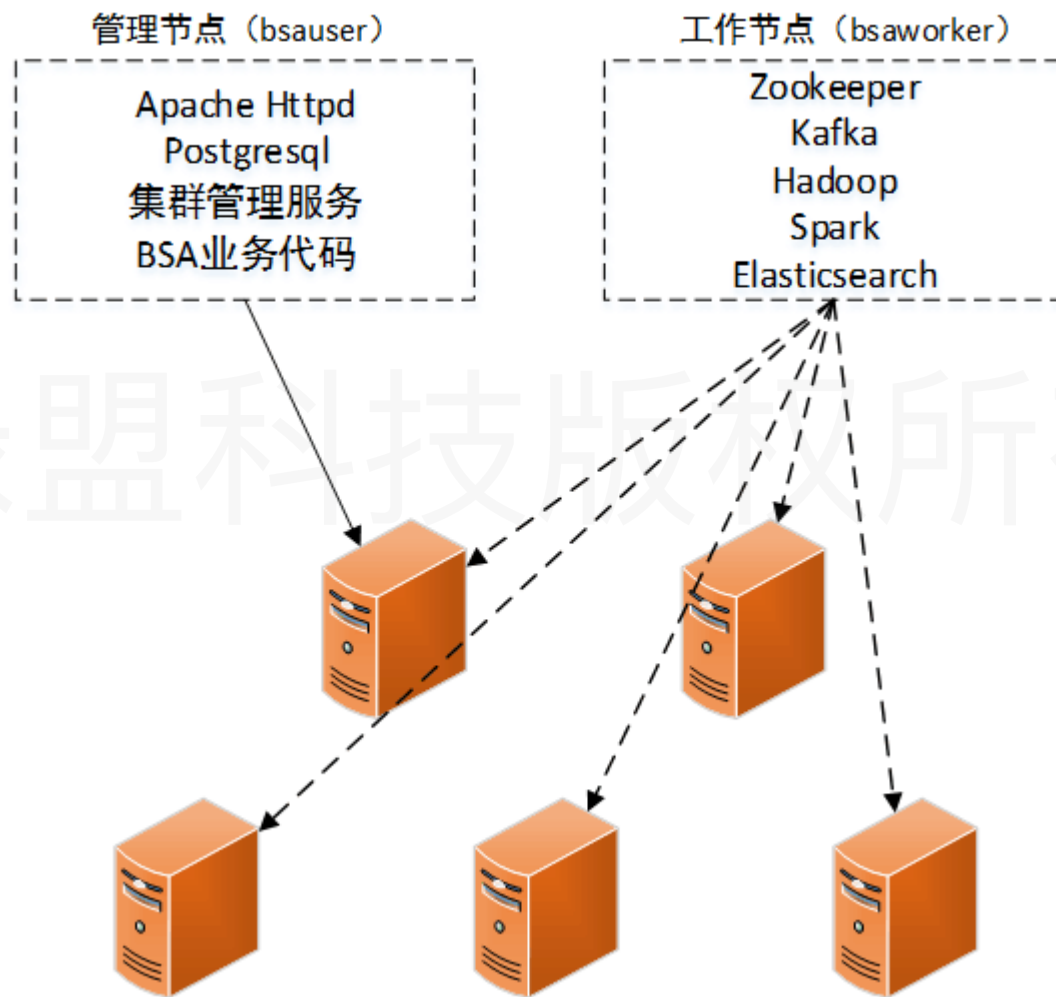
- 防火墙要保持开启，不要使用iptables -F
- /home；时间，时区；Ip，主机名唯一
- BSA F04主机名唯一，可通过界面更改ip
- 磁盘挂载尽量按照/home/sdb、/home/sdc目录挂载，方便进行分盘部署。
- /etc/hosts文件和prepareTools/hosts文件前两行不要删
- prepareTools/hosts末尾不要有空行
- 由于centos7.0本身内核存在缺陷会影响平台稳定性，不再使用centos7.0

准备项		描述
节点所在主机	IP 地址	确保网络连接正常。各节点所在主机处于同一个网段。
	操作系统登录帐号	必须具有 root 帐号权限。
	防火墙	处于开启状态。
	时间	所有节点的系统时间要保持同步。
	主机名	所有节点需要统一规范命名。
	hosts 文件	每个节点需要添加管理节点和所有工作节点的 IP、主机名。
	bsauser 帐号（管理节点）	安装前不允许存在 bsauser 帐号及/home/bsauser 目录，在安装管理节点时，会自动创建 bsauser 帐号。
	其他	已经开启 Yum、RPM、SSH。
	组件状态	<ul style="list-style-type: none"> • 停止已经运行的 Hadoop、Kafka、Zookeeper、Elasticsearch、Postgres SQL、Spark、Apache、Tomcat 组件。 • 确保 BSA 所需端口未被占用。
BSA	证书	<ul style="list-style-type: none"> • 与加密狗配套使用。 • 证书中包含授权节点数。
	加密狗	<ul style="list-style-type: none"> • 与证书配套使用。 • 安装在管理节点所在主机上。
	光盘	包含 BSA 管理节点的安装文件。
访问 BSA 的主机	浏览器	<ul style="list-style-type: none"> • IE 11 • 最新版本的 Firefox 或 Chrome

▶▶ 安装部署流程



管理节点和工作节点



组件部署

表3-2 Hadoop 组件路径参数

配置项	描述
NameNode Path	<p>NameNode 数据的存放路径，支持分盘部署，即除了操作系统磁盘以外，其他所有磁盘都可以存放 NameNode 数据，建议将 NameNode 部署在 2~3 块磁盘上。此时，NameNode Path 可以配置多个，中间用英文“,”分隔。</p> <p>例如，服务器有/home/sdd 和/home/sdc 两个可用磁盘，则 Namenode Path 输入框输入“/home/sdd/hes/hadoopDirs/name,/home/sdc/hes/hadoopDirs/name”。</p>
DataNode Path	<p>DataNode 数据的存放路径，支持分盘部署，即除了操作系统磁盘以外，其他所有磁盘都可以存放 DataNode 数据。此时，DataNode Path 可以配置多个，中间用英文“,”分隔。</p> <p>例如，服务器有/home/sdd 和/home/sdc 两个可用磁盘，则 Datanode Path 输入框输入“/home/sdd/hes/hadoopDirs/data,/home/sdc/hes/hadoopDirs /data”。</p>
Hadoop Temp Path	Hadoop 临时文件存放路径。
Yarn Local Path	<p>Yarn 中间结果的存放路径，支持分盘部署，即除了操作系统磁盘以外，其他所有磁盘都可以存放 Yarn 中间结果数据。此时，该参数可以配置多个，中间用英文“,”分隔。</p> <p>例如，服务器有/home/sdd 和/home/sdc 两个可用磁盘，则该参数的输入框输入“/home/sdd/hes/hadoopDirs/nm-local-dir,/home/sdc/hes/hadoopDirs/nm-local-dir”。</p>

组件部署

组件设置

<input checked="" type="checkbox"/> 全选	组件	配置	主机
<input checked="" type="checkbox"/>	Hadoop	保存 取消	选择主机
NameNode Path <input type="text" value="/home/sdb/hes/hadoopDirs/name,/hoi"/> 多路径请用逗号分隔			
DataNode Path <input type="text" value="/home/sdf/hes/hadoopDirs/data,/hom"/> 多路径请用逗号分隔			
Hadoop Temp Path <input type="text" value="/home/bsaworker/hes/hadoopDirs/had"/>			
Yarn Local Path <input type="text" value="/home/sdf/hes/hadoopDirs/nm-local-di"/> 多路径请用逗号分隔			
<input checked="" type="checkbox"/>	Zookeeper	编辑	选择主机
<input checked="" type="checkbox"/>	Kafka	编辑	选择主机
<input checked="" type="checkbox"/>	Spark	编辑	选择主机
<input checked="" type="checkbox"/>	Elasticsearch	编辑	选择主机

部署

▶▶ TSA APP

态势场景

- ❑ 将9个APP安装完整，否则某些功能无法使用（一键封堵选装）
- ❑ 证书没有的功能模块，也需将APP安装完整

序号	APP名称	APP详细描述	APP MD5
TAM APP			
1	威胁情报APP	bsa_ti.3.0.0.25443	772f82319005527061254f535ad61344
2	资产管理APP	bsa_am.2.1.3.25582	2d23de11b8d3c285e56621da4ff75d17
3	数据源APP	bsa_tds.2.0.2.30231	96845998740c1741f05341a7877421b3
4	诺亚引擎APP	bsa_mlengine.2.0.1.27818	9336BE36A12EC2A451B5A8549273CF27
5	全流量APP	bsa_tam2.2.0.3.29845	72f86d6829bc1ed0b23661d626409dbe
TSA APP			
1	网络入侵APP	bsa_ckc.2.1.0.29270	5AE7194623995BCB61A38BD06FAB2214
2	规则引擎APP	bsa_rule_engine.2.2.0.30018	F5E4C4EEAF0AB2E7F6F479A8812BB144
3	态势感知APP	bsa_tsa.2.2.0.29986	A921B9EFA4DCB582C30D979B5EE0A22E
4	网站安全APP	bsa_wss.2.1.0.29776	C88E6CC1EDBC0137498CD581ED9D78DA
5	僵木蠕APP	bsa_zsa.2.1.0.29667	235E5607AFAB140DC81F4E0A38ED5785
6	威胁情报APP	bsa_ti.3.0.0.25443	772F82319005527061254F535AD61344
7	资产管理APP	bsa_am.2.1.4.29961	E0776C65744E9F4311913A8F84E4E0D3
8	异常流量APP	bsa_ata.2.2.0.29271	84369D169C9CF7068CFA4EA00999171C
9	内置数据源APP	bsa_cds.2.1.0.29578	113D76B836D0AF93A937DCE1039BDD0C
10	一键封堵APP	bsa_okp.2.0.1.29913	96AAAC8575D659CDB4379A2F14055D42

数据接入

绿盟科技版权所有

▶▶ 支持的设备版本

TSA F02

序号	支持设备	设备版本
1	NIDS	V5.6.7 V5.6.8 V5.6.9 V5.6R10F00 及以上版本
2	NIPS	V5.6.7 V5.6.8 V5.6.9 V5.6R10F00 及以上版本
3	TAC	V2.0R01F00SP01 及以上版本
4	NTA	V4.5R89F00 及以上版本
5	WAF	V6.0.4.1.35887 及以上版本 V6.0.5.1.35359 及以上版本 V6.0R06F01SP01 及以上版本
6	BSA	V2.0R00F05 及以上版本
7	NFWD (转发器)	V1.1.0.18305 及以上版本
8	TVM (脆弱性管理主机)	V3.0R00F05SP02
9	RSAS	V6.0R02F01SP07 及以上版本
10	WVSS	V6.0R03F01SP09 及以上版本
11	WSM[H] (网站安全监测系统)	V6.0R00F00SP01
12	websafe	V2. 0. 3. 16
13	ADS (支持一键封堵)	V4. 5R90F00
14	WAF 定制 (支持一键封堵)	V6. 0. 6. 0. 40524

▶▶ 需要开放的端口

方向：入BSA方向

	端口	端口用途
BSA平台	443	BSAweb服务
	自定义数据源端口	数据源接收数据端口
A接口	5050	SFTP服务默认端口
	5051	FTP服务默认端口
	60000-60200	FTP服务数据端口
转发器	12306	转发器web访问端口
	12307	转发器服务端口
	5002	TCP端口
	5003	SSL端口
	50071	FTP服务端口
	60000-60200	FTP服务数据端口
态势感知	1111	异常流量数据源端口
	5005	网络入侵数据源端口
	5666	waf数据源端口
攻击溯源	异常流量数据源端口	异常流量数据源端口
	flow采集器端口	flow采集器端口
全流量	5008	会话日志数据源端口
	5009	DNS日志数据源端口
	5010	web日志数据源端口
	5011	其他流量日志数据源端口
	5012	UTS告警数据源端口
UTS	22	ssh端口
	443	web服务
	8081	restapi http

NTA

NTA 监控 告警 报表 日志 配置 管理

系统配置 网络配置 三方接口 诊断分析 数据管理 用户管理 双机热备 许可证 系统升级 告警白名单

管理 / 三方接口 / BSA配置

- Email服务
- SNMP服务
- Syslog服务
- 云平台
- 第三方云平台
- 云清洗平台
- BSA配置**
- 管理模 BSA配置
- NTA-ATM
- 绿盟威胁情报

BSA

是否启用 是 否

BSA地址1	<input type="text" value="192.168.0.2"/>	文件端口	<input type="text" value="5050"/>	日志端口	<input type="text" value="1111"/>
BSA地址2	<input type="text" value="IP地址"/>	文件端口	<input type="text" value="文件端口"/>	日志端口	<input type="text" value="日志端口"/>
BSA地址3	<input type="text" value="IP地址"/>	文件端口	<input type="text" value="文件端口"/>	日志端口	<input type="text" value="日志端口"/>
BSA地址4	<input type="text" value="IP地址"/>	文件端口	<input type="text" value="文件端口"/>	日志端口	<input type="text" value="日志端口"/>

保存

NTA

NTA 管理-三方接口-BSA配置，文件端口5050，日志端口1111

NTA 监控 告警 报表 日志 配置 管理 您好, admin | 简体中文 | 关于 | 退出

监控对象 批量配置 告警配置模板 全局告警配置 全局牵引配置 Flow采集与转发 数据字典 刷新 站点地图

配置 / Flow采集与转发

Flow采集与转发

Netflow/Netstream/IPFIX采集端口 *	9999
Sflow采集端口 *	6343
Flow统计间隔 ? *	<input checked="" type="radio"/> 30s <input type="radio"/> 60s
缺省流转发 ? *	<input checked="" type="radio"/> 打开 <input type="radio"/> 关闭
转发到下列主机	192.168.0.7/6666
每行一个IP/端口号,最多8条	
IP流量统计 ? *	<input type="radio"/> 是 <input checked="" type="radio"/> 否
最小统计阈值	1.0M bps
保存	

▶▶ TAC /NIDPS 5.6.10

- TAC和NIPS/NIDS 5.6.10及以后版本,在设备安全中心功能页面有直接联动的入口。文件端口5050，日志端口5005

TAC

大数据安全分析(BSA)

服务器地址	<input type="text"/>	文件端口	5050	安全日志端口	5005	<input type="checkbox"/> 启动	<input checked="" type="checkbox"/> 网络连通性测试
服务器地址	<input type="text"/>	文件端口	5050	安全日志端口	5005	<input type="checkbox"/> 启动	<input checked="" type="checkbox"/> 网络连通性测试
服务器地址	<input type="text"/>	文件端口	5050	安全日志端口	5005	<input type="checkbox"/> 启动	<input checked="" type="checkbox"/> 网络连通性测试
服务器地址	<input type="text"/>	文件端口	5050	安全日志端口	5005	<input type="checkbox"/> 启动	<input checked="" type="checkbox"/> 网络连通性测试

NIDPS

大数据安全分析(BSA)

服务器地址	192.168.17.88	隧道	文件端口	5050	安全日志(JSON)端口	5005	流量日志(Netflow)端口	<input type="text"/>	<input checked="" type="checkbox"/> 启动	<input checked="" type="checkbox"/> 已连接	<input checked="" type="checkbox"/> 网络连通性测试
服务器地址	<input type="text"/>	隧道	文件端口	5050	安全日志(JSON)端口	5005	流量日志(Netflow)端口	5006	<input type="checkbox"/> 启动	<input checked="" type="checkbox"/> 网络连通性测试	
服务器地址	<input type="text"/>	隧道	文件端口	5050	安全日志(JSON)端口	5005	流量日志(Netflow)端口	5006	<input type="checkbox"/> 启动	<input checked="" type="checkbox"/> 网络连通性测试	
服务器地址	<input type="text"/>	隧道	文件端口	5050	安全日志(JSON)端口	5005	流量日志(Netflow)端口	5006	<input type="checkbox"/> 启动	<input checked="" type="checkbox"/> 网络连通性测试	

▶▶ WAF 6061

□ WAF 系统管理-安全中心，安全日志端口和状态端口都是5666



The screenshot displays the 'WAF 系统管理-安全中心' (WAF System Management - Security Center) interface. The main navigation bar includes 'WAF', '系统监控', '安全管理', '日志报表', and '系统管理'. The sub-navigation bar contains '网络配置', '系统部署', '系统工具', '测试工具', '安全中心', and '用户管理'. The '安全中心' (Security Center) section is active, showing the following configuration:

- 本地IP地址** (Local IP Address): 10.66.250.159
- 绿盟云** (Green Alliance Cloud): 设备关怀服务 (Device Care Service) is set to '开启' (On) and '已连接' (Connected).
- 企业安全中心(ESPC)** (Enterprise Security Center):
 - 服务器地址 10.5.16.19, 端口 443, 发送数据 启动 已连接
 - 服务器地址 10.5.16.17, 端口 443, 发送数据 启动 已连接
 - 服务器地址 [Empty], 端口 443, 发送数据 启动
 - 服务器地址 [Empty], 端口 443, 发送数据 启动
- 大数据安全分析(BSA)** (Big Data Security Analysis):
 - 服务器地址 192.168.17.88, 安全日志端口 5666, 状态日志端口 5666, 启动 **正在连接**
 - 服务器地址 [Empty], 安全日志端口 5666, 状态日志端口 5666, 启动

03

查询分析

态势感知TSA

绿盟科技版权所有

▶▶ TSA

绿盟综合态势展示：

- 针对公网ip，有内置地理库，需要有事件产生，日志由绿盟安全设备传送至平台，规则引擎产生事件。
- 针对私网ip，形成必要条件为：资产+事件。资产可自己创建、导入等，也可联动ESP同步资产；资产或资产组需关联地理视图（例如：中国/北京/海淀）；日志由绿盟安全设备传送至平台，规则引擎产生事件。

第三方综合态势展示：

- 针对公网ip，有内置地理库，需自定义GROK规则解析日志，自定义事件规则，日志由第三方设备传送至平台，规则引擎产生事件。
- 针对私网ip，形成必要条件为：资产+事件。资产可自己创建、导入等，也可联动ESP同步资产，资产或资产组需关联三级地理视图（例如：中国/北京/海淀）；需自定义GROK规则解析日志，自定义事件规则，日志由第三方设备传送至平台，规则引擎产生事件。

▶▶ TSA



TSA

绿盟安全态势感知平台 | 综合态势 | **风险态势** | 资产态势 | 情报态势 | 数据分析 | 系统管理 | 态势感知

风险态势 / 网络入侵 / 查询分析

查询

2018-12-25 18:00:00 至 2018-12-26 18:54:58 查询 高级查询

查询结果

1 / 7 跳转 每页 10 共65条 设置指标 (已选9项)

序号	事件名称	开始时间	结束时间	目标IP	目标地域	源IP	源地域	事件类型	子类型	操作
1	端口扫描	2018-12-26 05:20:51	2018-12-26 05:20:51	192.168.1.10	中国北京	114.226.128.243	中国江苏常州	扫描窃听事件	扫描窃听	👁️ 🔍
2	暴力破解事件	2018-12-26 05:20:51	2018-12-26 05:20:51	192.168.1.10	中国北京	114.226.128.243	中国江苏常州	系统入侵事件	暴力破解	👁️ 🔍
3	频繁登录尝试	2018-12-26 05:20:51	2018-12-26 05:20:51	192.168.1.10	中国北京	114.226.128.243	中国江苏常州	系统入侵事件	非法访问	👁️ 🔍
4	DDoS攻击	2018-12-26 05:20:51	2018-12-26 05:20:51	192.168.1.10	中国北京	114.226.128.243	中国江苏常州	拒绝服务攻击事件	拒绝服务	👁️ 🔍
5	端口扫描	2018-12-26 05:20:50	2018-12-26 05:20:50	10.66.59.2	中国北京	36.149.85.186	中国江苏盐城	扫描窃听事件	扫描窃听	👁️ 🔍
6	暴力破解事件	2018-12-26 05:20:50	2018-12-26 05:20:50	10.66.59.2	中国北京	36.149.85.186	中国江苏盐城	系统入侵事件	暴力破解	👁️ 🔍
7	频繁登录尝试	2018-12-26 05:20:50	2018-12-26 05:20:50	10.66.59.2	中国北京	36.149.85.186	中国江苏盐城	系统入侵事件	非法访问	👁️ 🔍
8	DDoS攻击	2018-12-26 05:20:50	2018-12-26 05:20:50	10.66.59.2	中国北京	36.149.85.186	中国江苏盐城	拒绝服务攻击事件	拒绝服务	👁️ 🔍
9	端口扫描	2018-12-26 05:20:44	2018-12-26 05:20:44	10.66.59.2	中国北京	218.193.0.255	中国湖南岳阳	扫描窃听事件	扫描窃听	👁️ 🔍
10	暴力破解事件	2018-12-26 05:20:44	2018-12-26 05:20:44	10.66.59.2	中国北京	218.193.0.255	中国湖南岳阳	系统入侵事件	暴力破解	👁️ 🔍

数据分析 / 原始日志查询

查询

日志类型

入侵防护日志

2018-12-25 18:00:00 至 2018-12-26 18:56:18

查询

高级查询

查询结果

绿盟科技版权所有

导出结果

1 /12 跳转 每页 10 共119条

设置指标 (已选39项)

序号 时间 日志内容

1	2018-12-26 05:20:51	<p>sip: 114.226.128.243 sport: 17161 dip: 192.168.1.10 dport: 445 proto: -1 msg: SYN-Flood Half-open TCP Connection Denial of Service Attack dmac: 00:E0:4C:0B:92:E1 user_name: administrator smac: E8:40:40:97:C3:C1 gr_pop: 1 type: ds: SU1BUG5TZjBDdXNT vid: 0 last_times: 30 gr_type: 1 gr_os: 1 action: 0 gr_danger: 3 raw_info: AAAAm/9TTUJyAAAAABhTyAAAAAAAAAAAAAAAAAP/////4AAAAAHgAAIBDIE5FVfDPUksGUFJPR1JBTSAXLjAAkxBtk1BTjEuMAACV2luZG93cyBmb3lgV29ya2dyb3VwcyAzLjFhAAJMTTEuMlgwMDIAAakxBtk1BTjUuMQACTIQgTE0gMCA4xMgACU01CIDLuMDAyAAJTUuIgMi4/Pz8A msgtype: 1 app_id: module: 0 ar: 2 gr_tech: 8 app_name: actd: 2 gr_service: 3 raw_len: 212 rule_id: 41185 card: G1/6 msel: 0 snapshot: IMAP S log_date: 2018-12-26 05:20:51 sip_int: 1927446771 dip_int: 3232235786 src_asset: 2 dst_asset: 0 dev_id: 1FF6-FBE0-39CF-185C probe_id: 1FF6-FBE0-39CF-185C</p>
2	2018-12-26 05:20:51	<p>sip: 114.226.128.243 sport: 3306 dip: 192.168.1.10 dport: 445 proto: -1 msg: SSH登录请求认证 dmac: 00:E0:4C:0B:92:E1 user_name: smac: E8:40:40:97:C3:C1 gr_pop: 2 type: ds: U1NibiNmMEN1c1M vid: 0 last_times: 30 gr_type: 2 gr_os: 1 action: 0 gr_danger: 2 raw_info: AAAAm/9TTUJyAAAAABhTyAAAAAAAAAAAAAAAAAP/////4AAAAAHgAAIBDIE5FVfDPUksGUFJPR1JBTSAXLjAAkxBtk1BTjEuMAACV2luZG93cyBmb3lgV29ya2dyb3VwcyAzLjFhAAJMTTEuMlgwMDIAAakxBtk1BTjUuMQACTIQgTE0gMCA4xMgACU01CIDLuMDAyAAJTUuIgMi4/Pz8A msgtype: 1 app_id: module: 0 ar: 2 gr_tech: 16 app_name: act ed: 0 gr_service: 1 raw_len: 212 rule_id: 23369 card: G1/6 msel: 0 snapshot: SSH S5 log_date: 2018-12-26 05:20:51 sip_int: 1927446771 dip_int: 3232235786 src_asset: dst_asset: dev_id: 1FF6-FBE0-39CF-185C probe_id: 1FF6-FBE0-39CF-185C</p>
3	2018-12-26 05:20:51	<p>sip: 114.226.128.243 sport: 3306 dip: 192.168.1.10 dport: 445 proto: -1 msg: HTTP POST方法请求URL路径过长 dmac: 00:E0:4C:0B:92:E1 user_name: smac: E8:40:40:97:C3:C1 gr_pop: 2 type: ds: SFRUUG5TZjBDdXNT vid: 0 last_times: 30 gr_type: 2 gr_os: 3 action: 0 gr_danger: 3 raw_info: AAAAm/9TTUJyAAAAABhTyAAAAAAAAAAAAAAAAAP/////4AAAAAHgAAIBDIE5FVfDPUksGUFJPR1JBTSAXLjAAkxBtk1BTjEuMAACV2luZG93cyBmb3lgV29ya2dyb3VwcyAzLjFhAAJMTTEuMlgwMDIAAakxBtk1BTjUuMQACTIQgTE0gMCA4xMgACU01CIDLuMDAyAAJTUuIgMi4/Pz8A msgtype: 1 app_id: module: 0 ar: 2 gr_tech: 2 app_name: actd: 0 gr_service: 2 raw_len: 212 rule_id: 20347 card: G1/6 msel: 0 snapshot: HTTP S log_date: 2018-12-26 05:20:51 sip_int: 1927446771 dip_int: 3232235786 src_asset: dst_asset: dev_id: 1FF6-FBE0-39CF-185C probe_id: 1FF6-FBE0-39CF-185C</p>

系统状态

绿盟科技版权所有

▶▶ 日常运维

□ 关注的后台:

df -h查看硬盘空间 ;

free -g查看内存空间 ;

date -R查看时区及时间 ;

hostname及hostname -i查看主机和ip是否唯一;

top 查看CPU是否正常 ;

iotop 查看IO是否正常 ;

日常运维

关注的前台

在设置-集群管理-组件下查看当前组件的运行状态，确定所有组件运行状态正常。

在设置-应用管理下查看所有应用，确定要使用的应用已安装且为启动状态。

在综合态势下查看态势地图、事件类型分布图、资产风险分布图、最新安全事件列表，确定图表都有数据。

组件

全流程监控

应用

日志

数据

在设置-集群管理-全流程监控下查看当前对应的入库情况确认对应的数据源数据入库正常

在风险态势-态势子系统下通过查询分析查找数据，确定TSA能正常接受平台产品的日志数据。

组件状态检查

组件	操作
● Elasticsearch	查看 停用
● Hadoop	查看 停用
● Spark	查看 停用
● Zookeeper	查看 停用
● Kafka	查看 停用

查看组件是否都正常运行是平台是否正常运行的一个标准，每个组件都对应着不同的功能，平台的正常运行需要保证各组件都是正常运行中；组件页面状态，红色为异常，绿色为正常

还可以查看组件详情

Hadoop：除了启用和停组件实例外，还可以查看Hadoop分布式文件系统 (HDFS) 的节点状态、总块数、丢失块数，查看YARN的节点状态、总CPU核数和CPU已用核数、总内存和已用内存、Job总数和Job挂起数目、Job运行数目和Job完成数目、各个运行Job的详细信息。

Hadoop 返回

HDFS

文件块数: 0块/3302块 (丢失块数/总块数)

节点状态信息:

节点名称	状态
bsa113	alive
bsa252	alive
bsa115	alive

YARN

Application:

完成	挂起	运行	总
6	0	5	15

节点状态信息:

节点名称	状态
bsa252	RUNNING
bsa113	RUNNING

性能指标:

名称	单位	值	单位	值	单位	值
org.apache.spark.sql.hive.thriftserver.HiveThriftServer2		N/A		N/A		N/A
BSA_PERSISTENT_ES	Avg: 0.39 events/sec	Avg: 48 minutes 48 seconds	Avg: 23 seconds 952 ms			
BSA_PARSER	Avg: 0.00 events/sec	Avg: 11 seconds 525 ms	Avg: 9 seconds 208 ms			
BSA_PERSISTENT_HIVE	Avg: 0.39 events/sec	Avg: 18 seconds 495 ms	Avg: 18 seconds 160 ms			

主机状态检查

BSA 概览 组件 主机 管理 系统升级 高级配置 全流程监控 集群管理

添加主机

主机名	IP	操作系统	CPU使用率	物理内存	缓存	硬盘使用情况	操作
bsa66	10.67.1.66	Red Hat	7.98%	21.96G/31.24G	12.79G	45G/1802G	查看 删除
bsa67	10.67.1.67	Red Hat	17.11%	23.91G/31.24G	3.78G	24G/1802G	查看 删除
bsa68	10.67.1.68	Red Hat	7.93%	13.19G/31.24G	4.58G	10G/1802G	查看 删除

进入相应主机信息展示页面

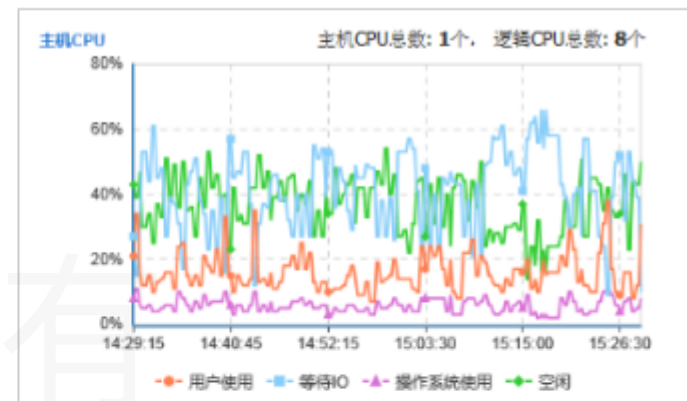
分别查看主机基本信息、主机CPU（包括该主机的物理CPU以及逻辑CPU的总数）、实例列表、主机内存、主机硬盘容量、主机硬盘IO、主机网络IO、主机负载信息、主机磁盘详情、每块磁盘的IO使用率

bsa252



实例列表

实例	所属组件	操作
SparkSqlServer	Spark	停用
Elasticsearch	Elasticsearch	停用
NodeManager	Hadoop	停用
DataNode	Hadoop	停用
JournalNode	Hadoop	停用
ResourceManager	Hadoop	停用

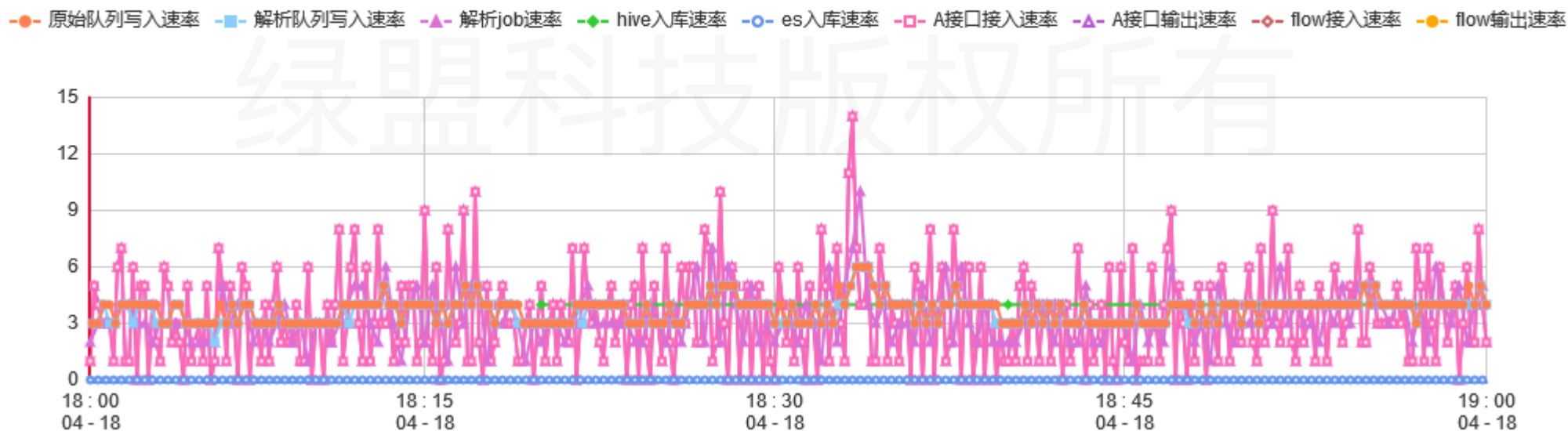


▶▶ 全流程监控

□ 集群管理-全流程监控，选择需要查看的数据源

bsaata_tcp

全流程监控



查看指定数据源的全流程监控信息，可查看最近一个小时内，该数据源的全流程监控信息，即数据源的各个topic的速度和组件解析速度对应的曲线

各应用启用状态检查

BSA		应用管理		应用管理		
名称	版本	接受证书系统管理	证书状态	类型	启用	操作
仪表盘	1.0	是	已授权	应用	<input checked="" type="checkbox"/>	查看 升级历史
报表引擎	1.0.2	是	已授权	组件	<input checked="" type="checkbox"/>	查看 升级历史
设备关怀服务	1.0.2	是	已授权	组件	<input checked="" type="checkbox"/>	查看 升级历史
搜索与报表	1.0.1	否	未授权	应用	<input checked="" type="checkbox"/>	查看 删除 升级历史
资产管理	2.1.0	否	未授权	组件	<input checked="" type="checkbox"/>	查看 删除 升级历史
异常流量	2.1.0	是	已授权	组件	<input checked="" type="checkbox"/>	查看 删除 升级历史
网络入侵	2.0.0	是	已授权	组件	<input checked="" type="checkbox"/>	查看 删除 升级历史
内置数据源	2.0.0	否	未授权	组件	<input checked="" type="checkbox"/>	查看 删除 升级历史
规则引擎	2.1.0	否	未授权	应用	<input checked="" type="checkbox"/>	查看 删除 升级历史
态势感知	2.1.0	是	已授权	应用	<input checked="" type="checkbox"/>	查看 删除 升级历史
僵木蠕	2.0.0	是	已授权	组件	<input checked="" type="checkbox"/>	查看 删除 升级历史
诺亚引擎	1.0.0	否	未授权	组件	<input checked="" type="checkbox"/>	查看 删除 升级历史
攻击溯源	2.0.2	是	已授权	应用	<input checked="" type="checkbox"/>	查看 删除 升级历史
网站安全	2.0.0	否	未授权	组件	<input checked="" type="checkbox"/>	查看 删除 升级历史

不同的应用对应着不同的功能模块，如果发现功能模块异常，需要先检查应用是否为启动状态；

▶▶ Hadoop检查, ip:8088

- 可以查看start time和finish time判断job是否运行; 查看内存和核数使用;
- 通过点击ApplicationMaster查看数据是否入库, 如果点完无法访问, 记得改下URL将hostname改成ip;
- ResourceManager部署在哪个节点, hadoop就在哪个节点。



RUNNING Applications

Cluster Metrics													
Apps Submitted	Apps Pending	Apps Running	Apps Completed	Containers Running	Memory Used	Memory Total	Memory Reserved	VCores Used	VCores Total	VCores Reserved	Active Nodes	Decommissioned Nodes	Lost Nodes
1181	0	5	1176	23	47.63 GB	137.47 GB	0 B	23	22	0	2	0	0

Scheduler Metrics			
Scheduler Type	Scheduling Resource Type	Minimum Allocation	Maximum Allocation
Capacity Scheduler	[MEMORY]	<memory:128, vCores:1>	<memory:70386, vCores:11>

ID	User	Name	Application Type	Queue	StartTime	FinishTime	State	FinalStatus	Progress	Tracking UI	Blacklisted Nodes
application_1528899824467_1131	bsauser	BSA_RULE_ENGINE	SPARK	default	Thu Jul 5 14:48:19 +0800 2018	N/A	RUNNING	UNDEFINED	<input type="checkbox"/>	ApplicationMaster	0
application_1528899824467_1130	bsaworker	org.apache.spark.sql.hive.thriftserver.HiveThriftServer2	SPARK	default	Thu Jul 5 14:33:59 +0800 2018	N/A	RUNNING	UNDEFINED	<input type="checkbox"/>	ApplicationMaster	0
application_1528899824467_1129	bsauser	BSA_APP_BSAATA_MERGE	SPARK	default	Thu Jul 5 14:32:51 +0800 2018	N/A	RUNNING	UNDEFINED	<input type="checkbox"/>	ApplicationMaster	0
application_1528899824467_1127	bsauser	BSA_PARSER	SPARK	default	Thu Jul 5 14:21:02 +0800 2018	N/A	RUNNING	UNDEFINED	<input type="checkbox"/>	ApplicationMaster	0
application_1528899824467_1126	bsauser	BSA_PERSISTENT_HIVE	SPARK	default	Thu Jul 5 14:19:49 +0800 2018	N/A	RUNNING	UNDEFINED	<input type="checkbox"/>	ApplicationMaster	0

Hadoop

实例

实例	主机	操作
● NameNode	bsa1788	停用
● NodeManager	bsa1788	停用
● DataNode	bsa1788	停用
● SecondaryNameNode	bsa1788	停用
● ResourceManager	bsa1788	停用



谢谢！

绿盟科技版权所有