



开源安全情报引擎Critical Stack使用入门

 [yysecurity](#)  2018-01-12 共63197人围观，发现 4 个不明物体

工具

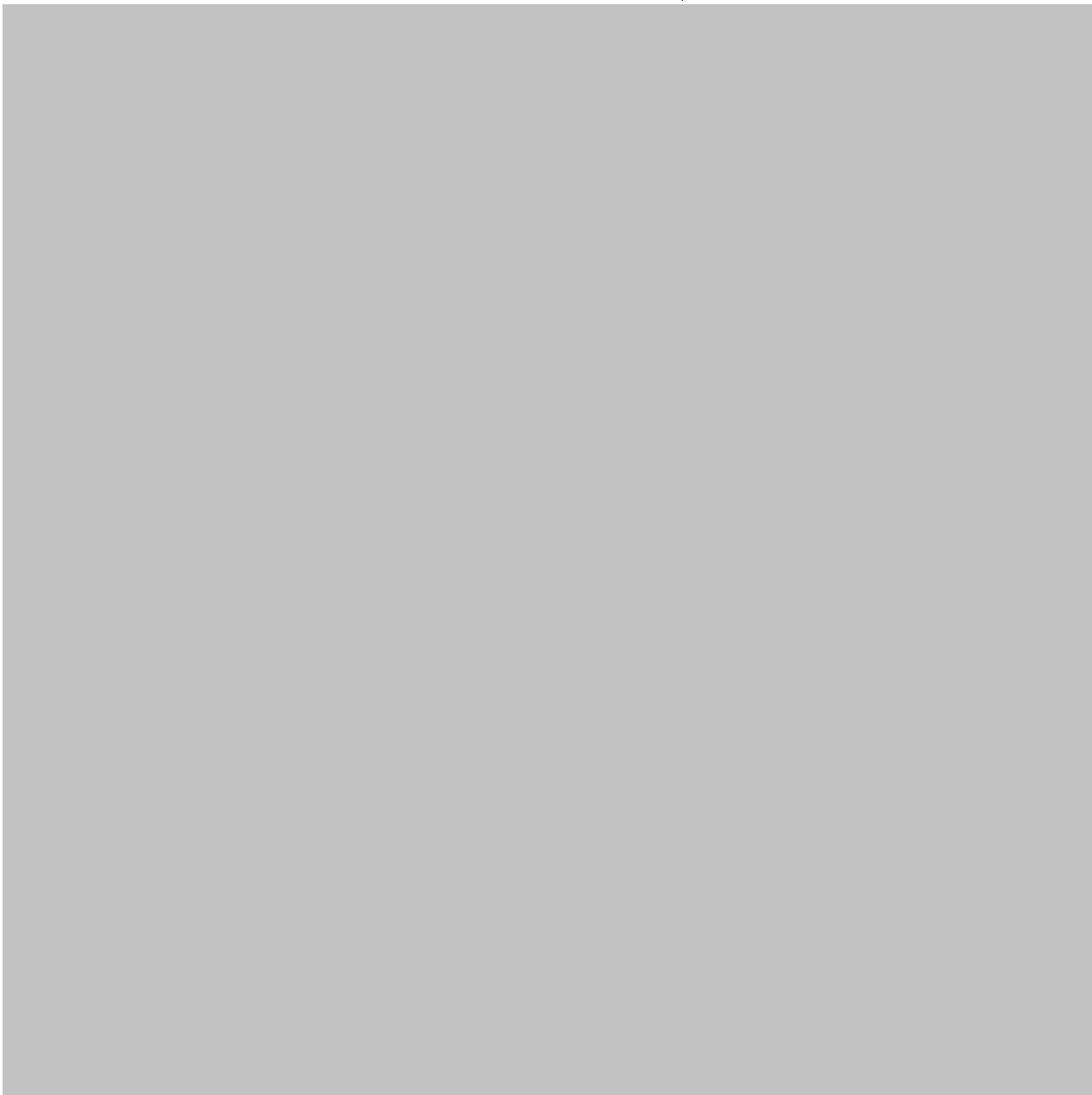
数据安全

前言：

笔者曾参与恶意IP库（IP画像）建设工作，恶意IP库的建立和完善，在初期确实有效的支援了安全运维工作，包括击流量黑名单，入侵检测与溯源等，但在建设的中后期逐渐暴露了一些问题：

1. 建设成本趋高：从0-1的过程当中，通过购买数据的方式，迅速积累起了足够规模的恶意IP数据，前期效益较为明显，后续通过外购或爬虫的方式，一方面形成费用的长期支出，另一方面反爬限制的日益严格，以及所购买和爬虫获取的数据当中存在大量的重复数据，恶意IP库规模增长放缓。
2. 更新困难：众所周知，IP是一个动态变化的标识，IP的行为记录只能代表其过去一段时间的特点，如果长期根据这些特点、记录判断一个IP的性质和来源，必然会造成偏差，甲方运维组织如果没有建立可靠的消息渠道，无从了解这种变化。
3. 随着云计算的可接受程度提高，企业搭建私有云，甚至是混合云的情况越来越普遍，只是单纯利用IP进行来源合法性的判断容易出现误判，同步建立恶意域名库，恶意文件特征库的需求变得迫切。

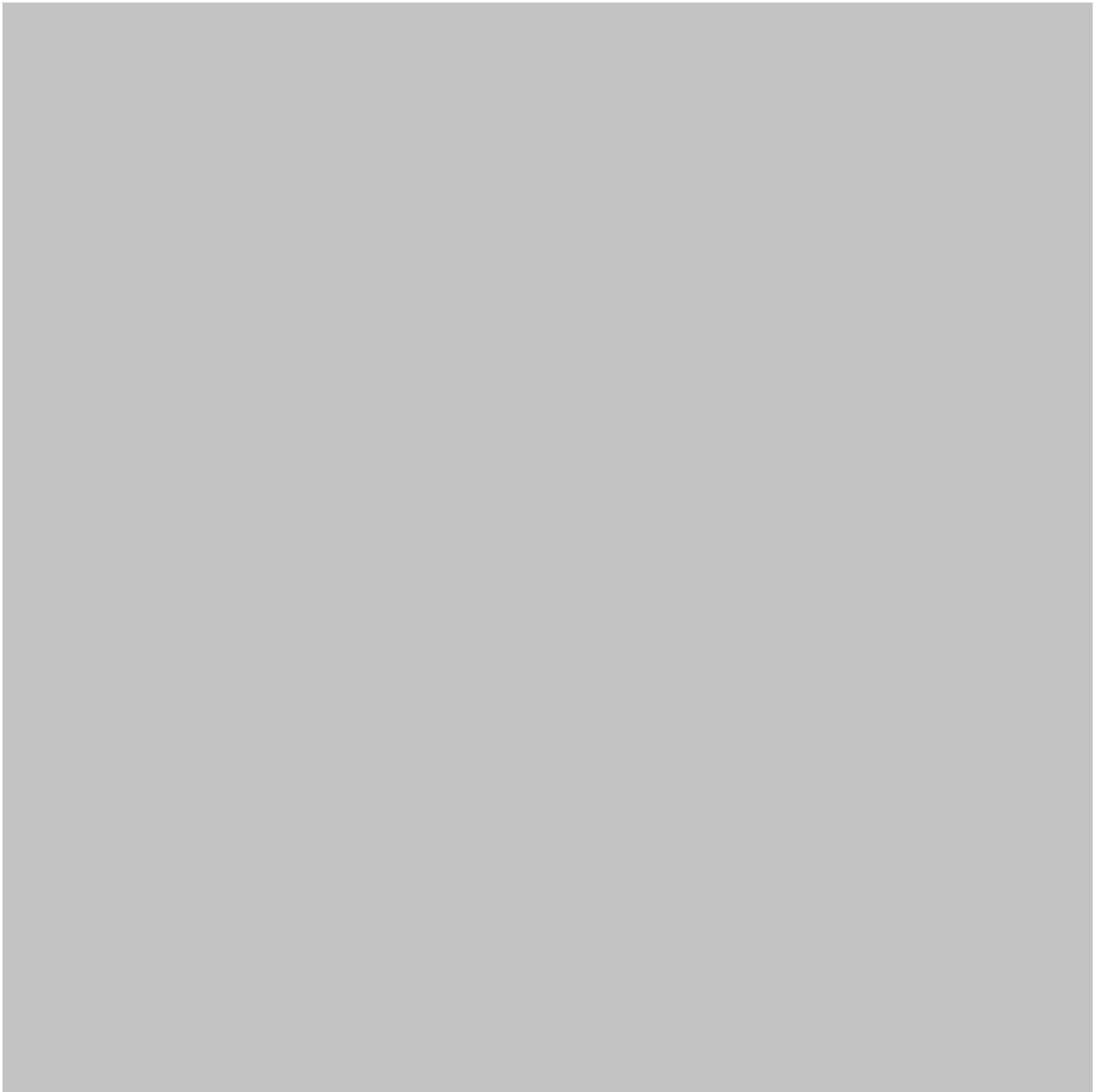




正文

[Critical-Stack-Intel](#)是由Critical Stack 公司开源的威胁情报数据集市，内置了超过130个情报来源（持续增加中），且个情报来源（Feeds）已自动去重，部分时效性的强的 Feed做到每小时更新数据和状态，对恶意 IP 黑名单，恶意 MD5列表是一个极大的补充。

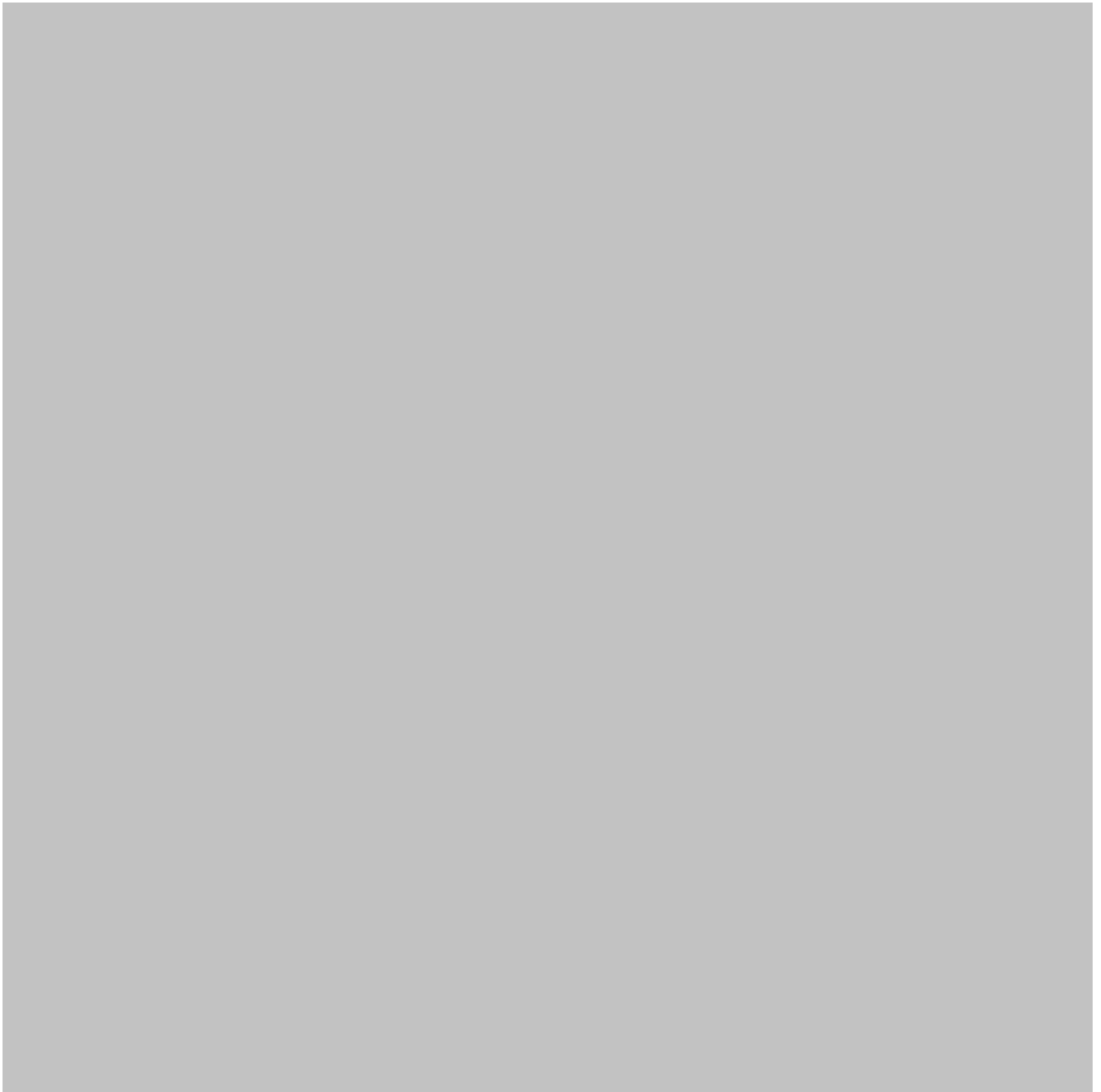




Critical-Stack-Intel主要架构分为**Sensors**，**Collections**，**Feeds**，**Indicators**，要想准确获取情报，就要梳理清楚这四要素的主要功能和关系，其中：

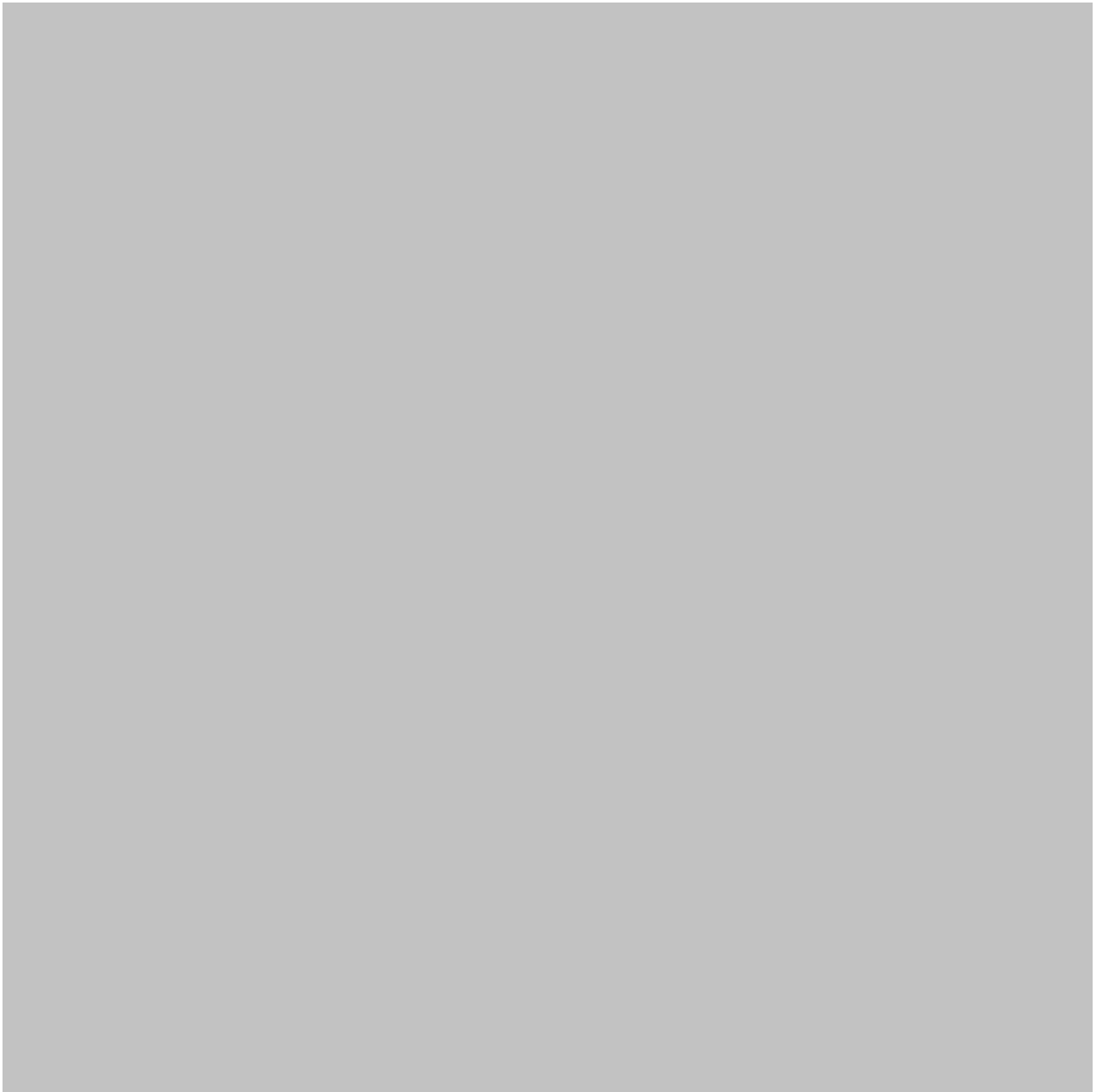
- **Collections**：新建Collection，描述 Collection名称和用途，举例，如专门用于收集远控端IP，专门用于收集恶意病来源IP，专门用于垃圾邮件网关等；





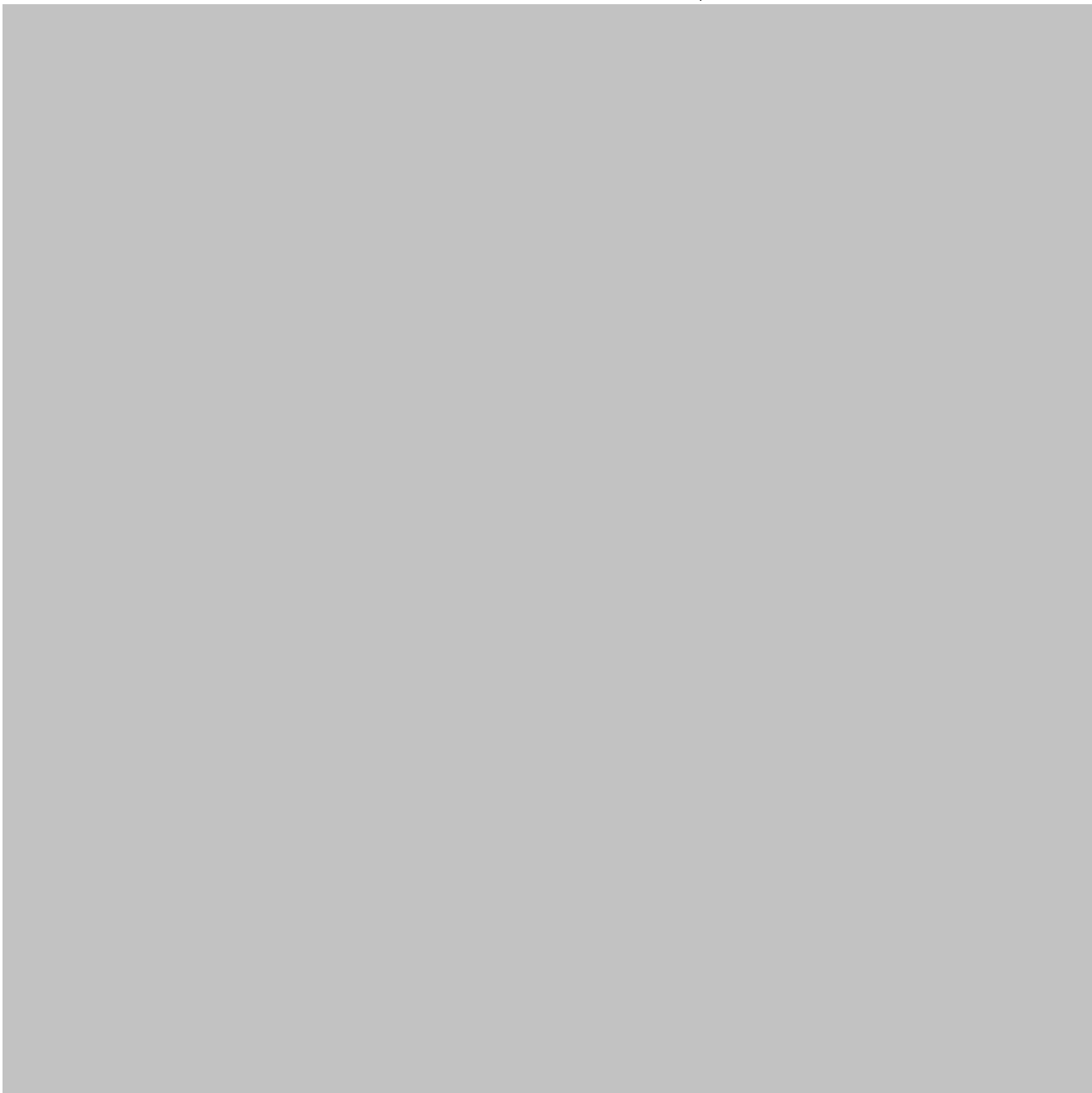
- **Sensors**: 绑定在具体用途的Collection 之下，一个Sensor对应一个API Key，API Key 可以通过接口进行拉取更新操作；





- **Feeds**: 消息源，可根据预设的 Collection和Sensor功能进行订阅关联。需注意：在导航Tab页 Feeds下只是对Feeds进行展示，订阅需在指定Collection下，通过 Add More Feedsa进行添加；





- **Indicators**：Feed里提供的威胁情报单条记录称为Indicator，可以是一个IP，域名，主机名称，文件MD5等，包括

```
Intel::ADDR
Intel::URL
Intel::SOFTWARE
Intel::EMAIL
Intel::DOMAIN
Intel::USER_NAME
Intel::FILE_HASH
Intel::FILE_NAME
Intel::CERT_HASH
```





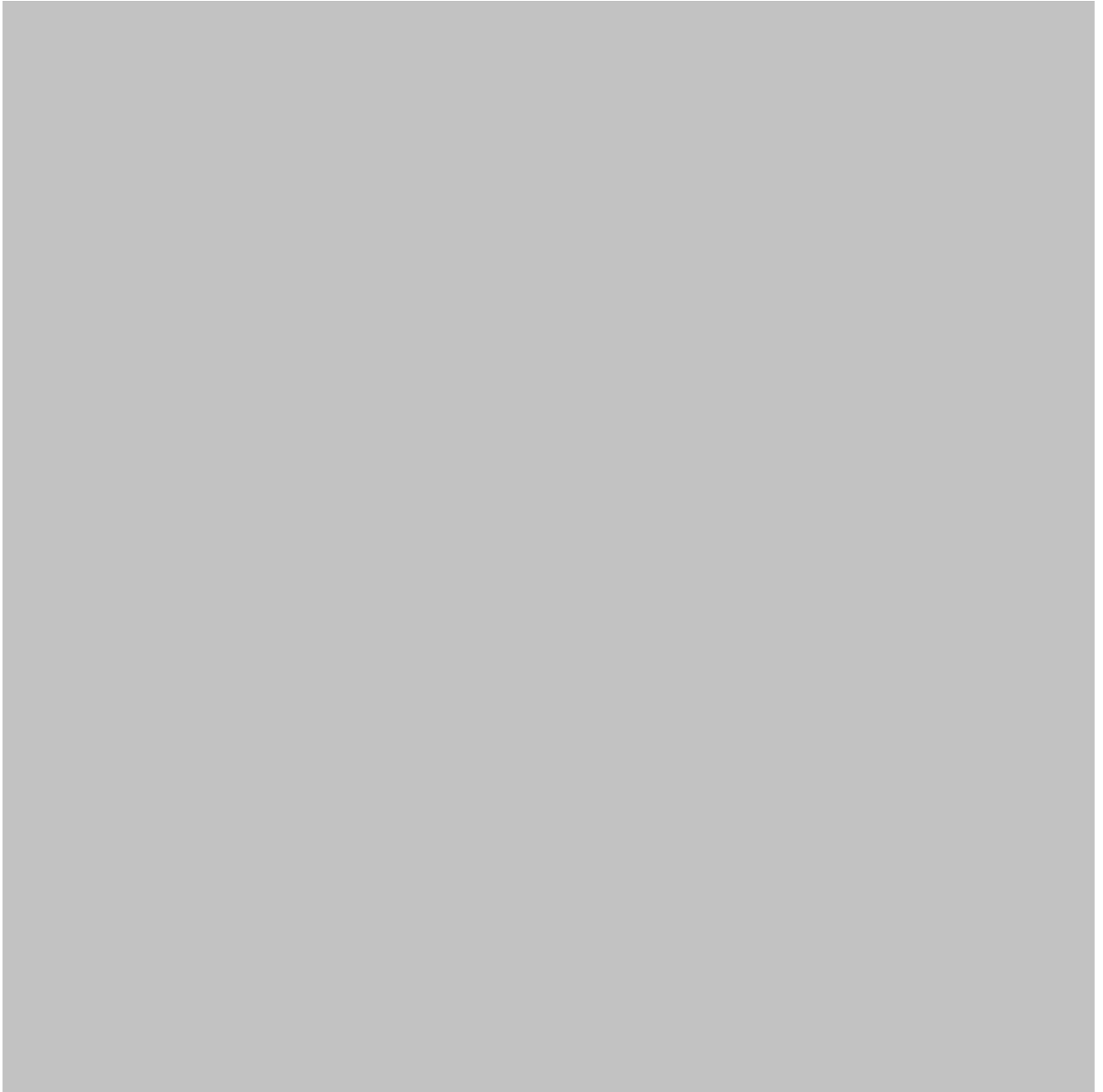
为了与内部运维平台或情报数据库整合，需要安装 **Critical-Stack-Intel-Client**，以便可通过程序命令对情报进行管理：

```
curl https://packagecloud.io/install/repositories/criticalstack/critical-stack-intel
sudo apt-get install critical-stack-intel
```

安装 **Critical-Stack-Intel**后，关联需要操作的Sensor的API Key：

```
sudo critical-stack-intel api <Your API Key>
```

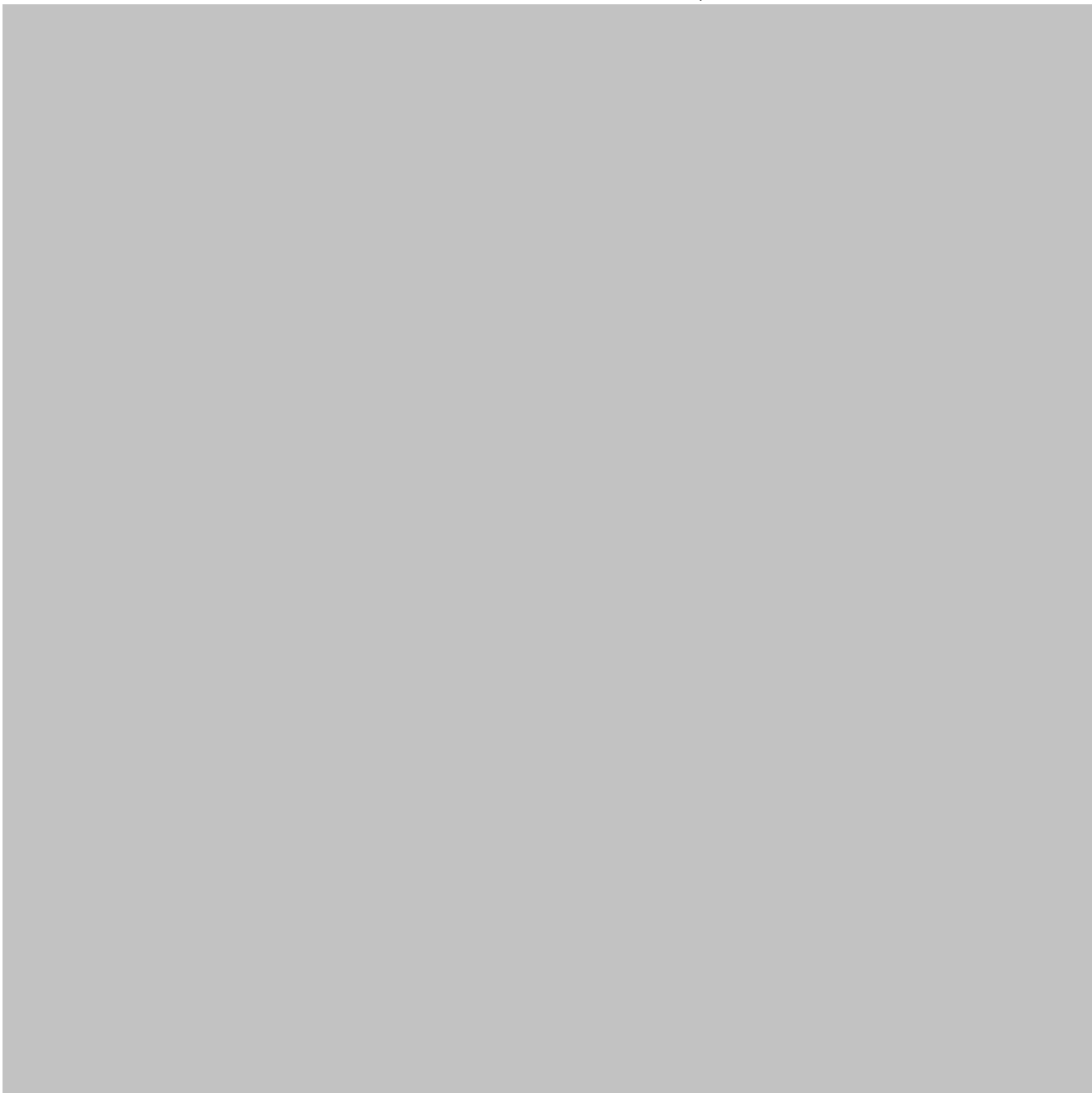
之后便可操作情报库的更新和获取，列出该Sensor下所有Feeds状态：



拉取该 **Sensor** 下的所有**Feeds**的最新数据：

```
sudo critical-stack-intel pull
```





后记

通过定时任务，自动拉取最新情报，恶意情报库规模得到快速壮大，在安全运维工作当中更好扮演“大脑”角色，对恶意文件检测，恶意 IP 拦截的精度预计得到提升。

*本文作者：yysecurity，转载请注明来自 FreeBuf.COM

上一篇： [Android恶意软件偷取Uber凭证](#)

下一篇： [本篇已是最新文章](#)

已有 4 条评论



abc123 (1级) 2018-01-12

1楼 回

这些情报来源一般也都是通过爬虫爬的吧?

亮了

softbug F Z (7级) 011101000110100001100001011011... 2018-01-12

2楼 回

国内谁可以做一个嘛，分享出来。

bat+360肯定是不共享的!

亮了

钱都是我的 2018-01-12

@ softbug 那肯定，还有给别人钱的道理?

亮了

神刀安全网 2018-01-12

3楼 回

没看到下载地址，不下了

亮了

选择文件 未选择任何文件

昵称

请输入昵称

必须 您当前尚未登录。[登陆?](#) [注册](#)

邮箱

请输入邮箱地址

必须 (保密)

表情

插图

提交评论(Ctrl+Enter)

[取消](#)

☒ 有人回复时邮件通知我



3
文章数

3
评论数

最近文章

- [开源安全情报引擎Critical Stack使用入门](#) 2018.01.12
- [Linux下恶意文件大规模共性分析探讨](#) 2017.12.22
- [YY安全中心的“蜜罐技术”应用实践](#) 2017.08.28

浏览更多

相关阅读

- [密码破解工具-Hashkill 0.3.1](#)
- [用Golang写的域名信息搜集工具](#)
- [调查报告：75%的企业不能对数据泄露...](#)
- [Exitmap：Tor出口中继节点扫描器](#)
- [CERT发布Linux安全工具Triage Tools 1.0](#)

特别推荐





[【FB TV】一周「PUE大事件」：
WPA2惊现高危漏洞，你的WiFi还](#)

[willhuang](#)

2017-10-21

[【已结束】第三届中国\(北京\)军民
融合技术装备博览会现场实况](#)

[Elaine_z](#)

2017-07-03

[技术剖析：海莲花（OceanLotus）
根本不是APT，它只是一个普通木](#)

[毒舌评论砖家](#)

2015-06-03


[Windows 10新变化：系统自动更新
将“强制化”，用户不再可选](#)

[dawner](#)

2015-07-20



Copyright © 2018 WWW.FREEBUF.COM All Rights Reserved [沪ICP备13033796号](#)

 阿里云 提供计算与安全服务

 css.php