NSFOCUS

TECHWORLD2019

绿 盟 科 技 技 术 嘉 年 华

探索 · DISCOVERY

NSFOCUS TECHWORLD

容器安全再思考

容器时代的到来?

5.3.1.2 容器安全

容器安全的要求如下：

a)
b)
c)
d)
e)
f)
g)
h)

缺陷等）；

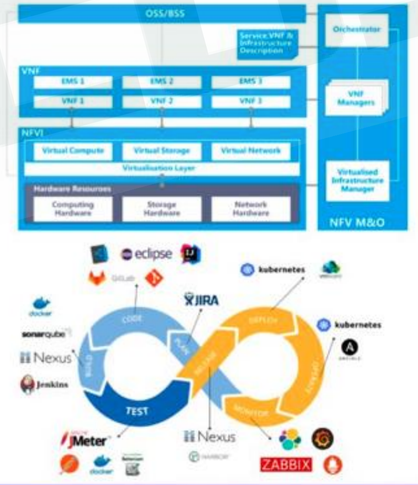
中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术　工业互联网平台安全要求及评估规范

将DevOps引入3GPP标准？

DOIS



虚假的架构

- 封闭的设计
- 没考虑面向运维
- 无用的功能
- ……

真正的架构

- 用Jenkins+Ansible+Python脚本替代闭源的运维工具软件
- 蓝鲸的大中台+Python脚本插件的方式替代定制化的网管系统
- ……

DevOps 国际峰会 2019·北京站

第四，现在我们这个网络云部署的通信网元全都是基于虚拟化的，但是未来 5G 引入了很多一些微服务、切片这种概念，那这种概念能不能够直接用容器化去实现呢？这个暂时目前还没有一个很好的时间的结论，我们也跟各个厂商都是在摸索就是看能不能虚拟化部署的，能不能改成容器化部署的，这是我们未来的四个方向。

NSFOCUS

TECHWORLD2019

绿 盟 科 技 技 术 嘉 年 华

目 录

01

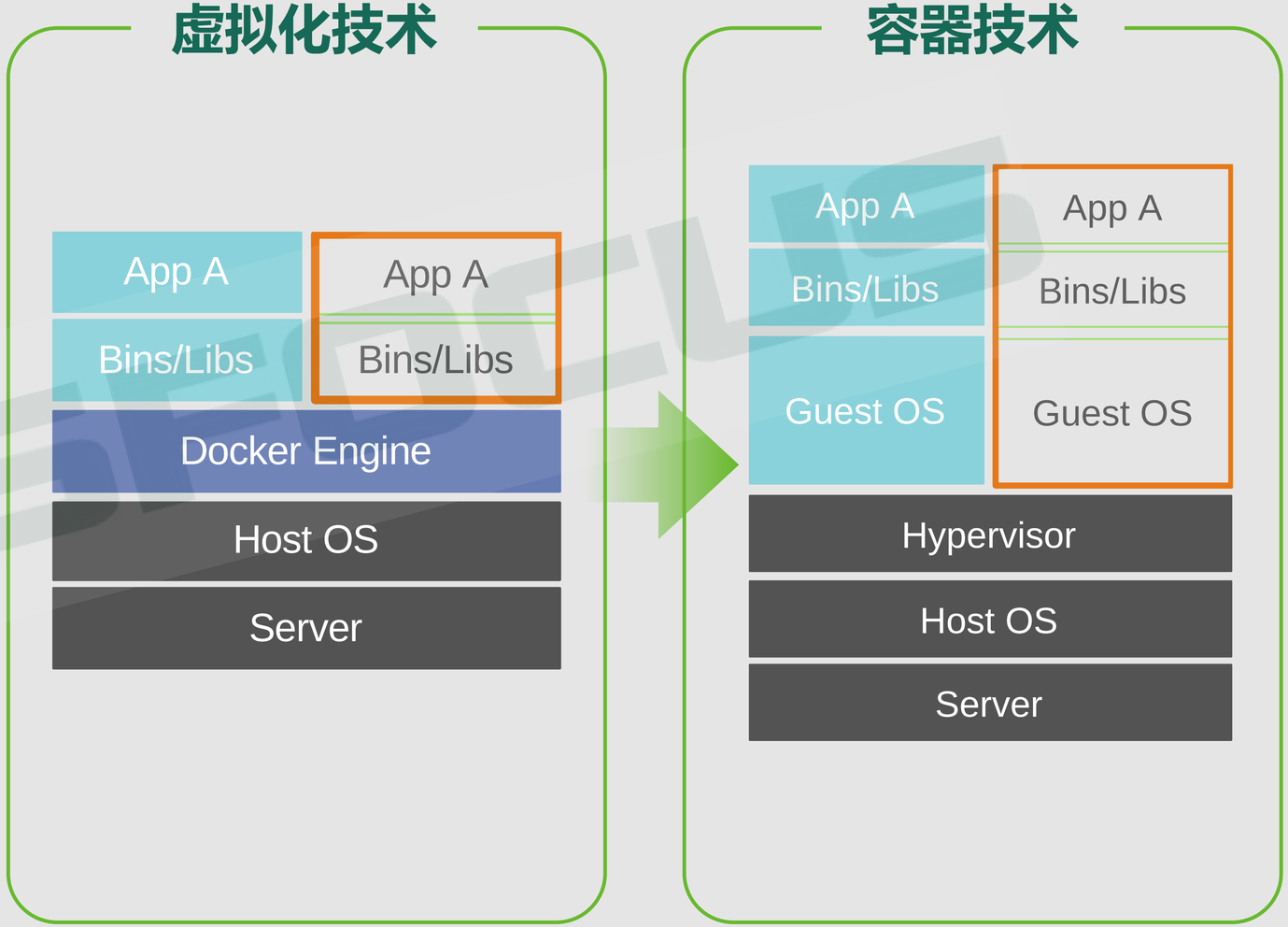
容器、编排和云原生

Container, Orchestration and Cloud native

容器：更轻，更快，然而更脆弱...

10 – 21x

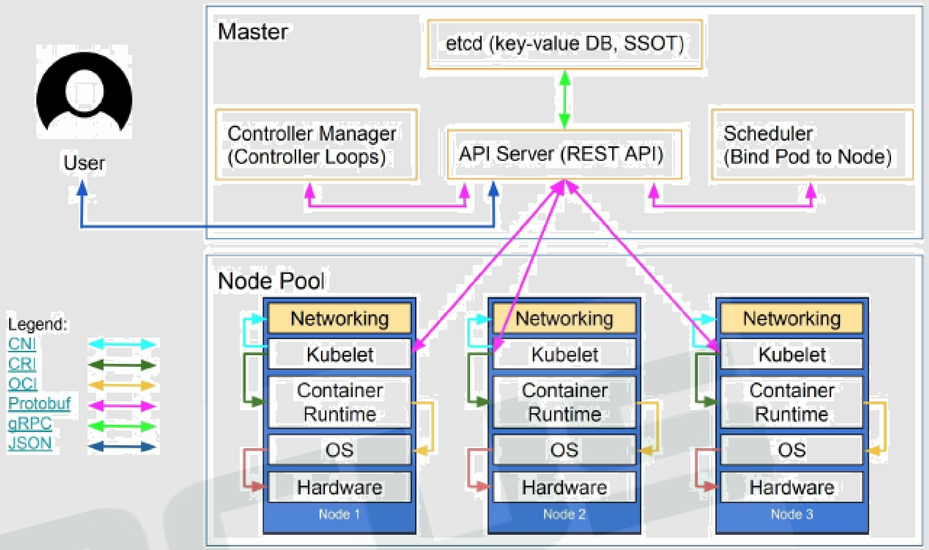
每台物理节点更多运行时实例

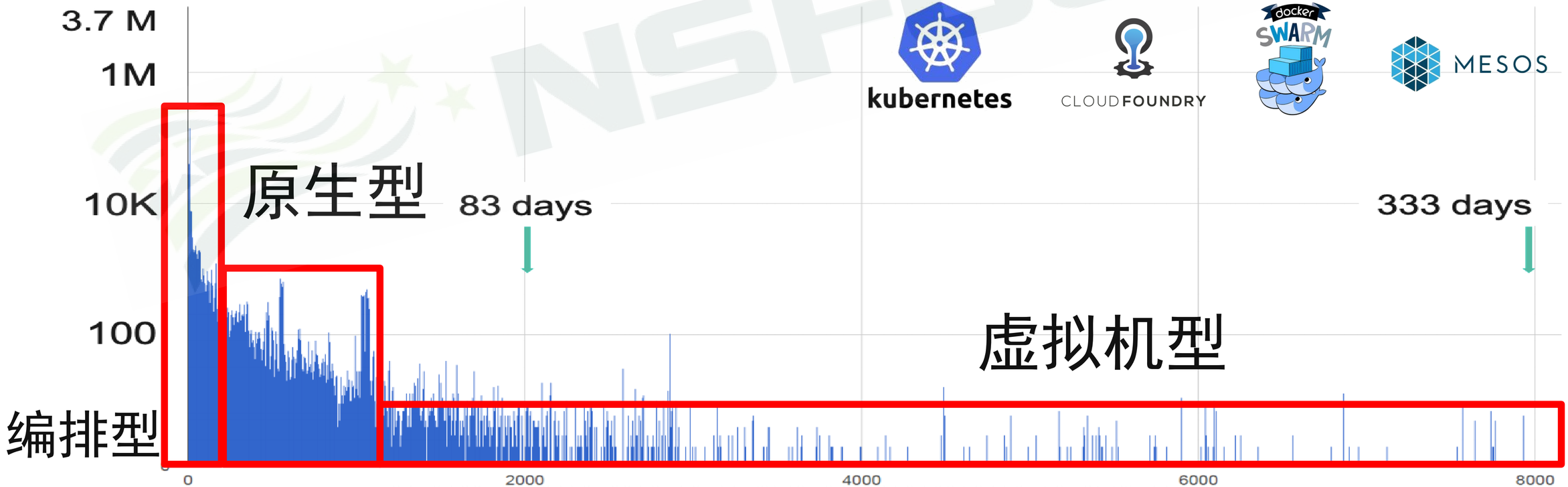


https://ubuntu.com/blog/how-many-containers-can-you-run-on-your-machine

编排：更快，更弹性

- 编排（orchestration），通常包括容器管理、调度、集群定义和服务发现等。
- 秒级伸缩
- ~~容器技术就是轻量级的虚拟化~~

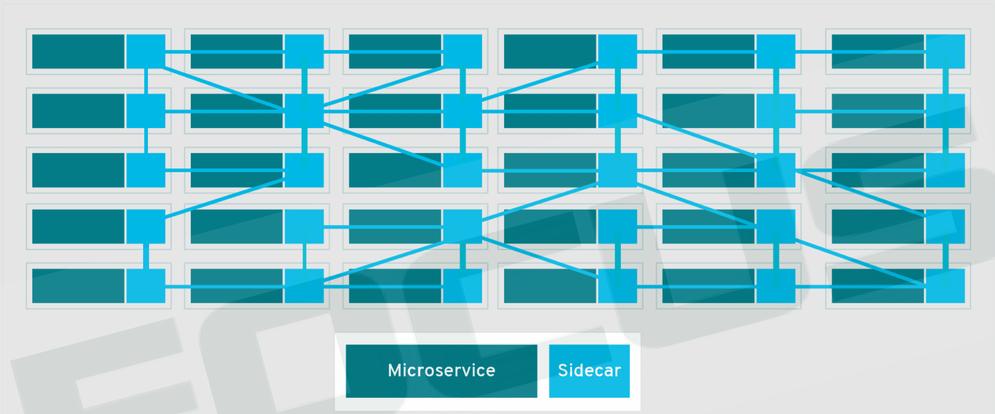




Source: https://events.static.linuxfound.org/sites/events/files/slides/cc15_mcguire.pdf

云原生、无服务、服务网格

- 访问规则？？？
- 行为模式？？？
- AD-HOC！！！



NSFOCUS
TECHWORLD2019
绿 盟 科 技 技 术 嘉 年 华

02

云原生之再思考

Rethinking of Cloud native security

NSFOCUS

TECHWORLD2019 绿盟科技技术嘉年华

Docker生态环境的风险和威胁

局域网攻击

同一主机上的容器之间可以构成局域网，因此针对局域网的ARP欺骗、嗅探、广播风暴等攻击方式将会对多个容器造成安全威胁

拒绝服务攻击

如果不对每个容器的可用CPU、内存等资源进行有效的限制和管理，容器之间就会造成资源使用不均衡等影响，严重时可能导致主机和集群资源耗尽，造成拒绝服务攻击

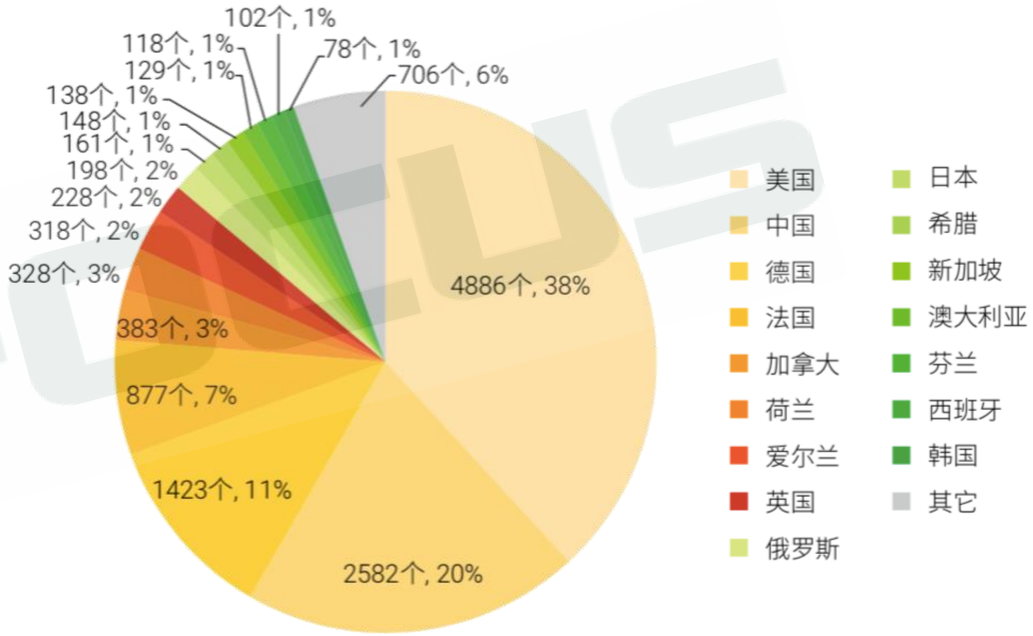
漏洞利用

Docker与主机共用一个操作系统内核，一旦主机内核存在横向越权或者提权漏洞，尽管Docker使用普通用户执行，一旦容器被入侵，攻击者还是可以利用内核漏洞逃逸到主机，进行恶意行为操作

服务暴露

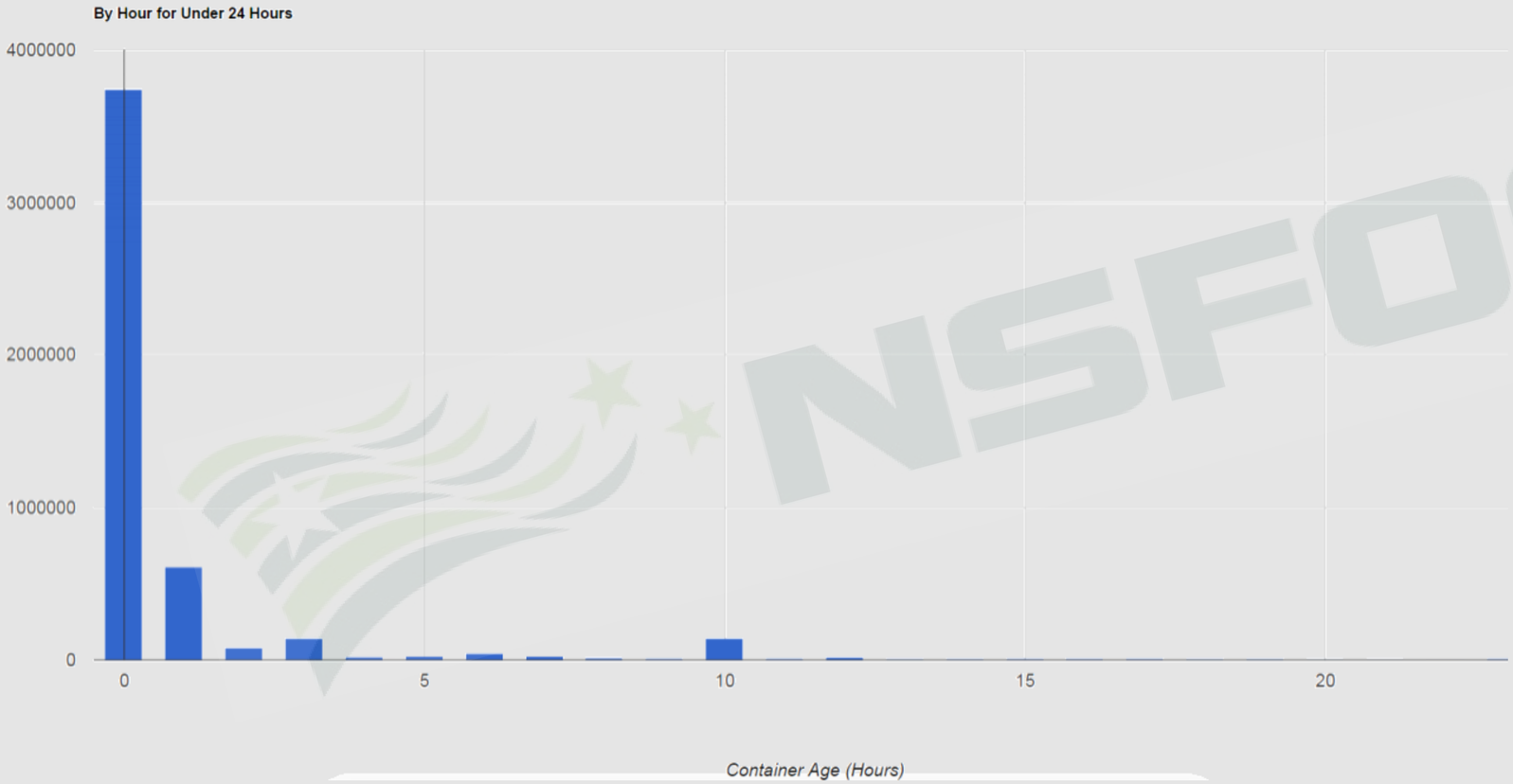
Docker默认服务端口为2375，开启没有任何加密和访问控制的Docker Remote API服务且暴露在互联网上是非常危险的。

2018 年 7 月，我们分析得Docker端口暴露数为337。此外，暴露在互联网上的Kubernetes API服务（6443 端口）达 12803 个。



暴露的 Kubernetes 服务的托管服务提供商全球分布图

TTL是容器安全的最大变化



TTL:

46%<1小时

11%<1分钟

对攻防双方
意味着什么？

Source: https://events.static.linuxfound.org/sites/events/files/slides/cc15_mcguire.pdf

硬币的正反面：没有Sec的DevOps

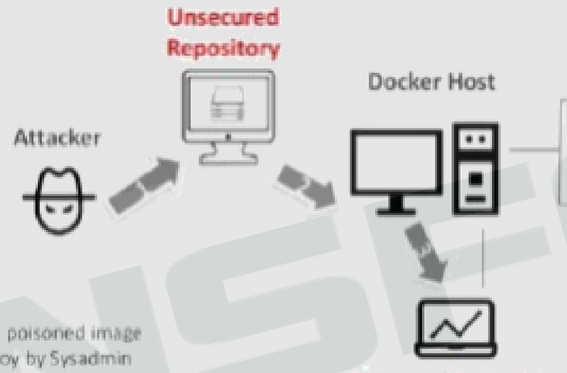
- 采用敏捷开发的团队一般会提高3-10倍的效率，软件的质量也有了更加可靠的保证。
- 20世纪四十年代美国马尔科姆·麦克莱恩改造并提高了**集装箱（Container）**的便利性，推动了整个运输行业的巨大变革

- 2018年，超过16000个开源软件的漏洞曝光
- 每8次下载开源软件，就有1次包括已知安全漏洞
- 67%审查的应用包括开源漏洞

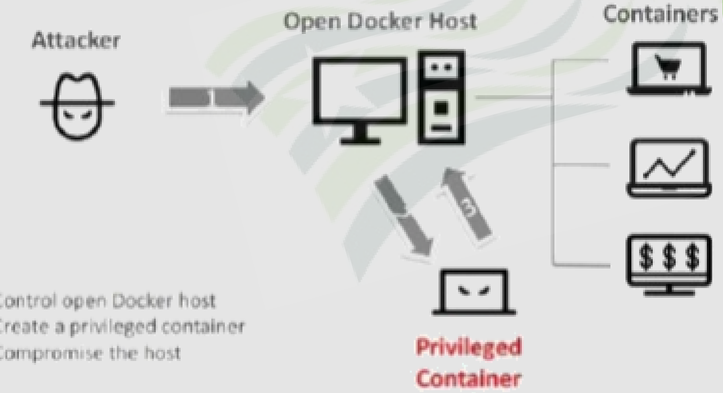
69% 的机构在评估或践行DevOps，其他31%已经积极实现或扩容DevOps了-Gartner

Docker面临的主要攻击方式

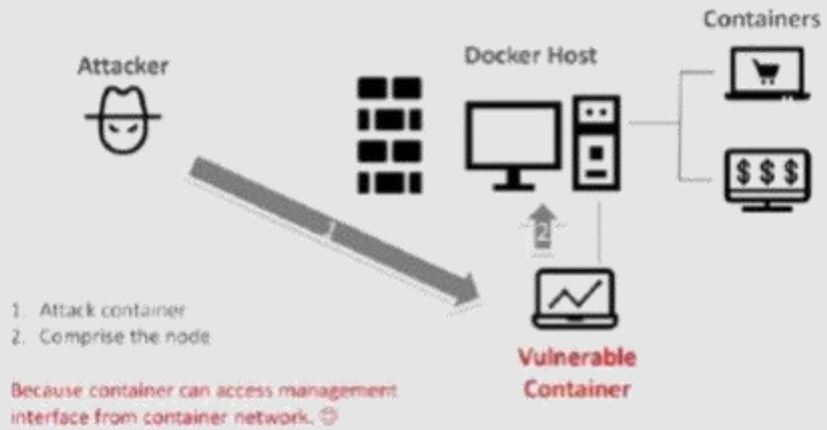
Attack-Poisoned image



Attack-Opened Node from Outside



Attack-Opened Node from Inside



02

应对之策

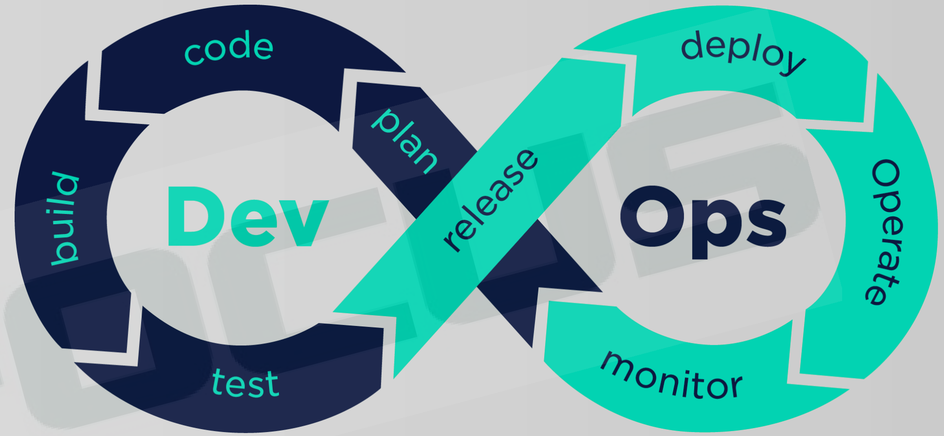
Countermeasures

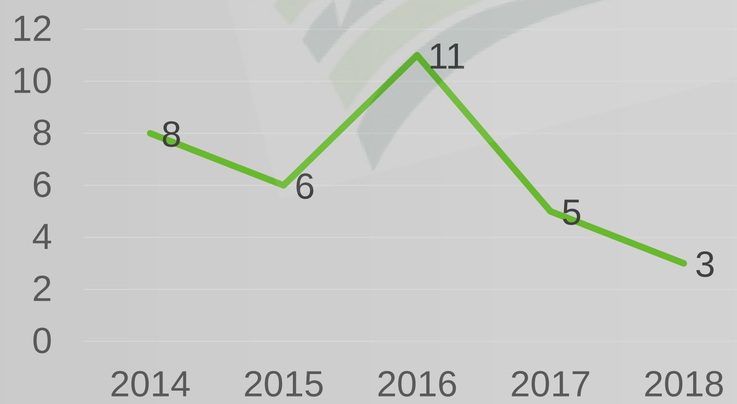
云原生新环境的安全对策

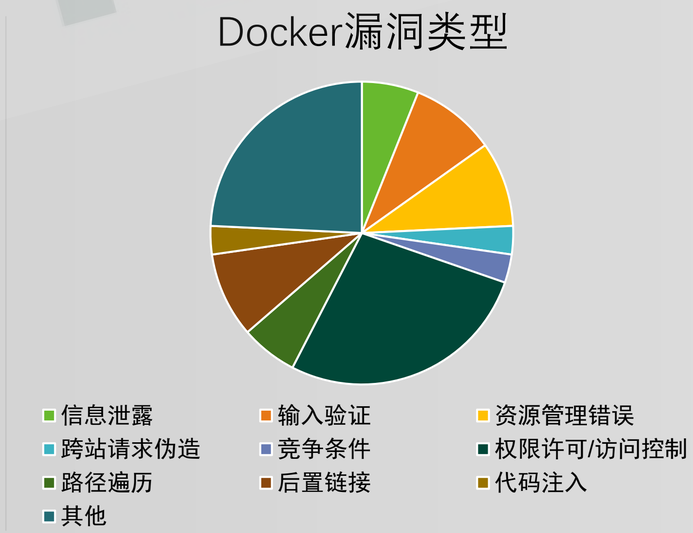
- 安全控制左移
- 变化是最大的不变
  - 寻找不变，聚焦持久化
  - 寻找混乱中的秩序：行为和业务
- 面向业务风险，解决客户真实问题

安全控制左移

- 最简单的事情意义最大
- 越靠左的安全控制效果最好
  - 代码漏洞
  - 第三方库
  - 用户凭证、密码硬编码
  - 可信镜像仓库
  - 服务器加固
  - 暴露面核查







- 容器相关中危及以上的漏洞占85%
- 2个CVSS评分10分的超危漏洞

聚焦持久化：仓库、镜像

- Docker Hub中**超过30%**的官方镜像包含高危漏洞，**接近70%**的镜像有着高危或中危漏洞。
  - *漏洞镜像主要集中在应用程序的镜像中；*
- 2018年6月，安全厂商发现17个受到感染的Docker容器镜像，镜像中包含了可用于挖掘加密货币的程序，更危险的是，这些镜像的下载次数已经高达500万次
- 开源的镜像扫描和漏洞库不能真正管理镜像漏洞生命周期

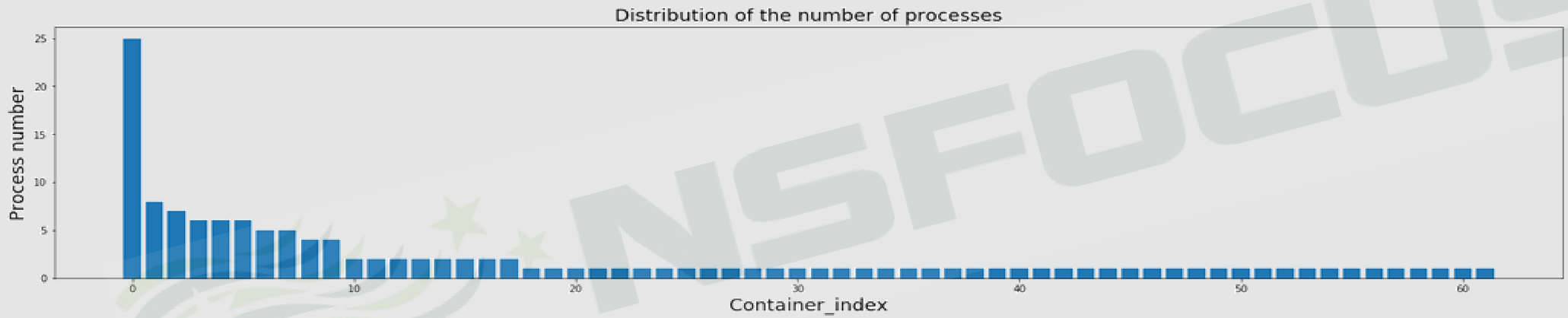
镜像	STARS	PULLS	HIGH	MEDIUM	LOW
nginx	8.1K	10M+	3	14	8
ubuntu	7.3K	10M+	0	6	14
mysql	5.8K	10M+	4	7	5
node	5.2K	10M+	68	193	71
redis	4.9K	10M+	6	11	9
postgres	4.7K	10M+	15	32	12
mongo	4.2K	10M+	6	11	9
centos	4.1K	10M+	0	0	0
jenkins	3.4K	10M+	11	25	21
alpine	3.3K	10M+	0	0	0

Docker Hub的官方镜像安全性分析

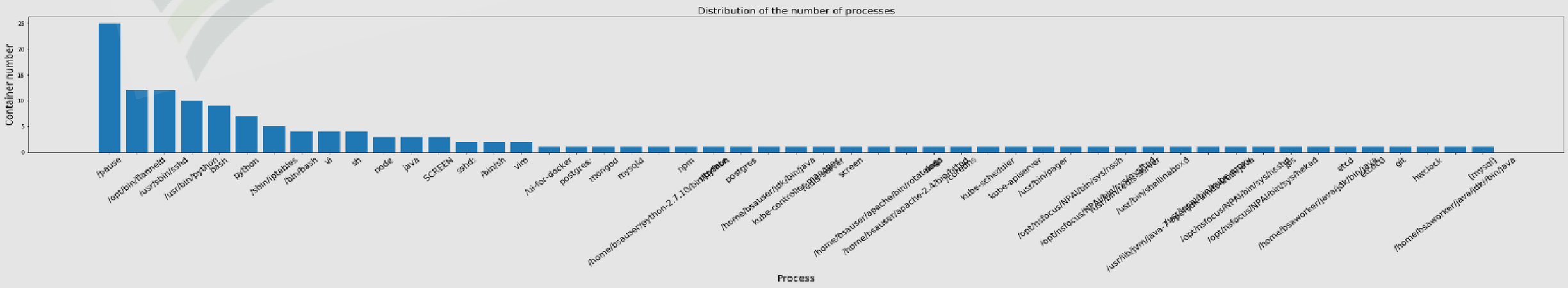
行为-寻找混乱中的秩序

经过进程名学习，除了第一个BSA的容器外，其他容器进程数量少且很稳定，可以通过学习
基线策略：给每一个container画一条进程基线，进行检测异常。

容器进程数的分布



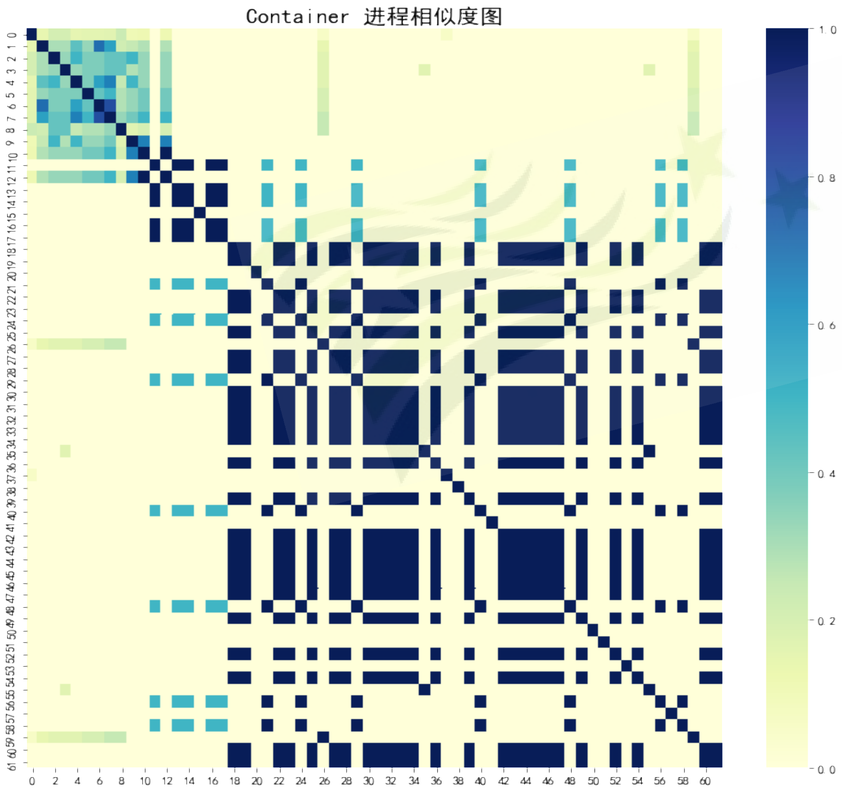
容器进程分布



行为-寻找混乱中的秩序

- 行为基线给容器异常检测带来了一种新思路
- 当某一个Container出现新进程行为，偏离自身基线；但这个行为在并没有偏离一类Container的总体基线，那么它很可能是正常行为，反之则可能为恶意攻击

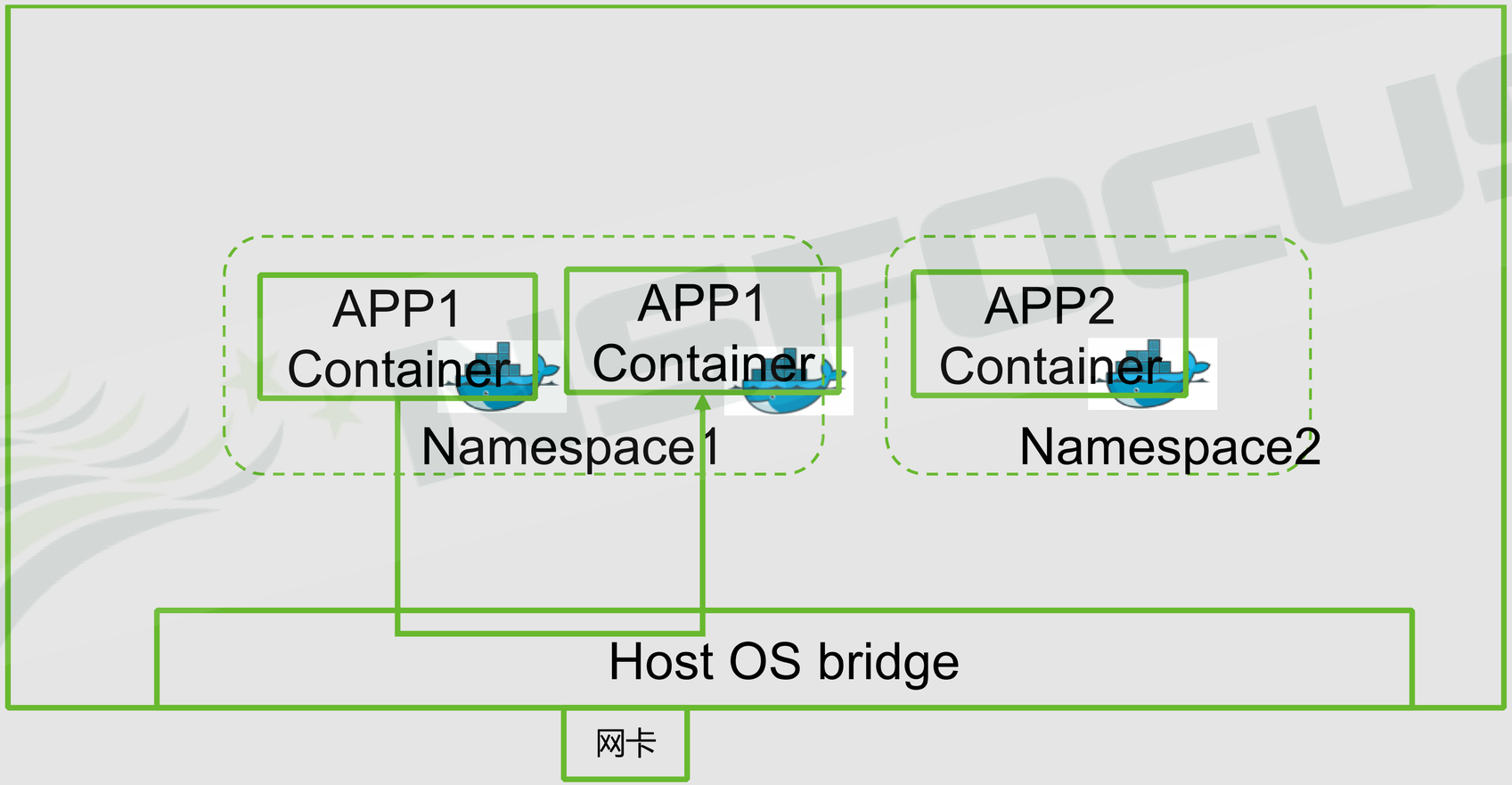
容器进程相似度分析



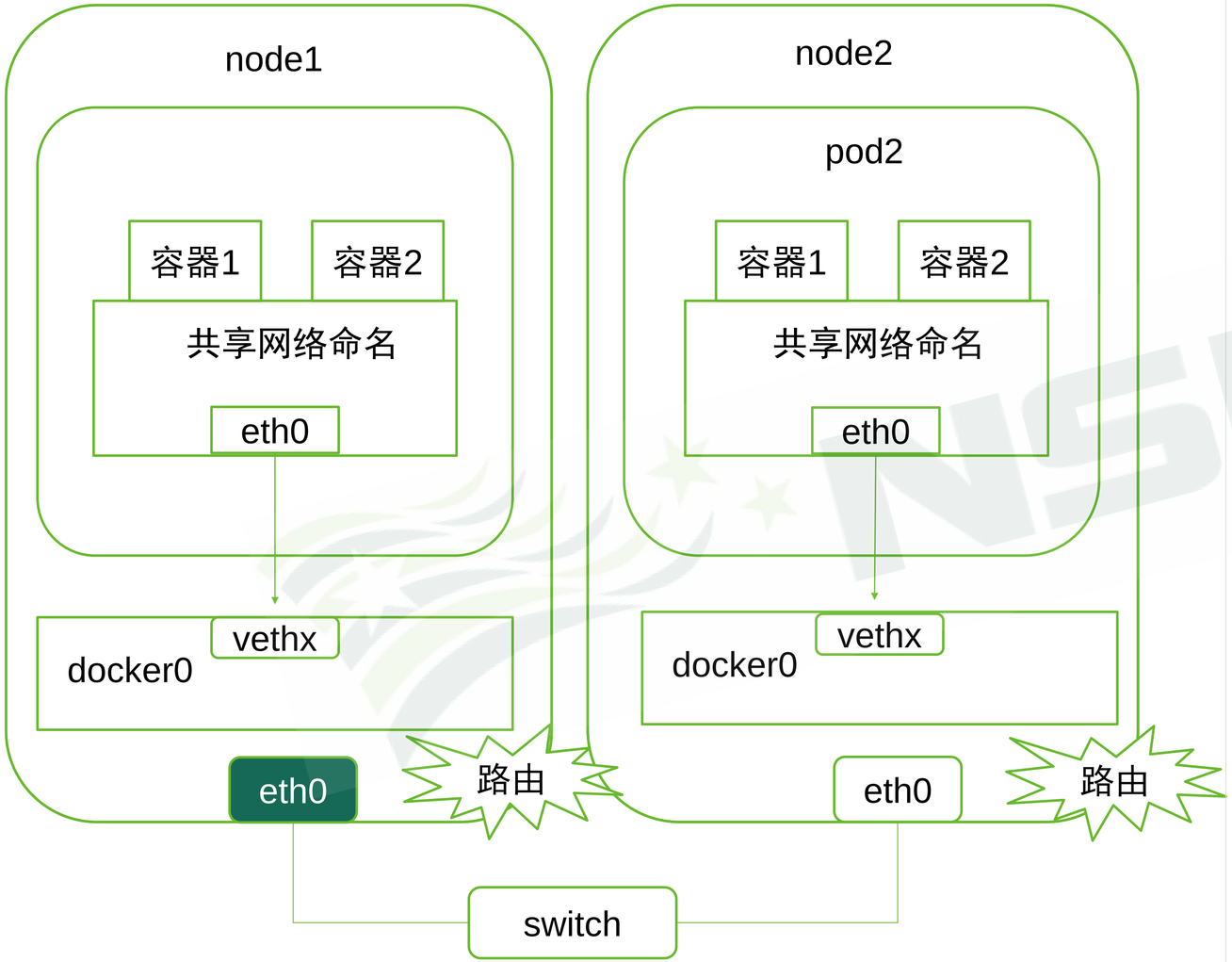
容器异常行为检测

	msg	event_type	process	user	cpu	process_len	container_name
0	原进程出现了新用户	01-02	bash	abc	0	4	k8s_data-dispatcher_data-dispatcher-deployment...
12	新进程启动，进程名长度过长异常	02-04	/usr/bin/python_abc	root	0	10	k8s_action-dispatcher_action-dispatcher-deploy...
7	原进程出现了新路径	01-03	/abc/bin/sh	root	0	2	k8s_zookeeper_zookeeper-1_default_9998eacf-85d...
11	原进程CPU偏高	01-01	/pause	root	100	5	k8s_POD_data-dispatcher-deployment-84d9f7f59d-...

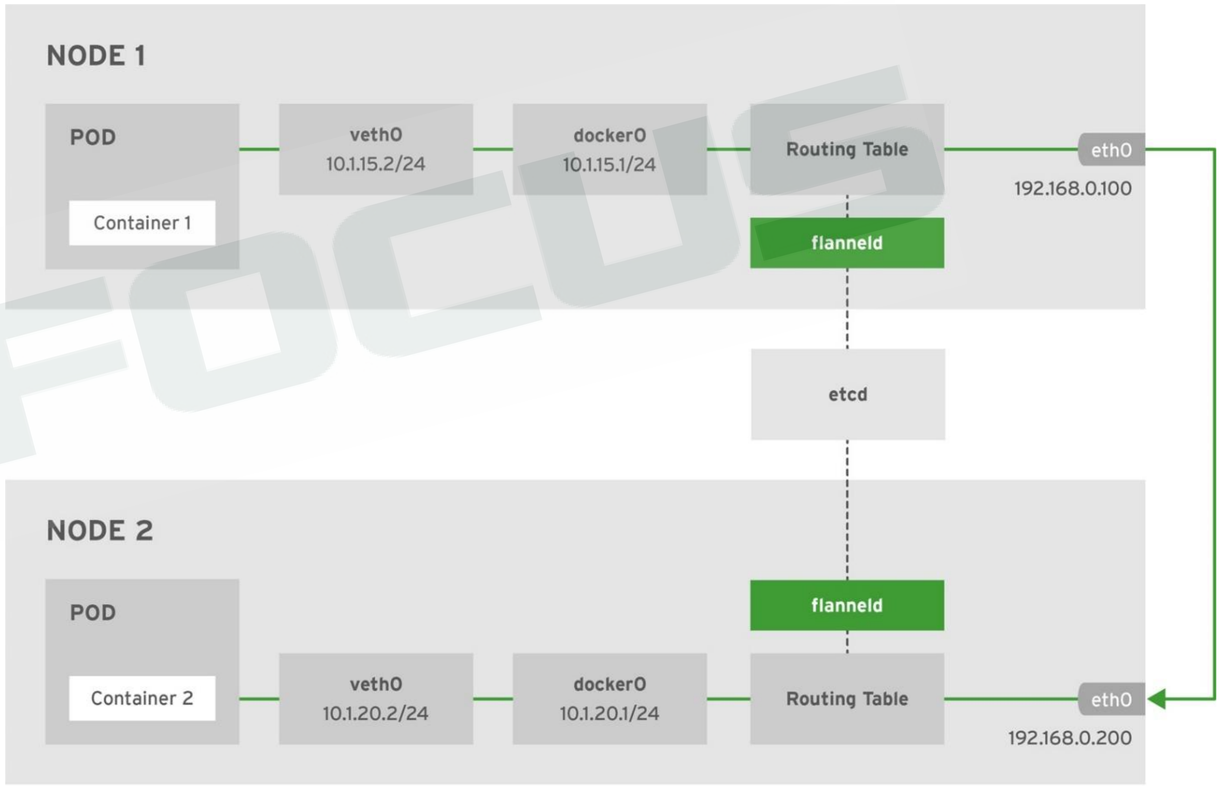
容器网络安全：同样重要


APP1
Container
APP1
Container
APP2
Container
Namespace1
Namespace2
Host OS bridge
网卡

容器网络全景图

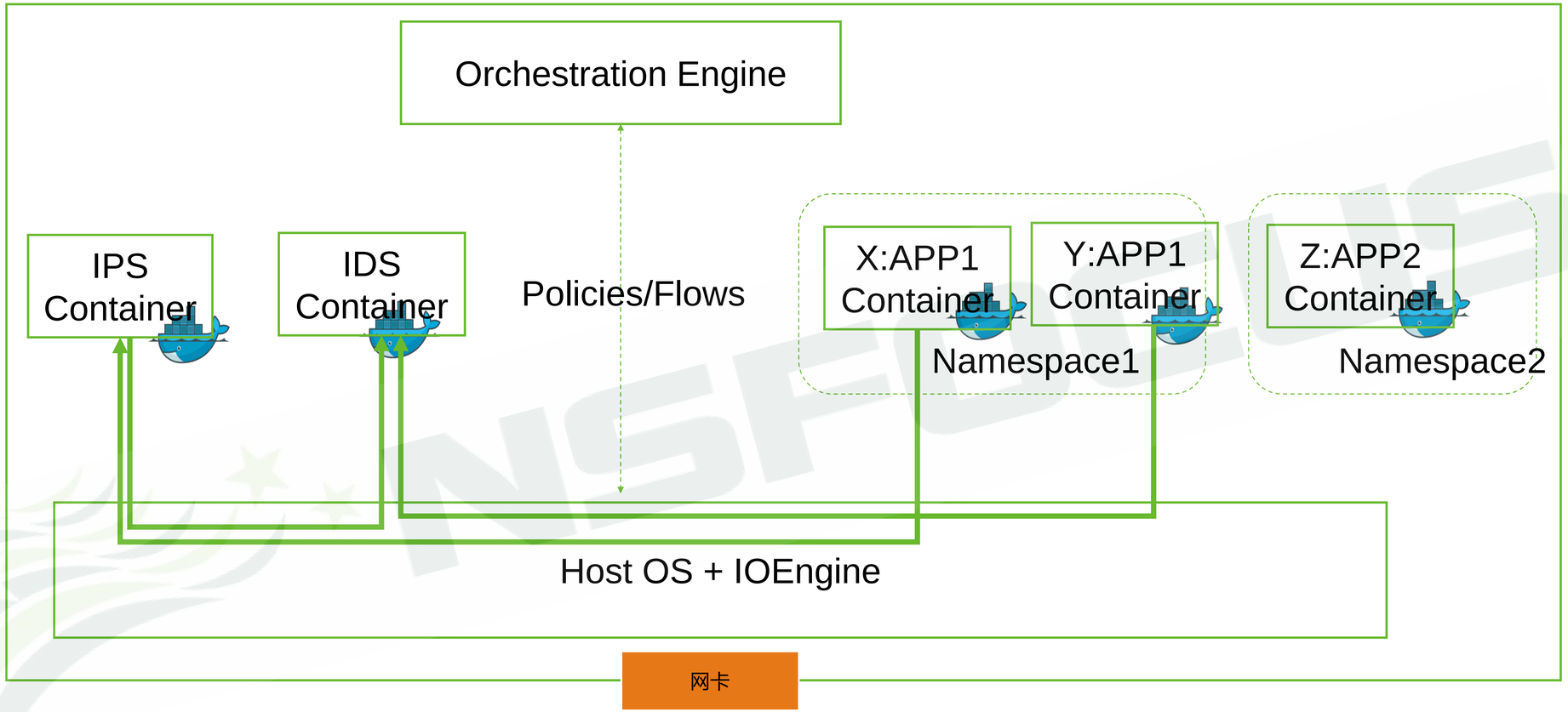


Kubernetes网络架构



flannel网络架构

“传统”的东西向防护（OVS和NSF服务链）



OVS IOEngine:

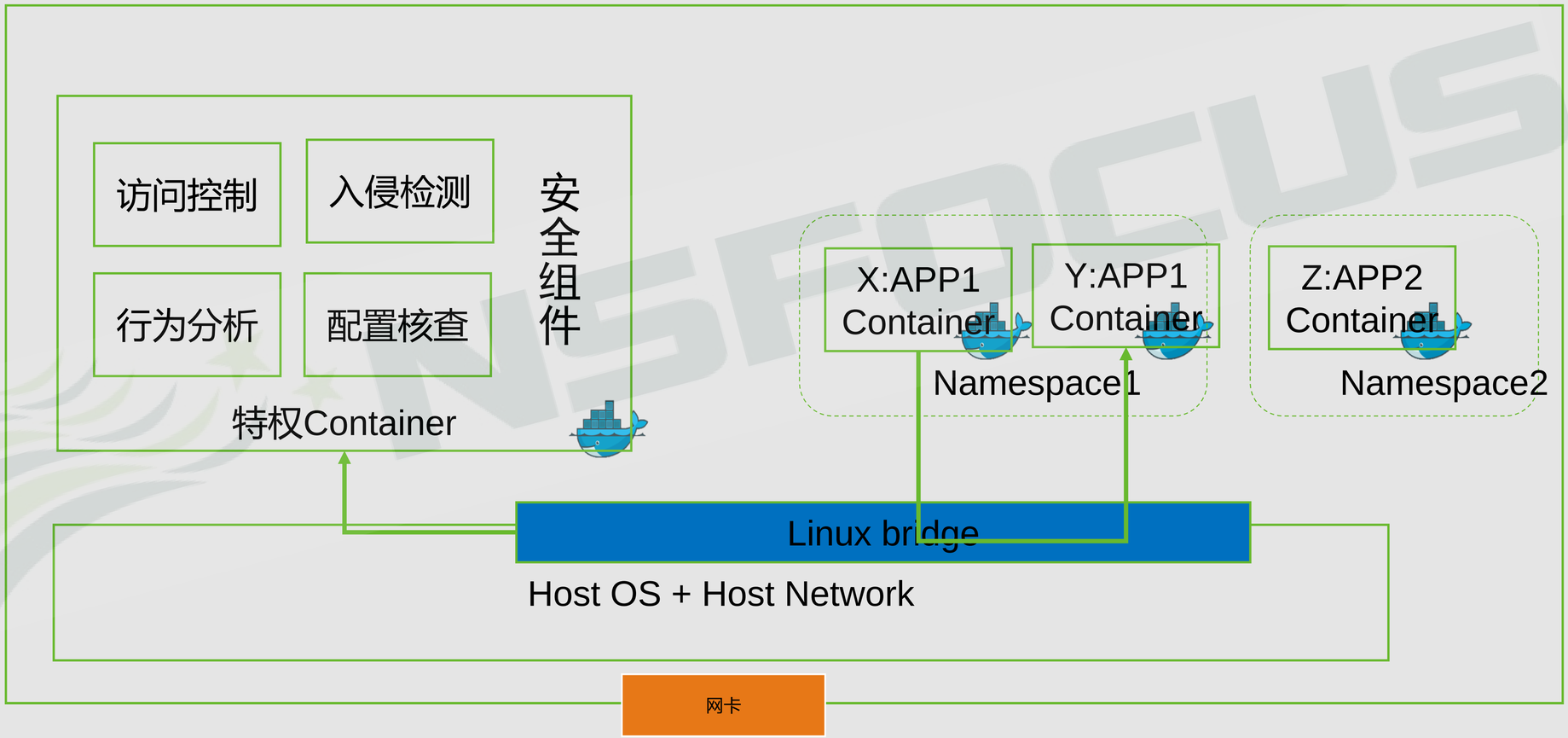
插件：docker-ovs-plgin
下流表：x>y:actions: output=IPS Container
input=IPS Container,x>y:output=IDS Container
input=IDS Container, x>y:output=y

服务链	64B	512 B	1518 B
OVS	800Mbps	3180Mbps	5600Mbps
NSF	2770Mbps	9460 Mbps	9500 Mbps

NSF IOEngine:

插件：docker-nsf-plugin
IOEngine收到x->y的数据包后，通过内核转递给IPS container和IDS container

新形态：容器环境东西向防护（特权容器）



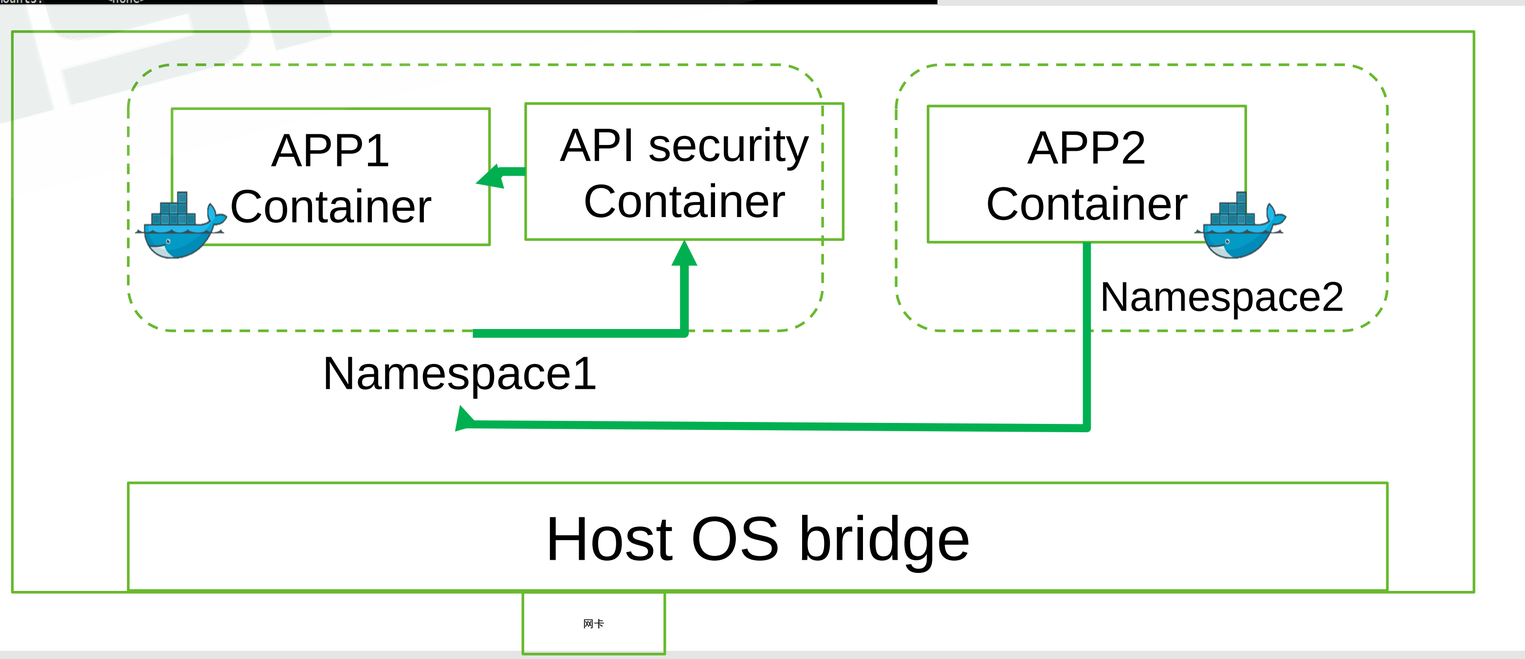
新业务：API安全（Sidecar）

- API认证授权
- API调用频次
- 恶意攻击（注入、拖库）
- 调用链画像
- …

```
Init Containers:
  istio-init:
    Container ID:  docker://55e4333a31fd4119583ed48172a98a706cc18571002b2ae6d6929b4419d55b2c
    Image:         gcr.io/istio-release/proxy_init:1.0.0
    Image ID:      docker-pullable://gcr.io/istio-release/proxy_init@sha256:345c40053b53b7cc70d12fb94379e5aa0befd979a99db80833cde671bd1f9fad
    Port:          <none>
    Host Port:     <none>
    Args:
      -p
      15001
      -u
      1337
      -m
      REDIRECT
      -i
      *
      -x

      -b
      9080,
      -d

    State:          Terminated
      Reason:       Completed
      Exit Code:    0
      Started:      Thu, 17 Jan 2019 15:47:42 +0800
      Finished:     Thu, 17 Jan 2019 15:47:42 +0800
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:         <none>
```



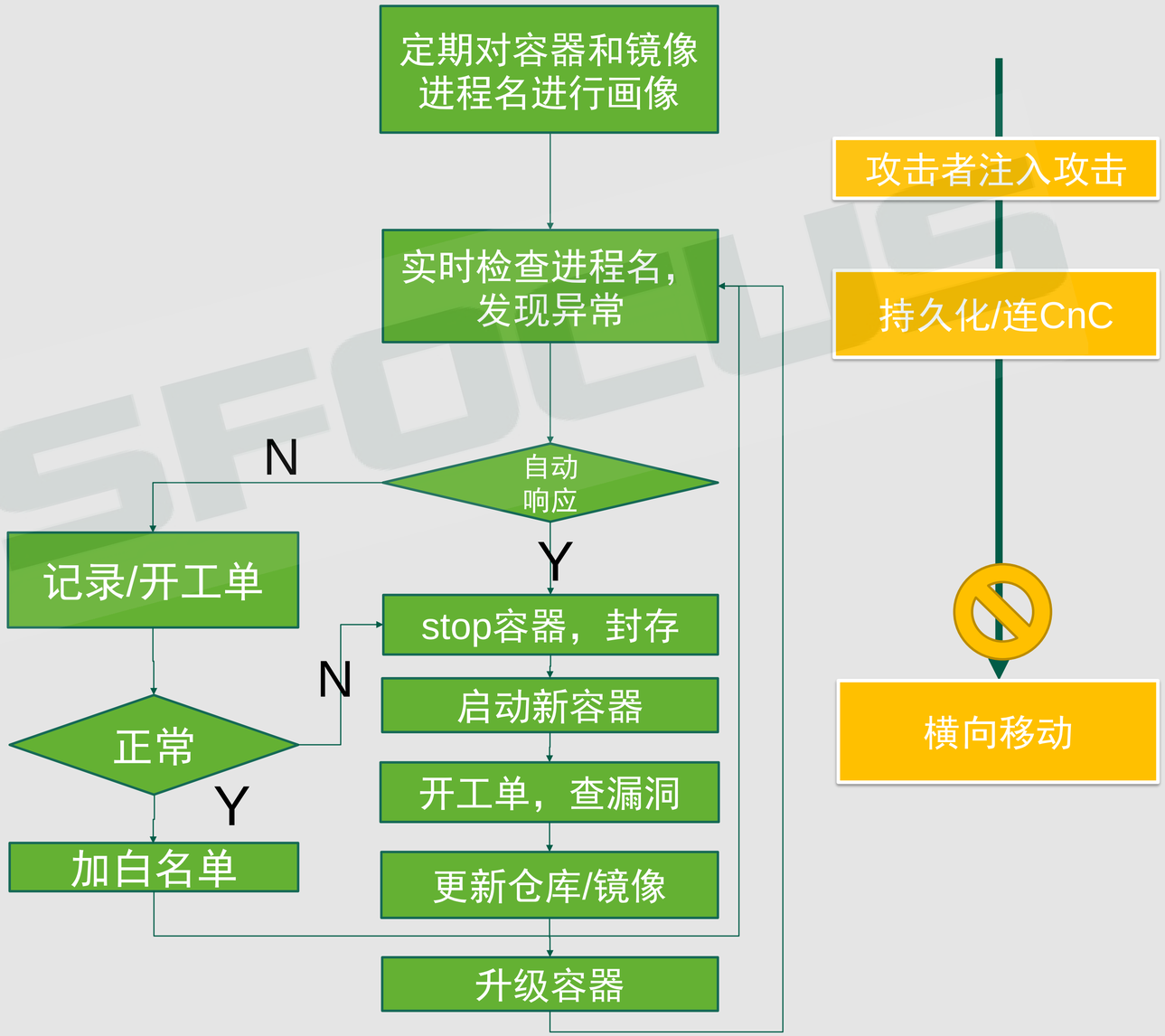
04

展望

About the Future

展望：CDR——Container Detection and Response

- AI是规模化同时，保证检测实时性的使能技术
- 自动化安全处置是容器环境中快速响应、恢复的必要的能力



自动化处置的Playbook

NSFOCUS

TECHWORLD2019 | 总结

绿 盟 科 技 技 术 嘉 年 华

世界没有那么简单，
容器安全不是虚拟化安全！

世界没有那么复杂，
简单的事情往往越重要...

天下武功，唯快不破

NSFOCUS

TECHWORLD2019

绿 盟 科 技 技 术 嘉 年 华

探索 · DISCOVERY

NSFOCUS TECHWORLD

感谢聆听！