基于openEuler的BC-Linux主机安全实践

演讲人：蔡启申

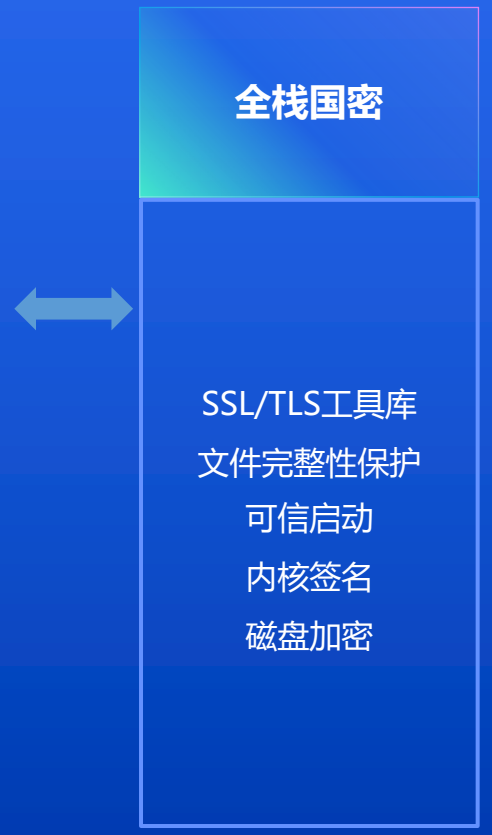
开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

主机全链安全可信，服务可信移动云

移动云

算力数据安全是移动云未来需要重点关注的安全方向

在云场景下，结合可信计算、机密计算、全栈国密等技术，在数据传输、存储和处理等阶段为云主机提供全方位的、多层次立体防御，打造“无死角”的数据安全闭环，构建全链路可信安全架构。



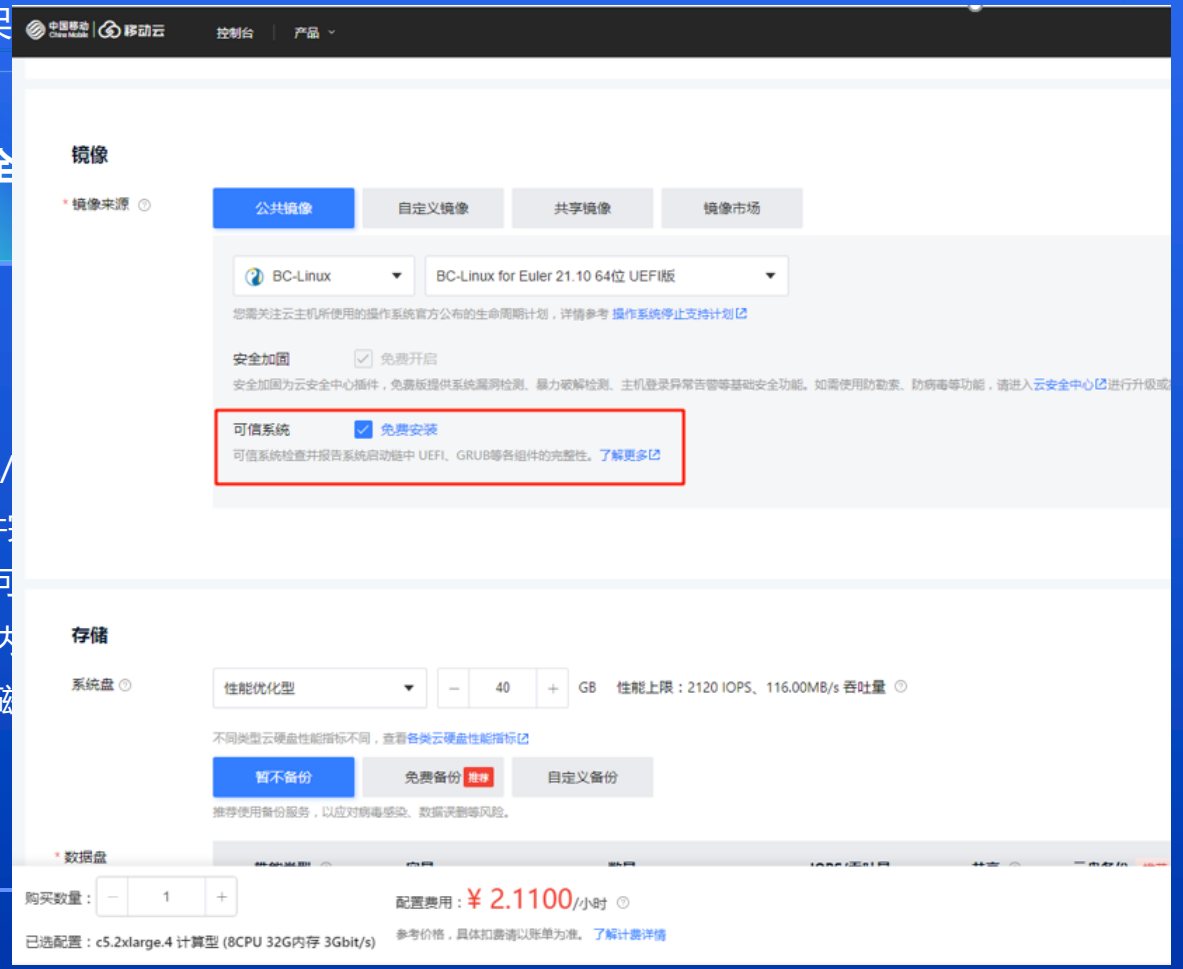
- ✓ **数据传输加密：** 利用数据先加密后落盘方式，保障数据在云主机实例和云硬盘间**传输的安全性**
- ✓ **数据生产加密：** 利用机密计算技术，将机密计算特性透传至云主机，保障云主机数据**产生时的安全性**
- ✓ **可信状态传递：** 支持物理可信设备与虚机可信设备的联动，能够将安全可信能力引导至安全实例，**确保云主机状态安全可信**
- ✓ **全栈国密算法：** 从内核、基础库到上层应用全栈支持国密算法，**满足我国最新等级保护2.0要求**

主机全链安全可信，服务可信移动云

移动云

算力数据安全是移动云未来需要重点关注的安全方向

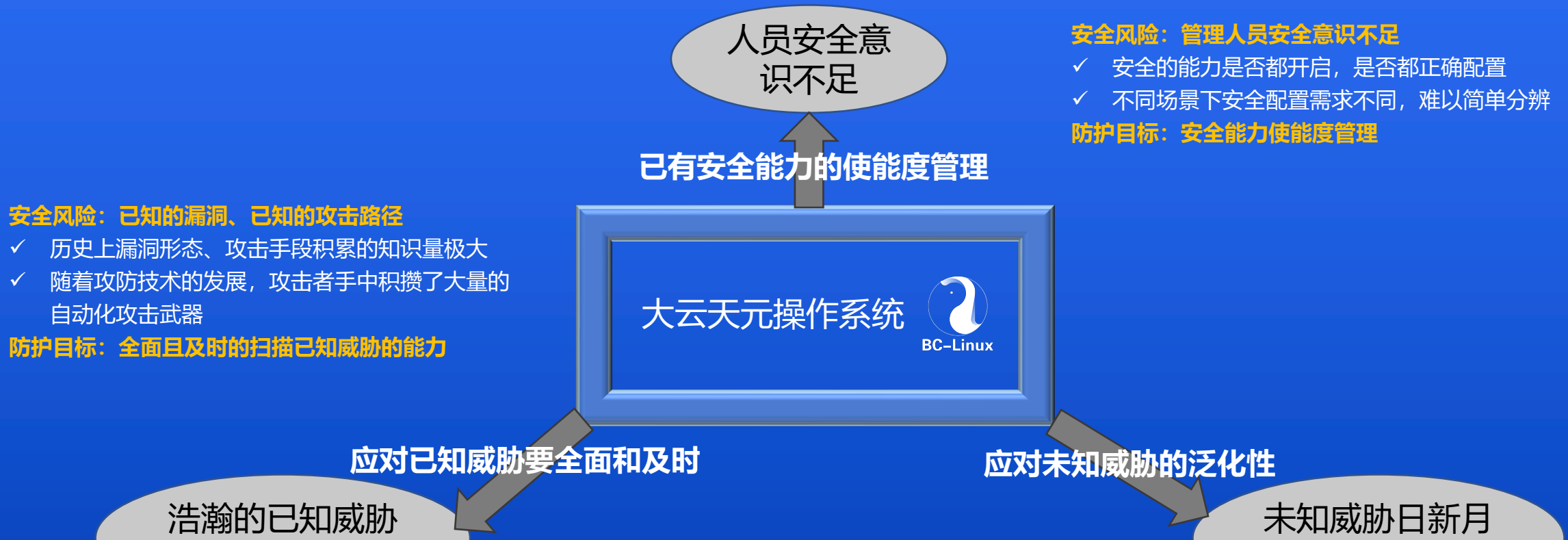
在云场景下，结合可信计算、机密计算、全栈国密等技术，在数据传输、存储和处理等阶段为云主机提供全方位的、多层次立体防御，打造“无死角”的数据安全闭环，构建全链路可信安全架



安全攻防实践中的安全风险无法避免

移动云

- BC-Linux面向软件和数据安全的全链路可信技术和端到端数据保护技术建立起全方位的的被动防御体系。
- 但在现实的安全攻防实践中，系统内外仍然面临一些无法避免的安全风险



安全风险：管理人员安全意识不足

- ✓ 安全的能力是否都开启，是否都正确配置
- ✓ 不同场景下安全配置需求不同，难以简单分辨

防护目标：安全能力使能度管理

安全风险：已知的漏洞、已知的攻击路径

- ✓ 历史上漏洞形态、攻击手段积累的知识量极大
- ✓ 随着攻防技术的发展，攻击者手中积攒了大量的自动化攻击武器

防护目标：全面且及时的扫描已知威胁的能力

安全风险：未知漏洞、未知攻击路径

- ✓ 新的漏洞形式、新的攻击手段层出不穷
- ✓ 新的威胁的特征不详，难以预先建模，精确识别

防护目标：强泛化检测未知威胁的能力

从被动到主动，主机安全持续演进

移动云

算力数据安全是移动云未来需要重点关注的安全方向

被动防护

在云场景下，结合可信计算、机密计算、全栈国密等技术，在数据传输、存储和处理等阶段为云主机提供全方位的、多层次立体防御，打造“无死角”的数据安全闭环，构建全链路可信安全架构。

主动防护

在云场景下，结合主动防护等技术，为云主机系统进一步提供安全免疫力，预防安全风险的发生。

天元操作系统

BC-Linux

端到端数据保护

- 机密计算
- 加密存储
- 加密传输
- 国密算法与协议

全链路可信

- 远程证明
- 虚拟可信设备
- 可信启动
- 信任链传递
- 文件完整性保护
- 内核签名

主动防护

- 安全管理
- 监测全局化
- 已知扫描 *
- 监测快反化
- 未知检测
- 监测智能化

硬件

- TPM
- ARM / X86

- ✓ **监测全局化：** 在系统内实施全面、有效的持续监控，不遗留任何的攻击死角和痕迹
- ✓ **监测快反化：** 在监控全局化的基础上，提升快速反应能力，对监控识别到的缺陷或者威胁进行快速处置，压缩攻击窗口
- ✓ **监测智能化：** 利用AI技术减少人工干预，提升对监控，分析，反应过程的性能，精度和效率

secScanner 3+3 技术架构，实践全面主动防护

secScanner基于“3核心能力 + 3公共能力”的技术架构，建设全面有效、实时自动、灵活易用的主动防护能力

三大核心能力

- ✓ **安全管理**：系统安全主动管理，主动看护系统已有安全能力健康状态
- ✓ **漏洞扫描**：已知攻击防护，及时消减现网风险
- ✓ **入侵检测**：使能openEuler-secDetector内构入侵检测系统，预置覆盖MITRE ATT&CK攻击的异常检测探针，精准采集、及时阻断

系统安全主动管理，保障系统安全防御使能

- ✓ **安全基线导入**: 已支持行业配置要求YDT 2701-2014《电信网和互联网安全防护基线配置要求及检测要求 操作系统》，首批支持《**openEuler安全配置基线 V1.0**》
- ✓ **系统全局巡检**：自动全局检测，识别系统中存在的安全配置风险
- ✓ **导出报告**：汇总系统异常信息，自动生成易读性报告，支持html等格式
- ✓ **一键加固**：按安全基线要求自动对不满足项进行加固
- ✓ **一键还原**：对无需加固场景可按需还原

系统安全主动管理，保障系统安全防御使能


```
[root@localhost ~]# secscanner check basic

[+] Initializing program
-----------------------------------
- Get the OS-ID:bclinux and OS-version:21.10...                          [ OK ]

  ------------------------------------------------
  Program version:           0.1.0
  Operating system:          Linux
  Operating system name:     BCLinux
  Operating system version:  BigCloud Enterprise Linux For Euler 21.10 LTS
  Kernel version:            None
  Hardware platform:         x86_64
  Hostname:                  None
  Profile:                   /etc/secScanner/secscanner.cfg
  Log file:                  /var/log/secScanner/secscanner.log
```

3	No password minLen set	1、执行备份： #cp -np /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 2、修改策略设置： #vi /etc/pam.d/system-auth password requisite pam_pwquality.so ... minlen=8 ... password sufficient pam_unix.so ...
4	No password minclass set	1、执行备份： #cp -np /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 2、修改策略设置： #vi /etc/pam.d/system-auth password requisite pam_pwquality.so ... minclass=-1 ... password sufficient pam_unix.so ...
5	No password ucredit set	1、执行备份： #cp -np /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 2、修改策略设置： #vi /etc/pam.d/system-auth password requisite pam_pwquality.so ... ucredit=-1 ... password sufficient pam_unix.so ...
6	No password lcredit set	1、执行备份： #cp -np /etc/pam.d/system-auth /etc/pam.d/system-auth_bak 2、修改策略设置： #vi /etc/pam.d/system-auth password requisite pam_pwquality.so ... lcredit=-1 ... password sufficient pam_unix.so ...

```
- No umask set...                                                       [ WARNING ]
```

已知攻击防护，及时消减现网风险

漏洞扫描子系统建立起持续更新漏洞数据库，已收录**2000多**条安全公告及**6000多**条CVE漏洞，支持社区及BC-Linux for Euler多个版本漏洞精准扫描，提供准确修复建议，高效支持现网风险及时消减

社区多成员发现 → 社区统一确认发布 → 一键获取漏洞数据 → 全量扫描定向扫描 → 漏洞报告

```
  ################################################################
  #                                                              #
  #   Start updating the system vulnerabilities database...      #
  #                                                              #
  ################################################################


[+] Updating database
-----------------------------------
0 SAs and 0 CVEs are updated!                                [ OK ]
```

```
 ---------------------------------------------------
- Found virtual machine (type: vmware, VMware product)                [ DONE ]

  ################################################################
  #                                                              #
  #   Start updating the system vulnerabilities database...      #
  #                                                              #
  ################################################################


[+] Updating database
-----------------------------------
Updated SA  openEuler-SA-2023-1886
Updated SA  openEuler-SA-2023-1887
Updated SA  openEuler-SA-2023-1888
Updated SA  openEuler-SA-2023-1889
Updated SA  openEuler-SA-2023-1890
Updated SA  openEuler-SA-2023-1891
Updated SA  openEuler-SA-2023-1892
Updated SA  openEuler-SA-2023-1893
Updated SA  openEuler-SA-2023-1894
Updated SA  openEuler-SA-2023-1895
Updated SA  openEuler-SA-2023-1896
Updated SA  openEuler-SA-2023-1897
Updated SA  openEuler-SA-2023-1898
Updated SA  openEuler-SA-2023-1899
Updated SA  openEuler-SA-2023-1900
Updated SA  openEuler-SA-2023-1901
Updated SA  openEuler-SA-2023-1902
Updated SA  openEuler-SA-2023-1903
Updated CVE  CVE-2023-45539
Updated CVE  CVE-2023-0836
Updated CVE  CVE-2023-49083
Updated CVE  CVE-2023-1193
Updated CVE  CVE-2023-44444
Updated CVE  CVE-2023-44442
Updated CVE  CVE-2023-6277
Updated CVE  CVE-2020-21428
Updated CVE  CVE-2020-21427
Updated CVE  CVE-2022-47630
Updated CVE  CVE-2023-49081
18 SAs and 11 CVEs are updated!                              [ OK ]
```

已知攻击防护，及时消减现网风险

漏洞扫描子系统建立起持续更新漏洞数据库，已收录**2000多**条安全公告及**6000多**条CVE漏洞，支持社区及BC-Linux for Euler多个版本漏洞精准扫描，提供准确修复建议，高效支持现网风险及时消减

社区多成员发现 → 社区统一确认发布 → 一键获取漏洞数据 → 全量扫描定向扫描 → 漏洞报告

```
  ############################################################
  #                                                          #
  #   Scan system components by db data...                   #
  #                                                          #
  ############################################################


[+] Vulnerability scanning...
-----------------------------------
Found 72 pieces of information about component vulnerabilities              [ WARNING ]
------------------------------------------------------------------------

According to openEuler-SA-2023-1723
Fix CVE-2023-4911
glibc should be updated to glibc-2.34-137
------------------------------------------------------------------------

According to openEuler-SA-2023-1751
Fix CVE-2023-45853
zlib should be updated to zlib-1.2.11-24
------------------------------------------------------------------------

According to openEuler-SA-2023-1762
Fix CVE-2023-38545;CVE-2023-38546
curl should be updated to curl-7.79.1-24
------------------------------------------------------------------------
```

```
  ############################################################
  #                                                          #
  #   Check system compounents targeted according to cfg file...   #
  #                                                          #
  ############################################################


[+] Vulnerability targeted scanning...
-----------------------------------
This machine doesn't have [activemq], pass...                               [ SKIPPING ]
This machine doesn't have [apr], pass...                                    [ SKIPPING ]
Can't find any SA data about [bash] in database...                          [ SKIPPING ]
[file] should be updated to file-5.41-3...                                  [ WARNING ]
[glibc] should be updated to glibc-2.34-137...                              [ WARNING ]
This machine doesn't have [httpd], pass...                                  [ SKIPPING ]
This machine doesn't have [mysql], pass...                                  [ SKIPPING ]
This machine doesn't have [nginx], pass...                                  [ SKIPPING ]
This machine doesn't have [ntp], pass...                                    [ SKIPPING ]
[openssh] should be updated to openssh-8.8p1-23...                          [ WARNING ]
[openssl] should be updated to openssl-1.1.1m-29...                         [ WARNING ]
This machine doesn't have [php], pass...                                    [ SKIPPING ]
This machine doesn't have [squid], pass...                                  [ SKIPPING ]
[sudo] should be updated to sudo-1.9.8p2-11...                              [ WARNING ]
This machine doesn't have [tomcat], pass...                                 [ SKIPPING ]
This machine doesn't have [vsftpd], pass...                                 [ SKIPPING ]
This machine doesn't have [ftp], pass...                                    [ SKIPPING ]
Can't find any SA data about [wget] in database...                          [ SKIPPING ]
This machine doesn't have [samba], pass...                                  [ SKIPPING ]
```

已知攻击防护，及时消减现网风险

漏洞扫描子系统建立起持续更新漏洞数据库，已收录**2000多**条安全公告及**6000多**条CVE漏洞，支持社区及BC-Linux for Euler多个版本漏洞精准扫描，提供准确修复建议，高效支持现网风险及时消减

社区多成员发现 → 社区统一确认发布 → 一键获取漏洞数据 → 全量扫描定向扫描 → 漏洞报告

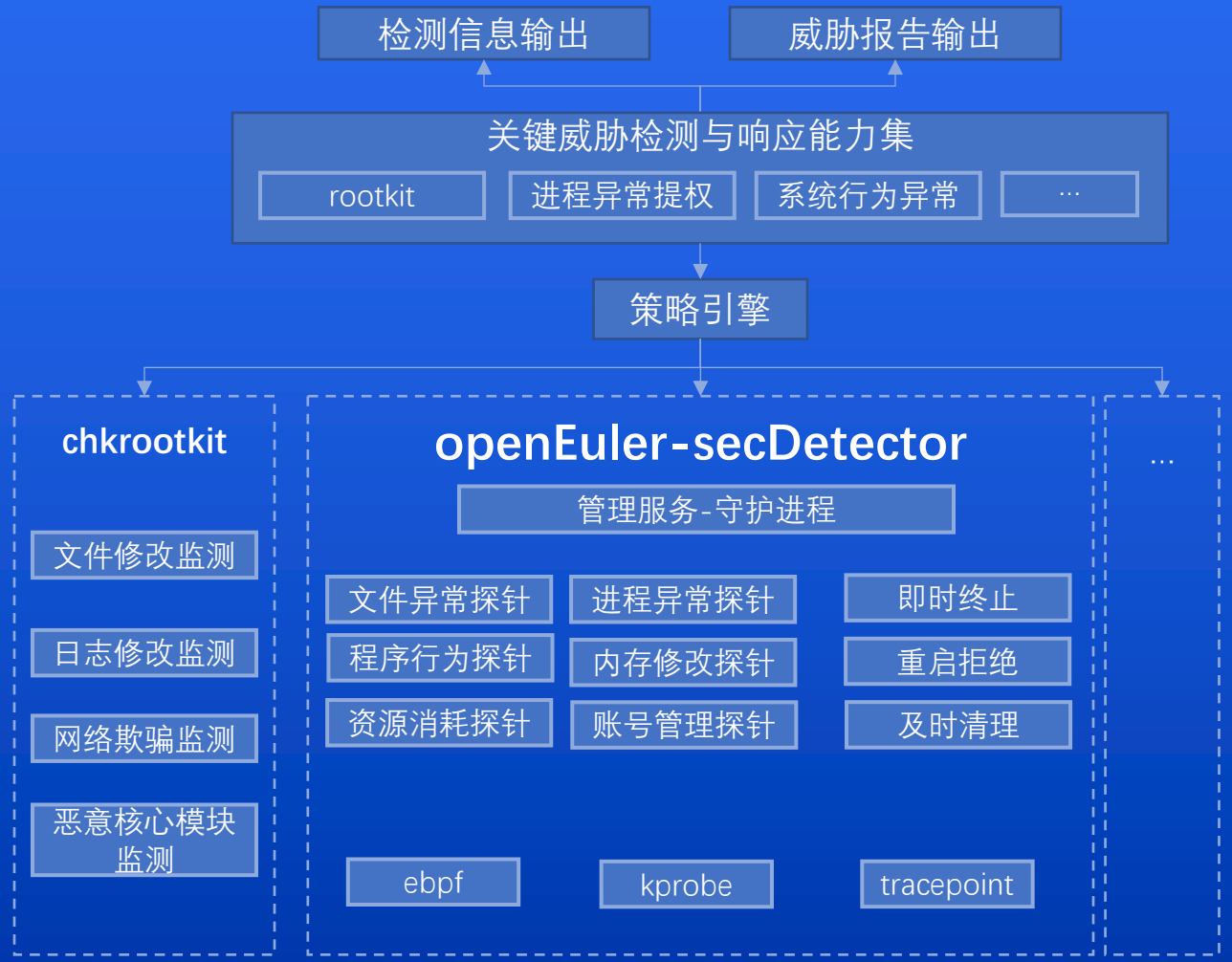
2.2 系统漏洞分布

Vulnerabilities Details (109): ----------

序号	CVE号	涉及软件包名	漏洞修复版本	漏洞评分	利用方式	利用复杂度	BLSA	CVE漏洞描述
1	CVE-2022-4415	systemd	systemd-249-43.oe2203sp1.x86_64	5.5	Local	Low	openEuler-SA-2023-1027	A vulnerability was found in systemd. This security flaw can cause a local information leak due to systemd-coredump not respecting the fs.suid_dumpable kernel setting.
2	CVE-2023-24056	pkgconf	pkgconf-1.8.0-2.oe2203sp1.x86_64	9.8	Network	Low	openEuler-SA-2023-1046	In pkgconf through 1.9.3, variable duplication can cause unbounded string expansion due to incorrect checks in libpkgconf/tuple.c:pkgconf_tuple_parse. For example, a .pc file containing a few hundred bytes can expand to one billion bytes.
3	CVE-2022-48281	libtiff	libtiff-4.3.0-21.oe2203sp1.x86_64	7.5	Network	Low	openEuler-SA-2023-1047	processCropSelections in tools/tiffcrop.c in LibTIFF through 4.5.0 has a heap-based buffer overflow (e.g., WRITE of size 307203) via a crafted TIFF image.
4	CVE-2023-22809	sudo	sudo-1.9.8p2-7.oe2203sp1.x86_64	7.8	Network	Low	openEuler-SA-2023-1049	In Sudo before 1.9.12p2, the sudoedit (aka -e) feature mishandles extra arguments passed in the user-provided environment variables (SUDO_EDITOR, VISUAL, and EDITOR), allowing a local attacker to append arbitrary entries to the list of files to process. This can lead to privilege escalation. Affected versions are 1.8.0 through 1.9.12.p

聚焦关键攻击场景，使能secDetector内构入侵检测能力

- 基于ATT&CK等攻击模式库识别rootkit、进程异常提权等关键攻击场景，结合chkrootkit、secDetector多种专业入侵检测工具构建综合检测能力
- 依托openEuler-secDetector这一OS内构入侵检测系统的形式筑造差异化的感知和响应竞争力 -》准确、即时、丰富

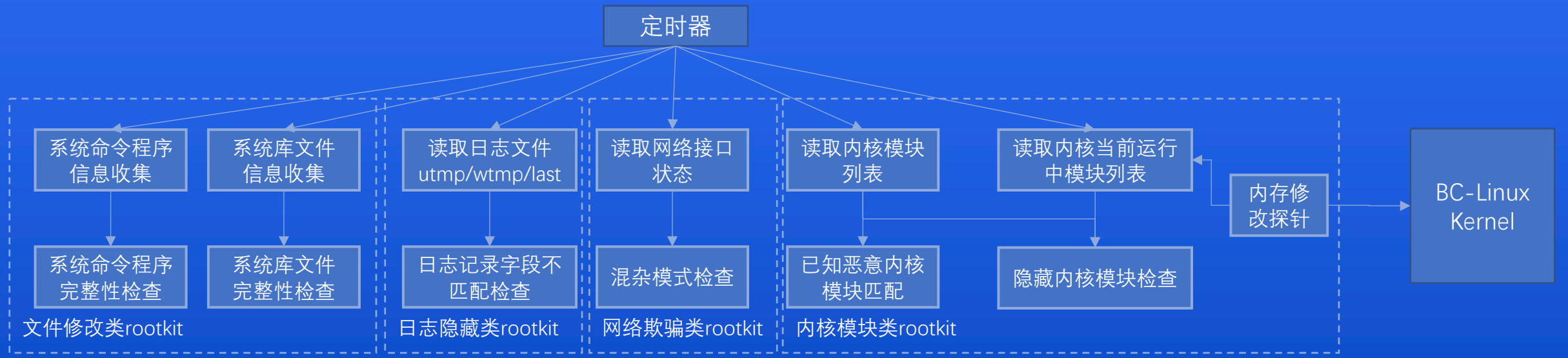


secDetector三大竞争力

- ✓ **准确的感知**：专业的采集和处理一手信息，面向关键恶意行为
- ✓ **即时的响应**：能够进行即时的分析与判断，立刻阻断攻击
- ✓ **丰富的溯源**：保留更多历史关联状态进行难以被打断的攻击溯源链条

准确的感知 之 rootkit检测

- rootkit是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息
- rootkit用来实现驻留和隐藏痕迹的作用，是高级持续威胁APT中必不可少的攻击环节，经常和其他攻击程序配合使用。
- 持续监控和识别多种类型的rootkit风险，以尽可能早的发现潜伏的威胁



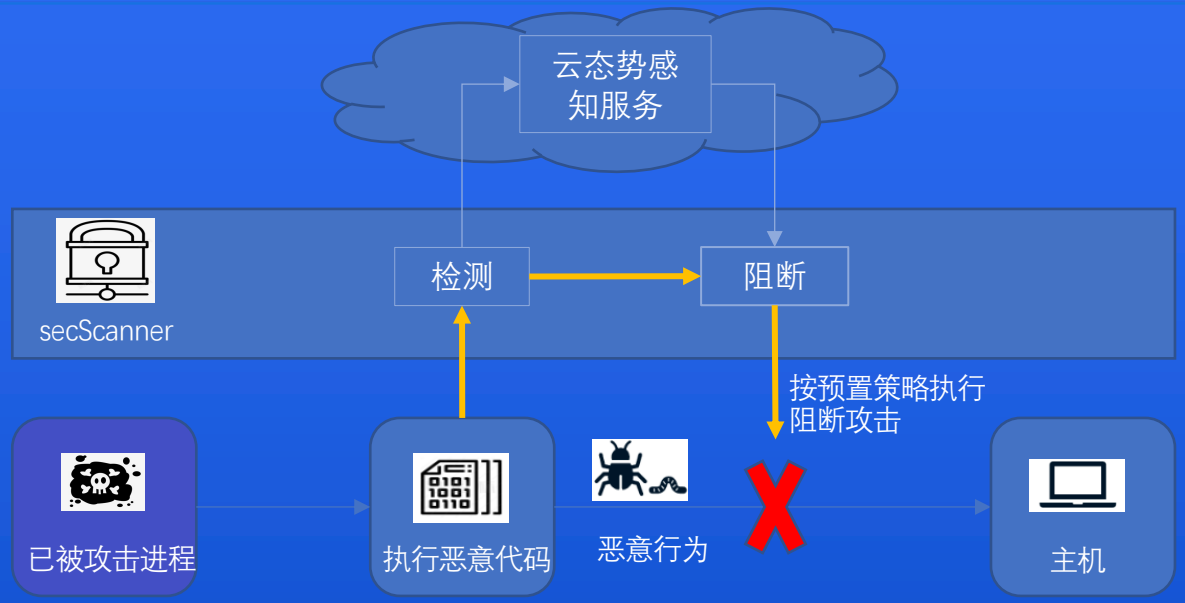
✓ **感知隐藏**：攻击者总是试图隐藏自己的痕迹以期达到长时间潜伏持续作恶的目的。发现隐藏这一动作也就意味着恶意的攻击正在发生

✓ **内核探针**：secDetector通过在操作系统内核中添加专用的**内存修改探针**，揭露被攻击者以特殊手段隐藏的rootkit内核模块

即时的阻断 之 恶意代码执行和内核rootkit模块加载

在主机本地实现攻击阻断能力，配合检测及时阻断攻击避免影响进一步扩大

恶意代码执行终止



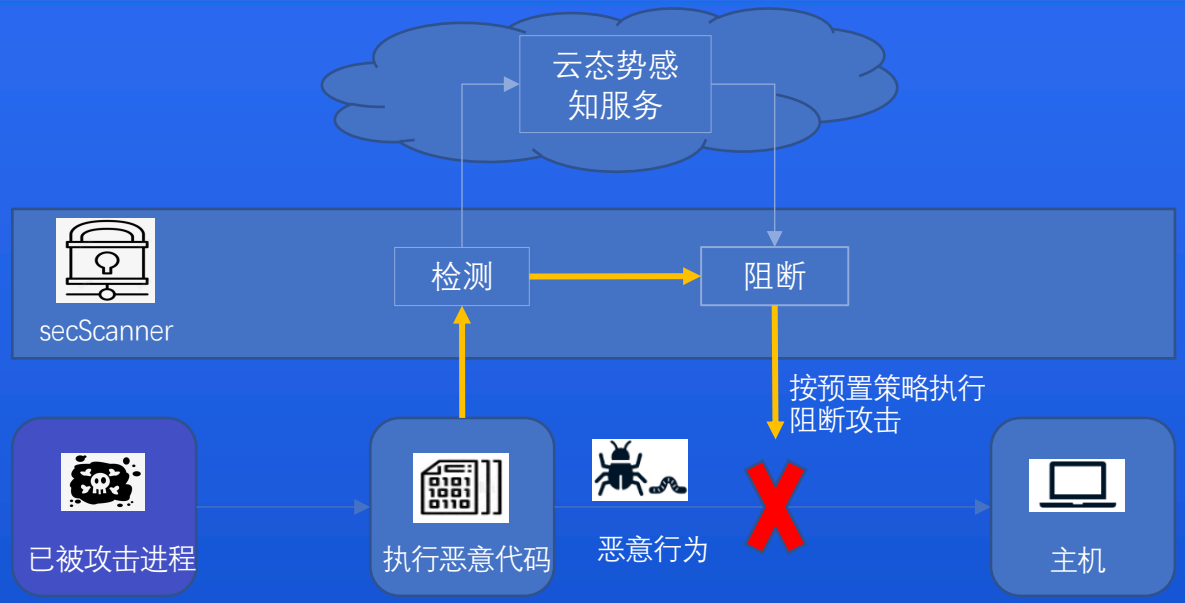
- ✓ **本地阻断**：基于secDetector可以暂停风险行为的动作，执行轻量化检测分析，使能内构阻断能力，通过预置策略无需外部人工干预
- ✓ **检测阻断联动**：检测特性可以调用阻断能力，及时阻断攻击、防范再次遭受攻击

Rootkit内核模块加载拒绝与清理

即时的阻断 之 恶意代码执行和内核rootkit模块加载

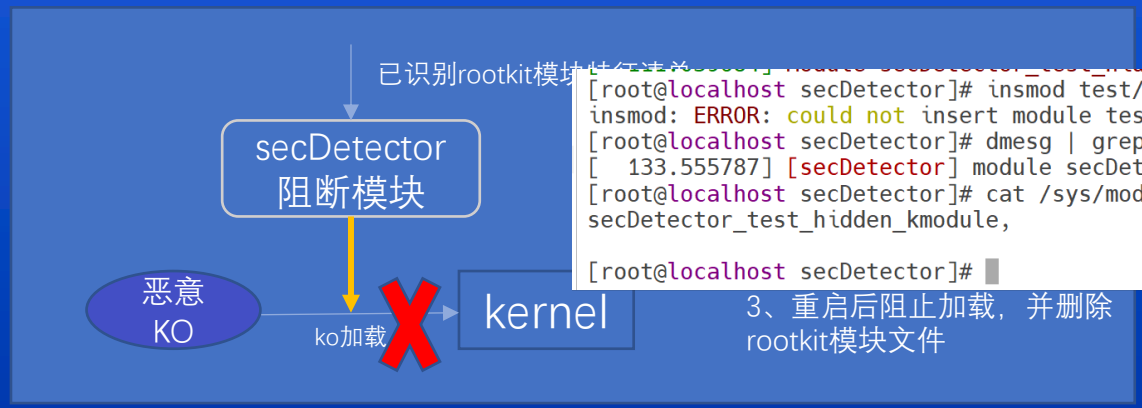
在主机本地实现攻击阻断能力，配合检测及时阻断攻击避免影响进一步扩大

恶意代码执行终止



- ✓ **本地阻断**：基于secDetector可以暂停风险行为的动作，执行轻量化检测分析，使能内构阻断能力，通过预置策略无需外部人工干预
- ✓ **检测阻断联动**：检测特性可以调用阻断能力，及时阻断攻击、防范再次遭受攻击

Rootkit内核模块加载拒绝与清理



再次插入 rootkit ko失败

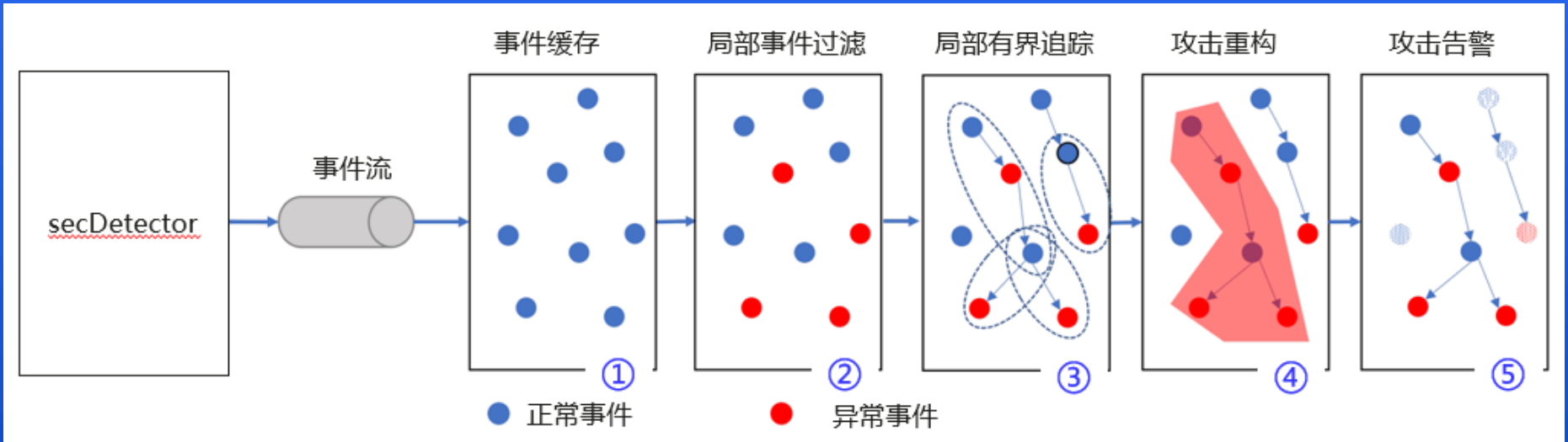
```
[root@localhost secDetector]# insmod test/test_hidden_kmodule/secDetector_test_hidden_kmodule.ko
insmod: ERROR: could not insert module test/test_hidden_kmodule/secDetector_test_hidden_kmodule.ko: Operation not permitted
[root@localhost secDetector]# dmesg | grep "\[secDetector"
[  133.555787] [secDetector] module secDetector_test_hidden_kmodule is rejected because of security policy
[root@localhost secDetector]# cat /sys/module/kernel/parameters/module_blocklist
secDetector_test_hidden_kmodule,

[root@localhost secDetector]#
```

日志显示插入失败是由于内构阻断成功

丰富的溯源 之 APT攻击检测增强

- APT高级持续性威胁攻击是一种针对性强、组织严密、手段高超、隐蔽性强且持续时间长的网络攻击
- 攻击行为往往经过多次进程创建深度分散隐藏，识别攻击行为需要对多进程的事件流进行溯源综合分析
- 攻击者在进程链上植入大量瞬态进程，完成下级进程创建后即自我关闭。事后溯源分析时已无从查找瞬态进程信息。



✓ **瞬态进程检测：** secDetector内核进程异常探针可以缓存实际父子进程链信息，增强针对瞬态进程的攻击溯源

✓ **效力提升：** 利用溯源图构建系统层业务行为基线，基于DARPA数据集的准确率达99%+，相比业界先进方案降低分析噪声2个量级（十万->千）

未来secScanner将向智能化主动防护方向持续演进

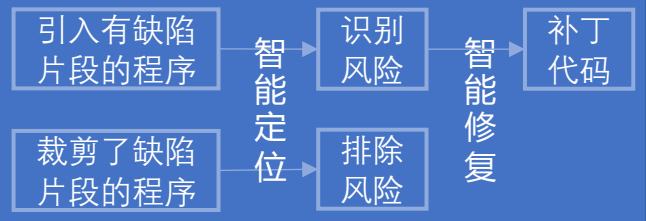
智能化是云主机安全的下半场，secScanner主动防护安全实践，将结合AI技术与3大核心能力打造原生安全可信的智能主动防护体系

安全主动管理 + 智能配置

- ✓ **智能推荐：** 根据用户原始需求与场景描述，智能化定制安全配置，无需专业人员设计
- ✓ **智能评估：** 智能化分析安全配置细节差异，评估安全影响，给出合理建议。

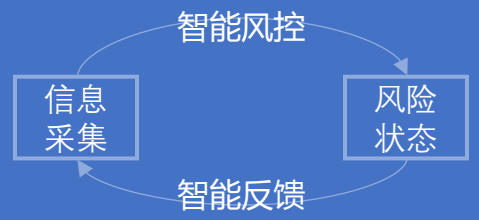
漏洞扫描 + 智能定位和修复

- ✓ **智能定位：** 指令集相似度分析，智能识别使用相同代码片段的潜在风险模块，和已裁剪缺陷代码的可排除风险模块
- ✓ **智能修复：** 智能化生成补丁，自动修复、屏蔽缺陷代码。



入侵检测 + 智能融合感知

- ✓ **智能风控：** 基于采集信息分析智能评估当前安全风险，识别潜在异常状态。
- ✓ **智能反馈：** 根据风险状态进一步调整信息采集与响应策略，追求性能与安全的极致平衡。



THANKS

openEuler 安全SIG组地址：

https://www.openeuler.org/zh/sig/sig-detail/?name=sig-security-facility

secScanner 项目地址：

https://gitee.com/openeuler/secscanner

secDetector 项目地址：

https://gitee.com/openeuler/secDetector

THANKS

openEuler 安全SIG组地址：

https://www.openeuler.org/zh/sig/sig-detail/?name=sig-security-facility

secScanner 项目地址：

https://gitee.com/openeuler/secscanner

secDetector 项目地址：

https://gitee.com/openeuler/secDetector

THANKS

openEuler 安全SIG组地址：

https://www.openeuler.org/zh/sig/sig-detail/?name=sig-security-facility

secScanner 项目地址：

https://gitee.com/openeuler/secscanner

secDetector 项目地址：

https://gitee.com/openeuler/secDetector