看雪

SDC · 2019

2019 安全开发者峰会

Security Development Conference

安全研究视角看macOS平台EDR安全能力建设

丰生强

非虫

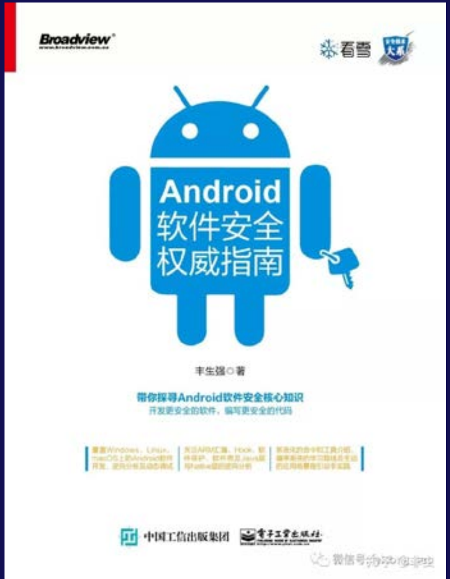
@fei_cong

概要

- 关于我
- EDR概述
- EDR系统架构
- macOS系统架构与安全机制
- macOS终端Agent技术实现方案
- 开发调试与注意事项

关于我

TURING 图灵原创
丰生强 著
Android 软件安全与逆向分析
国内第一本Android软件安全书
别让你的代码成为别人的炮灰！
eoe 全球最大中文Android开发者社区 (www.eoeandroid.com)
看雪论坛 (www.pediy.com)
安卓巴士 (www.apkbus.com)
联袂推荐
看雪版主非虫潜心力作
人民邮电出版社 POSTS & TELECOM PRESS
原创经典



_奇安信威胁情报中心

mail: ti_support@qianxin.com
twitter: @RedDrip7
site: ti.qianxin.com

EDR概述

- 安全产品何其多
- 安全能力象限
- EDR功能与定义
- EDR如何工作

安全产品何其多

- ATP(Advanced Threat Protection)
- CWPP(Cloud Workload Protection Platforms)
- DLP(Data Loss Prevention)
- ETDR(Endpoint Threat Detection and Response)
- EPP(Endpoint Protection Platform)
- EDR(Endpoint Detection and Response)
- HIDS(Host-based Intrusion Detection System)
- NIPS(Network-based Intrusion Prevention System)
- NIDS(Network Intrusion Detection System)
- NGAV(Next-Generation AntiVirus)
- NGAF(Next-Generation Application Firewall)
- NGFW(Next-Generation FireWall)
- NGSOC(Next-Generation Security Operation Center)
- WAF(Web Application Firewall)
- SSP(Safety Sensing Platform)
- SIEM(Security Information and Event Management)

安全能力象限-检测、防护、预测、响应

Detection **SSP DLP** **HIDS NIDS**	**Protection** **ATP HIPS NIPS WAF** **NGAV NGAF NGFW**

Prediction
SA(Situational Awareness)
TIP(Threat Intelligence Platform)
	Response
	SOC
	SIEM

EDR功能与定义

Gartner’s Anton Chuvakin first coined the term Endpoint Threat Detection and Response (ETDR) in July 2013 to define “the tools primarily focused on detecting and investigating suspicious activities (and traces of such) other problems on hosts/endpoints.” Commonly referred to as Endpoint Detection and Response (EDR), it is a relatively new category of solutions that is sometimes compared to Advanced Threat Protection (ATP) in terms of overall security capabilities.

Endpoint detection and response is an emerging technology that addresses the need for continuous monitoring and response to advanced threats. One could even make the argument that endpoint detection and response is a form of advanced threat protection.

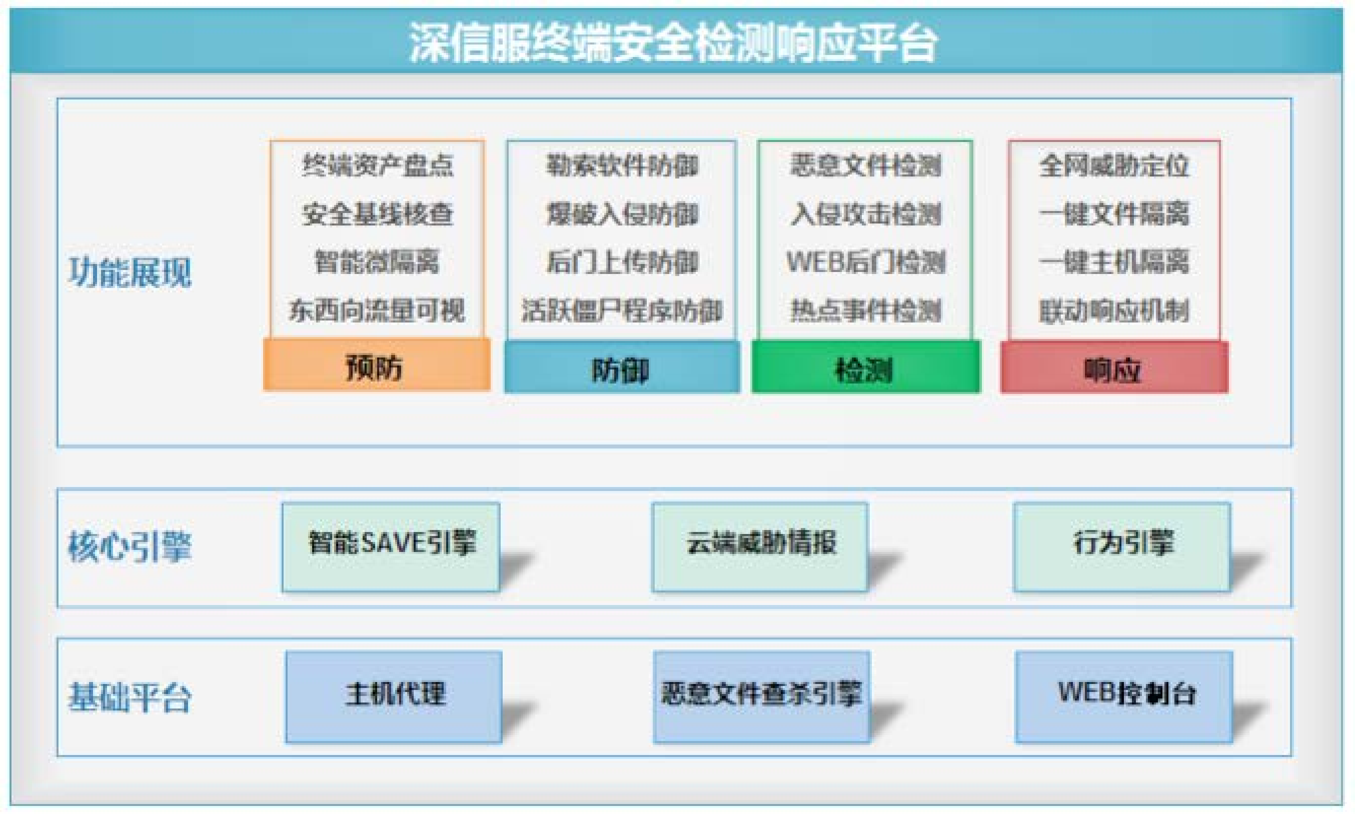
NOT JUST TOOLS, BUT CAPABILITIES

EDR如何工作

Endpoint detection and response tools work by monitoring endpoint and network events and recording the information in a central database where further analysis, detection, investigation, reporting, and alerting take place. A software agent installed on the host system provides the foundation for event monitoring and reporting.

Ongoing monitoring and detection are facilitated through the use of analytic tools. These tools identify tasks that can improve a company’s overall state of security by identifying, responding to, and deflecting internal threats and external attacks.

EDR系统架构



深信服终端安全检测响应平台

功能展现

预防
- 终端资产盘点
- 安全基线核查
- 智能微隔离
- 东西向流量可视

防御
- 勒索软件防御
- 爆破入侵防御
- 后门上传防御
- 活跃僵尸程序防御

检测
- 恶意文件检测
- 入侵攻击检测
- WEB后门检测
- 热点事件检测

响应
- 全网威胁定位
- 一键文件隔离
- 一键主机隔离
- 联动响应机制

核心引擎
- 智能SAVE引擎
- 云端威胁情报
- 行为引擎

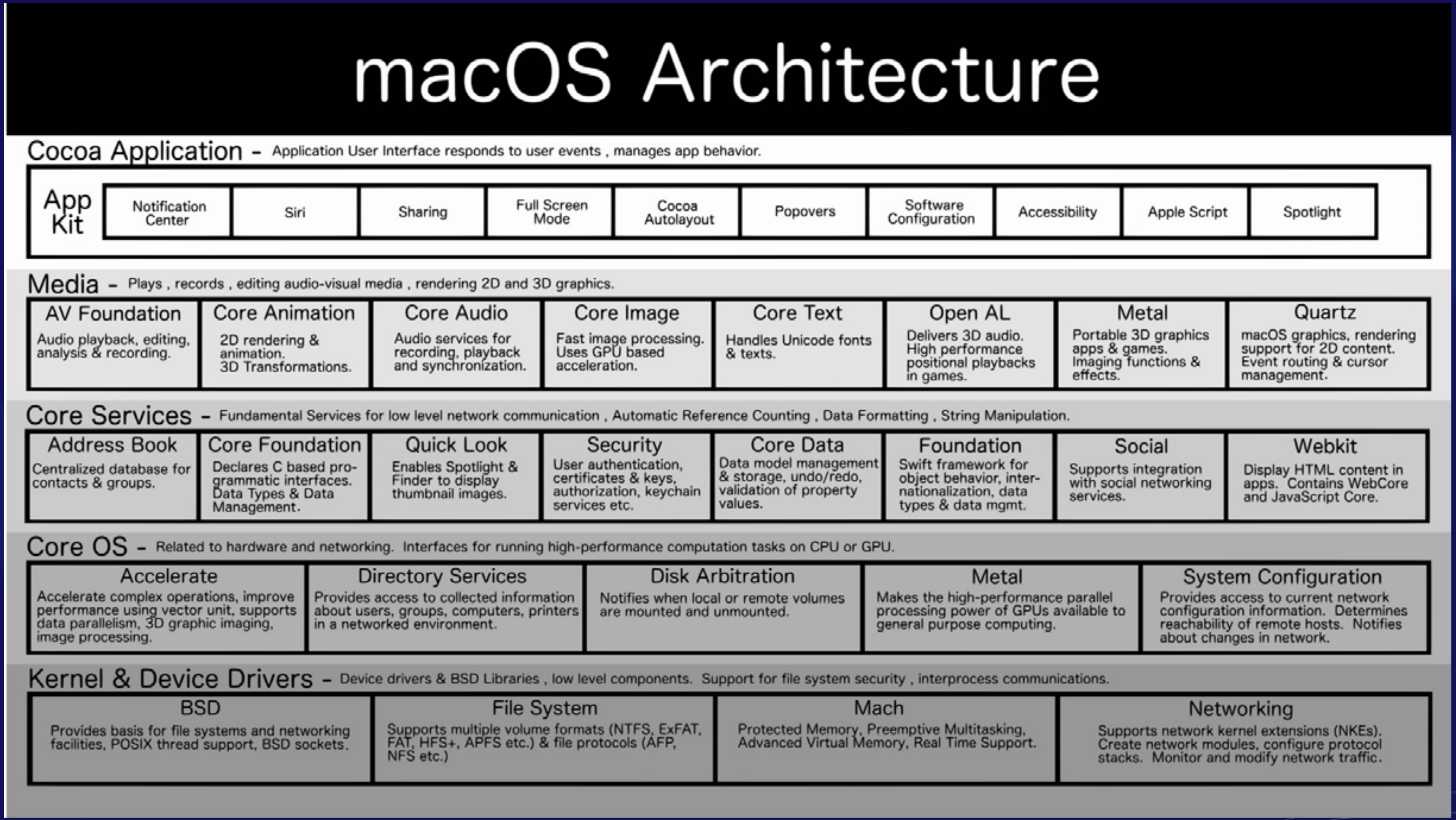
基础平台
- 主机代理
- 恶意文件查杀引擎
- WEB控制台

http://download.sangfor.com.cn/Uploads/File/edr/深信服_终端检测响应平台EDR_彩页.pdf

macOS系统架构与安全机制

- 系统架构
- 安全机制
- 安全限制

macOS系统架构



macOS Architecture

Cocoa Application – Application User Interface responds to user events , manages app behavior.

App Kit									
Notification Center	Siri	Sharing	Full Screen Mode	Cocoa Autolayout	Popovers	Software Configuration	Accessibility	Apple Script	Spotlight

Media – Plays , records , editing audio-visual media , rendering 2D and 3D graphics.

AV Foundation	Core Animation	Core Audio	Core Image	Core Text	Open AL	Metal	Quartz
Audio playback, editing, analysis & recording.	2D rendering & animation. 3D Transformations.	Audio services for recording, playback and synchronization.	Fast image processing. Uses GPU based acceleration.	Handles Unicode fonts & texts.	Delivers 3D audio. High performance positional playbacks in games.	Portable 3D graphics apps & games. Imaging functions & effects.	macOS graphics, rendering support for 2D content. Event routing & cursor management.

Core Services – Fundamental Services for low level network communication , Automatic Reference Counting , Data Formatting , String Manipulation.

Address Book	Core Foundation	Quick Look	Security	Core Data	Foundation	Social	Webkit
Centralized database for contacts & groups.	Declares C based programmatic interfaces. Data Types & Data Management.	Enables Spotlight & Finder to display thumbnail images.	User authentication, certificates & keys, authorization, keychain services etc.	Data model management & storage, undo/redo, validation of property values.	Swift framework for object behavior, internationalization, data types & data mgmt.	Supports integration with social networking services.	Display HTML content in apps. Contains WebCore and JavaScript Core.

Core OS – Related to hardware and networking. Interfaces for running high-performance computation tasks on CPU or GPU.

Accelerate	Directory Services	Disk Arbitration	Metal	System Configuration
Accelerate complex operations, improve performance using vector unit, supports data parallelism, 3D graphic imaging, image processing.	Provides access to collected information about users, groups, computers, printers in a networked environment.	Notifies when local or remote volumes are mounted and unmounted.	Makes the high-performance parallel processing power of GPUs available to general purpose computing.	Provides access to current network configuration information. Determines reachability of remote hosts. Notifies about changes in network.

Kernel & Device Drivers – Device drivers & BSD Libraries , low level components. Support for file system security , interprocess communications.

BSD	File System	Mach	Networking
Provides basis for file systems and networking facilities, POSIX thread support, BSD sockets.	Supports multiple volume formats (NTFS, ExFAT, FAT, HFS+, APFS etc.) & file protocols (AFP, NFS etc.)	Protected Memory, Preemptive Multitasking, Advanced Virtual Memory, Real Time Support.	Supports network kernel extensions (NKEs). Create network modules, configure protocol stacks. Monitor and modify network traffic.

https://en.wikipedia.org/wiki/File:MacOS_Architecture_v2.svg

macOS系统安全机制

- Core Services -> Security
  - Authentication <Security/Authorization.h>
  - Code Signing <Security/CodeSigning.h>
- Kernel -> BSD
  - Aduit <bsm/audit.h>
  - KAuth <bsd/sys/kauth.h>
- Kernel -> Mach
  - MACF <security/mac_policy.h>
- Kernel -> Networking
  - NKE <sys/kpi_socketfilter.h>

macOS系统安全限制

- Authd
- syspolicyd
- Gatekeeper
- App Translocation
- User-Approved kext
- App Notarization
- Rootless（SIP）
- Sandbox
- XProtect
- MRT(Malware Removal Tool)
- EndpointSecurity

macOS终端Agent技术实现方案

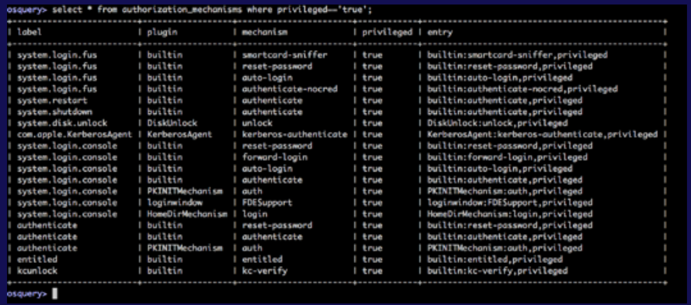
- Event & incident
- 安全加固 / 预防
- 攻击检测
- 安全防护

Event & incident

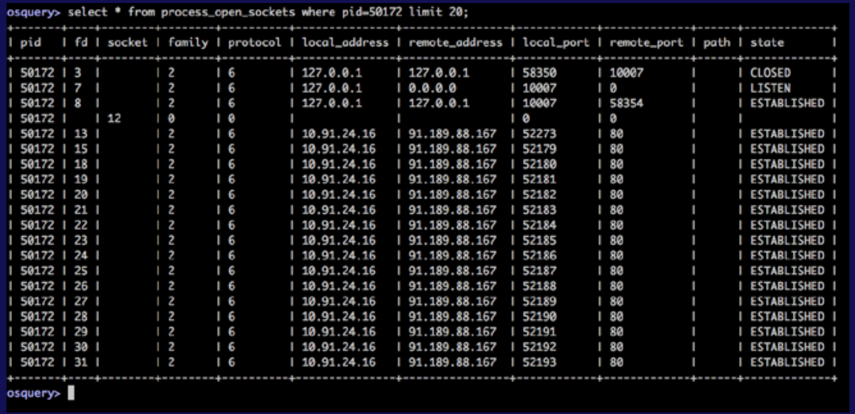
- 事件与事件响应
- 数据源
- 数据采集
- 威胁模型
- 复杂事件处理

Event & incident

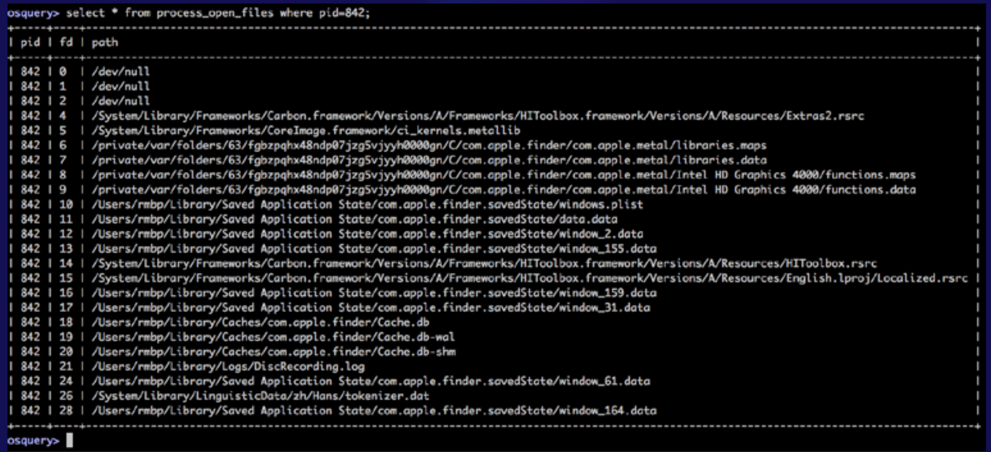
- ➢ 事件与事件响应
- ➢ 数据源
- ➢ 数据采集
- ➢ 威胁模型
- ➢ 复杂事件处理



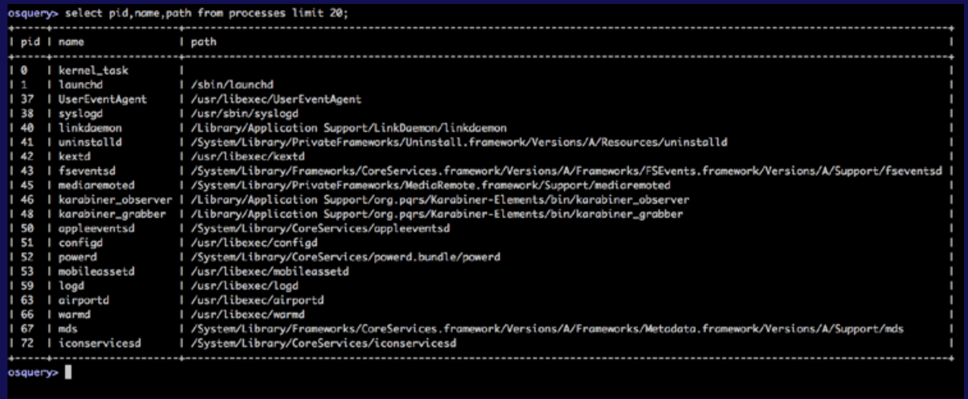
```
osquery> select * from authorization_mechanisms where privileged='true';
+-------------------------+------------------+-------------------------+------------+---------------------------------------------------+
| label                   | plugin           | mechanism               | privileged | entry                                             |
+-------------------------+------------------+-------------------------+------------+---------------------------------------------------+
| system.login.fus        | builtin          | smartcard-sniffer       | true       | builtin:smartcard-sniffer,privileged              |
| system.login.fus        | builtin          | reset-password          | true       | builtin:reset-password,privileged                 |
| system.login.fus        | builtin          | auto-login              | true       | builtin:auto-login,privileged                     |
| system.login.fus        | builtin          | authenticate-nocred     | true       | builtin:authenticate-nocred,privileged            |
| system.restart          | builtin          | authenticate            | true       | builtin:authenticate,privileged                   |
| system.shutdown         | builtin          | authenticate            | true       | builtin:authenticate,privileged                   |
| system.disk.unlock      | DiskUnlock       | unlock                  | true       | DiskUnlock:unlock,privileged                      |
| com.apple.KerberosAgent | KerberosAgent    | kerberos-authenticate   | true       | KerberosAgent:kerberos-authenticate,privileged    |
| system.login.console    | builtin          | reset-password          | true       | builtin:reset-password,privileged                 |
| system.login.console    | builtin          | forward-login           | true       | builtin:forward-login,privileged                  |
| system.login.console    | builtin          | auto-login              | true       | builtin:auto-login,privileged                     |
| system.login.console    | builtin          | authenticate            | true       | builtin:authenticate,privileged                   |
| system.login.console    | PKINITMechanism  | auth                    | true       | PKINITMechanism:auth,privileged                   |
| system.login.console    | loginwindow      | FDESupport              | true       | loginwindow:FDESupport,privileged                 |
| system.login.console    | HomeDirMechanism | login                   | true       | HomeDirMechanism:login,privileged                 |
| authenticate            | builtin          | reset-password          | true       | builtin:reset-password,privileged                 |
| authenticate            | builtin          | authenticate            | true       | builtin:authenticate,privileged                   |
| authenticate            | PKINITMechanism  | auth                    | true       | PKINITMechanism:auth,privileged                   |
| entitled                | builtin          | entitled                | true       | builtin:entitled,privileged                       |
| kcunlock                | builtin          | kc-verify               | true       | builtin:kc-verify,privileged                      |
+-------------------------+------------------+-------------------------+------------+---------------------------------------------------+
osquery> 
```



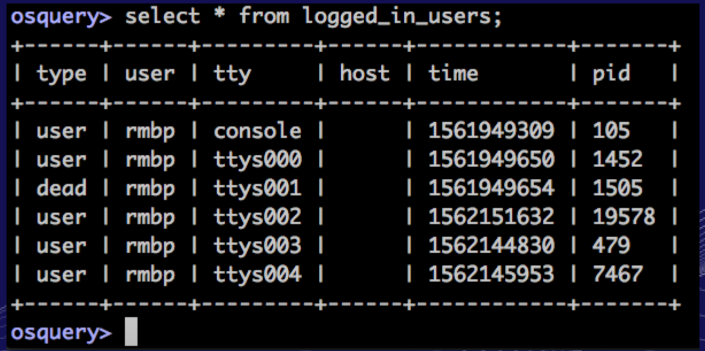
```
osquery> select * from process_open_sockets where pid=50172 limit 20;
+-------+----+--------+--------+----------+---------------+----------------+------------+-------------+------+-------------+
| pid   | fd | socket | family | protocol | local_address | remote_address | local_port | remote_port | path | state       |
+-------+----+--------+--------+----------+---------------+----------------+------------+-------------+------+-------------+
| 50172 | 3  |        | 2      | 6        | 127.0.0.1     | 127.0.0.1      | 58350      | 10007       |      | CLOSED      |
| 50172 | 7  |        | 2      | 6        | 127.0.0.1     | 0.0.0.0        | 10007      | 0           |      | LISTEN      |
| 50172 | 8  |        | 2      | 6        | 127.0.0.1     | 127.0.0.1      | 10007      | 58354       |      | ESTABLISHED |
| 50172 |    | 12     | 0      | 0        |               |                | 0          | 0           |      |             |
| 50172 | 13 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52273      | 80          |      | ESTABLISHED |
| 50172 | 15 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52179      | 80          |      | ESTABLISHED |
| 50172 | 18 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52180      | 80          |      | ESTABLISHED |
| 50172 | 19 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52181      | 80          |      | ESTABLISHED |
| 50172 | 20 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52182      | 80          |      | ESTABLISHED |
| 50172 | 21 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52183      | 80          |      | ESTABLISHED |
| 50172 | 22 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52184      | 80          |      | ESTABLISHED |
| 50172 | 23 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52185      | 80          |      | ESTABLISHED |
| 50172 | 24 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52186      | 80          |      | ESTABLISHED |
| 50172 | 25 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52187      | 80          |      | ESTABLISHED |
| 50172 | 26 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52188      | 80          |      | ESTABLISHED |
| 50172 | 27 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52189      | 80          |      | ESTABLISHED |
| 50172 | 28 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52190      | 80          |      | ESTABLISHED |
| 50172 | 29 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52191      | 80          |      | ESTABLISHED |
| 50172 | 30 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52192      | 80          |      | ESTABLISHED |
| 50172 | 31 |        | 2      | 6        | 10.91.24.16   | 91.189.88.167  | 52193      | 80          |      | ESTABLISHED |
+-------+----+--------+--------+----------+---------------+----------------+------------+-------------+------+-------------+
osquery> 
```



```
osquery> select * from process_open_files where pid=842;
+-----+----+----------------------------------------------------------------------------------------------------------------------------------------+
| pid | fd | path                                                                                                                                   |
+-----+----+----------------------------------------------------------------------------------------------------------------------------------------+
| 842 | 0  | /dev/null                                                                                                                              |
| 842 | 1  | /dev/null                                                                                                                              |
| 842 | 2  | /dev/null                                                                                                                              |
| 842 | 4  | /System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/Resources/Extras2.rsrc                 |
| 842 | 5  | /System/Library/Frameworks/CoreImage.framework/ci_kernels.metallib                                                                     |
| 842 | 6  | /private/var/folders/63/fgbzpqhx48ndp07jzg5vjyyh0000gn/C/com.apple.finder/com.apple.metal/libraries.maps                               |
| 842 | 7  | /private/var/folders/63/fgbzpqhx48ndp07jzg5vjyyh0000gn/C/com.apple.finder/com.apple.metal/libraries.data                               |
| 842 | 8  | /private/var/folders/63/fgbzpqhx48ndp07jzg5vjyyh0000gn/C/com.apple.finder/com.apple.metal/Intel HD Graphics 4000/functions.maps        |
| 842 | 9  | /private/var/folders/63/fgbzpqhx48ndp07jzg5vjyyh0000gn/C/com.apple.finder/com.apple.metal/Intel HD Graphics 4000/functions.data        |
| 842 | 10 | /Users/rmbp/Library/Saved Application State/com.apple.finder.savedState/windows.plist                                                  |
| 842 | 11 | /Users/rmbp/Library/Saved Application State/com.apple.finder.savedState/data.data                                                      |
| 842 | 12 | /Users/rmbp/Library/Saved Application State/com.apple.finder.savedState/window_2.data                                                  |
| 842 | 13 | /Users/rmbp/Library/Saved Application State/com.apple.finder.savedState/window_155.data                                                |
| 842 | 14 | /System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/Resources/HIToolbox.rsrc              |
| 842 | 15 | /System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/Resources/English.lproj/Localized.rsrc |
| 842 | 16 | /Users/rmbp/Library/Saved Application State/com.apple.finder.savedState/window_159.data                                                |
| 842 | 17 | /Users/rmbp/Library/Saved Application State/com.apple.finder.savedState/window_31.data                                                 |
| 842 | 18 | /Users/rmbp/Library/Caches/com.apple.finder/Cache.db                                                                                   |
| 842 | 19 | /Users/rmbp/Library/Caches/com.apple.finder/Cache.db-wal                                                                               |
| 842 | 20 | /Users/rmbp/Library/Caches/com.apple.finder/Cache.db-shm                                                                               |
| 842 | 21 | /Users/rmbp/Library/Logs/DiscRecording.log                                                                                             |
| 842 | 24 | /Users/rmbp/Library/Saved Application State/com.apple.finder.savedState/window_61.data                                                 |
| 842 | 26 | /System/Library/LinguisticData/zh/Hans/tokenizer.dat                                                                                   |
| 842 | 28 | /Users/rmbp/Library/Saved Application State/com.apple.finder.savedState/window_164.data                                                |
+-----+----+----------------------------------------------------------------------------------------------------------------------------------------+
osquery> 
```



```
osquery> select pid,name,path from processes limit 20;
+-----+-------------------+------------------------------------------------------------------------------------------------------------------+
| pid | name              | path                                                                                                             |
+-----+-------------------+------------------------------------------------------------------------------------------------------------------+
| 0   | kernel_task       |                                                                                                                  |
| 1   | launchd           | /sbin/launchd                                                                                                    |
| 37  | UserEventAgent    | /usr/libexec/UserEventAgent                                                                                      |
| 38  | syslogd           | /usr/sbin/syslogd                                                                                                |
| 40  | linkdaemon        | /Library/Application Support/LinkDaemon/linkdaemon                                                               |
| 41  | uninstalld        | /System/Library/PrivateFrameworks/Uninstall.framework/Versions/A/Resources/uninstalld                            |
| 42  | kextd             | /usr/libexec/kextd                                                                                               |
| 43  | fseventsd         | /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/FSEvents.framework/Versions/A/Support/fseventsd |
| 45  | mediaremoted      | /System/Library/PrivateFrameworks/MediaRemote.framework/Support/mediaremoted                                     |
| 46  | karabiner_observer | /Library/Application Support/org.pqrs/Karabiner-Elements/bin/karabiner_observer                                |
| 48  | karabiner_grabber | /Library/Application Support/org.pqrs/Karabiner-Elements/bin/karabiner_grabber                                   |
| 50  | appleeventsd      | /System/Library/CoreServices/appleeventsd                                                                        |
| 51  | configd           | /usr/libexec/configd                                                                                             |
| 52  | powerd            | /System/Library/CoreServices/powerd.bundle/powerd                                                                |
| 53  | mobileassetd      | /usr/libexec/mobileassetd                                                                                        |
| 59  | logd              | /usr/libexec/logd                                                                                                |
| 63  | airportd          | /usr/libexec/airportd                                                                                            |
| 66  | warmd             | /usr/libexec/warmd                                                                                               |
| 67  | mds               | /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mds |
| 72  | iconservicesd     | /System/Library/CoreServices/iconservicesd                                                                       |
+-----+-------------------+------------------------------------------------------------------------------------------------------------------+
osquery> 
```

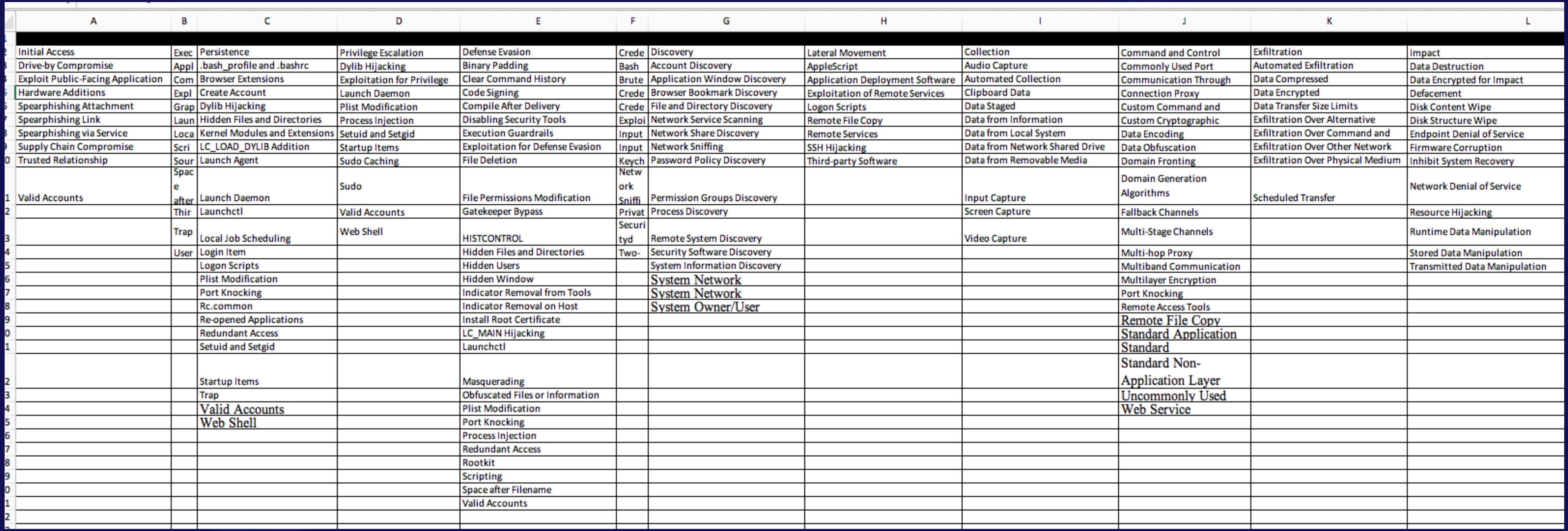


```
osquery> select * from logged_in_users;
+------+------+---------+------+------------+-------+
| type | user | tty     | host | time       | pid   |
+------+------+---------+------+------------+-------+
| user | rmbp | console |      | 1561949309 | 105   |
| user | rmbp | ttys000 |      | 1561949650 | 1452  |
| dead | rmbp | ttys001 |      | 1561949654 | 1505  |
| user | rmbp | ttys002 |      | 1562151632 | 19578 |
| user | rmbp | ttys003 |      | 1562144830 | 479   |
| user | rmbp | ttys004 |      | 1562145953 | 7467  |
+------+------+---------+------+------------+-------+
osquery> 
```

Event & incident

- ➢ 事件与事件响应
- ➢ 数据源
- ➢ 数据采集
- ➢ 威胁模型
- ➢ 复杂事件处理

Enterprise Matrix - macOS



A	B	C	D	E	F	G	H	I	J	K	L
Initial Access	Exec	Persistence	Privilege Escalation	Defense Evasion	Crede	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Appl	.bash_profile and .bashrc	Dylib Hijacking	Binary Padding	Bash	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Com	Browser Extensions	Exploitation for Privilege	Clear Command History	Brute	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through	Data Compressed	Data Encrypted for Impact
Hardware Additions	Expl	Create Account	Launch Daemon	Code Signing	Crede	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Spearphishing Attachment	Grap	Dylib Hijacking	Plist Modification	Compile After Delivery	Crede	File and Directory Discovery	Logon Scripts	Data Staged	Custom Command and	Data Transfer Size Limits	Disk Content Wipe
Spearphishing Link	Laun	Hidden Files and Directories	Process Injection	Disabling Security Tools	Exploi	Network Service Scanning	Remote File Copy	Data from Information	Custom Cryptographic	Exfiltration Over Alternative	Disk Structure Wipe
Spearphishing via Service	Loca	Kernel Modules and Extensions	Setuid and Setgid	Execution Guardrails	Input	Network Share Discovery	Remote Services	Data from Local System	Data Encoding	Exfiltration Over Command and	Endpoint Denial of Service
Supply Chain Compromise	Scri	LC_LOAD_DYLIB Addition	Startup Items	Exploitation for Defense Evasion	Input	Network Sniffing	SSH Hijacking	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network	Firmware Corruption
Trusted Relationship	Sour	Launch Agent	Sudo Caching	File Deletion	Keych	Password Policy Discovery	Third-party Software	Data from Removable Media	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Valid Accounts	Space after	Launch Daemon	Sudo	File Permissions Modification	Network Sniffi	Permission Groups Discovery		Input Capture	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
	Thir	Launchctl	Valid Accounts	Gatekeeper Bypass	Privat	Process Discovery		Screen Capture	Fallback Channels		Resource Hijacking
	Trap	Local Job Scheduling	Web Shell	HISTCONTROL	Securityd	Remote System Discovery		Video Capture	Multi-Stage Channels		Runtime Data Manipulation
	User	Login Item		Hidden Files and Directories	Two-	Security Software Discovery			Multi-hop Proxy		Stored Data Manipulation
		Logon Scripts		Hidden Users		System Information Discovery			Multiband Communication		Transmitted Data Manipulation
		Plist Modification		Hidden Window		System Network			Multilayer Encryption		
		Port Knocking		Indicator Removal from Tools		System Network			Port Knocking		
		Rc.common		Indicator Removal on Host		System Owner/User			Remote Access Tools		
		Re-opened Applications		Install Root Certificate					Remote File Copy		
		Redundant Access		LC_MAIN Hijacking					Standard Application		
		Setuid and Setgid		Launchctl					Standard		
		Startup Items		Masquerading					Standard Non-Application Layer		
		Trap		Obfuscated Files or Information					Uncommonly Used		
		Valid Accounts		Plist Modification					Web Service		
		Web Shell		Port Knocking							
				Process Injection							
				Redundant Access							
				Rootkit							
				Scripting							
				Space after Filename							
				Valid Accounts							

https://attack.mitre.org/matrices/enterprise/macos/

Event & incident

- 事件与事件响应
- 数据源
- 数据采集
  - syscall hook
  - Audit
  - Kauth
  - MACF hook
- 威胁模型
- 复杂事件处理

安全加固 / 预防

- 系统安全补丁
- 软件补丁
- 内核加固
- 自我防护
- 风险配置扫描

攻击检测

- 勒索攻击
- 挖矿攻击
- 鱼叉攻击
- 信息窃取
- DDOS攻击
- 权限提升
- 端口扫描
- 无文件攻击
- Rootkit攻击

攻击检测

- 勒索攻击
- 挖矿攻击
- 鱼叉攻击
- 信息窃取
- DDOS攻击
- 权限提升
- 端口扫描
- 无文件攻击
- Rootkit攻击

文件读写事件 + 进程执行事件

攻击检测

- 勒索攻击
- 挖矿攻击
- 鱼叉攻击
- 信息窃取
- DDOS攻击
- 权限提升
- 端口扫描
- 无文件攻击
- Rootkit攻击

网络读写事件 ＋ 进程执行事件

攻击检测

- 勒索攻击
- 挖矿攻击
- 鱼叉攻击
- 信息窃取
- DDOS攻击
- 权限提升
- 端口扫描
- 无文件攻击
- Rootkit攻击

敏感资源访问 ＋ 网络提交数据

攻击检测

- 勒索攻击
- 挖矿攻击
- 鱼叉攻击
- 信息窃取
- DDOS攻击
- 权限提升
- 端口扫描
- 无文件攻击
- Rootkit攻击

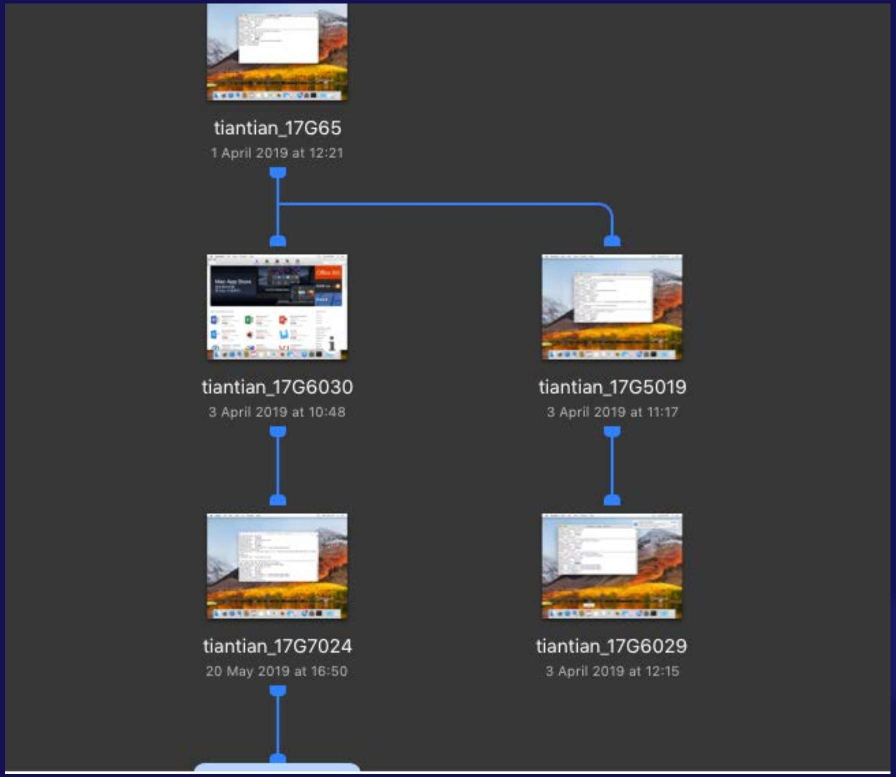
进程执行事件 ＋ 进程权限检查

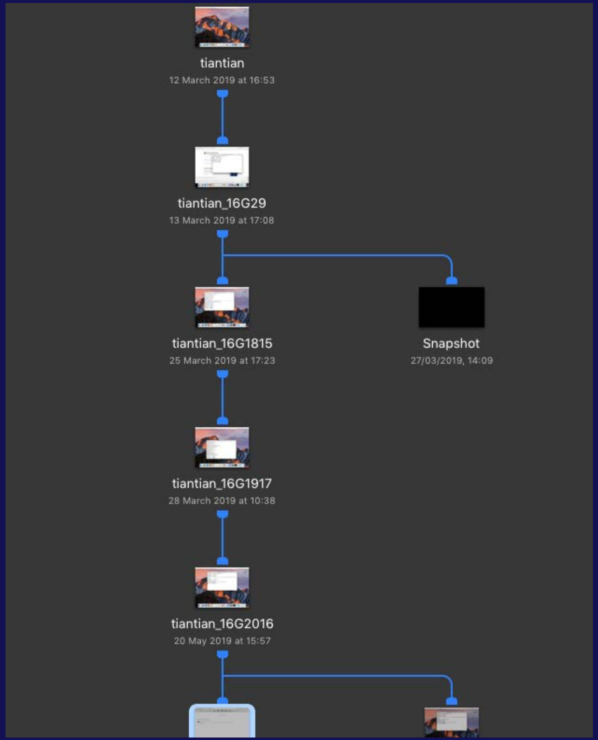
安全防护

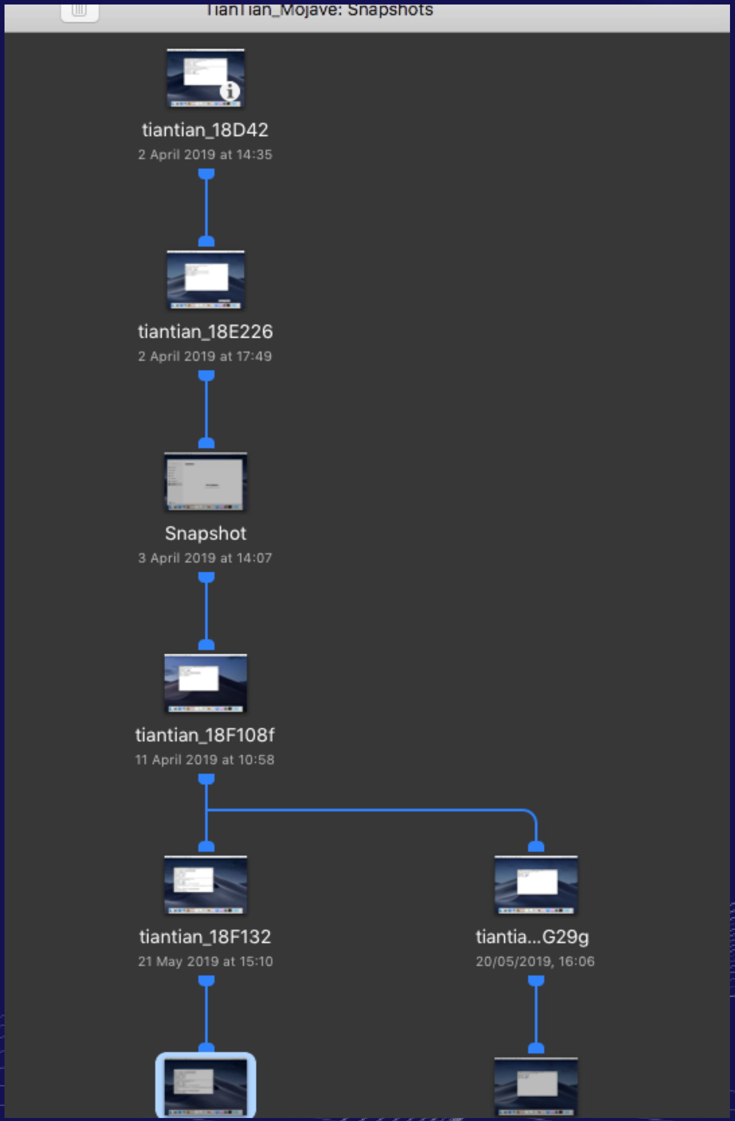
- 文件读写管理
- 文件执行管理
- 网络访问管理
- 进程管理
- 系统调用审计
- 终端隔离
- 资产报备

MACF

开发调试与注意事项


tiantian_17G65
1 April 2019 at 12:21
tiantian_17G6030
3 April 2019 at 10:48
tiantian_17G5019
3 April 2019 at 11:17
tiantian_17G7024
20 May 2019 at 16:50
tiantian_17G6029
3 April 2019 at 12:15


tiantian
12 March 2019 at 16:53
tiantian_16G29
13 March 2019 at 17:08
tiantian_16G1815
25 March 2019 at 17:23
Snapshot
27/03/2019, 14:09
tiantian_16G1917
28 March 2019 at 10:38
tiantian_16G2016
20 May 2019 at 15:57


TianTian_Mojave: Snapshots
tiantian_18D42
2 April 2019 at 14:35
tiantian_18E226
2 April 2019 at 17:49
Snapshot
3 April 2019 at 14:07
tiantian_18F108f
11 April 2019 at 10:58
tiantian_18F132
21 May 2019 at 15:10
tiantia...G29g
20/05/2019, 16:06

谢 谢