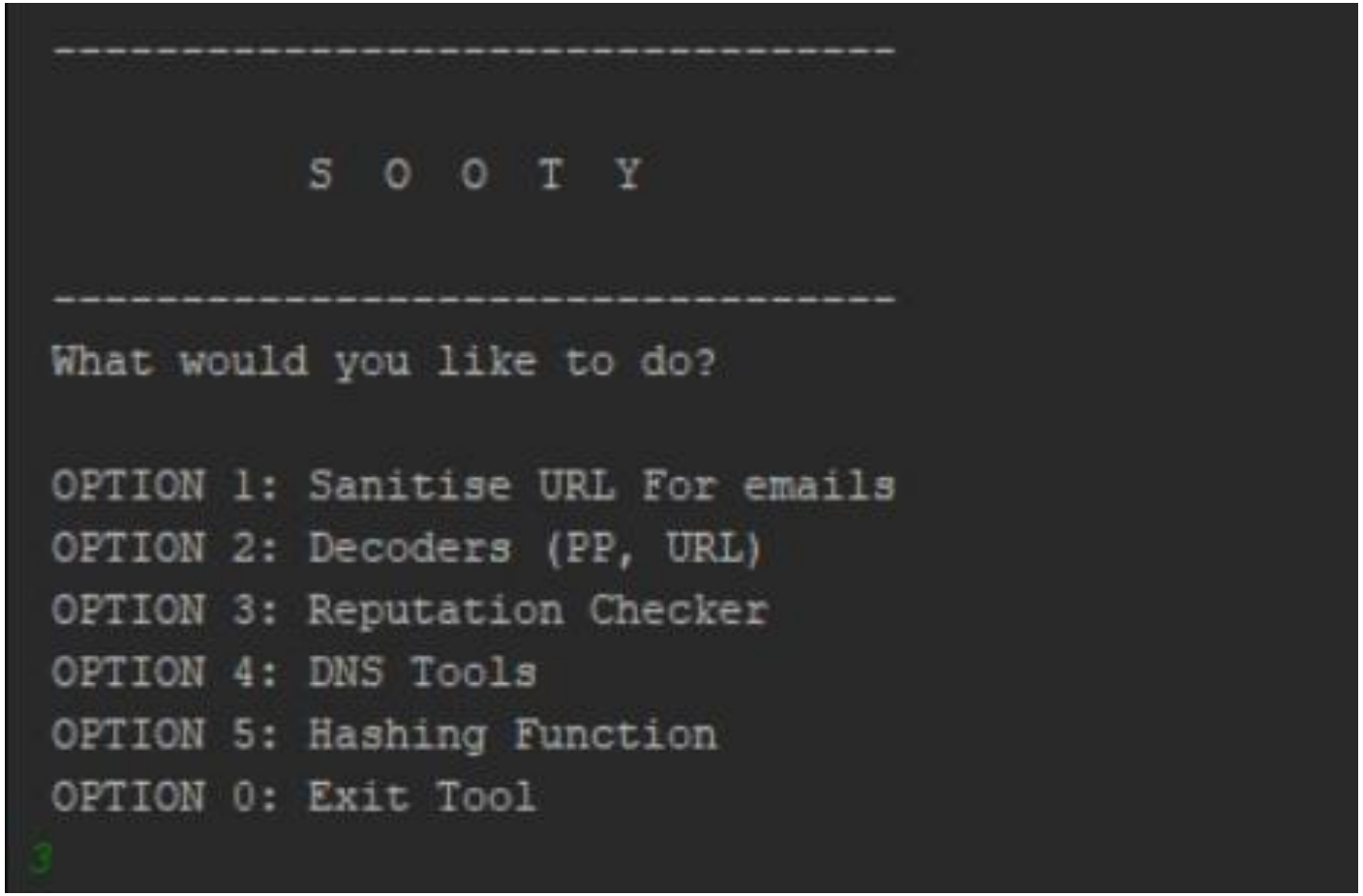
100 инструментов для SOC-аналитиков

Joas Antonio

Sooty

- Sooty - это инструмент, разработанный с целью помочь SOC-аналитикам автоматизировать часть их рабочего процесса. Одной из целей Sooty является выполнение как можно большего количества рутинных проверок, позволяя аналитику уделять больше времени более глубокому анализу. Подробную информацию о многих функциях Sooty можно найти по ссылке ниже.
- https://github.com/TheresAFewConors/Sooty



Peepdf

- peepdf - это Python-инструмент для исследования PDF-файлов с целью выяснить, может ли файл быть опасным или нет. Цель этого инструмента - предоставить все необходимые детали, которые могут понадобиться исследователю безопасности при анализе PDF-файлов. С помощью peepdf можно увидеть все объекты в документе, показывающие подозрительные элементы, он поддерживает наиболее используемые фильтры и кодировки, может анализировать различные версии файла, потоки объектов и зашифрованные файлы. При установке **PyV8** и **Pylibemu** он также предоставляет обертки для анализа Javascript и шеллкода. Кроме того, он способен создавать новые PDF-файлы, изменять существующие и обфусцировать их.
- https://eternal-todo.com/tools/peepdf-pdf-analysis-tool

```
Usage: ./peepdf.py [options] PDF_file

Options:
  -h, --help            show this help message and exit
  -i, --interactive     Sets console mode.
  -s SCRIPTFILE, --load-script=SCRIPTFILE
                        Loads the commands stored in the specified file and
                        execute them.
  -c, --check-vt        Checks the hash of the PDF file on VirusTotal.
  -f, --force-mode      Sets force parsing mode to ignore errors.
  -l, --loose-mode      Sets loose parsing mode to catch malformed objects.
  -m, --manual-analysis
                        Avoids automatic Javascript analysis. Useful with
                        eternal loops like heap spraying.
  -u, --update          Updates peepdf with the latest files from the
                        repository.
  -g, --grinch-mode     Avoids colorized output in the interactive console.
  -v, --version         Shows program's version number.
  -x, --xml             Shows the document information in XML format.
```

PyREBox

- PyREBox - это песочница для реверс инжиниринга с поддержкой сценариев на языке Python. Она основана на QEMU и призвана помочь исследователям, предоставляя возможности динамического анализа и отладки с иной точки зрения. PyREBox позволяет исследовать запущенную VM QEMU, модифицировать ее память или регистры, а также инструментировать ее выполнение, создавая простые скрипты на языке Python для автоматизации любого вида анализа. Кроме того, в состав PyREBox входит оболочка на базе IPython, предоставляющая богатый набор команд, а также Python API.
- https://talosintelligence.com/pyrebox

Fail2Ban

- Fail2ban сканирует лог-файлы (например, /var/log/apache/error_log) и блокирует IP-адреса, которые демонстрируют признаки вредоносности - слишком частое неправильное введение пароля, попытки эксплуатации и т.д. Обычно Fail2Ban используется для обновления правил брандмауэра, чтобы заблокировать IP-адреса на определенное время, хотя можно настроить и любое другое произвольное действие (например, отправку электронного письма). Из коробки Fail2Ban поставляется с фильтрами для различных сервисов (apache, courier, ssh и т.д.).

- Fail2Ban способен снизить количество неверных попыток аутентификации, однако он не может устранить риск, который представляет собой слабая аутентификация. Если вы действительно хотите защитить сервисы, настройте их на использование только двухфакторных или публичных/приватных механизмов аутентификации.
- https://www.fail2ban.org/wiki/index.php/Main_Page

OSSEC

- OSSEC - это полноценная платформа для мониторинга и контроля ваших систем. Она объединяет все аспекты HIDS (обнаружение вторжений на хосте), мониторинга журналов и SIM/SIEM в простом, мощном решении с открытым исходным кодом.

- https://github.com/ossec/ossec-hids
- https://www.ossec.net/

RKHunter и CHRookit

- http://rkhunter.sourceforge.net/
- http://chkrootkit.org/

Process Hacker

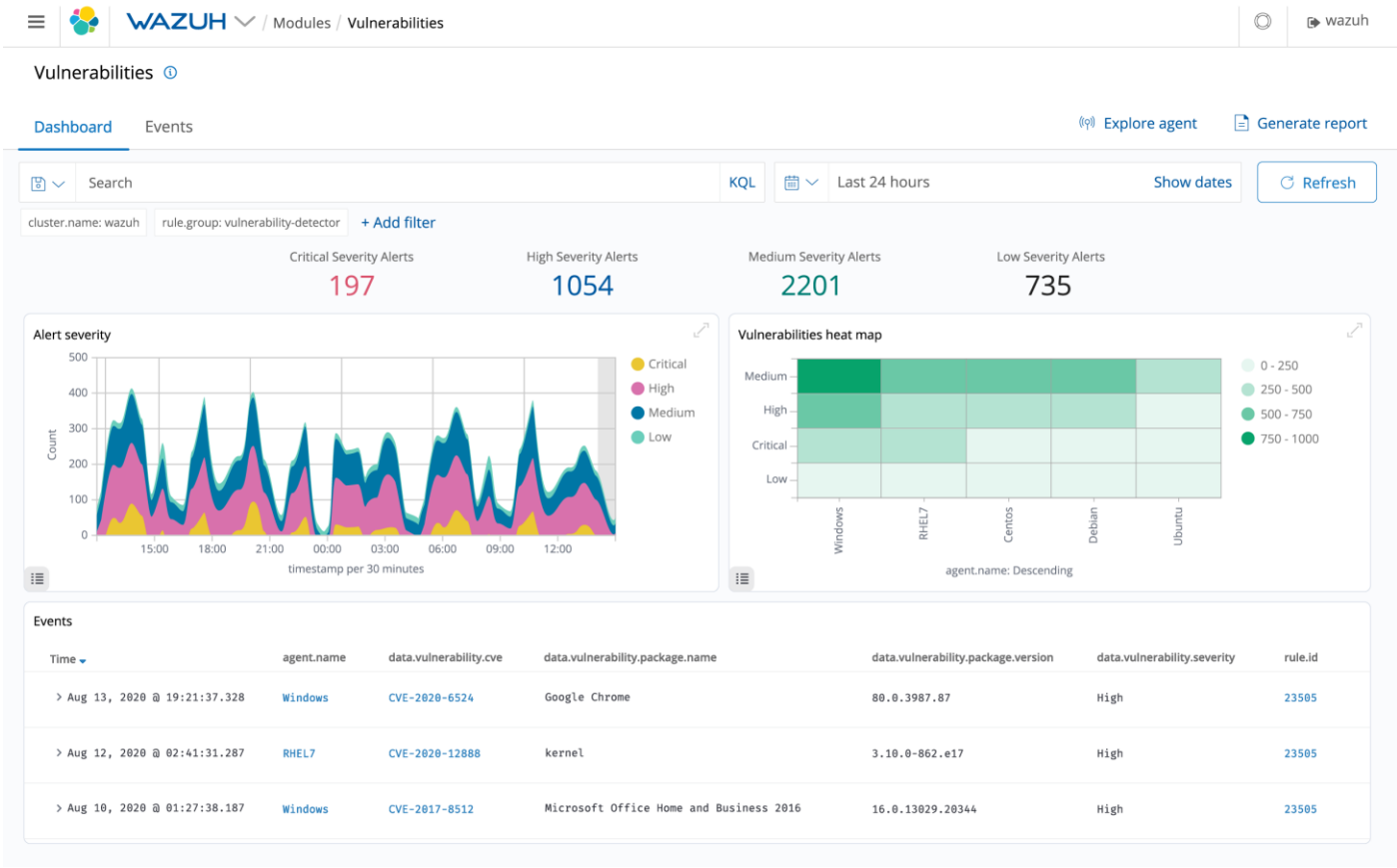
- Process Hacker, бесплатный, мощный, многоцелевой инструмент, позволяющий контролировать системные ресурсы, отлаживать программное обеспечение и обнаруживать вредоносные программы.
- https://processhacker.sourceforge.io/downloads.php

Splunk

- Ее программное обеспечение позволяет собирать, индексировать и коррелировать данные в режиме реального времени в хранилище с возможностью поиска на основе которого можно создавать графики, отчеты, алерты, информационные панели и визуализации. Splunk использует машинные данные для выявления закономерностей в данных, получения метрик, диагностики проблем и предоставления аналитических данных для бизнес-операций. Splunk - это горизонтальная технология, используемая для управления приложениями, обеспечения безопасности и соответствия нормативным требованиям, а также для бизнеса и веб-аналитики.
- https://www.splunk.com/

Wazuh

- Wazuh - это бесплатное решение для мониторинга безопасности с открытым исходным кодом, предназначенное для обнаружения угроз, контроля целостности, реагирования на инциденты и обеспечения соответствия нормативным требованиям.
- https://wazuh.com/



TheHive

- Масштабируемая бесплатная платформа реагирования на инциденты информационной безопасности с открытым исходным кодом, тесно интегрированная с MISP (Malware Information Sharing Platform), призванная облегчить жизнь SOC, CSIRT, CERT и любых специалистов по информационной безопасности, имеющих дело с инцидентами безопасности, требующими оперативного расследования и принятия необходимых мер.
- https://thehive-project.org/

Security Onion

- Их продукты включают в себя как программное обеспечение Security Onion, так и специализированные аппаратные устройства, созданные и протестированные для работы Security Onion. Их устройства позволят вам и вашим сотрудникам сэкономить время, ресурсы и сосредоточиться на обеспечении безопасности вашей организации.
- https://securityonionsolutions.com/

Caine

- CAINE (Computer Aided INvestigative Environment) - итальянский live-дистрибутив GNU/Linux, созданный как проект в области цифровой криминалистики.
- https://www.caine-live.net/

CALDERA

Что делает CALDERA?

- CALDERA помогает специалистам по кибербезопасности сократить количество времени и ресурсов, необходимых для рутинного тестирования кибербезопасности.
- CALDERA расширяет возможности киберкоманд по трем основным направлениям:

Эмуляция автономных противников

- С помощью CALDERA ваша киберкоманда может создать профиль конкретной угрозы (противника) и запустить его в сеть, чтобы увидеть, где вы можете быть уязвимы. Это помогает при тестировании средств защиты и обучении синих команд способам обнаружения конкретных угроз.

Автономное реагирование на инциденты

- Позволяет вашей команде выполнять автоматическое реагирование на инциденты на конкретном узле, что позволяет находить новые способы выявления и реагирования на угрозы.

Ручная работа с красной командой

- Помогает красной команде выполнять ручную оценку с помощью компьютера, дополняя существующие наборы инструментов для наступательных операций. Фреймворк может быть дополнен любыми пользовательскими инструментами.

- https://caldera.mitre.org/

Atomic Red Team

https://atomicredteam.io/

Metta

Metta - это инструмент для обеспечения готовности к защите информации.

В данном проекте используется Redis/Celery, python и vagrant с virtualbox для моделирования действий противника. Это позволяет тестировать (в основном) инструментарий, основанный на хосте, но также может позволить тестировать любые сетевые средства обнаружения и контроля, в зависимости от того, как вы настроите vagrant.

Проект анализирует yaml-файлы с действиями и использует celery для постановки этих действий в очередь и их одновременного выполнения без взаимодействия.

https://github.com/uber-common/metta

OSSIM

- AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM), предоставляет вам многофункциональный SIEM с открытым исходным кодом, включающий в себя сбор, нормализацию и корреляцию событий. AlienVault OSSIM, созданный инженерами по безопасности из-за отсутствия доступных продуктов с открытым кодом, был создан специально для решения проблемы, с которой сталкиваются многие специалисты по безопасности: SIEM, будь она с открытым исходным кодом или коммерческая, практически бесполезна без базовых средств контроля безопасности, необходимых для обеспечения видимости безопасности.
- https://cybersecurity.att.com/products/ossim

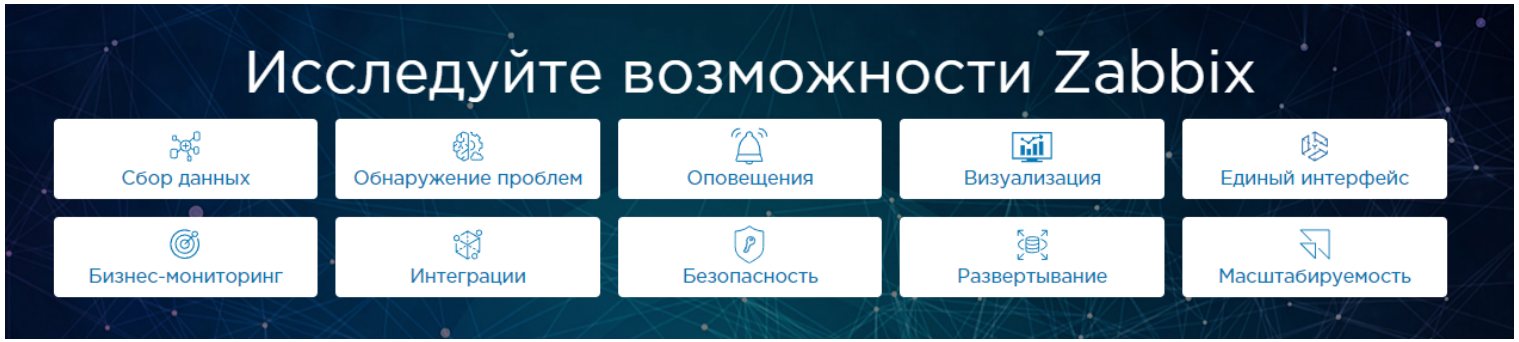
Prelude

- Prelude - это универсальная система управления информацией и событиями безопасности (SIEM). Prelude собирает, нормализует, сортирует, агрегирует, коррелирует и сообщает обо всех событиях, связанных с безопасностью, независимо от марки продукта или лицензии, породивших эти события; Prelude является "безагентной" системой.
- Помимо того, что Prelude способен восстанавливать любые типы журналов (системные журналы, syslog, flat файлы и т.д.), он имеет встроенную поддержку ряда систем, предназначенных для дополнительного обогащения информации (snort, samhain, ossec, auditd и т.д.).
- https://www.prelude-siem.org/

Nagios

- Nagios XI обеспечивает мониторинг всех критически важных компонентов инфраструктуры, включая приложения, сервисы, операционные системы, сетевые протоколы, системные метрики и сетевую инфраструктуру. Сотни сторонних аддонов обеспечивают мониторинг практически всех внутренних и внешних приложений, сервисов и систем.
- https://www.nagios.org/

Zabbix

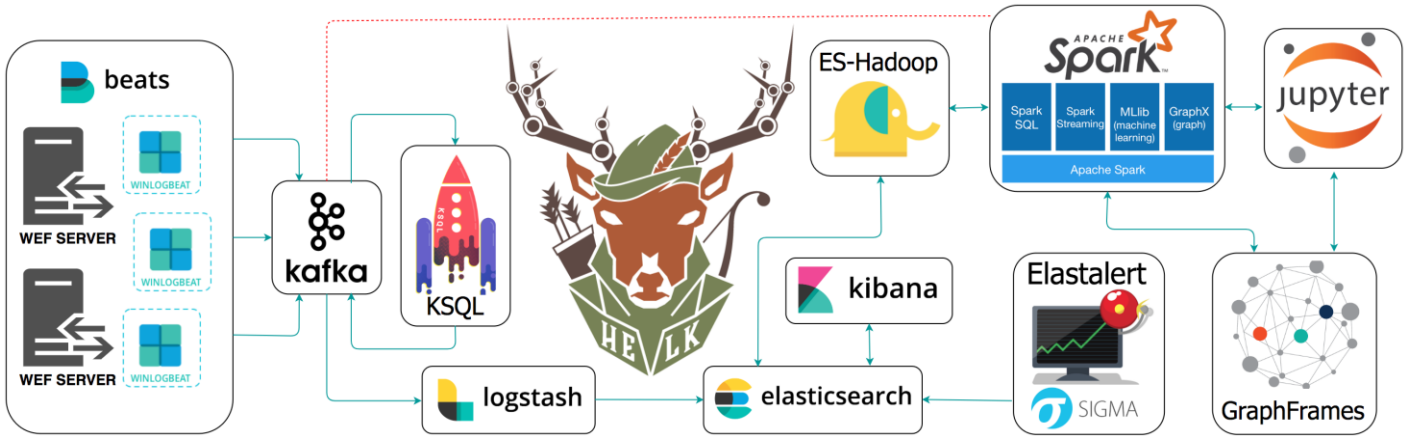


- https://www.zabbix.com/network_monitoring

Icinga

- Находите ответы, действуйте и решайте проблемы. Будьте гибкими и выбирайте свои собственные пути. Будьте любознательны, увлечены, будьте в курсе событий. Решайте задачи по мониторингу.
- https://icinga.com/

Helk



- Hunting ELK или просто HELK - одна из первых открытых платформ для хантинга с расширенными возможностями аналитики, такими как декларативный язык SQL, построение графиков, структурированные потоки и даже машинное обучение с помощью блокнотов Jupyter и Apache Spark поверх стека ELK. Этот проект разрабатывался в первую очередь для исследований, но благодаря гибкому дизайну и основным компонентам он может быть развернут в более крупных средах при правильных конфигурациях и масштабируемой инфраструктуре.
- https://github.com/Cyb3rWard0g/HELK

CimSweep

- CimSweep - это набор инструментов на базе CIM/WMI, позволяющий удаленно выполнять операции по реагированию на инциденты и поиску информации на всех версиях Windows. CimSweep также может использоваться для ведения наступательной разведки без необходимости сброса полезной нагрузки на диск. Windows Management Instrumentation устанавливается и работает по умолчанию начиная с Windows XP и Windows 2000 и полностью поддерживается в последних версиях Windows, включая Windows 10, Nano Server и Server 2016.
- https://github.com/PowerShellMafia/CimSweep

PowerForensics

- Цель PowerForensics - создать универсальную систему для криминалистического анализа жестких дисков. В настоящее время PowerForensics поддерживает файловые системы NTFS и FAT, начата работа над поддержкой Extended File System и HFS+.
- https://github.com/Invoke-IR/PowerForensics

RedLine

- Redline®, основное бесплатное средство защиты конечных точек от компании FireEye, предоставляет пользователям возможности по исследованию хоста для поиска признаков вредоносной активности путем анализа памяти и файлов, а также составления профиля оценки угроз.

С помощью Redline вы можете:

- Тщательный аудит и сбор всех запущенных процессов и драйверов из памяти, метаданных файловой системы, данных реестра, журналов событий, сетевой информации, служб, задач и веб-истории.
- Анализ и просмотр импортированных данных аудита, включая возможность фильтрации результатов по заданным временным рамкам с помощью функции Timeline в Redline с функциями TimeWrinkle™ и TimeCrunch™.
- Оптимизация анализа памяти с помощью проверенного рабочего процесса для анализа вредоносного ПО на основе относительного приоритета.
- Выполнение анализа индикаторов компрометации (IOC). Поставляемый с набором IOC, портативный агент Redline автоматически настраивается на сбор данных, необходимых для проведения анализа IOC и анализа результатов обнаружения IOC.
- https://fireeye.market/apps/211364

Yara

- YARA - это инструмент, предназначенный (но не ограничивающийся этим) для помощи исследователям в идентификации и классификации образцов вредоносного ПО. С помощью YARA можно создавать описания семейств вредоносных программ (или любые другие описания) на основе текстовых или бинарных шаблонов. Каждое описание, оно же правило, состоит из набора строк и булевого выражения, которые определяют его логику.
- https://github.com/VirusTotal/yara

Forager

- Задумывались ли вы когда-нибудь о том, что существует более простой способ получения, хранения и поддержки всех ваших данных по анализу угроз? Знакомьтесь, это Forager. Не все проекты по анализу угроз требуют наличия базы данных, которая "коррелирует триллионы точек данных...", вместо этого вам нужен простой интерфейс с простыми TXT-файлами, который позволяет извлекать данные об угрозах из других каналов, PDF-отчетов об угрозах или других источников данных с минимальными усилиями. Благодаря 15 предварительно настроенным каналам угроз вы можете начать работу с управлением данными об угрозах уже сегодня
- https://github.com/opensourcesec/Forager

Threat Bus

- Подключение средств безопасности с открытым исходным кодом: Threat Bus - это pub-sub брокер для данных разведки угроз. С помощью Threat Bus можно легко интегрировать платформы для сбора данных об угрозах, такие как OpenCTI или MISP, со средствами обнаружения и базами данных, такими как Zeek или VAST.
- Встроенный STIX-2: Threat Bus передает индикаторы и данные о наблюдениях, закодированные в соответствии со спецификацией открытого формата STIX-2.
- Архитектура на основе плагинов: Проект основан на плагинах и может быть легко расширен. Прочитайте о различных типах плагинов и о том, как написать свой собственный. Мы приветствуем вклад в создание новых инструментов с открытым исходным кодом!
- Официальные плагины: Мы поддерживаем множество плагинов прямо в официальном репозитории Threat Bus. Посмотрите наши интеграции для MISP, Zeek, CIFv3 и других приложений, подключающихся через ZeroMQ, например, vast-threatbus и наш коннектор OpenCTI.
- Снимки: Функция снимков позволяет подписчикам напрямую запрашивать данные об угрозах за определенный промежуток времени у других приложений. Threat Bus обеспечивает связь между всеми участвующими приложениями.
- https://github.com/tenzir/threatbus

Threat Ingestor

- ThreatIngestor может быть настроен на просмотр Twitter, RSS-каналов или других источников, извлечение значимой информации, например, вредоносных IP/доменов и сигнатур YARA, и отправку этой информации в другую систему для анализа.
- https://github.com/InQuest/ThreatIngestor

Misp

- Руководство пользователя для MISP - платформы обмена информацией об угрозах с открытым исходным кодом. Данное руководство пользователя предназначено для специалистов в области ICT, таких как аналитики по безопасности, специалисты по работе с инцидентами безопасности или реверс-инженеры вредоносных программ, которые обмениваются данными об угрозах с помощью MISP или интегрируют MISP в другие средства мониторинга безопасности. В руководстве описано повседневное использование графического пользовательского интерфейса MISP и его автоматизированных интерфейсов (API) для интеграции MISP в среду безопасности и управления одним или несколькими экземплярами MISP.
- https://github.com/MISP/misp-book

Malware-IOC

- Здесь представлены индикаторы компрометации (IOC), полученные в ходе наших различных расследований. Мы делаем это для того, чтобы помочь широкому сообществу специалистов по безопасности бороться с вредоносным ПО, где бы оно ни находилось.
- Файлы .yar - правила Yara
- Файлы .rules - правила Snort
- Файлы samples.md5, samples.sha1 и samples.sha256 представляют собой разделенные новой строкой списки шестнадцатеричных дайджестов образцов вредоносных программ.
- Если вы хотите внести свои предложения по улучшению версии, пожалуйста, отправьте им запрос на исправление.
- Если вы обнаружили ложные срабатывания, сообщите им об этом в отчете о проблеме, и они постараются улучшить их IOC.
- Они лицензированы под свободной лицензией BSD с двумя положениями. Вы можете модифицировать их и оставлять изменения для себя, даже если это было бы невежливо.
- https://github.com/eset/malware-ioc

Cobalt Strike Scan

- Сканирует файлы или память процесса на наличие маяков Cobalt Strike и анализирует их конфигурацию.
- CobaltStrikeScan сканирует память процесса Windows на наличие признаков DLL-инъекции (классической или рефлексивной) и/или выполняет YARA-сканирование памяти целевого процесса на наличие сигнатур маяков Cobalt Strike v3 и v4.
- В качестве альтернативы CobaltStrikeScan может выполнить такое же YARA-сканирование файла, указав в качестве аргумента командной строки абсолютный или относительный путь.
- Если в файле или процессе обнаружен маяк Cobalt Strike, то конфигурация маяка будет разобрана и выведена на консоль.
- https://github.com/Apr4h/CobaltStrikeScan

Harden Tools

- Hardentools предназначен для отключения ряда возможностей, предоставляемых операционными системами (на данный момент - Microsoft Windows) и некоторыми широко используемыми приложениями (на данный момент - Microsoft Office и Adobe PDF Reader). Эти функции, предназначенные, как правило, для корпоративных пользователей, в целом бесполезны для обычных пользователей и представляют собой скорее опасность, поскольку очень часто используются злоумышленниками для выполнения вредоносного кода на компьютере жертвы. Цель данного инструмента - просто уменьшить площадь атаки, отключив "низко висящие фрукты". Hardentools предназначен для людей, подверженных риску и желающих получить дополнительный уровень безопасности ценой некоторого снижения удобства использования. Он не предназначен для корпоративных сред.
- https://github.com/securitywithoutborders/hardentools

Windows Secure Host Baseline

- Система Windows Secure Host Baseline (SHB) представляет собой автоматизированный и гибкий подход к оказанию помощи DoD в развертывании последних версий Windows 10 с использованием структуры, которая может быть использована организациями любого размера.

- 20 ноября 2015 года CIO MO выпустил служебную записку, в которой командованию, службе, агентству и полевой деятельности (CC/S/As) было предписано быстро развернуть операционную систему Windows 10 в своих организациях с целью завершения развертывания к концу января 2017 года. 26 февраля 2016 г. заместитель министра обороны США издал служебную записку, предписывающую DoD завершить быстрое развертывание и переход на Microsoft Windows 10 Secure Host Baseline к концу января 2017 г.

- https://github.com/nsacyber/Windows-Secure-Host-Baseline

Any Run

- Недостаточно запустить подозрительный файл на тестовой системе, чтобы быть уверенным в его безопасности. Для некоторых типов вредоносного ПО или уязвимостей (например, APT) требуется непосредственное взаимодействие с человеком в процессе анализа. Набор онлайн-инструментов для анализа вредоносного ПО позволяет наблюдать за процессом исследования и при необходимости вносить изменения, как это делается на реальной системе, а не полагаться на полностью автоматизированную песочницу.
- https://any.run/

Hybrid Analysis

- Это бесплатный сервис анализа вредоносного ПО, который обнаруживает и анализирует неизвестные угрозы с помощью уникальной технологии Hybrid Analysis.
- https://www.hybrid-analysis.com/

PSHunt

- PSHunt - это модуль Powershell Threat Hunting Module, предназначенный для сканирования удаленных конечных точек на наличие признаков компрометации или их опроса для получения более полной информации о состоянии этих систем (активных процессов, автозапусков, конфигураций и/или журналов).
- PSHunt был создан как предшественник коммерческого продукта компании Infocyte - Infocyte HUNT - и в настоящее время является открытой разработкой для сообщества DFIR.
- https://github.com/Infocyte/PSHunt

GoPhish

- Gophish - это мощный фреймворк для фишинга с открытым исходным кодом, позволяющий легко проверить подверженность вашей организации фишингу.
- https://getgophish.com/

Solar Winds

- Менеджер журналов собирает сообщения журналов со всей системы, объединяя различные форматы их записи для совместного хранения и поиска. На панели управления все события отображаются в реальном времени, кроме того, имеется аналитический инструмент, позволяющий искать в сохраненных файлах журналов необходимую информацию о безопасности. Менеджер журналов также защищает журналы от несанкционированного доступа с помощью средства контроля целостности файлов.

- Security Event Manager - это не просто SIEM. Он включает в себя канал анализа угроз, который объединяет опыт обнаружения угроз, полученный от всех клиентов системы SolarWinds. При поиске индикаторов атак в журнальных сообщениях система безопасности использует рекомендации из этого канала.

- https://www.solarwinds.com/security-event-manager

SentinelOne

- Сегодня мы рады представить революционную технологию ActiveEDR. ActiveEDR решает проблемы EDR в том виде, в котором они известны, отслеживая и контекстуализируя все, что находится на устройстве. ActiveEDR способен выявлять вредоносные действия в режиме реального времени, автоматизируя необходимые меры реагирования и позволяя легко находить угрозы путем поиска по единому IOC. Ознакомьтесь с более подробной информацией, чтобы понять, как мы пришли к этому и как создали первый и единственный EDR, который действительно является активным.
- https://www.sentinelone.com/blog/active-edr-feature-spotlight/

Qualys

- Киберриск - это бизнес-риск, причем риски растут быстрее, чем с ними могут справиться традиционные средства VM и SIEM. Командам безопасности и ИТ-специалистам необходим новый подход к борьбе с киберугрозами, позволяющий четко понимать риски кибербезопасности и автоматизировать рабочие процессы для быстрого реагирования.

- https://www.qualys.com/apps/vulnerability-management-detection-response/

EzTools

- Эти средства цифровой криминалистики с открытым исходным кодом могут использоваться в самых разных исследованиях, включая перекрестную проверку инструментов, получение информации о технических деталях, не раскрываемых другими инструментами, и многое другое. За годы работы Эрик написал и постоянно совершенствует более десятка инструментов цифровой криминалистики, которыми ежедневно пользуются исследователи по всему миру.

- https://www.sans.org/tools/ez-tools/

Remnux

- REMnux® - это бесплатный набор инструментов Linux для помощи аналитикам в реверс инжиниринге вредоносного ПО. Он призван облегчить криминалистам и специалистам по реагированию на инциденты использование разнообразных свободно распространяемых инструментов, позволяющих исследовать вредоносное ПО, но при этом вызывающих затруднения в их поиске и настройке.
- Сердцем проекта является Linux-дистрибутив REMnux, основанный на Ubuntu. Этот легкий дистрибутив включает в себя множество инструментов для анализа вредоносного ПО для Windows и Linux, изучения браузерных угроз, таких как обфусцированный JavaScript, исследования подозрительных файлов документов и разбора других вредоносных артефактов. Исследователи также могут использовать этот дистрибутив для перехвата подозрительного сетевого трафика в изолированной лаборатории при проведении поведенческого анализа вредоносного ПО.

- https://sansgear.com/remnux/

Sift Workstation

- Почему SIFT? SIFT Workstation - это набор бесплатных инструментов с открытым исходным кодом, предназначенных для проведения сложных цифровых криминалистических экспертиз в различных условиях. Она может сравниться с любым современным набором инструментов для реагирования на инциденты и криминалистики. SIFT демонстрирует, что расширенные возможности реагирования на инциденты и глубокие методы цифровой криминалистической экспертизы вторжений могут быть реализованы с помощью современных свободно распространяемых и часто обновляемых инструментов с открытым исходным кодом.

- https://sansgear.com/sift-workstation/

Sof-Elk

- SOF-ELK® - это платформа анализа больших данных, ориентированная на типичные потребности криминалистов/аналитиков и сотрудников служб информационной безопасности. Платформа представляет собой специализированную сборку открытого стека Elastic, состоящую из системы хранения и поиска данных Elasticsearch, системы сбора и обогащения данных Logstash, фронтэнда дашборда Kibana и передатчика логов Elastic Beats (в частности, filebeat). Благодаря значительному количеству настроек и постоянному развитию, пользователи SOF-ELK® могут избежать длительного и сложного процесса настройки, обычно требуемого стеком Elastic. Вместо этого они могут просто загрузить предварительно созданное и готовое к использованию виртуальное устройство SOF-ELK®, которое потребляет различные типы исходных данных (многочисленные типы журналов, а также NetFlow), анализируя наиболее важные данные и визуализируя их на нескольких стандартных дашбордах. Продвинутые пользователи могут создавать визуализации, соответствующие их собственным требованиям к расследованию или оперативной работе, с возможностью внесения их в основной репозиторий кода.
- https://sansgear.com/sof-elk/

MXToolbox

- Этот тест выводит список MX-записей для домена в порядке приоритета. Поиск MX-записей осуществляется непосредственно на сервере имен домена, поэтому изменения в MX-записях должны отображаться мгновенно. Можно нажать кнопку Diagnostics (Диагностика), которая позволит подключиться к почтовому серверу, проверить обратные записи DNS, выполнить простую проверку Open Relay и измерить время отклика. Можно также проверить каждую MX-запись (IP-адрес) по 105 черным спискам DNS (обычно называемым RBL, DNSBL).

- https://mxtoolbox.com/

DevSec.io

- Система защиты серверов, обеспечивающая реализацию различных базовых конфигураций безопасности с помощью Ansible, Chef и Puppet.
- https://dev-sec.io/

Clevis

- Подключаемый фреймворк для автоматической расшифровки, часто используемый в качестве клиента Tang.
- https://github.com/latchset/clevis

Cortex

- Обеспечивает горизонтально масштабируемое, высокодоступное, многопользовательское, долгосрочное хранение данных для Prometheus.
- https://cortexmetrics.io/

Jaeger

- Бэкэнд платформы распределенной трассировки, используемый для мониторинга и устранения неисправностей в распределенных системах на базе микросервисов.
- https://www.jaegertracing.io/

KubeSec

- Статический анализатор манифестов Kubernetes, который может работать локально, как контроллер допуска Kuberenetes или как собственный облачный сервис.
- https://kubesec.io/

Linkerd

- Сверхлегкая сетка сервисов для Kubernetes, добавляющая наблюдаемость, надежность и безопасность приложениям Kubernetes, не требуя модификации самого приложения.
- https://linkerd.io/

Globaleaks

- Бесплатное программное обеспечение с открытым исходным кодом, позволяющее любому человеку легко создавать и поддерживать безопасную платформу для сбора информации.
- https://www.globaleaks.org/

Teleport

- Позволяет инженерам и специалистам по безопасности объединить доступ к SSH-серверам, кластерам Kubernetes, веб-приложениям и базам данных во всех средах.
- https://goteleport.com/

DynInst

- Инструменты для инструментирования, анализа и модификации бинарных файлов, для создания бинарных патчей.
- https://github.com/dyninst/dyninst

Dynamo Rio

- Система манипулирования кодом во время выполнения программы, поддерживающая преобразования кода в любой части программы во время ее выполнения, реализованная в виде виртуальной машины на уровне процесса.
- https://dynamorio.org/

Egalito

- Рекомпилятор двоичных файлов и инструментарий, позволяющий полностью дизассемблировать, трансформировать и регенерировать обычные двоичные файлы Linux, предназначенный для усиления двоичных файлов и исследования безопасности.
- https://egalito.org/

Kushtaka

- Устойчивый универсальный механизм организации honeypot и honeytoken для синих команд, не имеющих достаточных ресурсов.
- https://kushtaka.gitbook.io/documentation/

Manuka

- Поисковая система с открытым исходным кодом (OSINT), которая отслеживает попытки разведки со стороны участников угроз и генерирует полезную информацию для членов синей команды.
- https://github.com/spaceraccoon/manuka

Threat Note

- Веб-приложение, созданное компанией Defense Point Security для того, чтобы исследователи безопасности могли добавлять и извлекать индикаторы, связанные с их исследованиями.
- https://github.com/DefensePointSecurity/threat_note

AutoMacTC

- Модульная автоматизированная система сбора криминалистических материалов, предназначенная для доступа к различным криминалистическим артефактам на macOS, их разбора и представления в форматах, пригодных для анализа.
- https://github.com/CrowdStrike/automactc

Margarita Shotgun

- Утилита командной строки (работает как с инстансами Amazon EC2, так и без них) для распараллеливания удаленного получения памяти.
- https://github.com/ThreatResponse/margaritashotgun

Mailspoof

- Проверяет записи SPF и DMARC на наличие проблем, которые могут привести к подмене почты.
- https://github.com/serain/mailspoof

Phishing Catcher

- Настраиваемый скрипт для отслеживания выпусков подозрительных TLS-сертификатов по доменному имени в журнале Certificate Transparency Log (CTL) с помощью сервиса CertStream.
- https://github.com/x0rz/phishing_catcher

SentinelOne

- SentinelOne - это современное решение для безопасности информации, которое предоставляет инструменты и функциональность, ориентированные на синюю команду (Blue Team) и защиту информационной инфраструктуры организации от киберугроз
- https://www.sentinelone.com/

BadBlood

- Заполняет тестовый (непроизводственный) домен Windows данными, которые позволяют аналитикам и инженерам по безопасности попрактиковаться в использовании инструментов для получения понимания и рекомендаций по обеспечению безопасности Active Directory.
- https://www.secframe.com/badblood/

Drool

- Инструмент для воспроизведения DNS-трафика из файлов захвата пакетов и отправлять его на указанный сервер, например, для имитации DDoS-атак на DNS и измерения обычных запросов DNS.
- https://www.dns-oarc.net/tools/drool

Dumpster Fire

- Модульный, управляемый через меню, кроссплатформенный инструмент для создания повторяющихся, отложенных во времени, распределенных событий безопасности для учений синих команд и составления карт сенсоров и алертов.
- https://github.com/TryCatchHCF/DumpsterFire

GRR Rapid Response

- Система реагирования на инциденты, ориентированная на удаленную экспертизу в реальном времени и состоящая из Python-агента, установленного на объектах, и серверной инфраструктуры на базе Python, позволяющей аналитикам быстро сортировать атаки и проводить анализ в удаленном режиме.
- https://github.com/google/grr

MozDef

- Автоматизация процесса обработки инцидентов безопасности и облегчение работы специалистов по обработке инцидентов в режиме реального времени.
- https://github.com/mozilla/MozDef

Rastrea2r

- Многоплатформенный инструмент для обработки подозрительных IOC на многих конечных точках одновременно, интегрируемый с антивирусными консолями.
- https://github.com/rastrea2r/rastrea2r

AttackerKB

- Бесплатная и общедоступная платформа краудсорсинговой оценки уязвимостей, помогающая определить приоритетность применения патчей с высоким риском и бороться с усталостью от уязвимостей.
- https://attackerkb.com/

Data

- Средство анализа и автоматизации фишинг-адресов, которое может принимать предполагаемые фишинговые URL напрямую или срабатывать на наблюдаемый сетевой трафик, содержащий такой URL.
- https://github.com/hadojae/DATA

Forager

- Многопоточный сбор данных об угрозах, построенный на Python3, с простой текстовой конфигурацией и хранением данных, что обеспечивает простоту использования и переносимость данных.
- https://github.com/opensourcesec/Forager

Unfetter

- Выявление недостатков в системе защиты с помощью фреймворка ATT&CK компании Mitre.
- https://nsacyber.github.io/unfetter/

Onion Balance

- Обеспечивает балансировку нагрузки, а также повышает отказоустойчивость и надежность сервисов Onion за счет устранения единичных точек отказа.
- https://onionbalance.readthedocs.io/en/latest/

Nebula

- Полностью открытый и самодостаточный инструмент для создания масштабируемых оверлейных сетей, ориентированный на производительность, простоту и безопасность, созданный на основе tinc.
- https://github.com/slackhq/nebula

TailScale

- Управляемый сетчатый VPN-сервис freemium, построенный на базе WireGuard.
- https://tailscale.com/

Cobalt Strike Scan

- Сканирование файлов или памяти процесса на наличие маяков Cobalt Strike и разбор их конфигурации.
- https://github.com/Apr4h/CobaltStrikeScan

Sigcheck

- Аудит хранилища корневых сертификатов хоста Windows по списку Microsoft Certificate Trust List (CTL).
- https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck

Domain Hunter

- Проверка доменов с истекшим сроком действия на категоризацию/репутацию и историю Archive.org для определения подходящих кандидатов на фишинговые и C2-доменные имена
- https://github.com/threatexpress/domainhunter

Elastic for Red Team

- Репозиторий ресурсов для конфигурирования Red Team SIEM с использованием Elastic.
- https://github.com/SecurityRiskAdvisors/RedTeamSIEM

SharpEDRChecker

- Проверяет запущенные процессы, метаданные процессов, DLL, загруженные в текущий процесс, и метаданные каждой DLL, общие каталоги установки, установленные службы и метаданные исполняемых файлов каждой службы, установленные драйверы и метаданные каждого драйвера, а также наличие известных защитных продуктов, таких как AV, EDR и средства журналирования.
- https://github.com/PwnDexter/SharpEDRChecker

SeatBelt

- Seatbelt - это проект на языке C#, выполняющий ряд ориентированных на безопасность проверок защищенности хоста, актуальных как с точки зрения наступательной, так и оборонительной безопасности.
- https://github.com/GhostPack/Seatbelt

BloodHound

- Мощный инструмент для анализа привилегий и атак на Active Directory в среде Windows. Он предоставляет графический интерфейс для визуализации и анализа отношений между пользователями, группами и компьютерами в Active Directory.
- https://github.com/BloodHoundAD/BloodHound

Rubeus

- Rubeus - это набор инструментов на языке C# для работы с необработанным Kerberos и его злоупотреблениями. Он в значительной степени адаптирован из проекта Kekeo Бенджамина Дельпи (лицензия CC BY-NC-SA 4.0) и проекта MakeMeEnterpriseAdmin Винсента Ле Тукса (лицензия GPL v3.0).
- https://github.com/GhostPack/Rubeus

Mimikatz

- Mimikatz - это приложение с открытым исходным кодом, позволяющее пользователям просматривать и сохранять учетные данные аутентификации, например, билеты Kerberos.
- https://github.com/gentilkiwi/mimikatz

CredBandit

- CredBandit - это пробный вариант Beacon Object File (BOF), который использует статические системные вызовы x64 для выполнения полного дампа процесса в памяти и отправки его обратно по уже существующему каналу связи Beacon.
- https://github.com/xforcered/CredBandit

SharpChromium

- Проект .NET 4.0 CLR для получения данных Chromium, таких как cookies, история и сохраненные логины.
- https://github.com/djhohnstein/SharpChromium

Watson

- Watson - это инструмент для .NET, предназначенный для перечисления отсутствующих KB и предложения эксплойтов для уязвимостей с повышением привилегий.
- https://github.com/rasta-mouse/Watson

DNS Exfiltration

- Эксфильтрация данных по скрытому каналу DNS-запросов
- https://github.com/Arno0x/DNSExfiltrator

Prelude Operator

- Платформа для повышения уровня безопасности, ориентированная на разработчиков. Защитите свою организацию, имитируя реальные атаки противника.
- https://www.prelude.org/

Stratus Red Team

- Stratus Red Team - это "Atomic Red Team™" для облака, позволяющая эмулировать методы наступательных атак в гранулированном и автономном виде.
- https://github.com/DataDog/stratus-red-team

PowerForensic

- PowerForensics - фреймворк для криминалистического анализа дисков в реальном времени
- https://github.com/Invoke-IR/PowerForensics

FastFinder

- Быстрая настраиваемая кроссплатформенная программа для поиска подозрительных файлов. Поддерживает хэши md5/sha1/sha256, строки с literal/wildcard символами, регулярные выражения и правила YARA
- https://github.com/codeyourweb/fastfinder

Fireeye Memorize

- Бесплатная программа для судебной экспертизы памяти
- https://fireeye.market/apps/211368

KeeFarce

- Извлечение паролей KeePass из памяти
- https://github.com/denandz/KeeFarce

Logon Tracer

- Расследование вредоносного входа в Windows с помощью визуализации и анализа журнала событий Windows
- https://github.com/JPCERTCC/LogonTracer

RegRippy

- Фреймворк для чтения и извлечения полезных криминалистических данных из ветвей реестра Windows
- https://github.com/airbus-cert/regrippy

Pancake Viewer

- Программа просмотра образов дисков на основе dfvfs, аналогичная программе просмотра FTK Imager
- https://github.com/forensicmatt/PancakeViewer

AWESOME!

- https://github.com/fabacab/awesome-cybersecurity-blueteam
- https://github.com/CyberSecurityUP/Awesome-Red-Team-Operations
- https://github.com/infosecn1nja/Red-Teaming-Toolkit
- https://github.com/an4kein/awesome-red-teaming
- https://github.com/cugu/awesome-forensics
- https://github.com/dcarlin/Blue-Team-Tools
- https://github.com/fabacab/awesome-cybersecurity-blueteam