История одного SOC

SOC_SO-UPS V 2.2

Лев Палей
АО «СО ЕЭС»

Системный оператор ЕЭС

Структура Общества

ИА с центральным диспетчерским управлением (ЦДУ)
7 объединенных диспетчерских управлений (ОДУ)
51 региональное диспетчерское управление (РДУ)
14 представительств

Основные задачи

- управление технологическими режимами работы объектов ЕЭС России в реальном времени
- обеспечение перспективного развития ЕЭС России
- обеспечение единства и эффективной работы технологических механизмов оптового и розничных рынков электрической энергии и мощности

3-й этап –совершенствование и систематизация

- реагирование в непрерывном режиме (создание подразделения **24\7**);
- выведение подпроцессов эксплуатации SOC (создание-изменение правил корреляции, оповещений, методик реагирования);
- типизация инцидентов, правил корреляции, алгоритмов реагирования;
- систематизация и совершенствование работы с данными (BI).

Функции оперативной смены

- круглосуточный мониторинг, анализ и обработка событий, поступающих от средств защиты Общества;
- создание и рассмотрение заявок на обработку выявленных инцидентов и событий ИБ;
- выявление актуальных уязвимостей и угроз в информационных системах Общества;
- участие в проектах по исследованию решений, самомовершенствование
- участие в расследовании инцидентов ИБ.

Что мы делаем Enterprise или около

- Забор информации из сервисов TI
- Создание правил корреляции для уменьшения «шума»

Сервисы TI:

- Hail a TAXII - http://hailataxii.com/
- OTX - https://www.alienvault.com/open-threat-exchange

Поиск информации по внешним источникам

- На первом этапе использование https://www.inoreader.com/.
- Преимущества – кросплатформенность, удобство.
- Итерационное обновление ресурсов-источников
- В итоге – набор ресурсов собственной подборки, проверенные временем

Перечень информационных ресурсов для мониторинга уязвимостей
https://www.securitylab.ru/
https://threatpost.ru/
https://www.anti-malware.ru/
https://xakep.ru/
https://vulners.com/search?query=order:published
https://threats.kaspersky.com/
https://www.talosintelligence.com/vulnerability_reports#disclosed

Бюллетени информационной безопасности

№	Необходимые действия	Срок выполнения	Описание	Отчетность\ срок предоставления отчета
1	**Обновить Adobe Flash до версии 30.0.0.113 и выше**	До __.06.2018	Зафиксированы факты эксплуатации уязвимости CVE-2018-5002 в ПО Adobe Flashplayer в т.ч. через распространение писем со вложенными файлами MS Office.	Не требуется
2	**Обновить ПО Chrome до версии 67.0.3396.79 и выше**	До __.06.2018	В Google Chrome обнаружена уязвимость, затрагивающая версии браузера для Windows, Mac, Linux и других операционных систем, связанная с «некорректной обработкой CSP заголовка» (CVE-2018-6148).	Не требуется
3	**Принять к сведению**	До поступления рекомендаций	Уязвимости в библиотеке scrrun.dll в составе Microsoft Windows позволяют браузеру Microsoft Internet Explorer 11 производить добавление или удаление файлов или папок в системе. Злоумышленник может вносить изменения в файловую систему жертвы, заманив ее на специально созданный веб-сайт	Не требуется

Методики реагирования

Реагирование на детектирование вредоноса (вирусная активность):

Временные рамки реагирования: - часа.

Алгоритм действий: При срабатывании оповещения и обнаружении зловреда, если он был удален средствами антивирусной защиты, требуется провести исследование метода, с использованием которого произошло проникновение:

1. Определить как попал зловред на ИТ-актив (исследовать логи, журнал ПК)
2. Открывал ли пользователь\администратор файл при получении;
3. Сколько времени прошло с момента получения\проникновения зловреда до момента обнаружения антивирусными средствами.

***на текущий момент сформировано более 18-ти методик**

Унификация рабочих мест SOC и CSIRT

5	Process Monitor(Process hacker)	Контролирует и следит за всей работой операционной системы и отображает все происходящие процессы, работающие библиотеки, различные драйвера устройств, а также все изменения, происходящие с файлами, и выводит сообщение об их удалении или открытии. Включает в себя инструмент для мониторинга системного реестра и показывает, какие программы обращаются к нему (какие ключи читают и пытаются в них что-либо записать).	Изучение состояния системы в ретроспективе
6	Process Explorer	Мощная утилита для отслеживания в режиме реального времени запущенных в системе процессов. Показывает подробнейшую информацию о всех процессах, включая использование памяти, задействованных DLL библиотеках и многое другое.	Изучение состояния системы в ретроспективе
7	Nmap	Свободная утилита, предназначенная для разнообразного настраиваемого сканирования IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб). Изначально программа была реализована для систем UNIX, но сейчас доступны версии для множества операционных систем.	Получение информации о объектах внутри IP-сети
8	DebugView	Бесплатная утилита из сборника SysInternals Suite для просмотра отладочного вывода программ и драйверов в ОС Windows как на локальном ПК, так и на любом компьютере в сети, подключенного по протоколу TCP/IP. DebugView поддерживает вывод как в Kernel-mode, так и User-mode.	Изучение состояния системы в ретроспективе
1	Firefox+Firebug+Burp+Owasp zap	Веб-браузер для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; а также для решения других задач, отличается собственной надстройкой прокси. Отладчик web-приложений, используется как отдельное расширение для браузера Mozilla Firefox, являющееся консолью, отладчиком, и DOM-инспектором JavaScript, DHTML, CSS, XMLHttpRequest. Firebug показывает в консоли вызвавшую ошибку функцию, стек вызовов функций, вызвавших эту ошибку. Он предупреждает, что правило CSS или метод/свойство JavaScript, которое вы пытаетесь использовать, не существует.	Анализ веб-страниц, просмотр кода, включений , вставок, перенаправлений
	Wireshark	Программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Имеет графический пользовательский интерфейс. Приложение «знает» структуру самых различных сетевых	Анализ pcap файлов

Сервисы для обработки событий ИБ - 1

ОТВЕТИТЬ | Поиск в теме... | Поиск

Перечень дополнительных инструментов для обработки событий

ПРАВКА ЦИТАТА

В повседневной деятельности, связанной с обработкой событий, помимо основных методов реагирования, возникает потребность в использовании дополнительных инструментов. В связи с этим возникла идея создания данного раздела, в котором будет публиковаться пополняемый перечень. Данный набор является дополнением к основному списку и нацелен упростить процесс обработки.

Базы данных угроз

1 https://www.cvedetails.com/ CVE Database(список уязвимостей безопасности)
2 https://www.vulnerabilitycenter.com База уязвимостей, содержит описание уязвимостей и решения по их нейтрализации.
3 http://www.mcafee.com/us/threat-center.aspx ТОП 10 угроз на текущее время по статистики McAfee
4 https://bdu.fstec.ru/threat Банк данных угроз и язвимостей ФСТЭК
5 https://cybermap.kaspersky.com/ru/stats/#country=213&type=oas&period=w Статистика атак от Kaspersky Lab
6 https://www.securitylab.ru/vulnerability/page1_1.php База уязвимостей лаборатория SecurityLab
7 https://threats.kaspersky.com/ru/ База угроз и уязвимостей, содержащая данные об уязвимостях программного обеспечения, перечень и описания угроз безопасности от Kaspersky Lab.
8 https://threatpost.ru/ Блог компании Kaspersky, свежая аналитика уязвимостей и вредоносных программ.

Сетевые инструменты

9 http://ping.eu Online Ping, Traceroute, DNS lookup, WHOIS, Port check, Reverse lookup, Proxy checker, Bandwidth meter, Network calculator, Network mask calculator, Country by IP, Unit converter
10 https://pentest-tools.com Набор инструментов для оценки безопасности веб-сайтов и сетевых инфраструктур
11 https://ip-calculator.ru Сетевой калькулятор
12 https://www.robtex.com IP/DNS/WHOIS look-ups Различные виды исследований IP-адресов и доменов
13 https://2ip.ru/ IP/ISP/Domain, and WHOIS look-ups(широкий набор сервисов для исследования Ip-адресов и доменов)
14 https://www.abuseipdb.com Отчет о ресурсе, включен ли IP-адрес в blacklist. (проверка черног списка для системных администраторов и других

Сервисы для обработки событий ИБ - 2

Сетевые инструменты

9 http://ping.eu Online Ping, Traceroute, DNS lookup, WHOIS, Port check, Reverse lookup, Proxy checker, Bandwidth meter, Network calculator, Network mask calculator, Country by IP, Unit converter
10 https://pentest-tools.com Набор инструментов для оценки безопасности веб-сайтов и сетевых инфраструктур
11 https://ip-calculator.ru Сетевой калькулятор
12 https://www.robtex.com IP/DNS/WHOIS look-ups Различные виды исследований IP-адресов и доменов
13 https://2ip.ru/ IP/ISP/Domain, and WHOIS look-ups(широкий набор сервисов для исследования Ip-адресов и доменов)
14 https://www.abuseipdb.com Отчет о ресурсе, включен ли IP-адрес в blacklist. (проверка черног списка для системных администраторов и других заинтересованных сторон для отчета и поиска IP-адресов, связанных с вредоносными действиями в Интернете.)
15 https://www.talosintelligence.com Отчет о ресурсе, включен ли IP-адрес в blacklist(интеллектуальная платформа для анализа угроз)
16 https://www.virustotal.com IP and Domain analysis for malware or web-based threats(бесплатная служба, осуществляющая анализ подозрительных файлов и ссылок (URL) на предмет выявления вирусов, червей, троянов и всевозможных вредоносных программ.)
17 https://vms.drweb.ru/online IP and Domain analysis for malware or web-based threats(проверка сайтов на вирусы и перенаправления по базам Dr.Web)
18 https://tools.cisco.com/security/center/home.x Набор инструментов для проверки ПО оборудования cisco на наличие необходимых обновлений ПО и т.д.
19 https://safeweb.norton.com Оценка репутации сайта от Symantec
20 http://www.projecthoneypot.org/search_ip.php IP and Domain analysis for malware or web-based threats(поиск информации об определенном IP-адресе.)
21 http://urlquery.net Анализ сайта на предмет заражения, предоставляет информацию о активности сайта во время посещения
22 http://www.ipvoid.com "IP and Domain analysis for malware or web-based threats(широкий спектр инструментов IP-адреса, чтобы узнать подробности о IP-адресах.
Проверка черного списка IP-адресов, поиск whois, поиск в DNS, пинг и т.д.)"
23 http://www.urlvoid.com Оценка репутации сайта (бесплатный сервис, который анализирует веб-сайт с помощью нескольких движков черного списка и онлайн-инструментов репутации для облегчения обнаружения мошеннических и вредоносных веб-сайтов)
24 http://global.sitesafety.trendmicro.com "IP and Domain analysis for malware or web-based threats(
одна из крупнейших в мире репутационных баз данных сайтов)"
25 https://sitecheck.sucuri.net/ IP and Domain analysis for malware or web-based threats(проверка сайта на наличие известных вредоносных программ, черного списка, ошибки веб-сайта и устаревшего программного обеспечения)
26 https://virusdesk.kaspersky.ru/ Проверка файлов или ссылок на известные угрозы от Kaspersky Lab

Прочее

27 https://docs.microsoft.com/en-us/sysinternals/downloads/index Пакет Microsoft Sysinternals(технические средства и утилиты для управления, диагностики, устранения неполадок и мониторинга всей среды Microsoft Windows)

Сервисы для обработки событий ИБ - итог

- Нет идеальных источников, всегда надо проверять в 2-3 разных местах
- Собрали базу из 70 он-лайн и оф-лайн сервисов разного характера
- Выработали алгоритмы и очередность проверки (СЗИ-VT-песочница)
- Отобрали любимые ресурсы

Сервисы для обработки событий ИБ - любимые

- Базы с информацией о компроментации:

https://www.talosintelligence.com
https://www.projecthoneypot.org/search_ip.php
https://www.abuseipdb.com/
https://viz.greynoise.io
http://osint.bambenekconsulting.com/feeds/c2-ipmasterlist.txt

- Проверка сработок на вирусные заражения\сработок в трафике:

http://try.zeek.org/#/trybro
https://vms.drweb.ru/online
https://safeweb.norton.com/

- Песочницы\агрегаторы:

https://app.any.run/
https://hackertarget.com/
https://www.hybrid-analysis.com/

Антивирусные утилиты - подтверждение детектирования

1. Kaspersky Virus Removal Tool

Краткое описание: Программа для проверки и лечения зараженных компьютеров под управлением операционных систем Windows.
Лицензия: Позволяет бесплатно использовать в корпоративной среде.
Примечание: Ввиду того, что в Обществе используется KES, использование данной утилиты представляется мало эффективным.

2. ESET's Free Online Scanner

Краткое описание: Инструмент для простого и эффективного удаления вредоносных программ с любого компьютера без установки антивирусного программного обеспечения.
Лицензия: Позволяет бесплатно использовать в корпоративной среде.

3. Dr.Web LiveDisk

Краткое описание: Утилита, предназначенная для аварийного восстановления системы с диска DVD или загрузочного USB-накопителя в случаях, если действия вредоносных программ сделали невозможной загрузку компьютера под управлением Windows.
Лицензия: Позволяет бесплатно использовать в корпоративной среде.
Примечание: Требует создания загрузочного носителя. Для загрузки с флеш-накопителя, BIOS компьютера должен поддерживать устройство USB-HDD в качестве загрузочного.

4. Norton Security Scan

Краткое описание: Инструмент, предназначенный для сканирования компьютера на наличие вирусов, программ-шпионов и других угроз безопасности.
Лицензия: Позволяет бесплатно использовать в корпоративной среде.

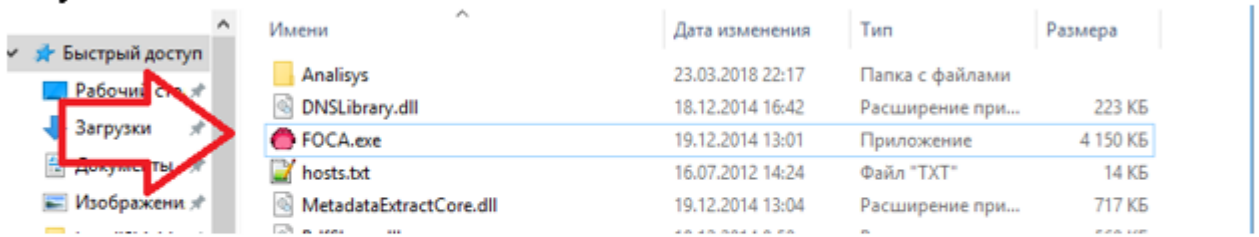
5. McAfee Stinger

Краткое описание: Утилита, используемая для обнаружения и удаления вирусов. Это не замена для полной антивирусной защиты, а специализированный инструмент для помощи администраторам и пользователям при работе с зараженной системой.
Лицензия: Позволяет бесплатно использовать в корпоративной среде.

Проверка отсутствие чувствительной информации

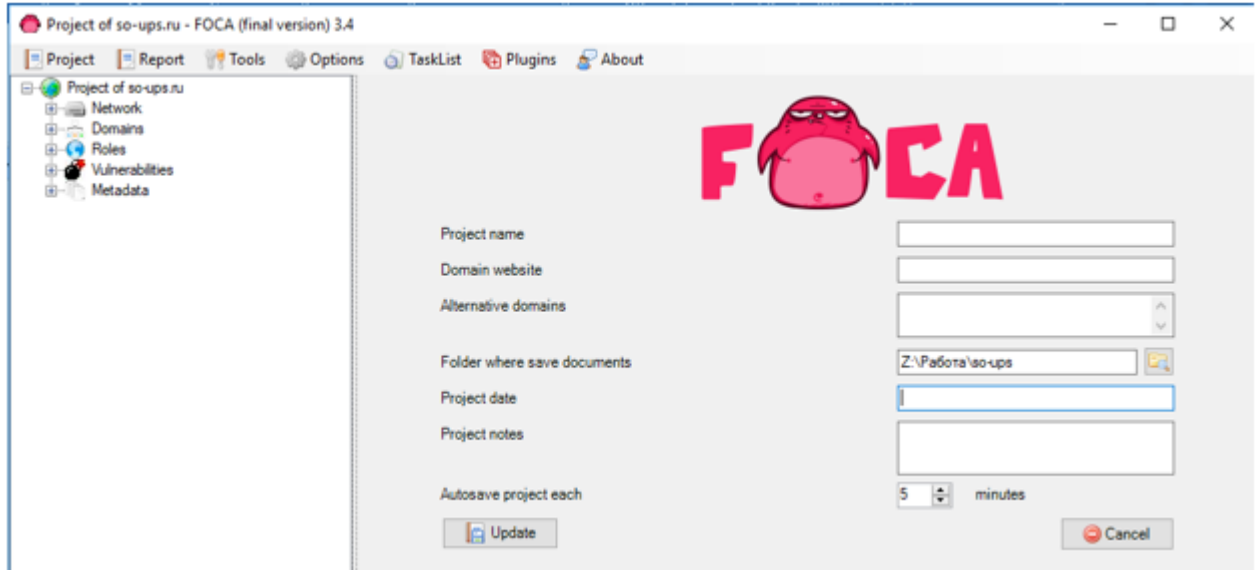
Инструкция к ПО FOCA

1. Чтобы провести исследование с помощью ПО FOCA необходимо запустить исполняемый FOCA.exe.



2. Если появится всплывающее окно предупреждение о безопасности, нажмите ***Run***.

3. Появится главное окно FOCA.



- Еженедельная проверка внешних данных по системам Общества
- Дополнение метаданных и новых индикаторов по итогам аудитов-пентестов

Поиск известных внешних уязвимостей - история

Начало:

- Известный очень позитивный сканер - 1 раз в год
- Использование других сканеров – спорадически
- Попытка Nmap всего периметра (Nmapь меня полностью)

Осознание:

- Ломают и\или пытаются то, о чем знают
- Самостоятельное сканирование - зло
- 80\20

Поиск известных внешних уязвимостей - итог

О нас уже все известно:

- https://www.shodan.io – много возможностей, самая разветвленная сеть сканеров. API.
- https://censys.io/ -аналог. Больше ориентирован на поиск уязвимостей.
- https://www.zoomeye.org/ - китайский аналог.

Не лениться, сделать скрипт:

- Автопоиск по своим сетям информации во всех базах, с учетом частоты обновления информации от сканеров
- Автоматически консолидировать информацию
- Проверять (вручную) с использованием внешних сканеров найденную информацию

To be continued

?_ _?_ _?

Лев Палей
АО «СО ЕЭС»