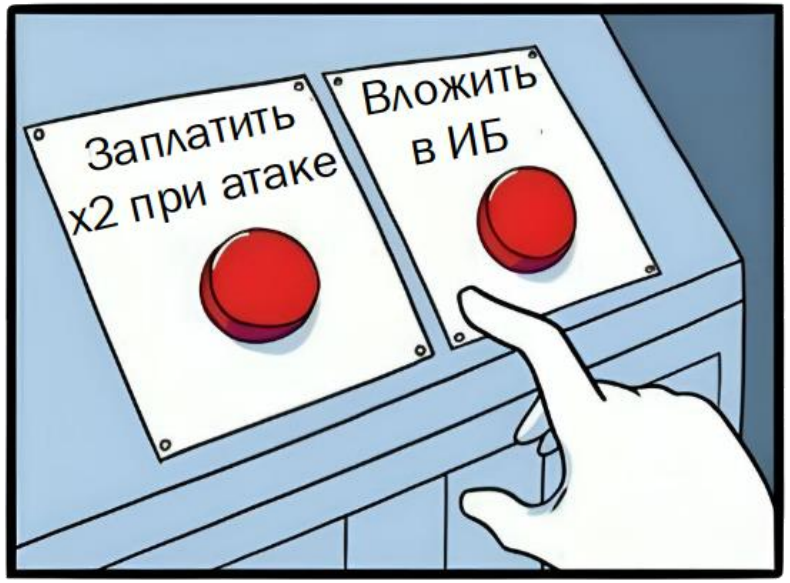
Докладчик:
Иван Ларионов
компания 5.25

КЛЮЧЕВЫЕ ТРЕНДЫ 2023 ГОДА

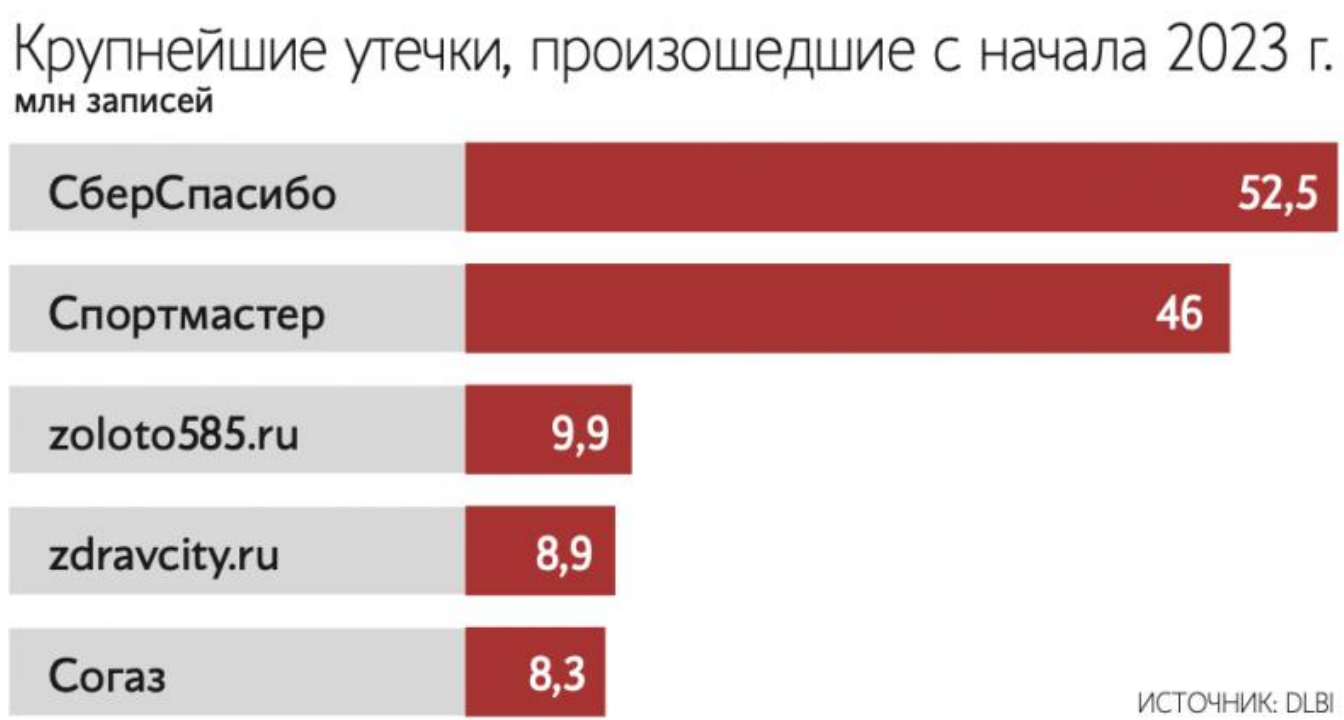
- Подход российского бизнеса сменился с формального на вдумчивый. Произошел массовый уход западных вендоров с российского рынка.
- Атаки стала более персонализированными — мошенники начали применять нейросети и QR-коды для организации целевых фишинговых рассылок.
- 60% компаний финсектора столкнулись с атаками на цепочки поставок.
- Злоумышленники атакуют предприятия госсектора, энергетики, транспорта и других отраслей реального сектора экономики, пытаясь дестабилизировать работу объектов критической инфраструктуры.

РОСТ КОЛИЧЕСТВА АТАК ПОВЛИЯЛ НА ОБЪЕМ ВЛОЖЕНИЙ В ЗАЩИТНЫЕ РЕШЕНИЯ

- Ужесточение законодательства. Штрафы и контроль.
- NGFW (Next Generation Firewall) — межсетевые экраны нового поколения.
- SIEM (Security Information and Event Management) — системы управления информацией и событиями ИБ.
- SOC (Security Operations Center) — центры мониторинга и реагирования на киберугрозы.



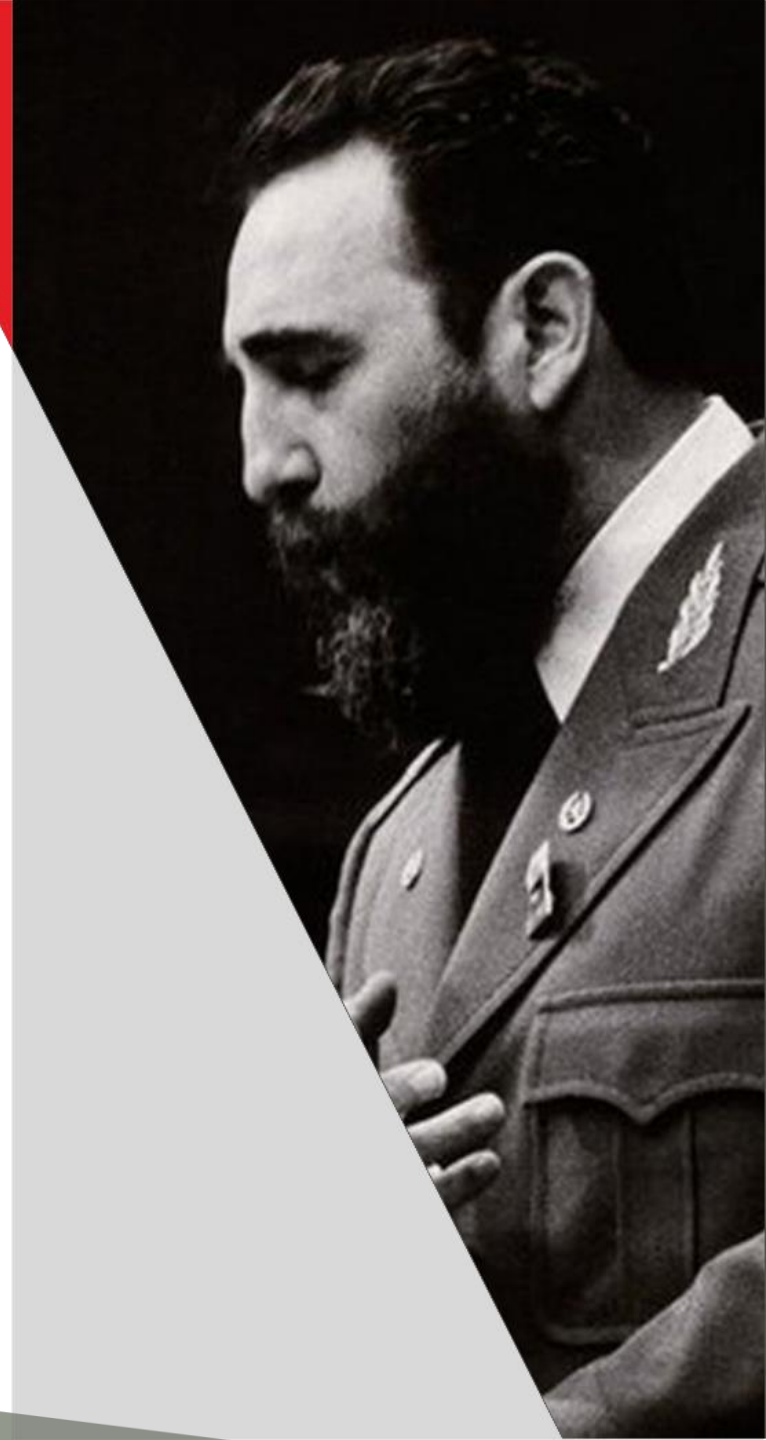
«ЕСЛИ ЗАХОТЯТ – ОБЯЗАТЕЛЬНО УГОНЯТ»



ФИДЕЛЬ КАСТРО

~600
покушений

90 лет
умер своей смертью



ВЫВОД: «Грамотно выстроенная защита все-таки работает»

РЕАЛЬНАЯ БЕЗОПАСНОСТЬ – ЭТО:

- правильные бумаги
- оптимальные продукты
- РЕГУЛЯРНЫЙ КОНТРОЛЬ!!!

КОНТРОЛЬНЫЕ ТОЧКИ ДЛЯ ПРОВЕРКИ ЗАЩИЩЕННОСТИ

- Внешний периметр
- Электронная почта
- Внутренняя IT-инфраструктура
- Персонал

GROUP-IB ESET

Панель управления
Управление
Проблемы
Активы
Граф
Поддержка
Отчеты
Справка

Attack Surface Management

Управление поверхностью атаки на основе данных киберразведки

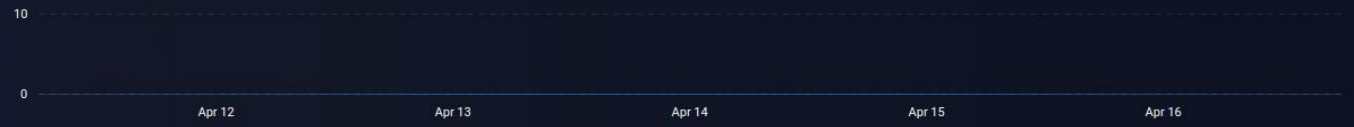
Динамика общей оценки

Обновлено 17 апр. 2023 15:07

Предыдущая оценка 0

Оценка 0

Изменение оценки 0



Выберите период: Все время | С последнего логина | Неделя | Месяц | 2 месяца | Квартал | Год | Свой период 11.04.2023 - 18.04.2023 | ESET

Последние изменения

Подтвержденные активы, связанные с проблемами

14 мар. 2023	ela.eset.com	1 проблема
12 апр. 2023	esac-test.eset.com	1 проблема
07 авг. 2022	int.form.eset.com	1 проблема
11 сент. 2022	notify.eset.com	1 проблема

Новые активы 184 130%

Новые проблемы 373 108%

Решенные проблемы 1654 -30%

Игнорируемые проблемы 0 100%

Динамика оценок по категориям

Всего проблем: Высокая опасность 953 | Средняя опасность 9922

	Оценка	Новые	Всего
Уязвимости	0	27 / 45	145 / 282
Сетевая безопасность	0	1 / 162	5 / 4735
Утечки	0	1 / 3	80 / 12
Вредоносные программы	0	0 / 1	0 / 2977
Упоминания в дарквебе	3.6	10 / 0	24 / 28
Безопасность SSL/TLS сертификатов	0	0 / 99	8 / 1167
Почтовая безопасность	0	8 / 2	579 / 29
DNS и домены	0	3 / 11	112 / 692

Карта активов

Активы, обнаруженные для вашей компании, на мировой карте

PT Knockin

Сервис для проверки защищенности эл. почты

Введите адрес корпоративной почты

Эл. почта

Я принимаю условия использования сервиса

Я даю согласие на получение рекламных и информационных сообщений

positive technologies

REDCheck ДЕЙСТВИЯ ИНСТРУМЕНТЫ СПРАВКА

ГЛАВНАЯ | ХОСТЫ | ЗАДАНИЯ | ИСТОРИЯ | КОНТРОЛЬ | ОТЧЁТЫ

Аудит обновлений

Топ обновлений по количеству — Топ 10

- Обновление USN-4154-1 -- уязвимость Sudo
  OVALDB | USN-4154-1 | CVE-2019-14287
- Обновление USN-4710-1 -- уязвимость Linux kernel
  OVALDB | USN-4710-1 | CVE-2020-25704
- Обновление USN-5378-2 -- уязвимость XZ Utils
  OVALDB | USN-5378-2 | CVE-2022-1271
- Обновление USN-5463-1 -- уязвимости NTFS-3G
  OVALDB | USN-5463-1 | CVE-2021-46790 | CVE-2022-30783 | CVE-2022-30784 | CVE-2022-30786 | CVE-2022-30788 | CVE-2022-30789 | CVE-2022-30785 | CVE-2022-30787
- Обновление USN-5473-1 -- обновление ca-certificates
  OVALDB | USN-5473-1
- Обновление USN-5766-1 -- уязвимость Heimdal
  OVALDB | USN-5766-1 | CVE-2022-41916
- Накопительный пакет для Windows 10 и Windows Server 2016 для систем на базе 64-разрядных (x64) процессоров (KB4284880)
  OVALDB |

Обновлено в 16:30:06 | Обновить

Необновлённые хосты

Топ необновлённых хостов — Топ 10

- 192.168.56.102
  Обновлений : 542
- localhost
  Обновлений : 75

Обновлено в 16:30:05 | Обновить

Аудит уязвимостей

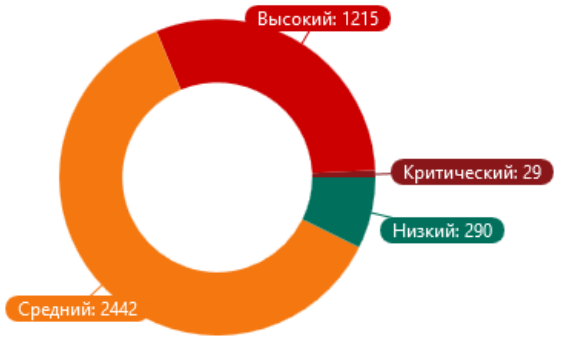
Топ уязвимостей по количеству — Топ 10

- Уязвимость в OpenSSL 3.0.0, 3.0.1, 1.1.1 до 1.1.1m, и 1.0.2 до 1.0.2zc (CVE-2022-0778)
  OVALDB | CVSS 5,0 |
- Уязвимость в OpenSSL 3.0.0, 3.0.1, 3.0.2, 1.1.1 до 1.1.1n (CVE-2022-1292)
  OVALDB | CVSS 10,0 |
- Уязвимость в OpenSSL 3.0.0, 3.0.1, 3.0.2, 3.0.3, 3.0.4, и 1.1.1 до 1.1.1p (CVE-2022-2097)
  OVALDB | CVSS 5,0 |
- Уязвимость в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t (CVE-2023-0286)
  OVALDB | CVSS |
- Уязвимость в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t (CVE-2023-0215)
  OVALDB | CVSS |
- Уязвимость в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t (CVE-2022-4450)
  OVALDB | CVSS |
- Уязвимость в OpenSSL 3.0.0 до 3.0.8, и 1.1.1 до 1.1.1t (CVE-2022-4304)
  OVALDB | CVSS |

Обновлено в 16:30:07 | Обновить

Распределение уязвимостей по уровням риска

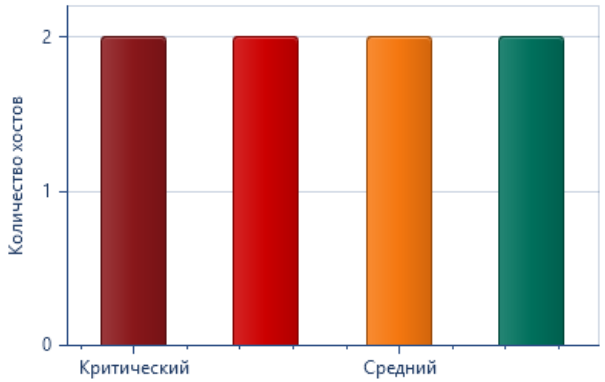
Использованы данные на основе всех актуальных сканирований



Обновлено в 16:30:07 | Обновить

Распределение уязвимостей по хостам

Использованы данные на основе всех актуальных сканирований



Уязвимые хосты

Топ уязвимых хостов — Топ 10

- localhost
  Уязвимостей : 2181
- 192.168.56.102
  Уязвимостей : 1795

Обновлено в 16:30:07 | Обновить

Синхронизация: не удалось подключиться к серверу синхронизации

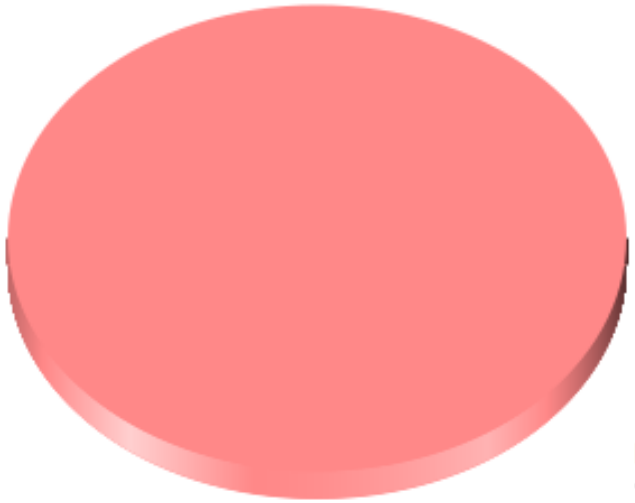
2.6.9.6467

Kaspersky Security Center

Отчет об уязвимостях

Апрель 2, 2024 18:06:03

Отчет об обнаруженных уязвимостях ПО. Отчет формируется для группы: "Управляемые устройства"



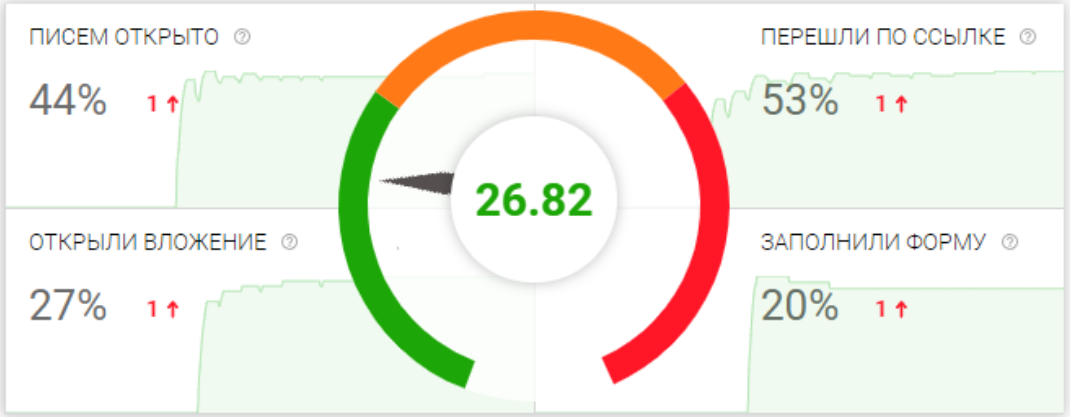
Количество устройств:

- Устройств без уязвимостей: 0
- Устройств с уязвимостями средней критичности: 0
- Устройств с уязвимостями высокой критичности или высокой и средней критич...: 0
- Устройств с уязвимостями предельной критичности или высокой и любой друго...: 3

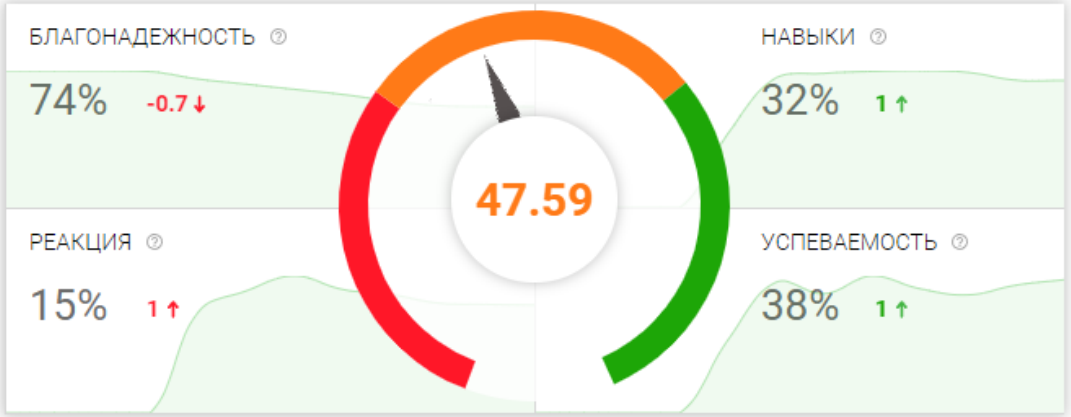
ГЛАВНАЯ

Неделя | Месяц | Год

Уровень риска: низкий



Уровень устойчивости: приемлемый



ОХВАТ АУДИТОРИИ

Всего сотрудников атаковано: 2000

Атаки с ссылками: 2000

Атака с фишинговой формой: 1998

Атаки с вложениями: 2000

ЭФФЕКТИВНОСТЬ ОБУЧЕНИЯ

Всего назначено: 16099

Курсов завершено: 1474

Курсов пройдено: 1926

Курсов забыто: 12699

КАК СДЕЛАТЬ ЭТО БЫСТРО и БЕСПЛАТНО?

www.5-25.ru

Есть ли в зале представители следующих городов и территорий? Для вас есть анализ поверхности атаки.

1. Астрахань
2. Волгоград
3. Грозный
4. Краснодар
5. Магас
6. Майкоп
7. Махачкала
8. Нальчик
9. Ростов-на-Дону
10. Ставрополь
11. Черкесск
12. Элиста

1. Адыгея
2. Астраханская область
3. Волгоградская область
4. Дагестан
5. Ингушетия
6. Кабардино-Балкария
7. Калмыкия
8. Карачаево-Черкесия
9. Краснодарский край
10. Ростовская область
11. Ставропольский край

www.5-25.ru

5.25

СТЕНД №2

Иван Ларионов

компания 5.25

www.5-25.ru | ib@5-25.ru | 8 8512 525-525

Тел. 8 800 30 25 525