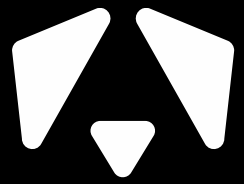


ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Найти
Улучшить
Повторить

Алексей Васильев, Руководитель Центра мониторинга

Вы следите за угрозами?

The Shadow Brokers — Lost in Translation

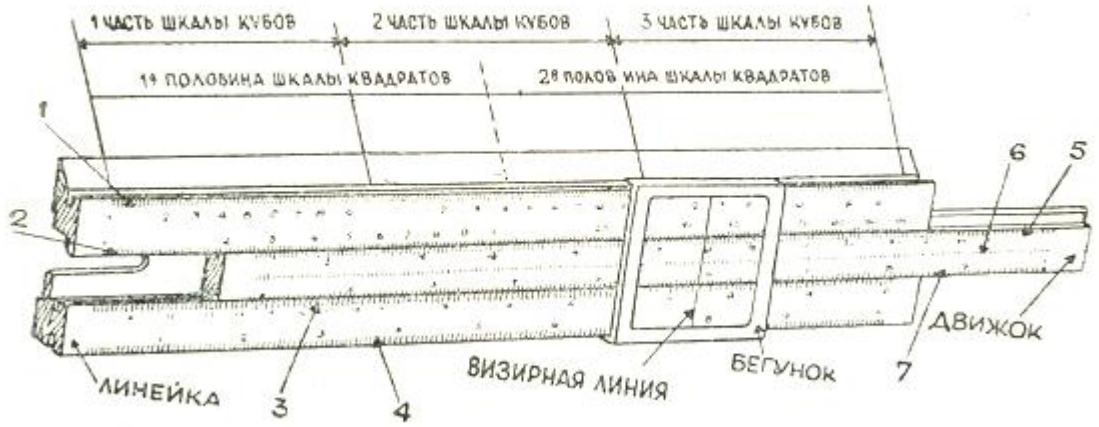
Доступные всем источники открывают вашу инфраструктуру!

Microsoft Security Bulletin MS17-010

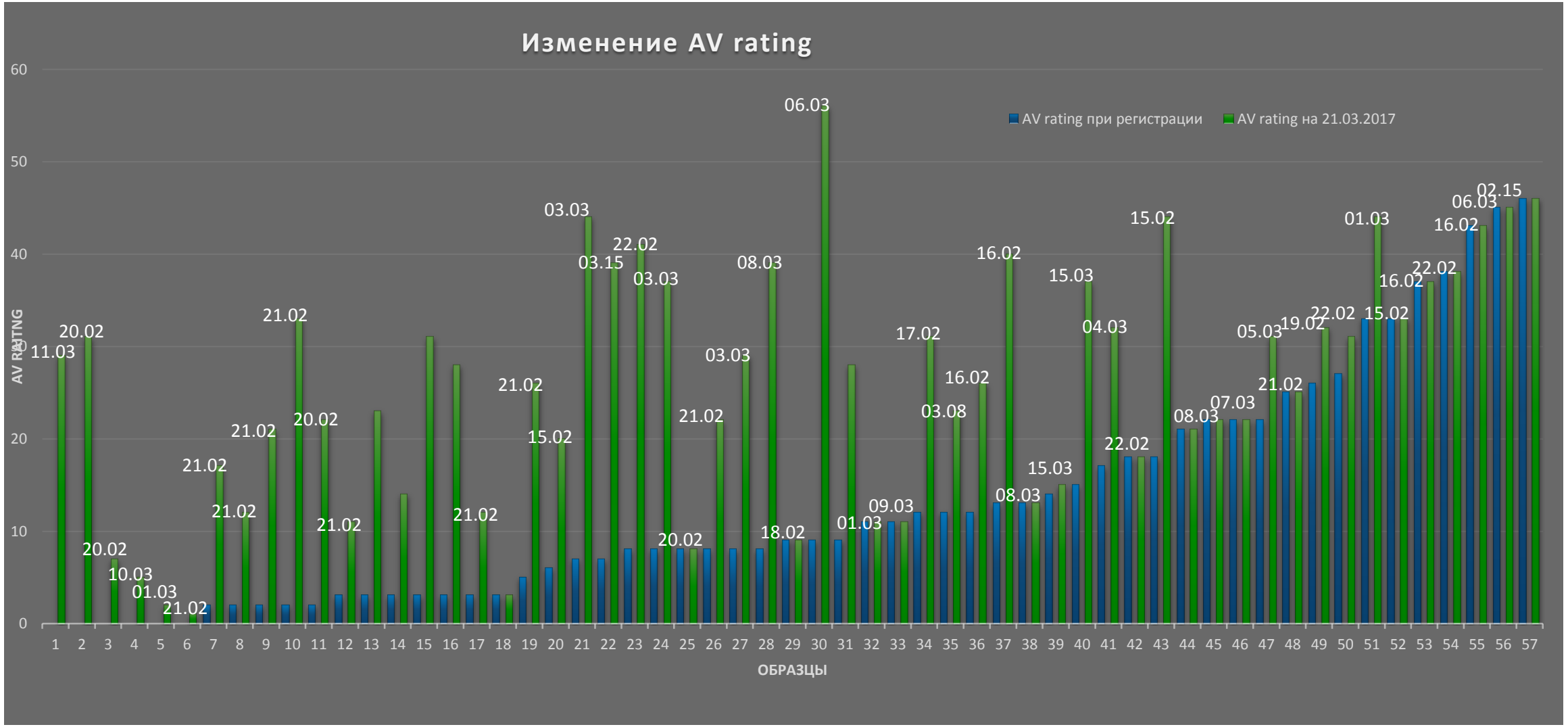
AM Rules для IDS NS/HS детектирует попытки эксплуатации через 2 часа

Выбор источников данных об угрозах

- Построение системы обработки информации
- Анализ
- Оценка
- Применение полученных данных



Анализ угроз



Зачем нужна Threat Intelligence

Определение стратегии и тактики противодействия

- Скорость
- Предупреждение
- Готовность принять решение

Приоритизация и управление

Предупреждение с учётом изменения ландшафта угроз

Источники данных Threat Intelligence

Обновляемые данные	Накапливаемые данные	Инструменты, техники и процедуры
50+	50+	300+
URL, IP, Domain	Hash	TTPs

Результаты Threat Intelligence

Правила для сетевых IDS	200 в месяц
Правила для хостовых IDS	200 в месяц
Хэши вредоносного ПО	30 млн.
База данных IP, URL, Domain	10 млн.
Модель выявления угроз	Регулярно перестраивается

Не только SIEM`ply собрать информацию

Сбор

Корреляция

Анализ

Сохранение

Что огранивает ВАС в принятии решения по событиям?

Логи / события / инциденты

Классика

Инциденты =
настройка логов +
анализ событий +
индикаторы компрометации

Новая классика

Инциденты =
(настройка лога + анализ событий) X
Threat Intelligence

Сбор информации, управление событиями

Сбор логов
Анализ логов
Корреляция событий
Расследование по логам
Стандарты
Контроль доступа
Предупреждение в реальном времени
Мониторинг активностей пользователей
Визуализация
Отчётность
Мониторинг целостности файлов

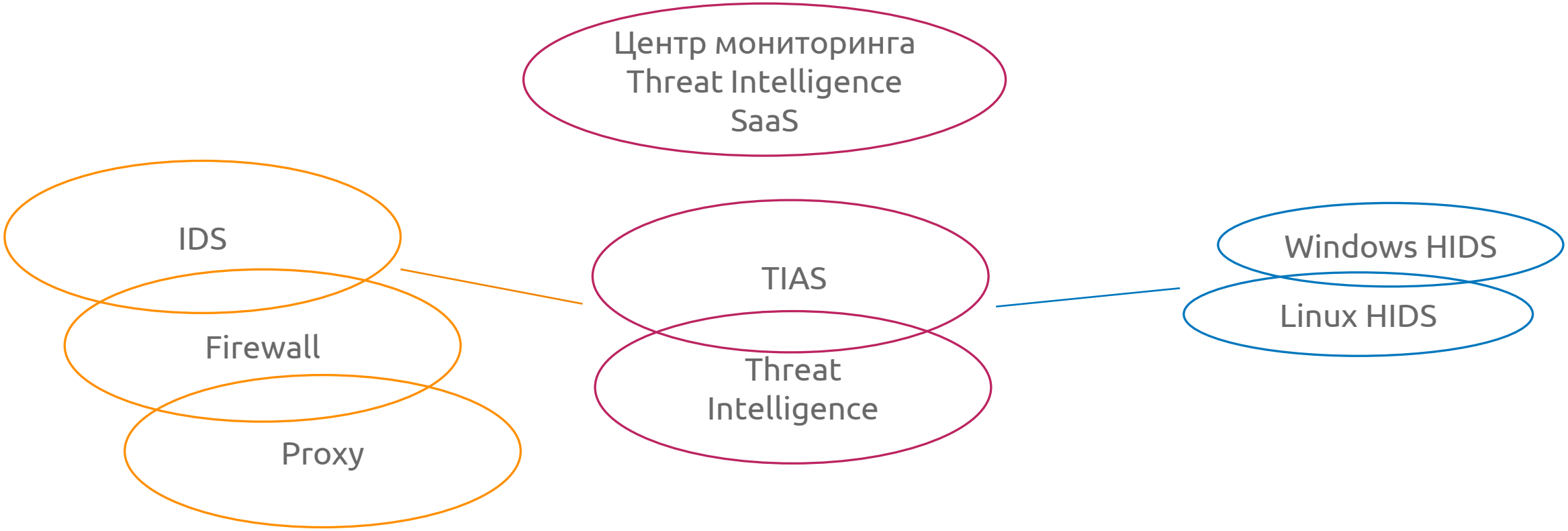
X Threat Intelligence


ОСТОРОЖНО!
ТАМ ИГОЛКА

TI оптимизирует работу с данными

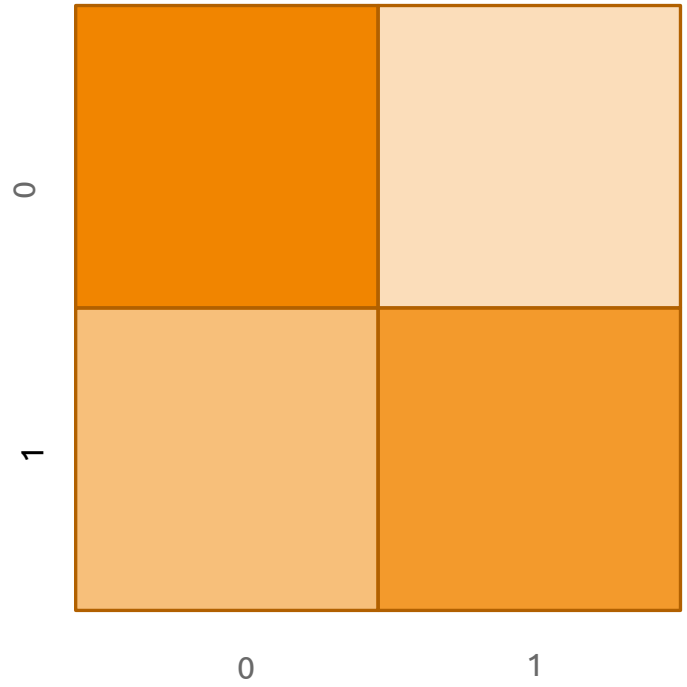
- Не нужно выбирать между масштабом / глубиной / скоростью обработки событий
- Ускоряет анализ
- Учитывает изменения и обновления источников
- Снижает количество false-positive срабатываний
- Не требуется постоянная настройка правил и адаптация

Экосистема Threat Intelligence



Оценка данных Threat Intelligence

Точность — 0,99



Accuracy = (TP + TN) / (TP + TN + FP + FN)

TIAS — Система выявления угроз

- Интеллектуальный алгоритм выявления инцидентов по событиям СОА/СОВ
- Карточка инцидента (вовлеченные активы, рекомендации и т.д.)
- Интерфейс расследования инцидентов
- Отправка карточки инцидента во внешние системы (Система управления инцидентами и др.)
- Подключение дополнительных источников

HIDS

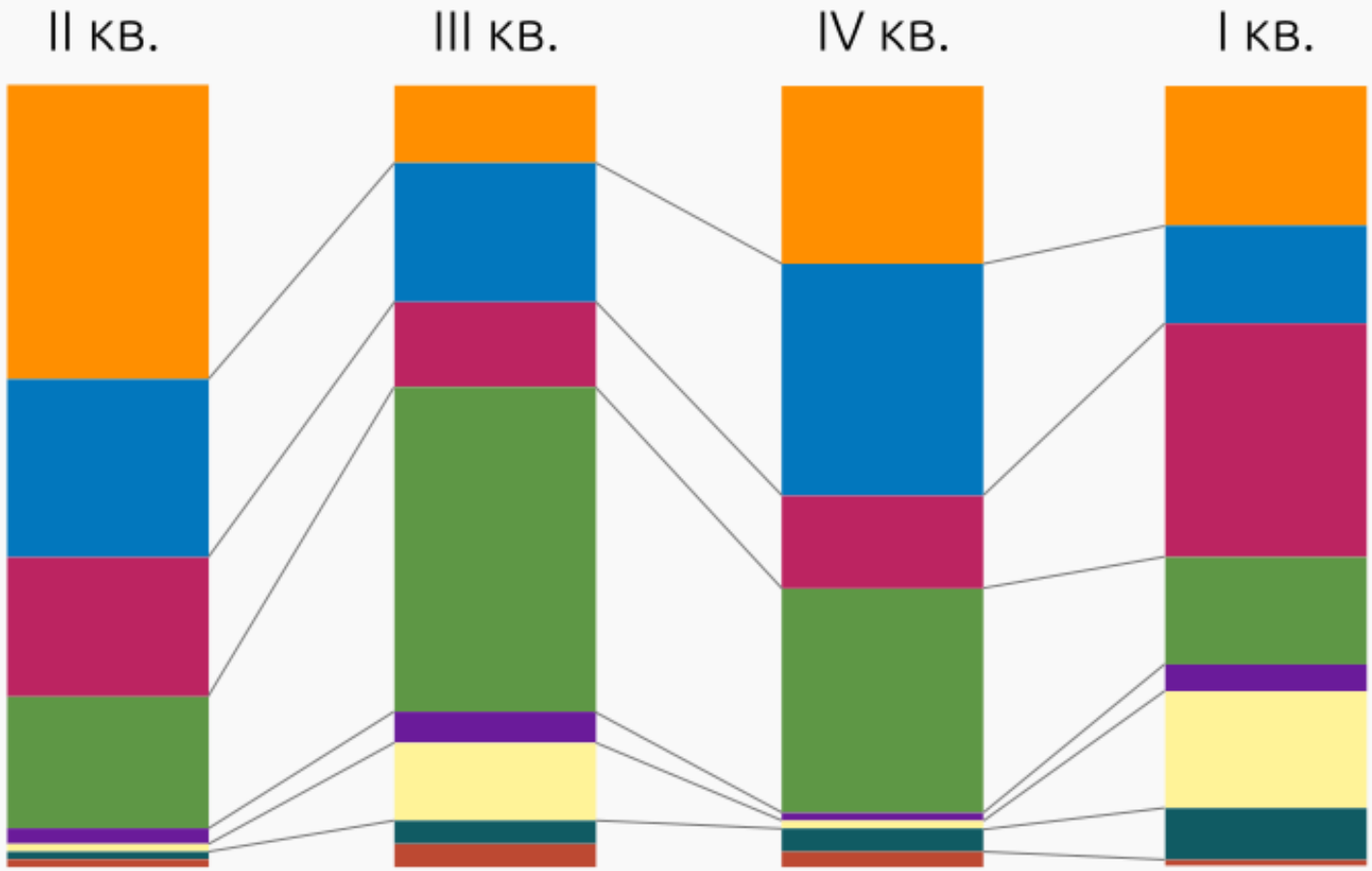
Локальные угрозы

- Закрепление в системе
- Деактивация защитных механизмов ОС
- Повышение привилегий
- Вредоносное поведение

Сетевые угрозы

- Подозрительный трафик
- Подбор паролей
- DNS запросы на разрешение вредоносных, подозрительных доменов

Как менялись доли типов событий ИБ в течение года



Информационное событие

Нарушение политики ИБ

Сканирование

Другое

DDoS

Подбор паролей

Трояны и вирусы

Атака или эксплуатация

amonitoring.ru/astana

Спасибо за внимание!

Алексей Васильев

Начальник отдела разработки и эксплуатации систем мониторинга и аналитики

Руководитель Центра мониторинга

Aleksey.Vasilyev@amonitoring.ru