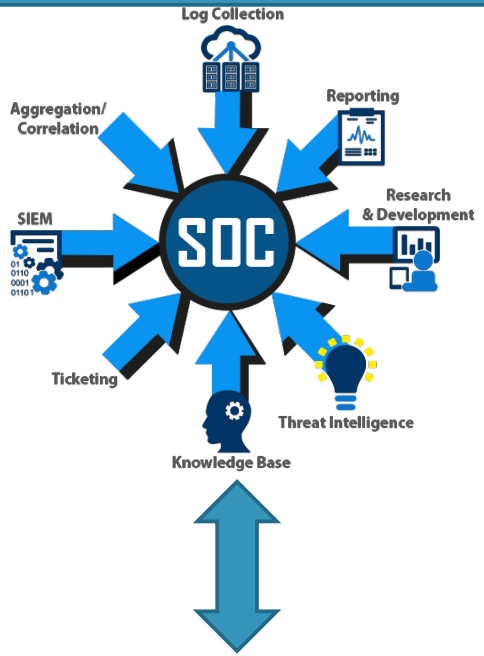
Не совсем про SOC.
или
Можно ли мониторить хаос?

ТОО «TENGRI SECURITY», 2019 Г.

Немного о SOC

Мониторинг событий

Информирование

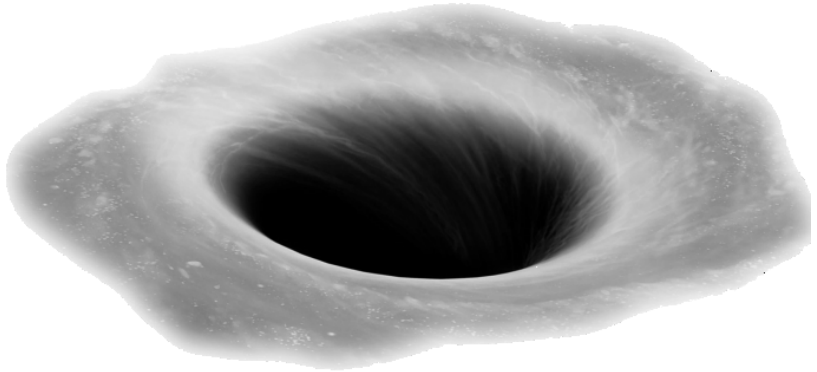


Выявление инцидентов

Анализ

Реагирование

Расследование



«У нас можно ВСЁ!»

- правила корреляции для событий во внутренней инфраструктуре невозможно формализовать;
- легитимная активность пользователей практически не отличается от действий злоумышленника;
- не настроены политики безопасности на целевых системах – может отличаться содержимое однотипных журналов событий, системное время и тому подобное;
- огромное количество false positive, либо «загрубление» правил мониторинга.

Процессы

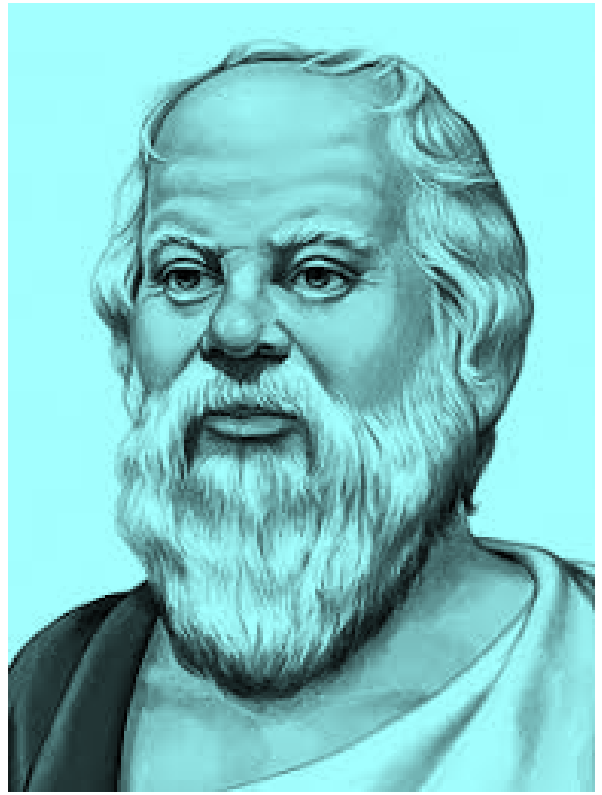
«Это не моя работа!»

- системы не обновляются или обновляются периодически, усложняется поддержка разбора журналов с устаревших систем;
- после изменения конфигураций информационных систем, теряются журналы событий и подключение к SOC;
- реагирование на уже выявленный инцидент растягивается на недели и месяцы.

Люди

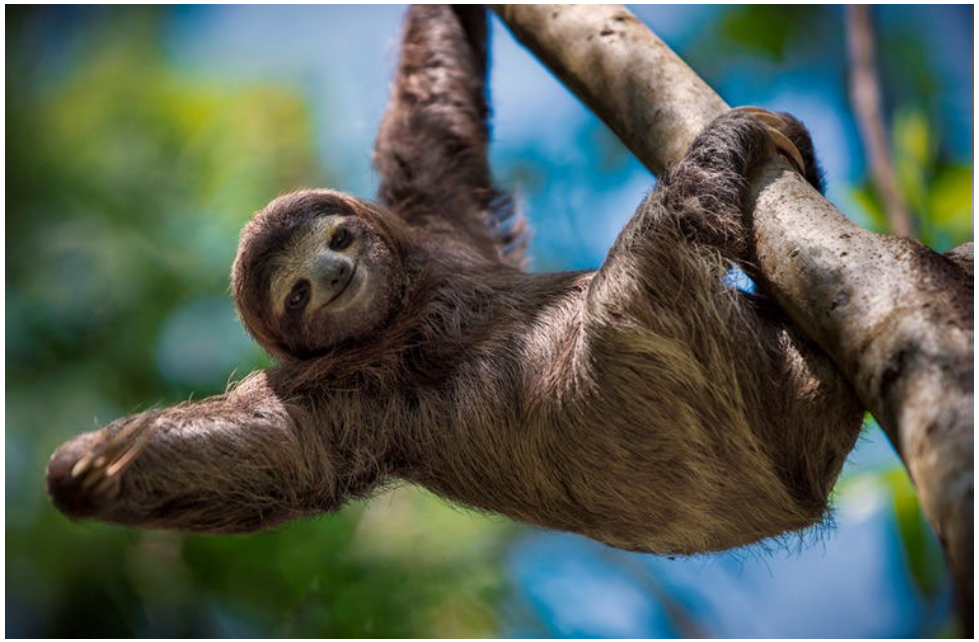
«Я знаю то, что ничего не знаю…»

- невозможность сформулировать задачи для SOC;
- неправильная настройка контролируемых систем, функций журналирования, подсистем передачи журналов в SOC;
- невозможность провести оперативное и/или всестороннее расследование выявленного инцидента.



Культура

«Ну и чт о с т ого!?»



- постоянно повторяющиеся однотипные инциденты;
- уязвимости не устраняются, даже если с их использованием произошла атака;
- если все-таки уязвимости устранены на атакованном узле, остальные узлы остаются с теми же уязвимостями.

Понимание собственной ИТ-инфраструктуры

«Эт о где-т о здесь!»

- не понятно, что подключено к мониторингу, а что нет;
- в случае возникновения инцидента большая часть времени уходит на то, чтобы понять, где проблема;
- потерянные хосты с «букетом» уязвимостей, как лакомый кусочек для злоумышленника.

Системы обеспечения ИБ

«Ну мы же купили SOC!»

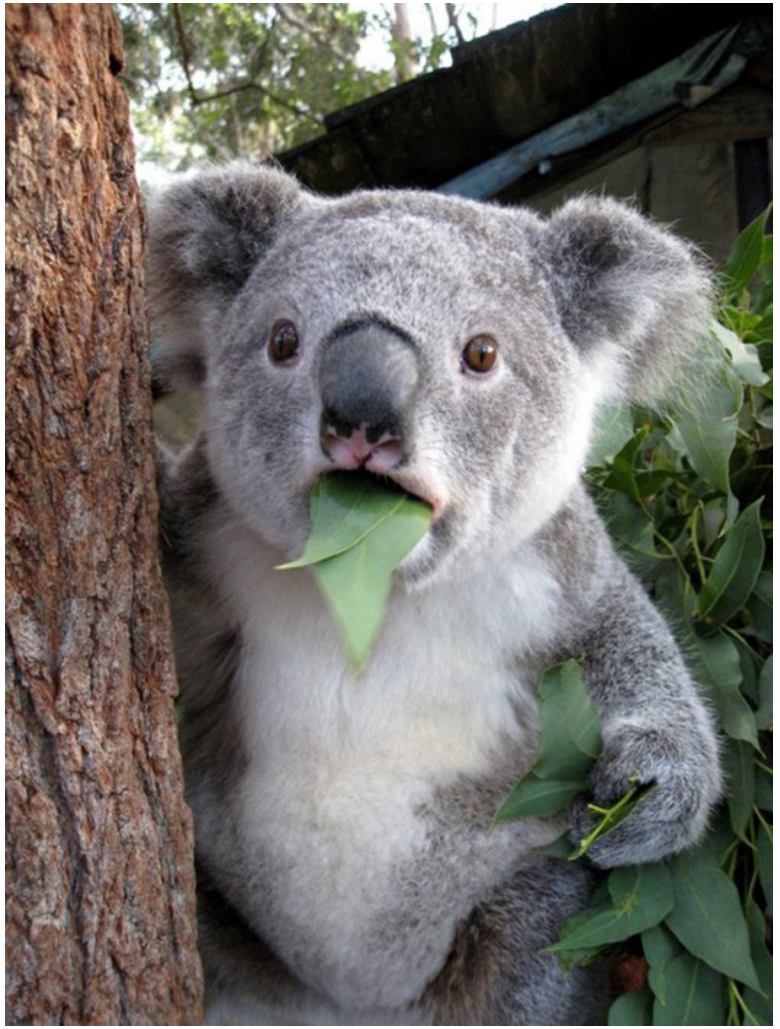
- фактически отсутствует минимальная защита от атак;
- недостаточно журналов событий для своевременного выявления и полноценного анализа инцидента;
- многие атаки не будут выявлены вообще;
- выявленные атаки практически невозможно заблокировать.

Правильно настроенные журналы

«Там чт о-т о записывает ся?!»

Журналы событий:

- либо не поступают вообще;
- либо не полностью;
- либо журналируется абсолютно всё, перегружая и целевую систему, и каналы связи, и системы SOC.



Решение

«Что делать?»

Самостоятельно или с привлечением консультантов довести уровень обеспечения информационной безопасности хотя бы до минимального.

Передать часть функций обеспечения информационной безопасности на аутсорсинг.

НО. Перед этим выделить функции, которые необходимо исполнять самим, исходя из регуляторных требований, внутренних политик и здравого смысла. И…

«И зачем тогда SOC?»

Без централизованной службы мониторинга:

- часть атак может остаться незамеченной, практически однозначно не будут выявлены комплексные целевые атаки (APT);
- выявление, реагирование и расследование инцидента затянется на гораздо больший срок.

Спасибо за внимание

Любое совпадение с реальным положением дел у наших действующих или потенциальных клиентов является случайным!!! 😉