POSITIVE TECHNOLOGIES

Обмен информацией о кибер-угрозах: сказать нельзя промолчать

Владимир Кропотов

Positive Technologies

Как узнать об инциденте

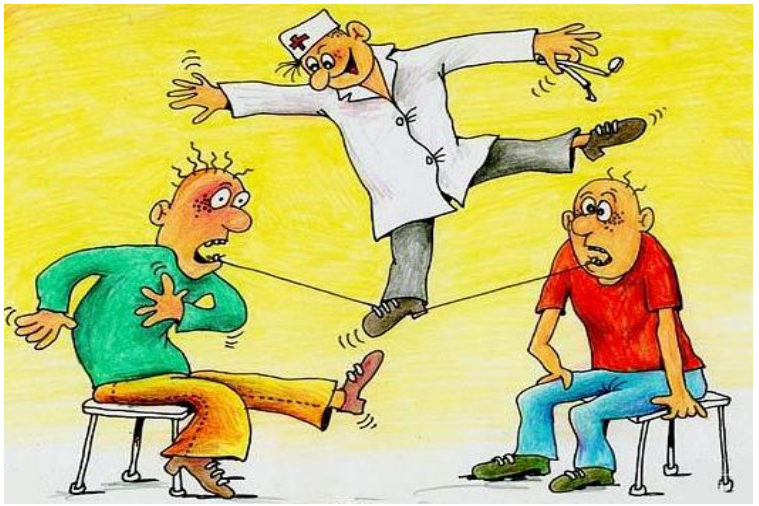
- Выявить
- Почувствовать
- Вас тихо “Порадуют”
- Вас громко “Обрадуют” (пресса, twitter, соц.сети…)

Цели присутствия

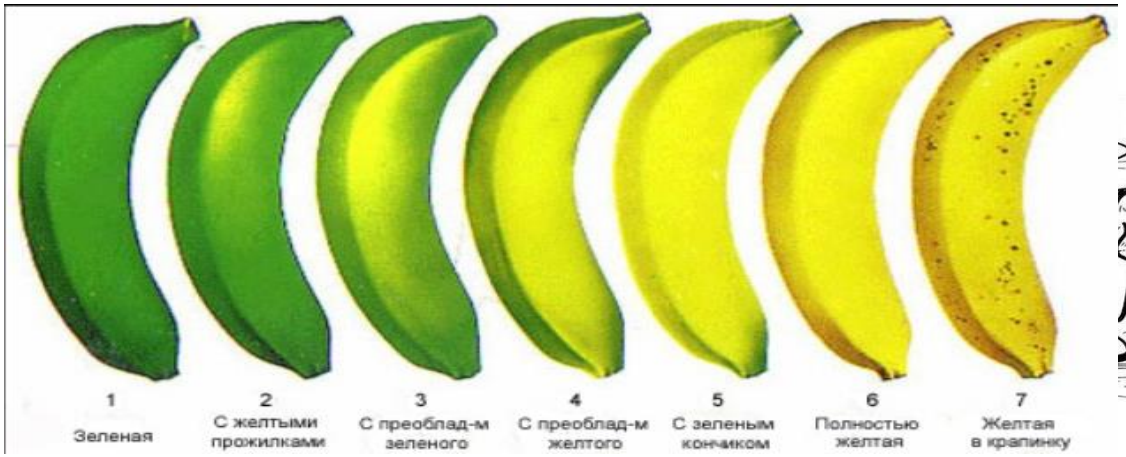
- Решение тактических задач
  - Достижение результатов, связанных с конкретным субъектом-целью
  - Достижение целей, связанных с предшествующим или наступающим событием (получение преимуществ в переговорах)
- Стратегическое долговременное присутствие

Целевая аудитория

- Patient 0 - В этот раз не Ваш день
- Patient 1 - Отчасти повезло
- Patient 2 - (В этот раз) Сторонний Наблюдатель
- “Доктора-Координаторы”



Зрелость приходит, когда возникает понимание, что *в каждый момент организация может оказаться в любой из ролей*



Модель угроз

Защищающиеся

Атакующие

* Картинки взяты с
http://alekskrasnov.blogspot.ru/2012/02/blog-post_14.html
http://lukatsky.blogspot.ru/2015/02/blog-post_17.html

Эксплуатация уязвимостей атакующих защищающимися

- Высокотехнологичный инструментарий часто эволюционирует, редко революционирует
- Затраты на обучение персонала
- Привычки
- Многократное использование вместо полностью атомарных операций (аналог одноразового блокнота)

Что отдают и получают

- Стратегическая информация об угрозах
- Операционная информация об угрозах
- Тактическая информация об угрозах
- Техническая информация об угрозах

Как отдают и получают: Уровень автоматизации обмена

- По запросу (ищем постфактум)
- Ручной
- Ручной с форматированием
- Автоматизированный пассивный
- Автоматизированный активный

Примеры: сказать нельзя промолчать

- Отдал не то
- Отдал не тому
- Отдал не тогда
- Получил

accounts.facbook.com.continuelogs.info
accounts.yandex.ru.continuelogs.info
accounts.ymail.com.mailcache.info

140e8b63cf23e0cbe1dc7c927430b153
D:\Classified\Breaches\JSC Critical infrastructures\styles.css

13:54:38	dvp	C:\Program Files\Outlook Express\msimn.exe	Fw: Директору Департамента
13:55:25	dvp	C:\Program Files\Outlook Express\msimn.exe	Отправленные - Outlook Express - DVP
13:55:29	dvp	C:\Program Files\Outlook Express\msimn.exe	Удаленные - Outlook Express - DVP

Вопросы?

Спасибо!

POSITIVE TECHNOLOGIES