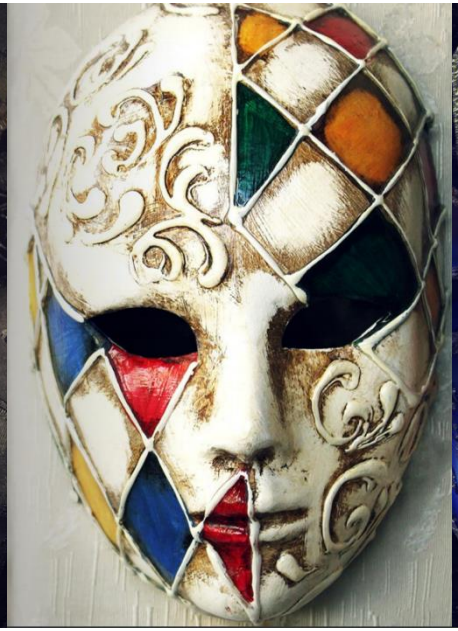
Security Operation Center: роскошь или необходимость?

IT.Integrator

Что происходит

Locky

Cerber



Spora

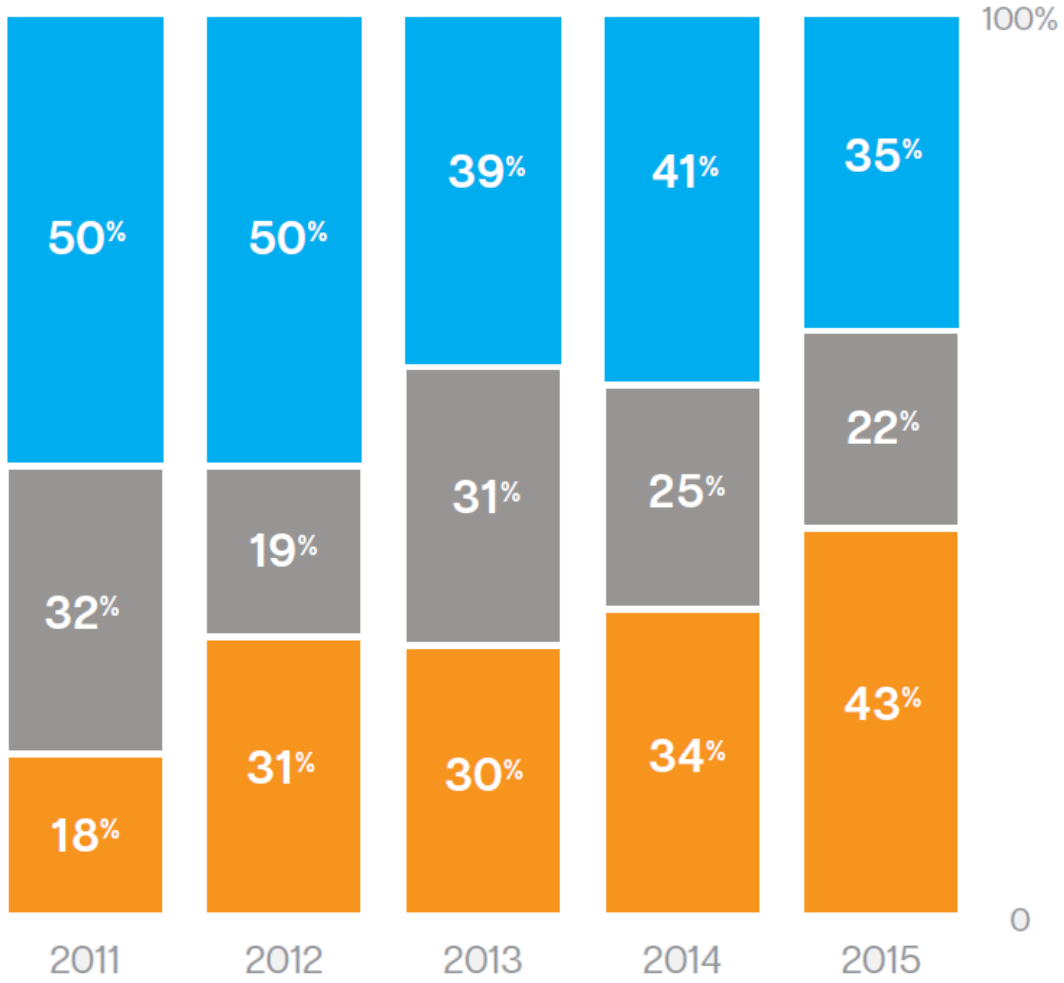
Wannacry

Nyetya

Следующий !

Что происходит

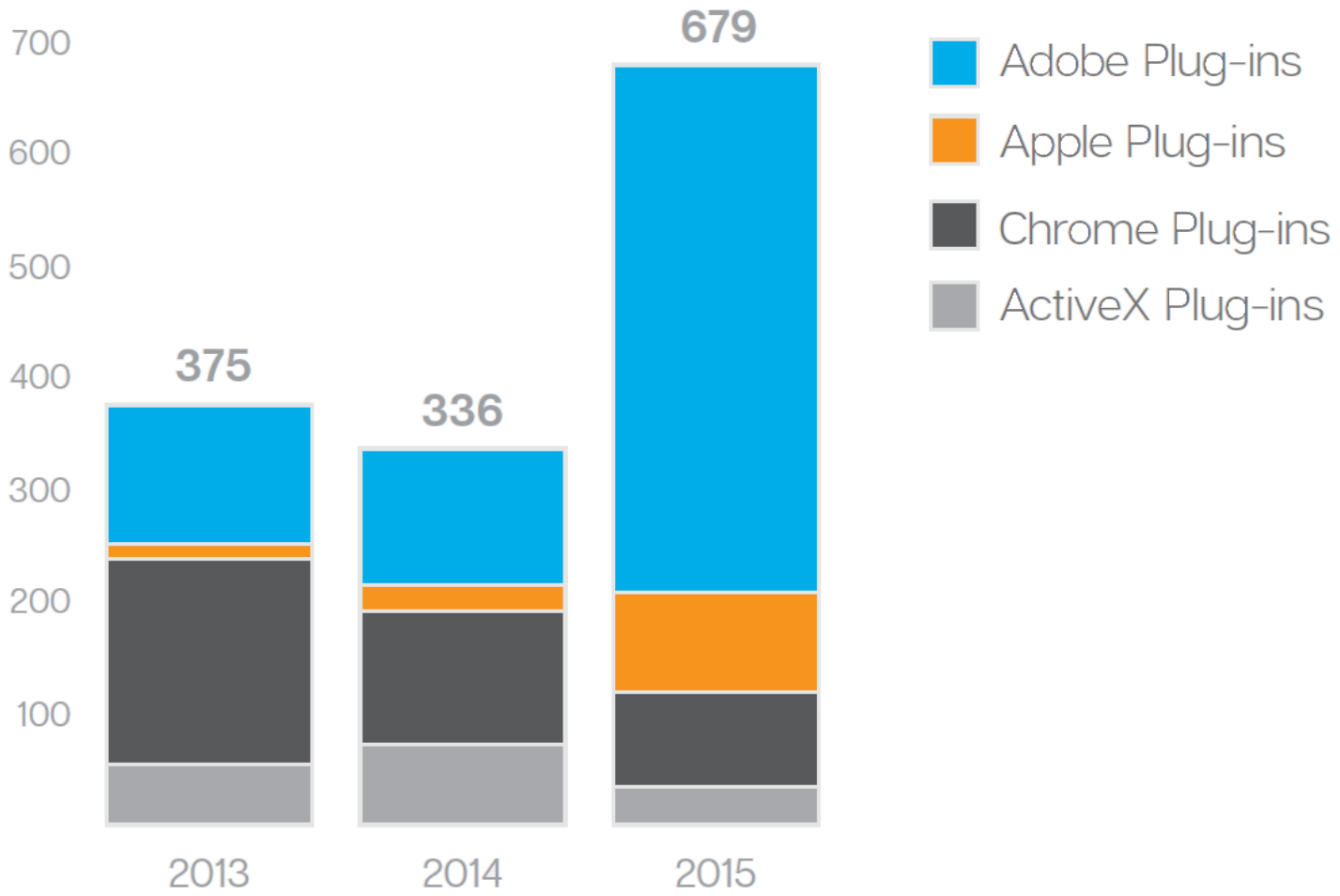
Под прицелом бизнес всех размеров



Исследование **Symantec**

Что происходит

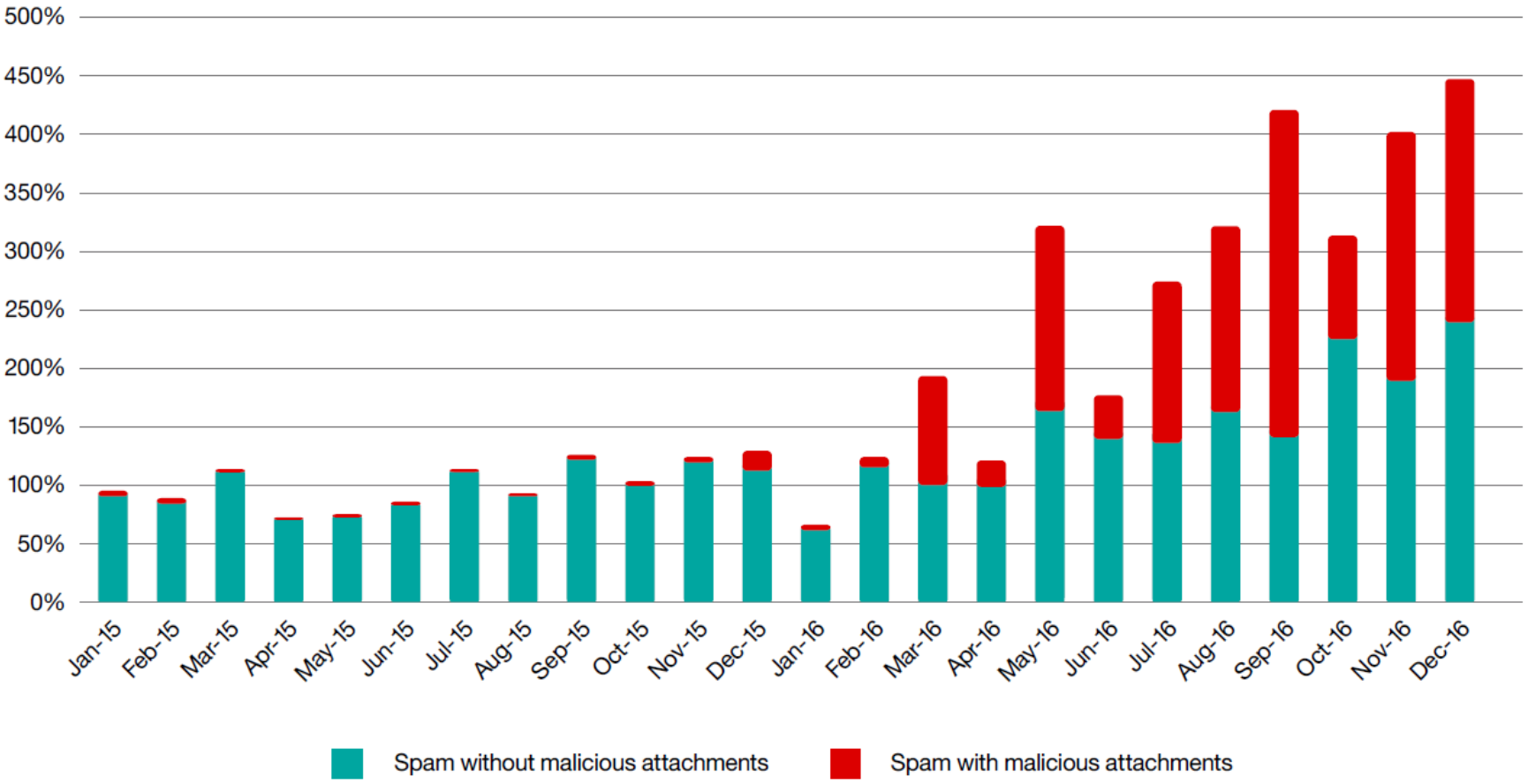
Источник угроз: WEB-браузеры



Исследование **Symantec**

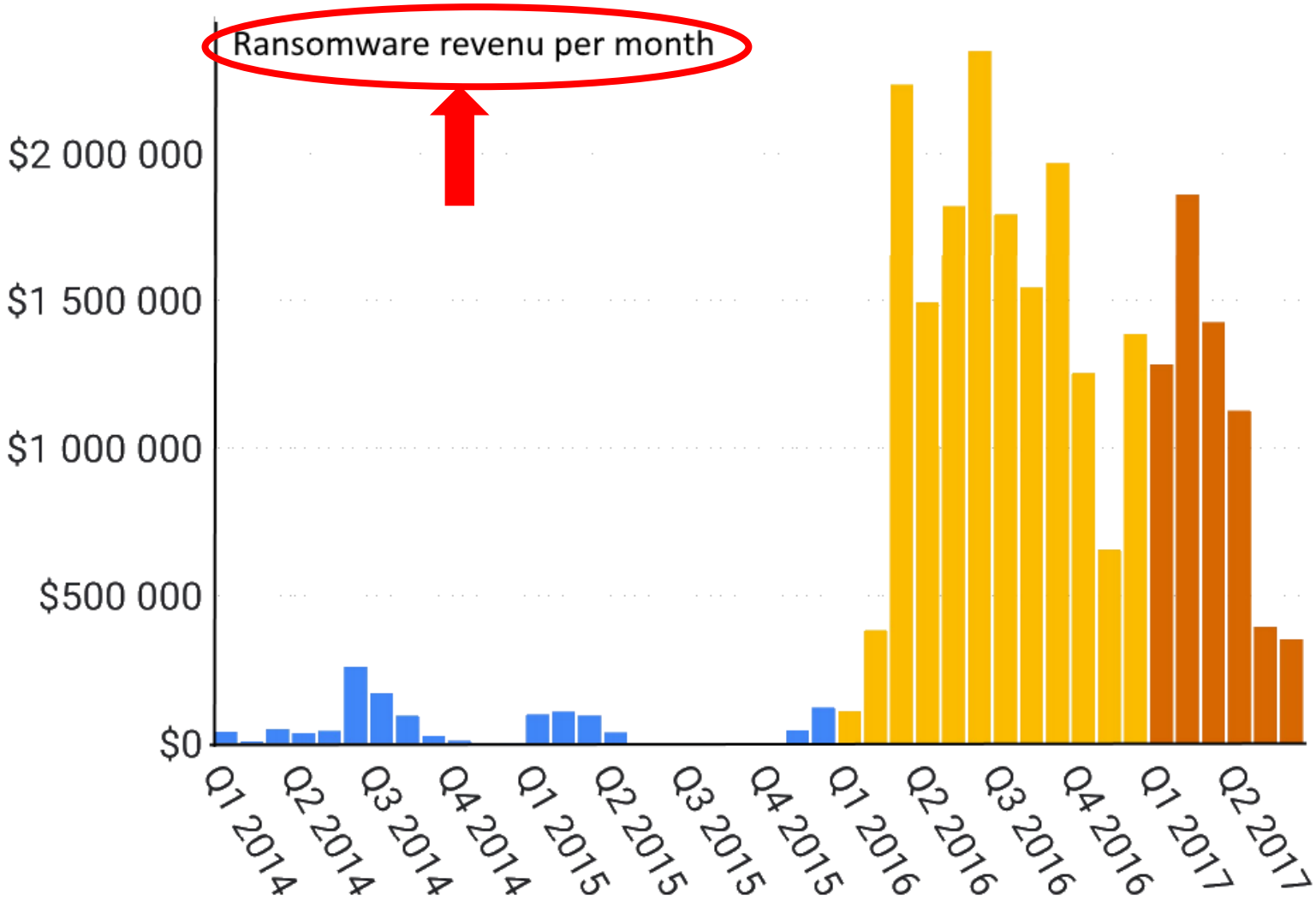
Что происходит

Источник угроз: E-MAIL



Исследование **IBM Security**

Почему происходит



Исследование **Google**

Предпосылки «успеха»

Мы готовимся к уже прошедшей войне

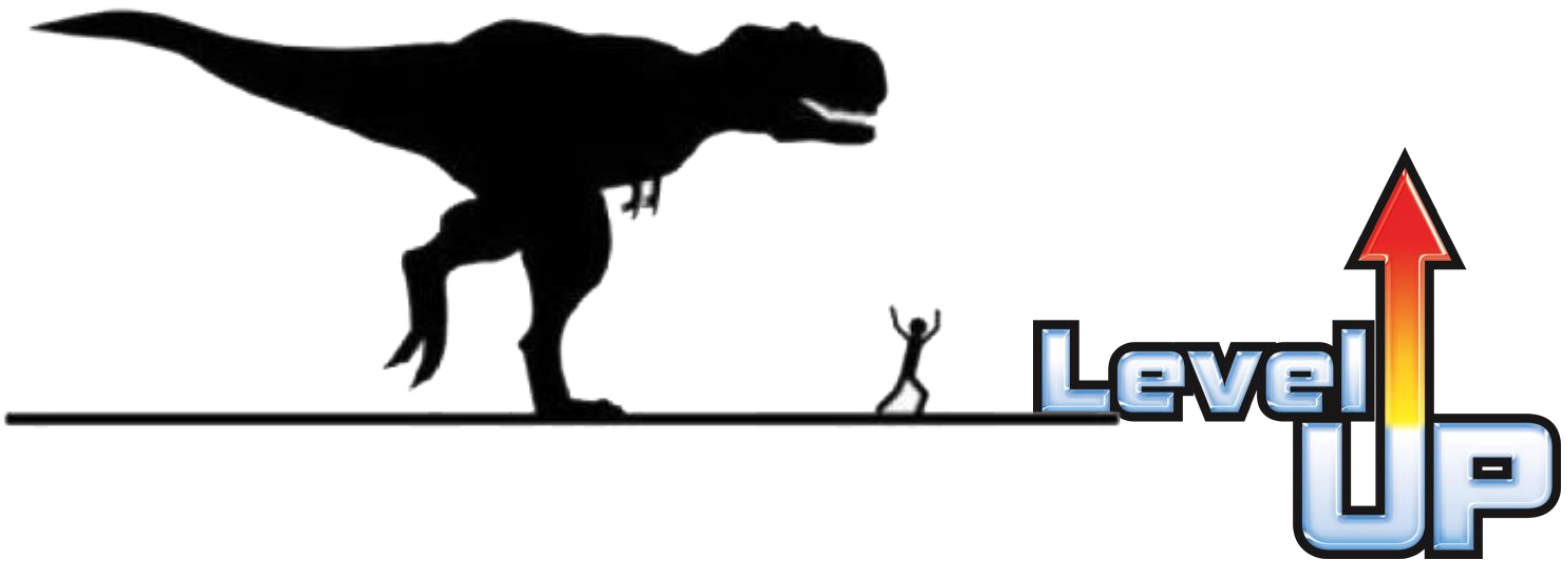
- Известных угроз в общем «пуле» - до 95%
- Действительно опасны - оставшиеся 5%

Нехватка ресурсов

- Неподъёмные объёмы событий для ручного анализа
- Отсутствие квалифицированного персонала
- Отсутствие непрерывности мониторинга
- Отсутствие единой точки контроля

Отсутствие как средств, так и процессов:
безопасность НЕ разовая акция !

Что делать ?



Ответ есть

NIST Best Practices:

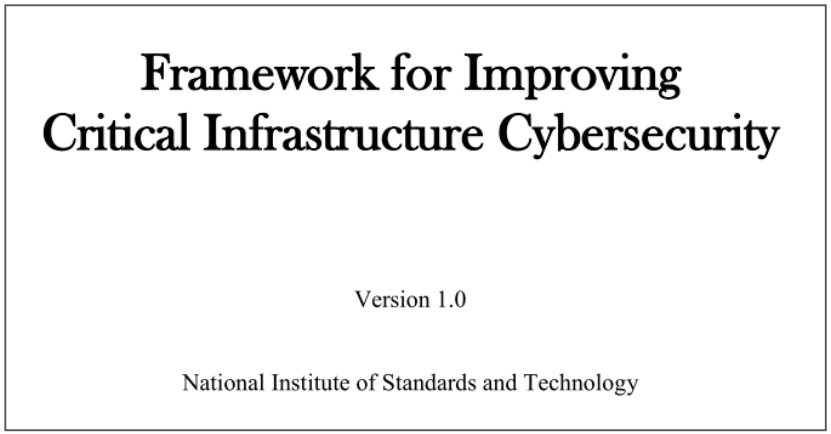
1. Develop your defenses based on the principle that your systems will be breached.
2. Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem.

…


NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

ol and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS),
Control System Configurations such as Programmable Logic Controllers (PLC)


Framework for Improving Critical Infrastructure Cybersecurity

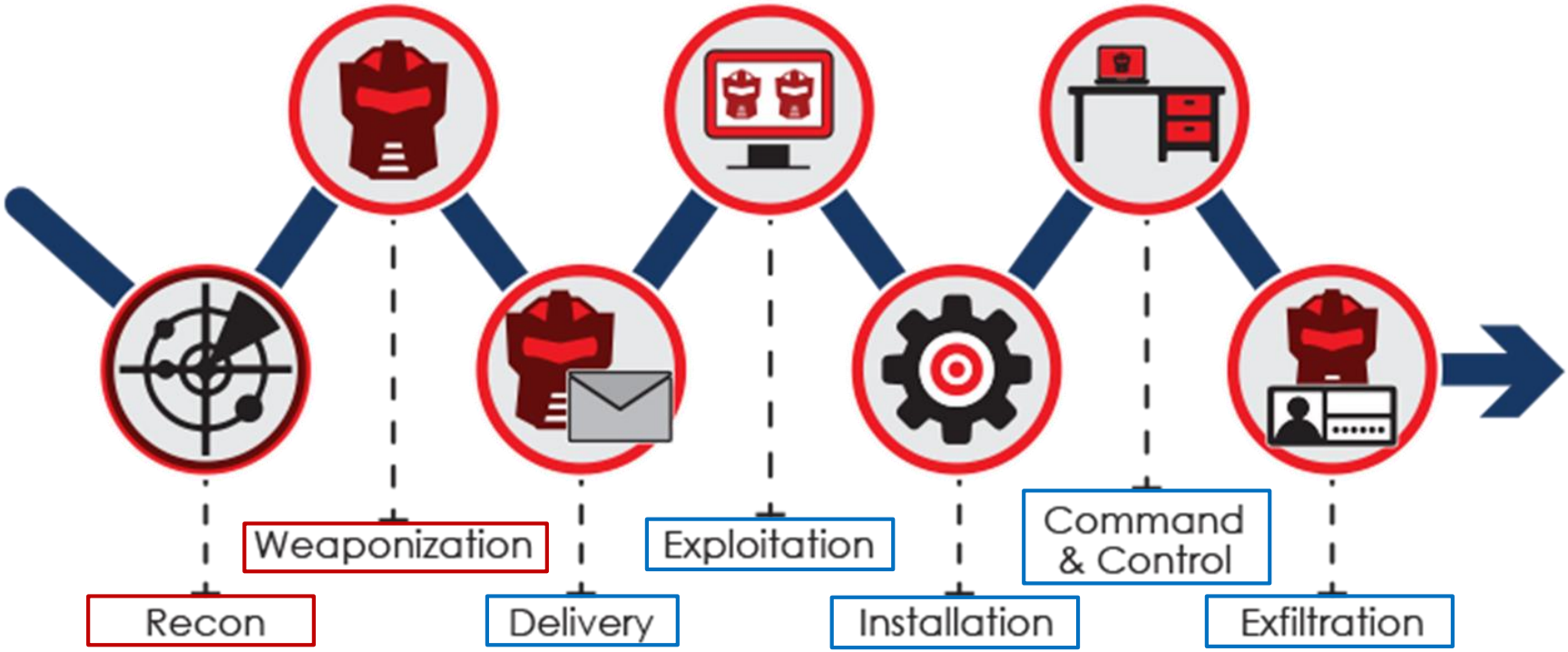
Version 1.0

National Institute of Standards and Technology

Security is a process, not a product. *(Bruce Schneier, CTO of IBM Resilient)*

Ответ очевиден

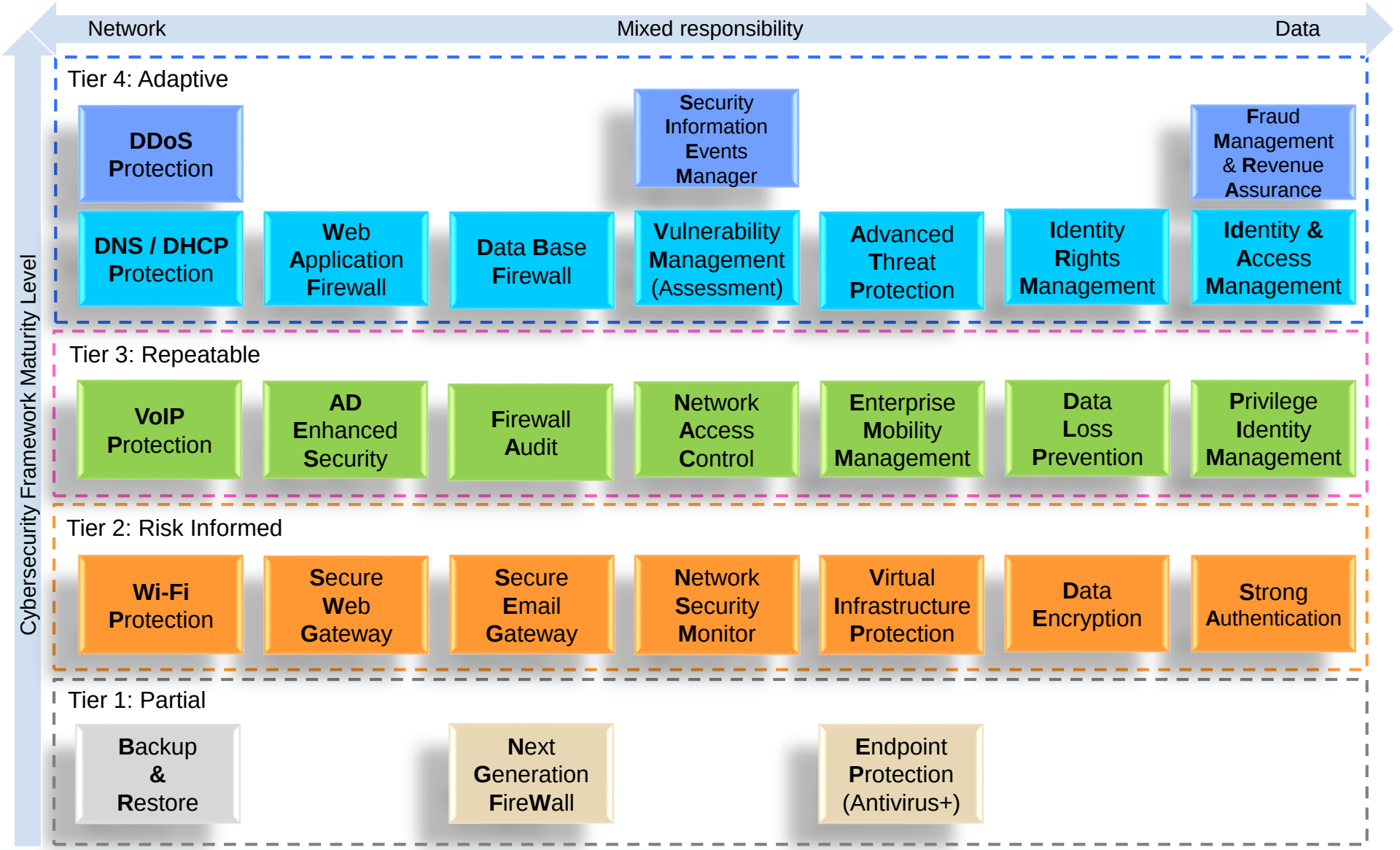
- Любая атака – это цепь событий
- Главное – оборвать **kill chain** !



- вне зоны влияния организации

- в зоне влияния организации

Ответ очевиден ?

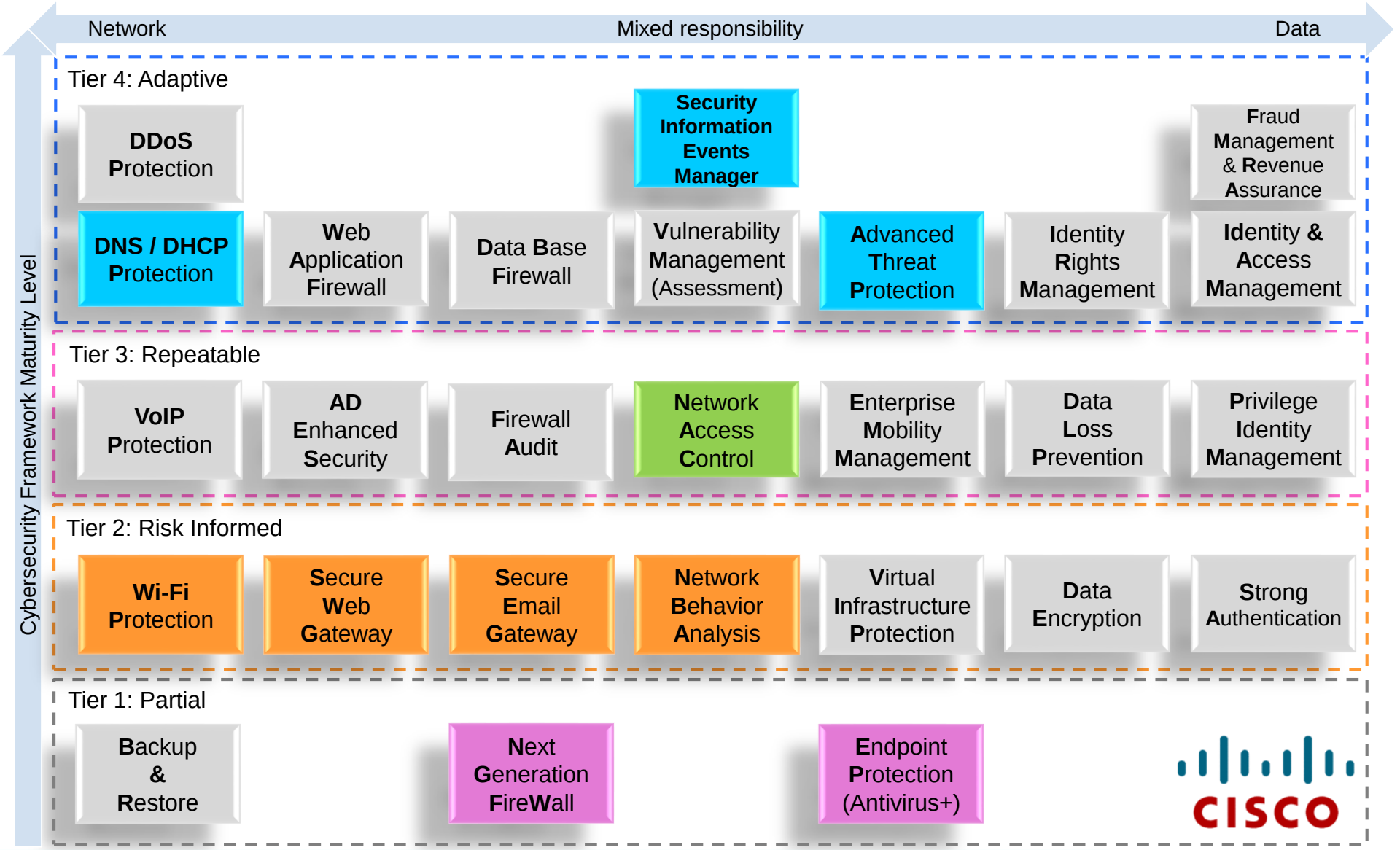


Формула успеха

Security Operation Center

- **Технологии** – оперативное выявление и автоматическое подавление угроз (тех самых «5% опасных»)
- **Процессы** – отлаженные процедуры мониторинга и реагирования, строгие SLA
- **Люди** – квалифицированный персонал, дежурная смена с режимом 24 x 7

Формула успеха - технологии



Формула успеха - технологии

Выявление и автоматическое подавление угроз:

- **Cisco** FirePower
- **Cisco** Web Security Appliance
- **Cisco** Email Security Appliance
- **Cisco** Stealth Watch
- **Cisco** Identity Service Engine
- **Cisco** Advanced Malware Protection
- **Cisco** FirePower Management Center
- **Cisco** Umbrella

Влияние «человеческого фактора» сведено к минимуму

Формула успеха - процессы

SOC – это:

- сбор, хранение и обработка событий ИБ
- выявление и расследования инцидентов ИБ

И ещё вот это:

- управление активами и конфигурациями
- управление уязвимостями

И вот это:

- Cyber Threat Intelligence – разведка и выявление угроз, которые могут вызвать проблемы в будущем
- взаимодействие – с CERT по всему миру, с ответственными структурами в государстве (CERT.ua, СБУ, Киберполиция)

…и многое другое

Точное понимание целей и задач
Строгое соблюдение SLA

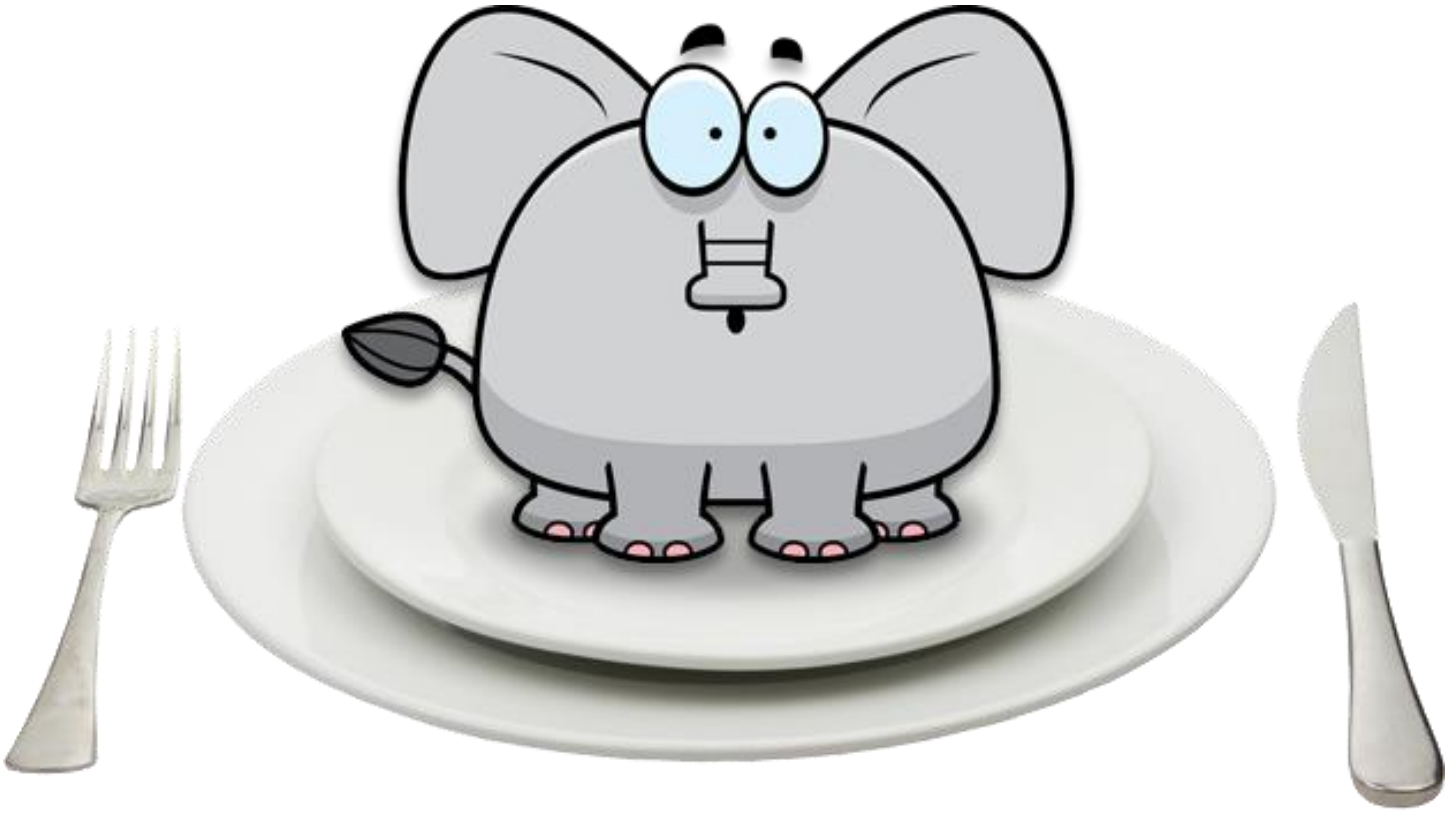
Формула успеха - люди

Необходимые категории персонала:

- **Security Analytics**
  - расследование высокоприоритетных инцидентов
  - аналитика и отчётность
  - Cyber Threat Intelligence
- **Certified Engineer**
  - доскональное знание внедрённых технологий
  - эффективное администрирование
- **Дежурная смена**
  - первая линия поддержки
  - оперативная реакция на события

Технологии – в умелых руках
Процессы – в непрерывном исполнении

SOC: Step by step



SOC: Step by step

Подводные камни

- Отсутствие владельца процесса или точной цели
- SOC как самоцель
- Нехватка людей для развёртывания и запуска процессов (1-2 специалиста задачу не решат)
- Концентрация на технологиях в ущерб остальному
- Недостаточная полнота охвата задач технологической базой
- Отсутствие формализации процессов и четких SLA

SOC: С чего начать

Оценить текущее состояние

- инвентаризация информационных активов
- инструментальная оценка защищённости
- анализ архитектуры сети и сервисов
- оценка стоимости рисков

Что бы выбрать верное направление движения, необходимо точно знать, где находишься.

Просчитать и запланировать

- технологическую базу SOC
- методологию функционирования SOC
- объёмы трудозатрат персонала на обработку событий и инцидентов
- целевые показатели и KPI

SOC: Итоги

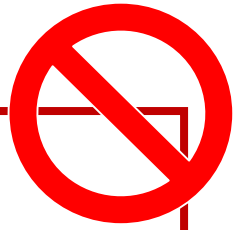
- Мониторинг и уведомление в режиме 24x7
- Обнаружение атак с фокусом на «5% опасных» угроз
- Блокирование атак в реальном времени
- Быстрая адаптация под новые угрозы
- Расследование инцидентов и улучшение защиты

А также:

- Управление уязвимостями
- Антивирусная защита
- Контроль рабочего времени
- Compliance

…и многое другое

SOC: Итоги



Безопасность – убыточная статья.

- Постоянные затраты
- Не понятно, что делает
- Не понятно, как оценить результаты
- Обойдёмся и так

Безопасность – **прибыльная** статья

- Сохранение инвестиций в бизнес
- Непрерывность бизнес-процессов
- Точное понимание стоимости рисков
- Не обойдётесь, см. выше

Мы поможем !

- У нас есть опыт восстановления
- У нас есть опыт предотвращения
- Мы – рядом: *Киев, Днепр, Запорожье, Одесса, Харьков, Мариуполь, Кривой Рог, Полтава, Хмельницкий, Львов, Винница, Николаев, Кременчуг, Луцк, Сумы, Тернополь*

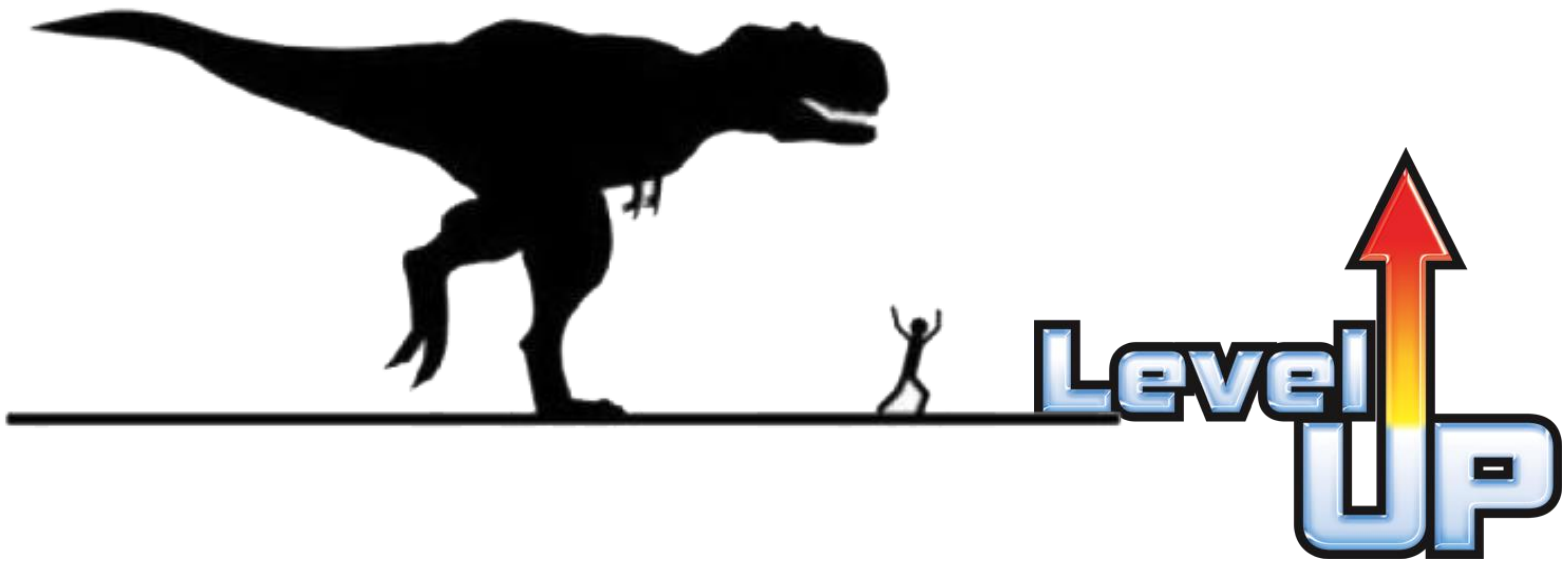
Контакты:

Phone: +38 (044) 538-00-69
Email: info@it-ntegrator.ua
Web: http://it-ntegrator.ua

IT-Integrator

Ваши вопросы ?

Выученный урок



Security Operations Maturity Model

SOMM-уровень	SOC-уровень	Детализация
Уровень 0	Отсутствует	Ключевые составляющие SOC (мониторинг, документирование, SLA) отсутствуют.
Уровень 1	Начальный	«Реагирование по ситуации» (есть мониторинг, нет документированных процессов).
Уровень 2	Базовый	Выполняются все основные нормативные требования с учетом актуальных бизнес-требований. Большая часть процессов документирована, пересматривается по ситуации.
Уровень 3	Надлежащий	Процессы полностью документированы, регулярно актуализируются с учетом «лучших практик».
Уровень 4	Осмысленный	Проводится регулярная оценка эффективности SOC, производится выстраивание процессов для достижения максимальных ключевых показателей эффективности (KPI) бизнеса.
Уровень 5	Максимальный (экстремальный)	Максимальная конкретизация процессов, есть план дальнейшего развития SOC.