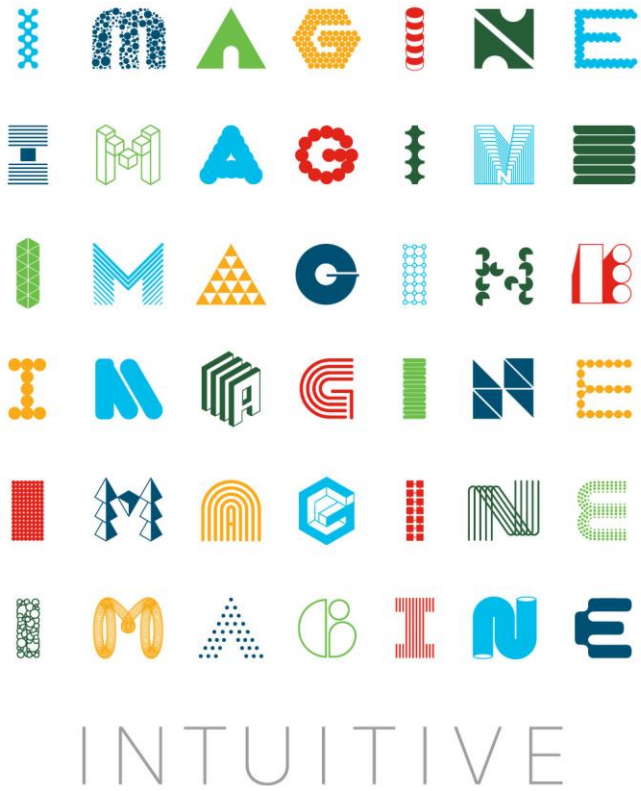
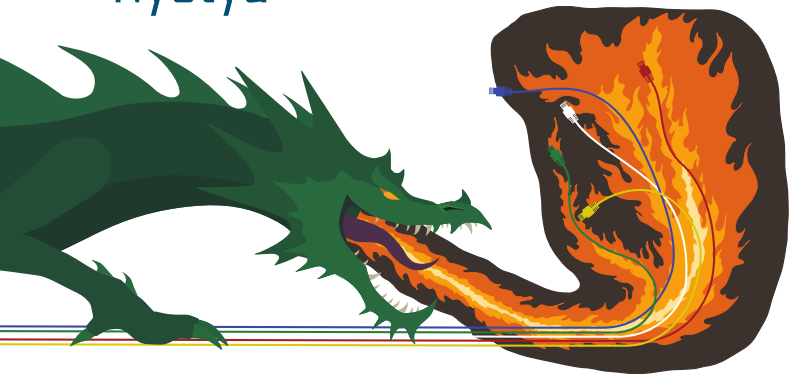
Измерение эффективности ИБ промышленных систем

Лукацкий Алексей, бизнес-консультант по ИБ



Nyetya



Описание

- Продвинутый актор, ассоциированный с государством
- Деструктивная атака маскировалась под Ransomware
- Наиболее дорогой инцидент в истории

Инструменты

- Ransomware с тактикой червя
- Спроектирован для распространения внутри, не снаружи
- Использование Eternal Blue / Eternal Romance и Admin Tools (WMI/PSExec)

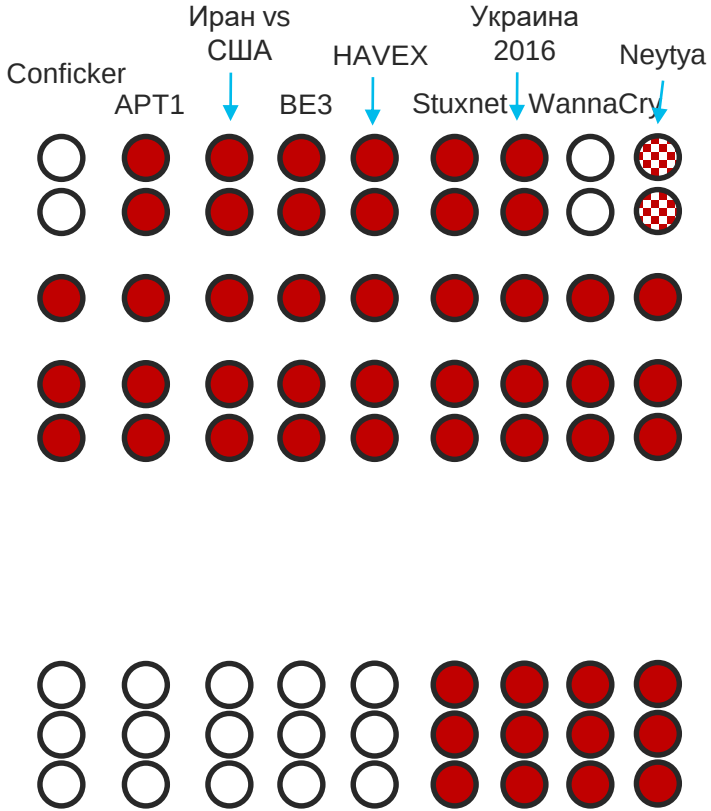
Тактики

- Цепочка поставок и от жертвы к жертве
- Быстрое распространение
- Разрушение систем / сетей

Процессы

- Разработан для максимально быстрого и эффективного нанесения ущерба
- Похож на вымогателя, но является деструктивным по сути

ICS Kill Chain



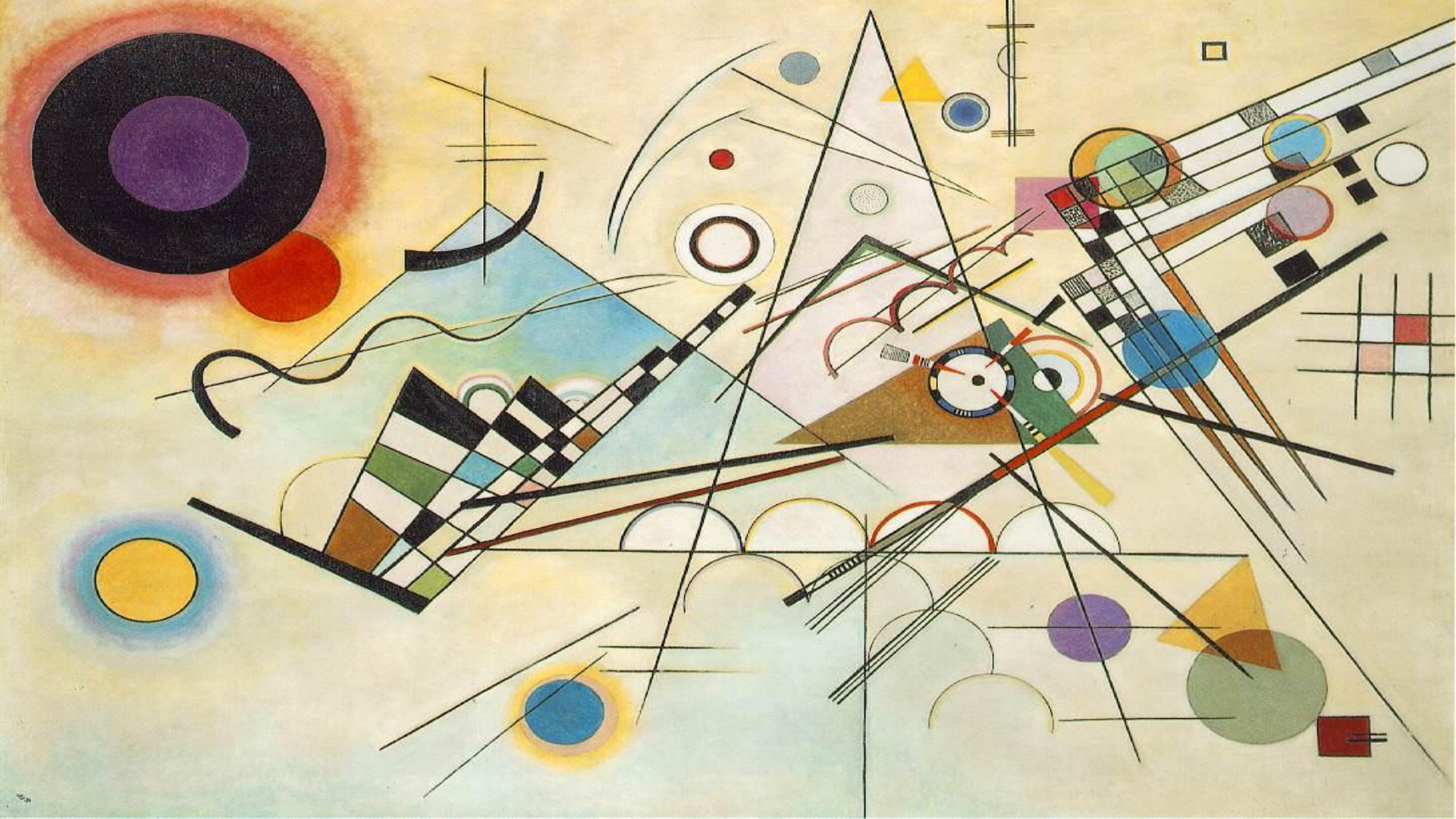
Зачем нужно измерять эффективность?

- Хорошо обеспечиваемая безопасность не видна
- Мы хотим показать, что мы работаем хорошо
- Руководство часто хочет сравнивать себя с другими
- Мы хотим видеть динамику

Как обычно измеряют ИБ?

	Почти нереально	Маловероятно	Возможно	Вероятно	Очень вероятно
Катастрофически	6	7	8	9	10
Значительно	5	6	7	8	9
Умеренно	4	5	6	7	8
Незначительно	3	4	5	6	7
Несущественно	2	3	4	5	6
	Принять (уровень = 2,3)	Мониторить (уровень = 4,5)	Управлять (уровень = 6)	Избежать / разрулить (уровень = 7)	Немедленно избежать / разрулить (уровень = 8, 9, 10)

- Неконкретно, не количественно, условно…



Или процесс? Не столь важно!

Информационная безопасность - состояние защищенности интересов стейкхолдеров предприятия в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества, государства и бизнеса

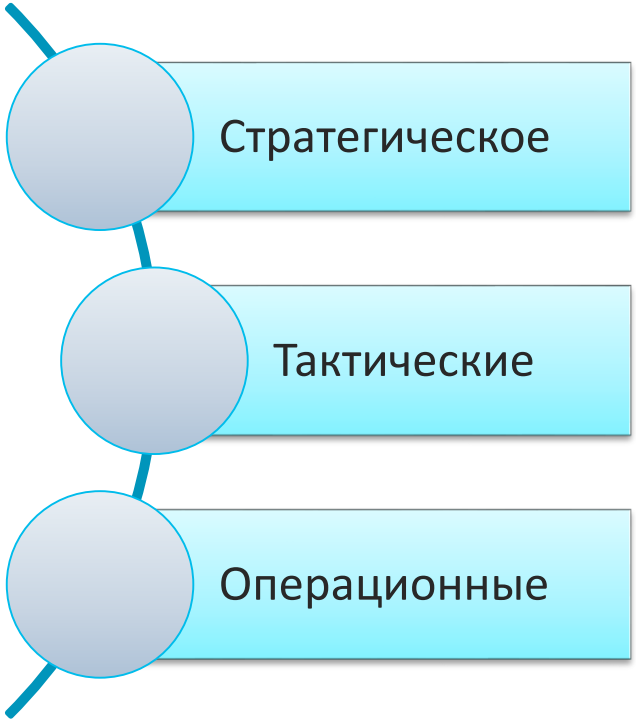
Эффективность – это поддающийся количественному определению вклад в достижение конечных целей

Какие у нас могут быть цели?

- Выполнение требований NERC CIP или ISA/IEC 62443
- Категорирование всех объектов КИИ
- Сертификация ключевых процессов на соответствие ISO/IEC 27019
- Сокращение числа инцидентов ИБ до 3 в месяц
- Внедрение защищенного доступа к АСУ ТП для подрядных организаций
- Снижение времени простоя от инцидентов до 2 часов в среднем
- Снижение затрат на ИБ на 15%

Измерения бывают разные

- Операционные (наиболее привычные)
  - В реальном времени, ежедневные
  - Базируются на логах, правилах СрЗИ
  - Насколько хороши наши защитные меры?
- Тактические
  - Отслеживание изменений
  - Результаты аудита
  - Насколько хороша наша программа ИБ?
- Стратегические
  - Корпоративные риски и связь с бизнесом
  - Насколько мы защищены?



Примеры тактических метрик

- Число инцидентов, требующих ручного управления
- Mean-Time-to-Fix (время восстановления после инцидента)
  - Также TTR (Time-to-Recovery) или TTC (Time-to-Contain)
- Mean-Time-to-Detect (время обнаружения инцидента)
- Mean-Time-to-Patch
- Вовлеченность персонала в ИБ
- Стоимость устранения уязвимостей

Примеры тактических метрик

- % систем АСУ ТП без уязвимостей с CVSS 7.0+
- % изменений с security review
- % изменений с security exceptions
- Стоимость защитной меры в % от бюджета (общего, ИТ, ИБ, АСУ ТП)
- Уровень соответствия требованиям compliance
- Стоимость инцидента

Примеры тактических метрик

- Время между созданием и закрытием заявки (ticket) об инциденте
- Соотношение открытых и «закрытых» заявок об инцидентах
- Соотношение инцидентов и заявок
- Число повторных инцидентов
- Соотношение методов коммуникаций (e-mail / звонков / портал)
- Число false positives (несуществующих инцидентов)

Принцип SMART для выбора метрик

- SMART – **S**pecific, **M**easurable, **A**chievable, **R**elevant, **T**imely
  - Как можно конкретнее, без двойных толкований, для правильной целевой аудитории
  - Результат должен быть измеримым, а не эфемерным
  - Зачем выбирать цель, которая недостижима?
  - Соответствие целям, а не «вообще»
  - Своевременность и актуальность

Пример использования SMART

Характеристика	Пример плохой метрики	Пример хорошей метрики
Конкретная	Число неудачных попыток входа в HMI	Число неудачных попыток входа в HMI в неделю на одного сотрудника
Измеримая	Доход от внедрения системы защиты АСУ ТП	Уровень лояльности сотрудников подразделения АСУ ТП
Достижимая	Отсутствие инцидентов ИБ в АСУ ТП за текущий квартал	Число инцидентов ИБ в АСУ ТП в текущем квартале < 5
Релевантная	Число запущенных проектов по ИБ АСУ ТП	Число проектов по ИБ АСУ ТП, завершенных в срок
Актуальная	Число пропатченных узлов в сегменте АСУ ТП в прошлом году	Число непропатченных узлов в сегменте АСУ ТП в этом году

Как перейти от сотен операционных метрик к одной-двум стратегических?

От отдельных метрик к программе измерения

- EPRI (Electric Power Research Institute) Research Program
  - Creating Security Metrics for the Electric Sector (Parts I, II, III, IV)
- Применима к широкому спектру промышленных предприятий за пределами электроэнергетики

От отдельных метрик к программе измерения

Стратегическая метрика	Тактическая метрика
Уровень нейтрализации	Уровень защиты сетевого периметра
	Уровень защиты оконечных устройств
	Уровень контроля физического доступа
	Уровень безопасности персонала
	Уровень контроля сетевых уязвимостей
	Уровень контроля сетевого доступа
	Уровень защиты данных
	Уровень управления ИБ - Нейтрализация
Уровень обнаружения	Уровень осведомленности об угрозах
	Уровень обнаружения угроз
	Уровень управления ИБ - Обнаружение
Уровень реагирования	Уровень реагирования на инциденты
	Уровень управление ИБ - Реагирование

От отдельных метрик к программе измерения

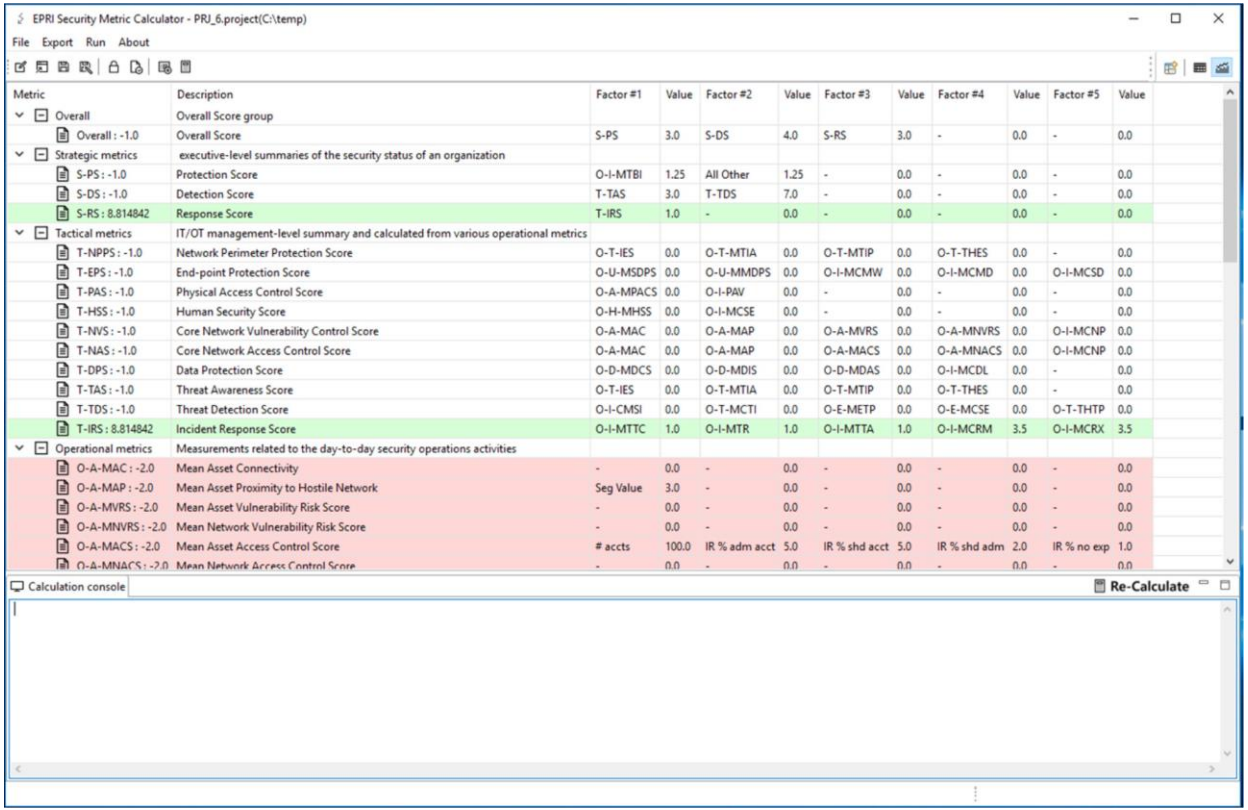
Операционная метрика	Составные части
Уровень защиты сетевого периметра	Уровень защиты точек доступа
	Уровень защиты беспроводных точек доступа
	Уровень защиты электронной почты
	Уровень защиты от вредоносных URL
	Уровень проникновения в сеть
Уровень управления ИБ - Нейтрализация	Уровень бюджета ИБ
	Уровень персонала ИБ
	Уровень толерантности к рискам ИБ

От отдельных метрик к программе измерения

Составная часть операционной метрики	События от средств защиты
Уровень защиты точек доступа	Число входящих соединений в день
	Число отброшенных входящих соединений в день
	Число алертов в день
	Число алертов ИБ в день
	Число подтвержденных DoS-атак в месяц
	Число сканирований в день
	Число подтвержденных вторжений в месяц
	Число подтвержденных инцидентов, требующих участия человека в месяц

$$APScore(n) = Score_{dropRate}(n) \times W_{dropRate} + Score_{alertRate}(n) \times W_{alertRate} + Score_{probRate}(n) \times W_{probRate}(n) + Score_{dos}(n) \times W_{dos} + Score_{intrusion}(n) \times W_{intrusion} + Score_{humanInt}(n) \times W_{humanInt} + Val(n.N16) \times W_{nac};$$

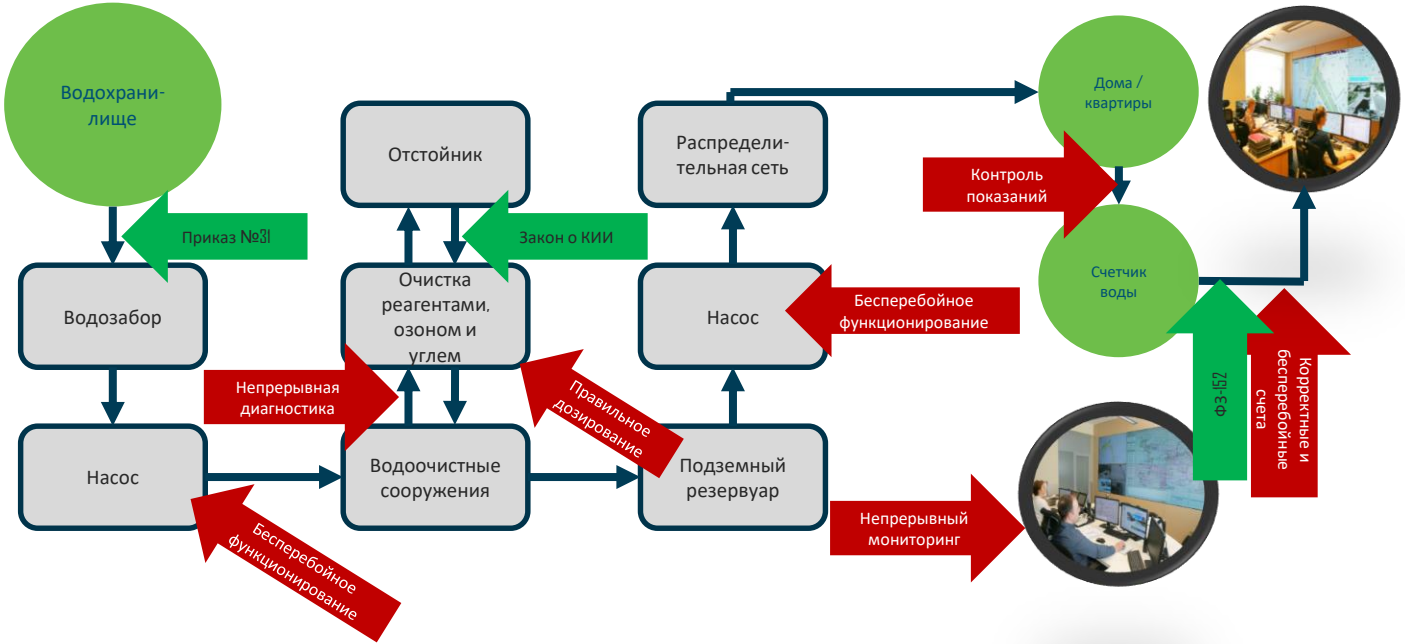
Средство автоматизации: EPRI MetCalc



Metric	Description	Factor #1	Value	Factor #2	Value	Factor #3	Value	Factor #4	Value	Factor #5	Value
Overall	Overall Score group										
Overall : -1.0	Overall Score	S-PS	3.0	S-DS	4.0	S-RS	3.0	-	0.0	-	0.0
Strategic metrics	executive-level summaries of the security status of an organization										
S-PS : -1.0	Protection Score	O-I-MTBI	1.25	All Other	1.25	-	0.0	-	0.0	-	0.0
S-DS : -1.0	Detection Score	T-TAS	3.0	T-TDS	7.0	-	0.0	-	0.0	-	0.0
S-RS : 8.814842	Response Score	T-IRS	1.0	-	0.0	-	0.0	-	0.0	-	0.0
Tactical metrics	IT/OT management-level summary and calculated from various operational metrics										
T-NPPS : -1.0	Network Perimeter Protection Score	O-T-IES	0.0	O-T-MTIA	0.0	O-T-MTIP	0.0	O-T-THES	0.0	-	0.0
T-EPS : -1.0	End-point Protection Score	O-U-MSDPS	0.0	O-U-MMDPS	0.0	O-I-MCMW	0.0	O-I-MCMD	0.0	O-I-MCSD	0.0
T-PAS : -1.0	Physical Access Control Score	O-A-MPACS	0.0	O-I-PAV	0.0	-	0.0	-	0.0	-	0.0
T-HSS : -1.0	Human Security Score	O-H-MHSS	0.0	O-I-MCSE	0.0	-	0.0	-	0.0	-	0.0
T-NVS : -1.0	Core Network Vulnerability Control Score	O-A-MAC	0.0	O-A-MAP	0.0	O-A-MVRS	0.0	O-A-MNVRS	0.0	O-I-MCNP	0.0
T-NAS : -1.0	Core Network Access Control Score	O-A-MAC	0.0	O-A-MAP	0.0	O-A-MACS	0.0	O-A-MNACS	0.0	O-I-MCNP	0.0
T-DPS : -1.0	Data Protection Score	O-D-MDCS	0.0	O-D-MDIS	0.0	O-D-MDAS	0.0	O-I-MCDL	0.0	-	0.0
T-TAS : -1.0	Threat Awareness Score	O-T-IES	0.0	O-T-MTIA	0.0	O-T-MTIP	0.0	O-T-THES	0.0	-	0.0
T-TDS : -1.0	Threat Detection Score	O-I-CMSI	0.0	O-T-MCTI	0.0	O-E-METP	0.0	O-E-MCSE	0.0	O-T-THTP	0.0
T-IRS : 8.814842	Incident Response Score	O-I-MTTC	1.0	O-I-MTR	1.0	O-I-MTTA	1.0	O-I-MCRM	3.5	O-I-MCRX	3.5
Operational metrics	Measurements related to the day-to-day security operations activities										
O-A-MAC : -2.0	Mean Asset Connectivity	-	0.0	-	0.0	-	0.0	-	0.0	-	0.0
O-A-MAP : -2.0	Mean Asset Proximity to Hostile Network	Seg Value	3.0	-	0.0	-	0.0	-	0.0	-	0.0
O-A-MVRS : -2.0	Mean Asset Vulnerability Risk Score	-	0.0	-	0.0	-	0.0	-	0.0	-	0.0
O-A-MNVRS : -2.0	Mean Network Vulnerability Risk Score	-	0.0	-	0.0	-	0.0	-	0.0	-	0.0
O-A-MACS : -2.0	Mean Asset Access Control Score	# accts	100.0	IR % adm acct	5.0	IR % shd acct	5.0	IR % shd adm	2.0	IR % no exp	1.0
O-A-MNACS : -2.0	Mean Network Access Control Score	-	0.0	-	0.0	-	0.0	-	0.0	-	0.0

А что думает бизнес обо всех этих метриках?

Бизнес думает об ИБ, но по своему



Процесс водоснабжения

Разница в восприятии топ-менеджмента и безопасника / айтишника / асутпшника

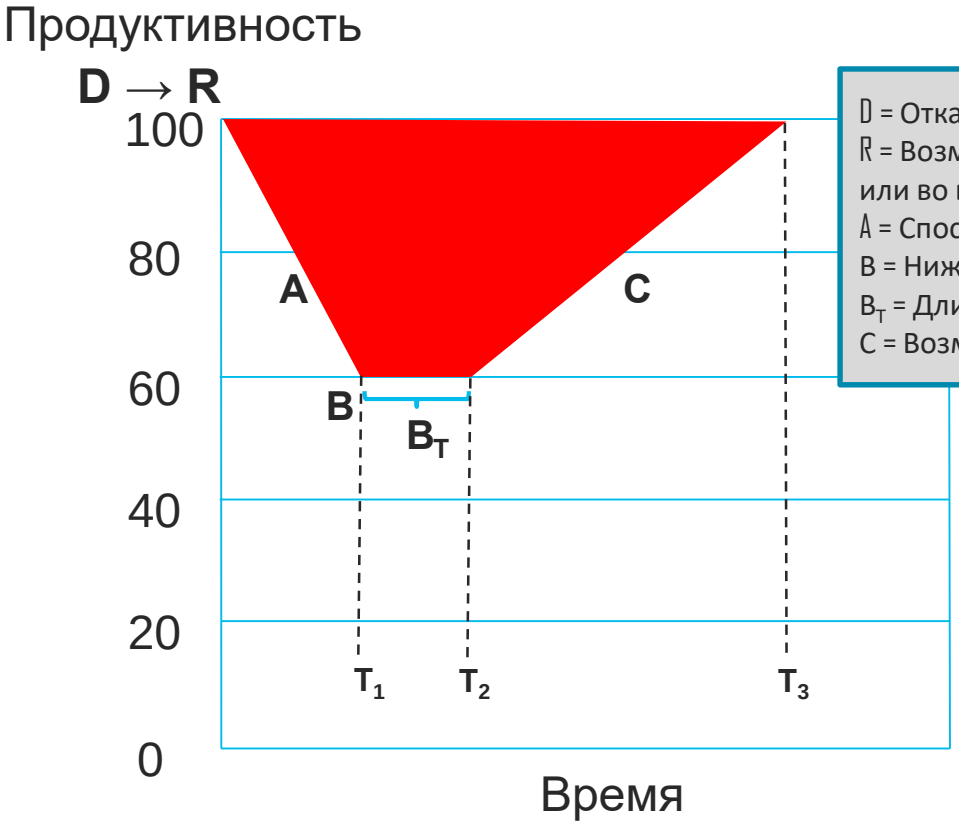
Безопасник / айтишник / асутпшник

- Погружение в детали
- Нежелание расстаться с собранными данными
- Данные ради данных
- Что? Где? Когда?

Топ-менеджмент

- Нужна общая картина
- Данные для принятия решения
- Что будет? Что делать?

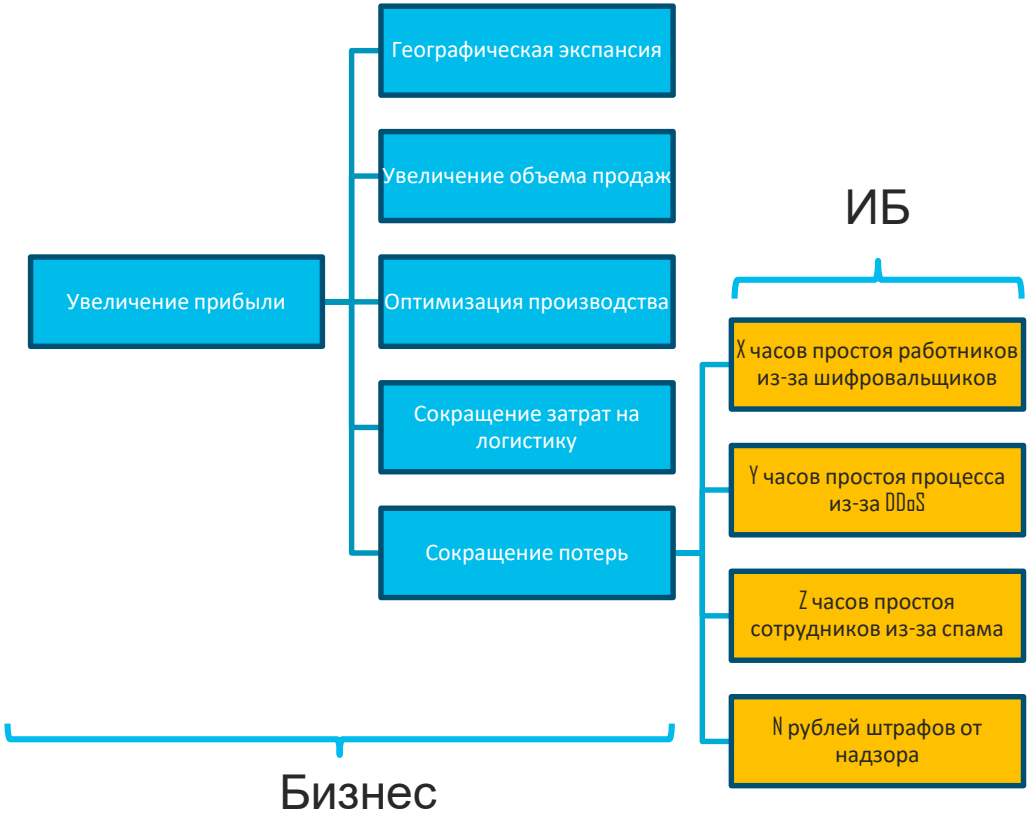
Как инциденты ИБ видит бизнес?



D = Отказ/сбой системы
R = Возможность ослабления или смягчения эффекта до или во время негативного события
A = Способность амортизировать и деградировать
B = Нижний предел; пороговое значение
B_T = Длительность нижнего предела
C = Возможность вернуться к исходному уровню

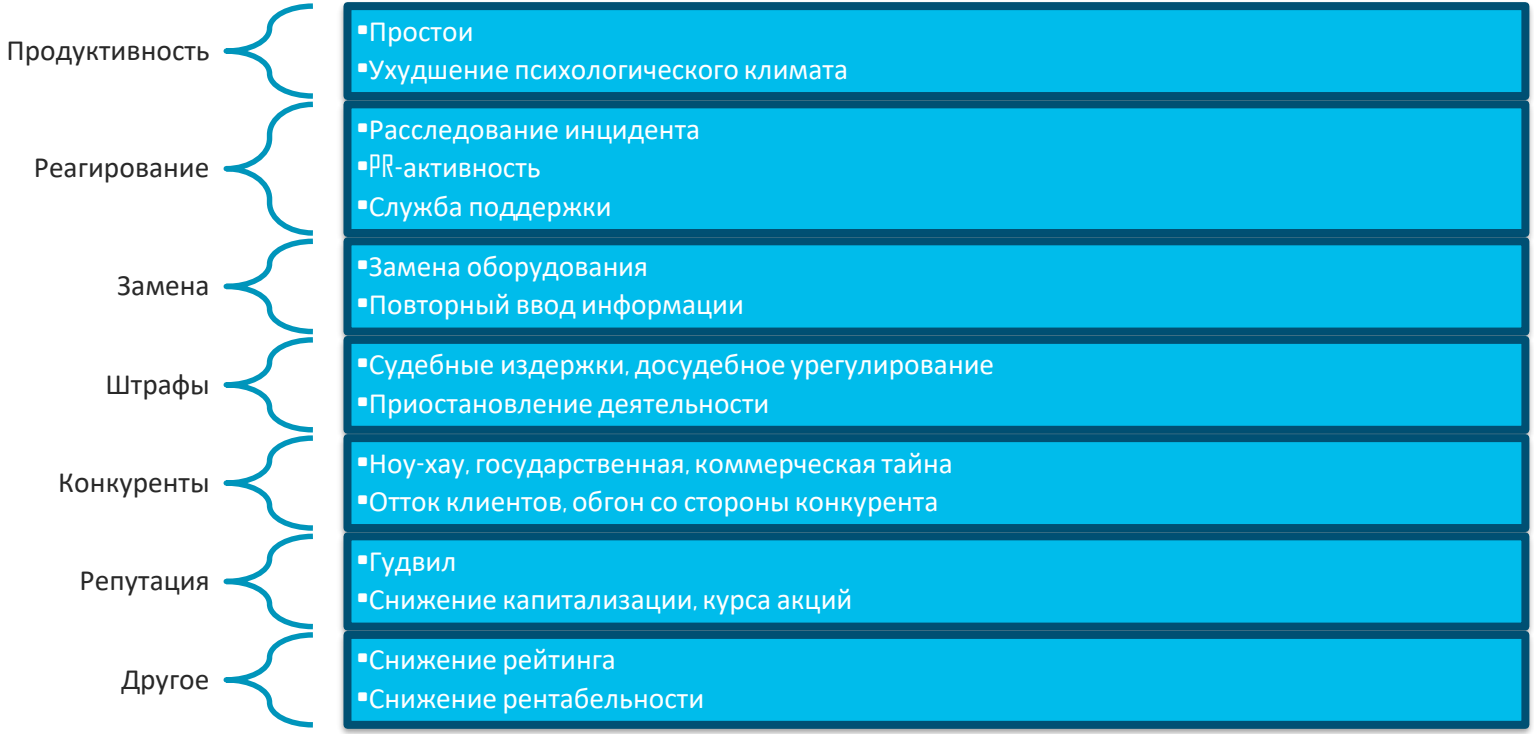
Уменьшить A?
Уменьшить B_T?
Уменьшить C?
Уменьшить T_1, T_2 и T_3?

Попробуем переформулировать наши цели



От измерения «для себя» к измерению для бизнеса

Формы потерь от инцидентов ИБ



Давайте быть конкретнее и считать рублем

	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Финансовый ущерб на более чем Y миллионов рублей	₽1M	₽5M	₽10M	₽50M	₽100M

- Стоимость прямых потерь от нарушения бизнес-операций
- Стоимость восстановления бизнес-операций
- Снижение стоимости акций (стрёмный показатель, но иногда тоже поддается измерению)
- Размер штрафов
- Упущенная выгода (если вы можете ее посчитать)
- Снижение лояльности заказчиков
- Замена оборудования или повторный ввод информации
- Взаимодействие с пострадавшими заказчиками и т.д.

Вопросы для определения стратегических бизнес-метрик ИБ

- Что остановит или замедлит операции в вашей организации?
- Что приведет к снижению прибыли / выручки / маржинальности / доли рынка вашей компании?
- Что приведет к снижению качества предоставляемого продукта / услуги?
- Что приведет к негативному влиянию на цель компании / бизнес-подразделения / бизнес-проекта / executive sponsor?

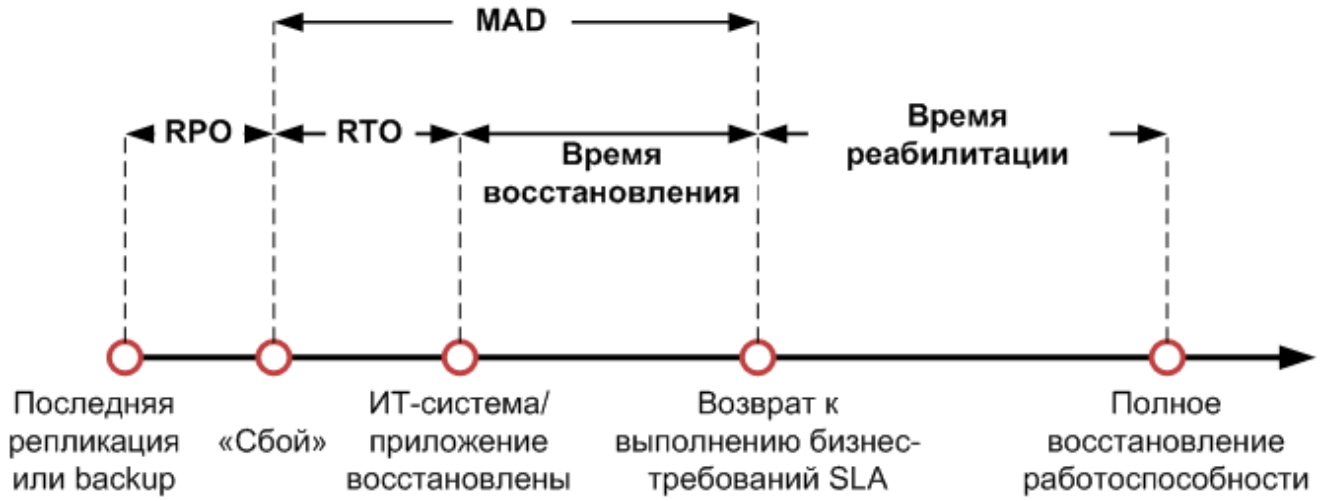
А если нельзя посчитать рублем?

	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Перебой в работе для более чем **X** заказчиков	10 заказчиков	100 заказчиков	500 заказчиков	1000 заказчиков	5000 заказчиков
Прерывание бизнес операций на **Z** часов	1 час	4 часа	8 часов	2 дня	5 дней
Нанесение вреда жизни и здоровью **A** человек	0 человек	0 человек	1 человек	10 человек	50 человек
Утечка данных **B** заказчиков	100 заказчиков	1000 заказчиков	5000 заказчиков	10000 заказчиков	100000 заказчиков
Отток **C** заказчиков	5 заказчиков	10 заказчиков	25 заказчиков	50 заказчиков	100 заказчиков
Потеря доли рынка на **D**%	0%	0%	1%	3%	7%
Снижение продуктивности на **E**%	0%	1%	3%	5%	10%

Длительность инцидента ИБ с точки зрения ИБ и бизнеса

- Степень влияния и составляющие цены инцидента меняется с течением времени

  Эта иллюстрация может использоваться при оценке времени восстановления после атаки



RPO – Recovery Point Objectives, RTO – Recovery Time Objectives, MAD – Maximum Allowable Downtime

Специфичные отраслевые метрики

	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Снижение мощности электрогене-рации на F мегаватт	Снижение мощности допустимо	Снижение мощности допустимо	100 МВт	1000 МВт	10000 МВт

	Несущественно	Незначительно	Умеренно	Значительно	Катастрофически
Публикация в СМИ	Отсутствуют	В местных потребительских печатных изданиях	По местному ТВ или в местных отраслевых печатных изданиях	По национальному ТВ или в национальных потребительских печатных изданиях	Выделенная передачи или репортаж по национальному ТВ или в национальных отраслевых печатных изданиях

А как измерить ИБ для бизнеса, но не рублем?

Может сравнить себя с конкурентами?

Лайфхак: вместо сравнения с конкурентами (если данных нет), можно сравнивать себя в разных состояниях (было – сейчас – через год – идеал)

5 более важных метрик

- % активностей по ИБ, несвязанных с бизнес-целями
- Количество проектов/активностей, связанных с бизнес-целями
- % важных для бизнеса проектов/активов/услуг, неудовлетворяющих требованиям ИБ
  - Неконтролируемый удаленный доступ подрядчиков
- % важных для бизнеса проектов/активов/услуг, меры защиты которых неадекватны или неэффективны
  - Или для которых во время инцидента не сработал план реагирования
- Вероятность предоставления услуг в течение инцидента ИБ

Можно еще поиграться с рисками…

Типичные ошибки при измерении эффективности

- Выбор сотен метрик вместо концентрации на стратегических
- Измерение того, что проще измерить, вместо концентрации на целях измерения
- Отсутствие бизнес-фокусировки
- Фокус на операционных результат-ориентированных метриках вместо оценки эффективности процесса
- Отсутствие контекста
  - Снижение цены ИБ при росте инцидентов

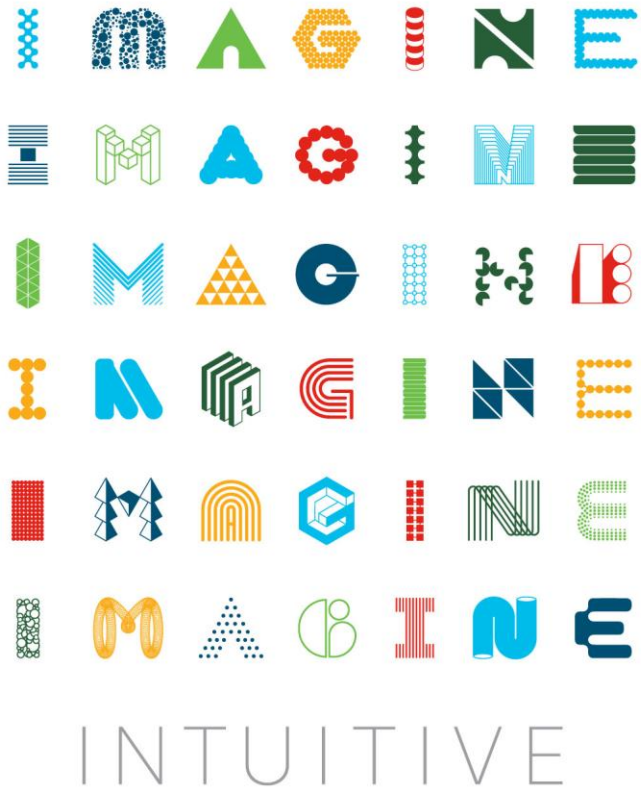
Ключевые факторы успеха

- Вы должны понимать, что вы делаете в области ИБ
- Вы должны понимать бизнес своего предприятия
- Вы должны понимать свою целевую аудиторию
- Вы должны уметь совмещать эти три элемента вместе
- Вы должны знать, где лежат данные
- Вы должны уметь программировать

Новый взгляд на измерение безопасности

Спасибо!

security-request@cisco.com



CISCO

INTUITIVE