

POSITIVE TECHNOLOGIES

Эволюция SIEM: маркетинг или вынужденные меры



Олеся Шелестова

системный аналитик
Positive Technologies

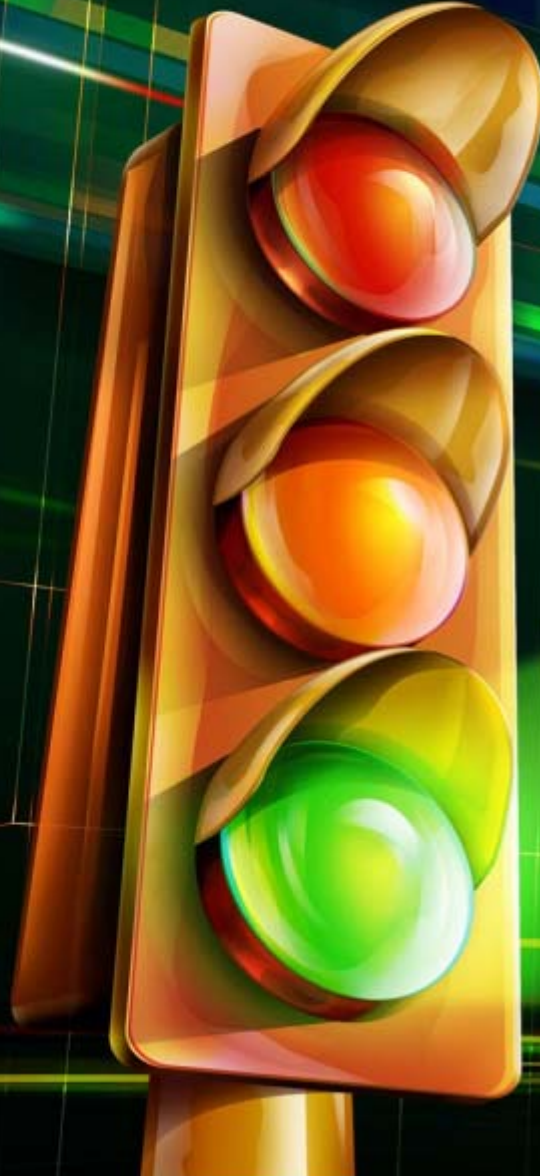
Что необходимо бизнесу



- Чтобы все работало без сбоев;
- Информация должна быть защищена от внутренних и внешних угроз;
- Инциденты должны решаться быстро;
- Регуляторы должны быть удовлетворены;
- Обоснование затрат исходя от задач бизнеса и потерь, а не уязвимостей;
- Минимальные издержки на СЗИ и персонал

Можно ли предотвратить
инцидент ?

SYSTEM FAILURE



Problem
(or single incident)



Case



Symptom

Где искать симптомы

- Application logs;
- Transaction logs;
- Connection logs;
- Access logs;
- System performance;
- User activity;
- Different system and security alerts

Откуда взять информацию

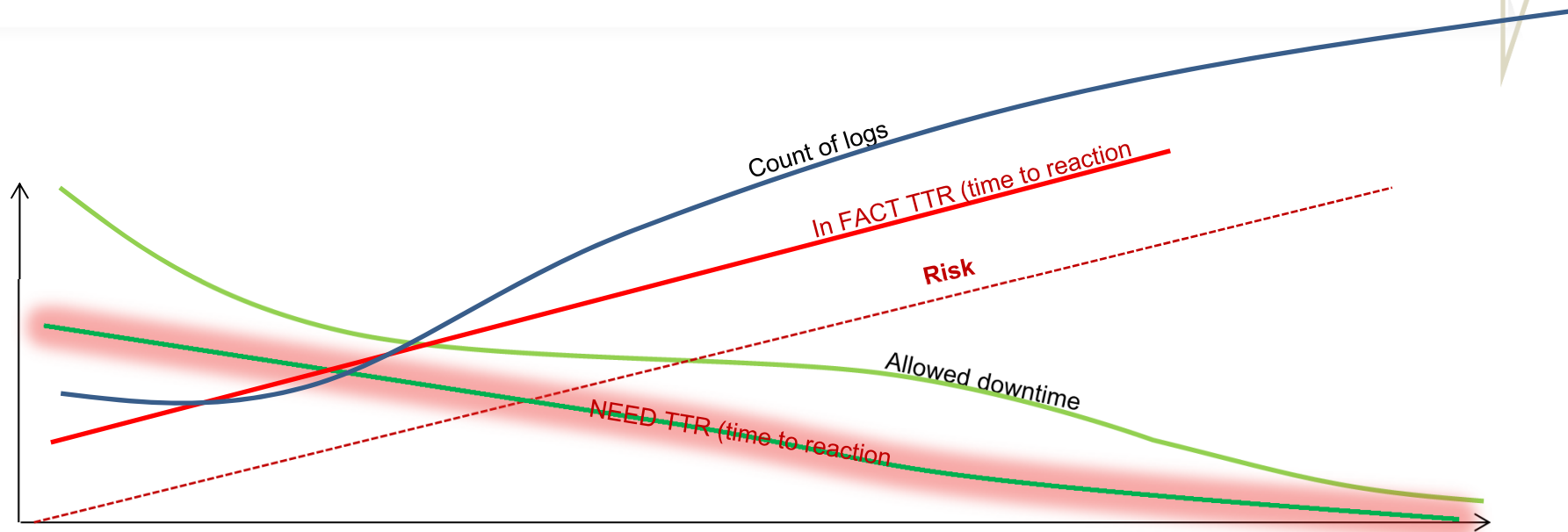
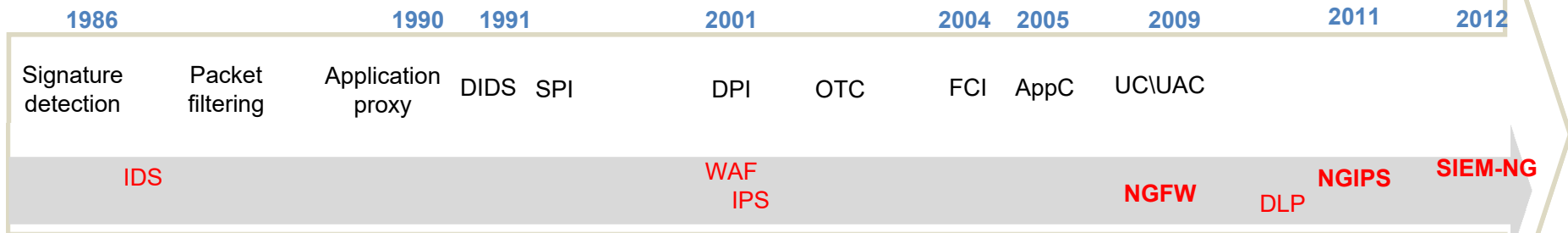
- IDS\IPS;
- Servers\desktops;
- Business applications;
- Database;
- Switches\Routers;
- DLP;
- SAC (СКУД);
- Antivirus software;
- VPNs;
- Web and file services



или почерпнуть информацию из новостных лент, премии или на новом месте работы ...

Источники

Legend:
 DIDS – Distributed IDS
 SPI – Statefull Packet Inspection
 DPI – Deep packet Inspection
 OTC – Outbound traffic control
 FCI - Full content Inspection
 AppC – Application control
 UC – user control



Рост порождает проблемы

- Множество консолей управления
- Долгий ре-логин в консоли управления
- Недостаточно памяти для хранения событий
- События могут быть удалены (затерты, ротейт, злоумышленник, крах)
- Сложная навигация
- Тяжелое восприятие



Трудозатраты

- Инфраструктура объемом в 1000 единиц генерирует около 23 000 - 30 000 EPS в секунду
- Даже «уникуму» требуется около 38 минут для просмотра 25 000 событий
- Человек не способен воспринимать более 10 событий в секунду на протяжении длительного времени

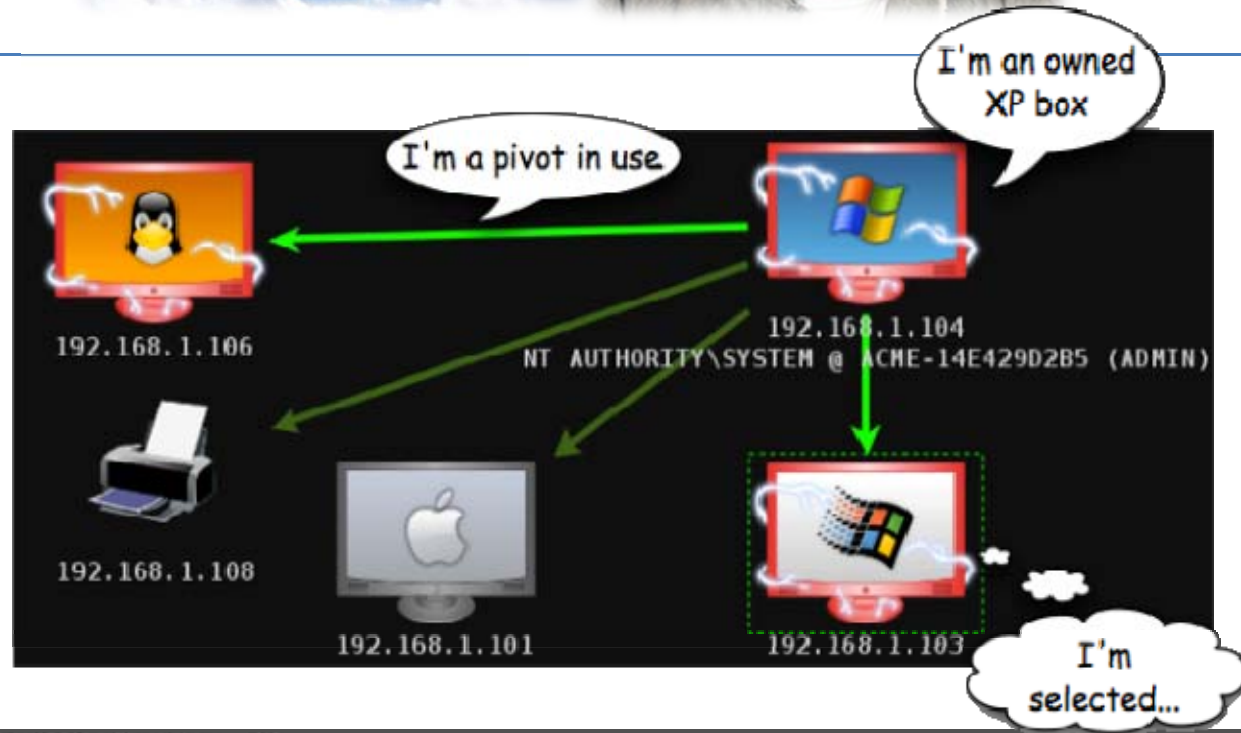


ИЛИ

- 1 SIEM, работающий 24x7 без усталости и просьб о повышении зарплаты
- + 1 инженер

А если не смотреть логи?

Прогноз погоды: Пасмурно, местами временами
ЛИВНИ.



Можно ли обнаружить
угрозу (аномалию)
не зная её?!



WARNING
JUMPING INTO TOXIC WASTE
DOES NOT GIVE YOU
SUPER POWERS*



Fig. 1a

USE ADVERSE HEALTH EFFECTS - See Fig. 1a

mon0 [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 169.254.192.118 and ip.addr eq 169.254.255.255) Expression... Clear Apply Save exclude_pine

No.	Time	Source	Destination	Protocol	Length	Info
86773	2755.760546000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
88282	2805.373093000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
90016	2870.185470000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
90123	2873.524333000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
91685	2926.475003000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
92394	2951.264893000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
95235	3043.725531000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB U.SUXIAZAI.COM<00>
101438	3253.715523000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
102231	3281.827424000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
104908	3389.260570000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
105503	3412.575101000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
108242	3516.197155000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
110130	3582.657328000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
114697	3752.910395000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
121577	3997.591699000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>
122187	4022.394078000	169.254.192.118	169.254.255.255	NBNS	140	Name query NB WWW.BAIDU.COM<00>

WTF?!

Type/Subtype: Data (0x20)


- ▶ Frame Control: 0x0208 (Normal)
- Duration: 0
- Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
- BSS Id: Ubiquiti_9a:0a:49 (00:27:22:9a:0a:49)
- Source address: Azurewav_dd:08:4e (00:25:d3:dd:08:4e)
- Fragment number: 0
- Sequence number: 3323
- ▶ Frame check sequence: 0xdc82c6ff [correct]
- ▶ Logical-Link Control
- ▶ Internet Protocol Version 4, Src: 169.254.192.118 (169.254.192.118), Dst: 169.254.255.255 (169.254.255.255)
- ▶ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
- ▶ NetBIOS Name Service

```

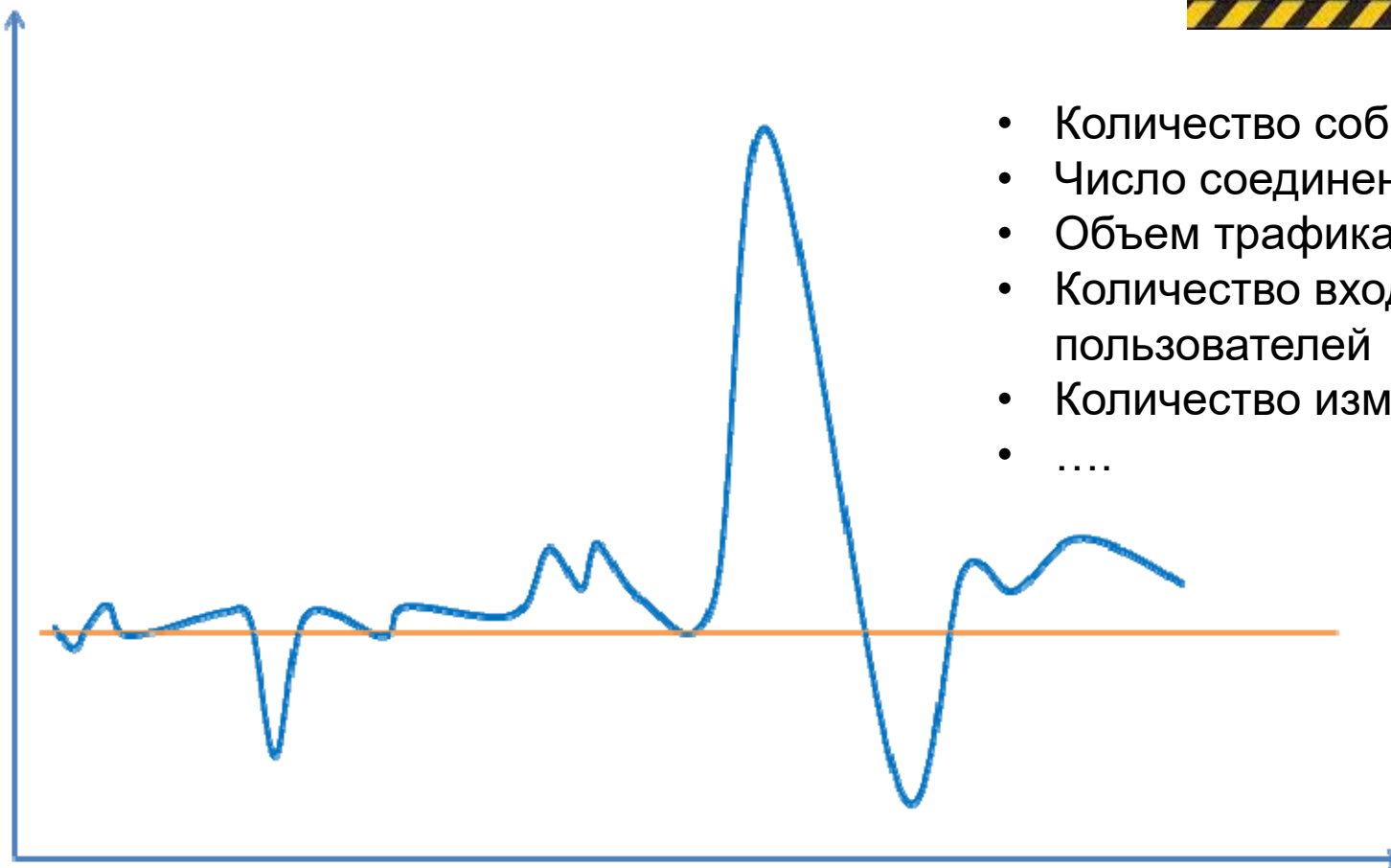
0030 b0 cf aa aa 03 00 00 00 00 00 45 00 00 45 57 5b ..E..NW[
0040 00 00 40 11 0e d1 a9 fe c0 76 a9 fe ff ff 00 89 ..@.....V.....
0050 00 89 00 3a 64 d6 e1 9c 01 10 00 01 00 00 00 00 ...:d.....
0060 00 00 20 46 46 43 4f 46 44 46 46 46 49 45 4a 45 ...CCOE DEEFFE3L
0070 42 46 4b 45 42 45 4a 43 4f 45 44 45 50 45 4e 43 BFKEBEJC OEDEPENC
0080 41 41 41 00 00 20 00 01 dc 82 c6 ff AAA.....

```

Logical-Link Control (llc), 8 bytes Packets: 179925 Displayed: 23 Marked: 0 Dropped: 0 Profile: Default

- 
- Что это за ИТ-актив
 - Что это за процесс
 - Кто запустил этот процесс
 - На месте ли пользователь
 - Какой процесс генерирует подозрительные события
 - Наличие уязвимостей для данного ИТ-актива
 - Связанные события
 - Похожие события (база знаний и алгоритмы корреляции)
 - События в мире
 - Baseline для данного процесса
 - Последствия
 - Оценка ущерба

Baseline



- Количество событий
- Число соединений
- Объем трафика
- Количество входов пользователей
- Количество изменений
-

Follow the white rabbit.

Где серебряная пуля ?

Syslog – решение?!

Плюсы:

- Можно подключить множество источников (халява)
- Фактически, события однообразны по формату и легче читаются
- Можно делать regex скриптами
- Дешевый коннектор для гетерогенных систем

Минусы:

- Отсутствует автоматизация;
- UDP не имеет гарантированной доставки;
- Подавляющая масса устройств и приложений не поддерживает **tcp** syslog;
- При флуде порядка 5 000 EPS на один порт udp пакетами происходят значительные потери



Минусы «коленочных» решений

- События мало собрать, их еще нужно анализировать;
- При достаточном количестве источников, syslog в файл или syslog в mysql недостаточно по производительности (а события необходимо хранить от полугода до 2х лет по стандартам);
- Front-end + механизмы по интерпретации и поиску все придется написать, поскольку open source решения не удовлетворят ваши потребности;
- События syslog без TLS(DTLS) можно подделать по сети;
- События могут быть удалены\изменены из хранилища журналов событий в случае open source решений;
- Не имеют юридической значимости.



Что необходимо бизнесу (2)



- Чтобы все работало без сбоев;
- Информация должна быть защищена от внутренних и внешних угроз;
- Инциденты должны решаться быстро;
- Регуляторы должны быть удовлетворены;
- Обоснование затрат исходя от задач бизнеса и потерь, а не уязвимостей;
- Минимальные издержки на СЗИ и персонал

Требования стандартов

	SOX	GLBA	FISMA	PCI DSS	HIPAA	ISO 2700*
Object Access	+		+	+	+	+
Logon	+	+	+	+	+	+
Policy Changes	+			+		+
System Events	+	+		+	+	+
Process Tracking	+					
Account Logon	+					+
User Access	+		+	+	+	+
Account Management	+					+
Security Assesment			+			+
Contigency Planning			+			+
Configuration Management			+	+		+



SEM SIM SIEM SIEM-NG

SEM

- Единое хранилище
- Сбор с различных источников
- Архивация старых событий
- Поиск по событиям
- Разбивка по категориям событий
- Построение отчетов
- Удовлетворение аппетита регуляторов



SIM

- Минималистичный Dashboard
- Оповещение об определенном событии
- Compliance (вывод списка событий)
- Сортировка IP адресов по группам
- Инструменты для расследования инцидентов
- Важны не только журналы OS и приложений, но и сетевых устройств
- Обеспечение защиты серверного хранилища
- Обеспечение юридической значимости



SIEM

- Продвинутый Dashboard
- Корреляция по множеству событий
- Расширенный репортинг
- Инцидент-менеджмент
- Workflow
- Baseline
- Ценность актива (КДЦ)
- Добавлены новые стандарты
- Compliance SIM == Compliance SIEM



Что было дальше



- Убраны алгоритмы корреляции, оставлены RBR
- Статистика по мировым угрозам
- Возможность переопределения угроз
- Интеграция с Service Desk
- Добавление Netflow как источника
- Интеграции с системами СКУД
- Добавление различных метрик (KPI, RO(s)I)
- Интеграции с Risk Management
- Интеграции с network-behavior и anomaly-detection
- Направление на SOC
- Облачные решения
- Эволюция понятия «актива»

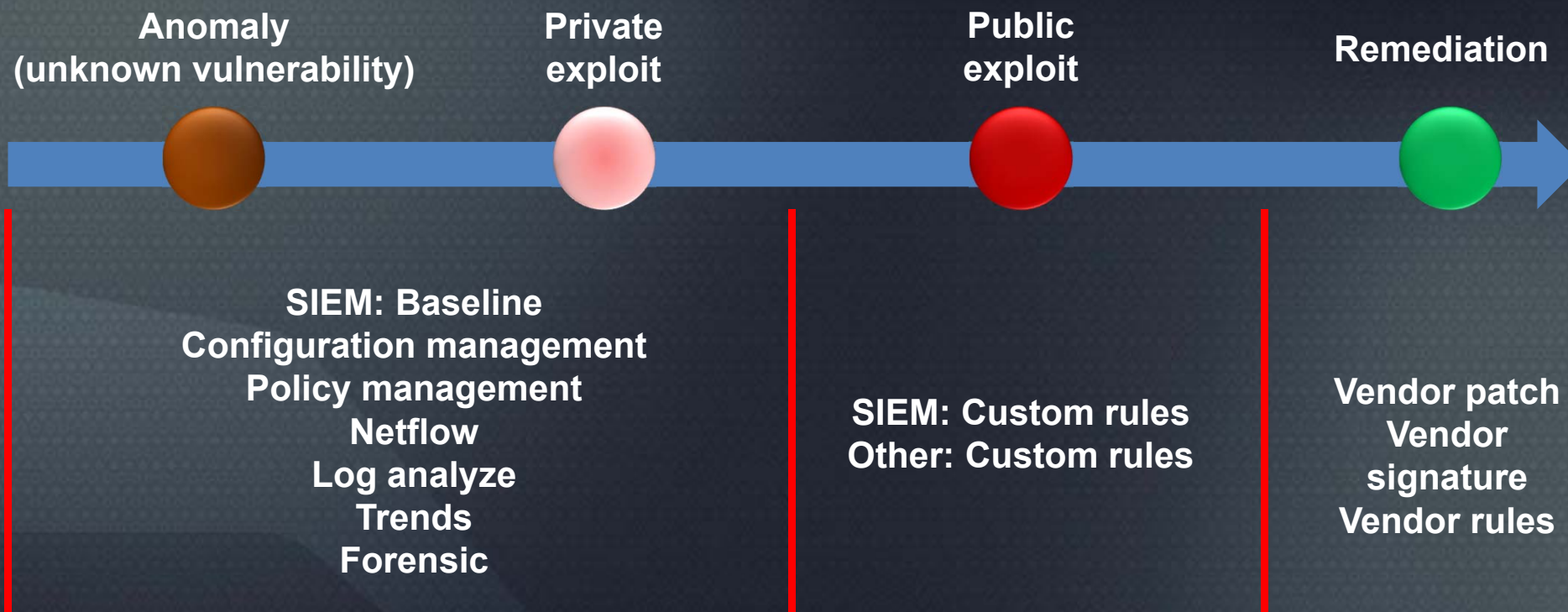
Timeline

Накопленный опыт



Timeline	2000-2005	2004-2009	2005-2012	2012-2013
Этапы	SEM	SIM	SIEM	SIEM-NG
Цели	Защита периметра, консолидация событий	Анализ, исследование, разбор инцидентов, compliance	Real-time обнаружение, мониторинг активности приложений, траффика, пользователей	Оценка влияния на бизнес-процессы
Источники	Журналы событий	Сетевые устройства, журналы приложений	Netflow, DLP, IPS, SPI, SCADA, VM	DPI, NGFW, NGIPS, VM
Объемы хранилища	Десятки GB	Сотни GB	Терабайты	От десятков терабайт без лимита
Архитектура	Плоская, мало агентов	Агентная, распределенная	Многосвязная, распределенная	Кластеры, облако, с единым SOC
EPS	До 3 000	До 5-7 000	От 15 000	→ ∞
Пользователи	ИТ, ИБ специалисты	Преимущественно ИБ специалисты, аудиторы	Операторы SOC, Руководители, аудиторы, мало ИТ	Все предыдущие пользователи + Бизнес

Обнаружение уязвимостей





Лог-менеджмент



Автоматизация

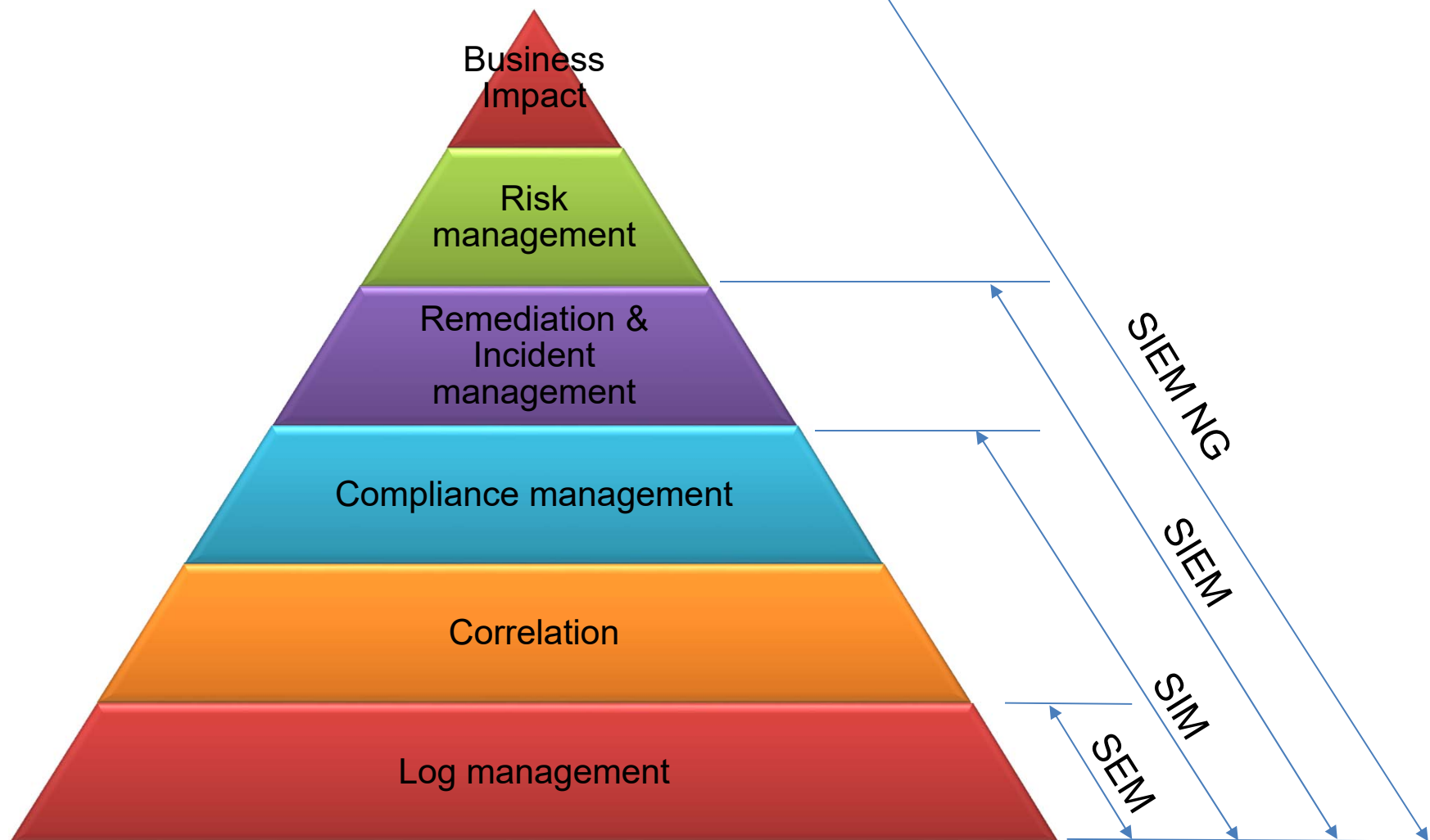


Корреляция

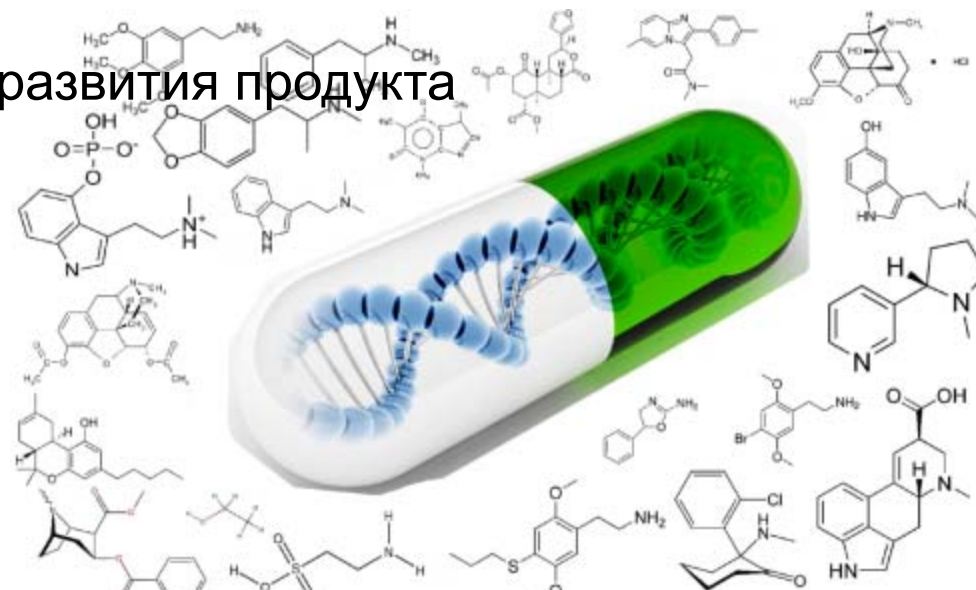


Влияние на бизнес

Пирамида процессов



«SIEM-NG» - это новая ступень развития продукта



- SIEM* продавался и будет продаваться, это устоявшееся на рынке необходимое решение
- Необходимость рождается в большей степени из задач, а не требований регуляторов
- Развитие продукта обусловлено требованиями к эффективности и оперативности обнаружению угроз и оценки их влияния на бизнес
- «SIEM-NG» - это попытка создать более интеллектуальную систему с новыми, еще более широкими возможностями

Что ожидать в будущем

- Увеличение количества и качества источников
- Повышение чувствительности обнаружения угроз с уменьшением количества ложных срабатываний
- Оценка влияния симптомов на бизнес
- Оценка последствий инцидентов для бизнеса
- Появление бизнес-активов
- Возвращение алгоритмов корреляции
- Автоматизация, уменьшение TTR
- Развитие процессов инцидент-менеджмент
- Увеличение и развитие показателей



Что необходимо бизнесу (3)



- Чтобы все работало без сбоев;
- Информация должна быть защищена от внутренних и внешних угроз;
- Инциденты должны решаться быстро;
- Регуляторы должны быть удовлетворены;
- Обоснование затрат исходя от задач бизнеса и потерь, а не уязвимостей;
- Минимальные издержки на СЗИ и персонал



Стоимость



Влияние на бизнес-процессы и
информацию



Несоответствия, нарушения
политик, инциденты



Ошибки, сбои, предупреждения,
нарушения

Все «включено»

Offense 3063

Magnitude		Relevance	0	Severity	8	Credibility	3
Description	Target Vulnerable to Detected Exploit preceded by Exploit Attempt Preceded by Recon preceded by Exploit/Malware Events Across Multiple Targets preceded by Recon - External - Potential Network Scan		Event count	1428 events in 3 categories			
Attacker/Src	202.153.48.66		Start	2009-09-29 16:05:01			
Target(s)/Dest	Local (717)		Duration	1m 32s			
Network(s)	Multiple (3)		Assigned to	Not assigned			
Notes	Vulnerability Correlation Use Case illustrates a scenario involving correlation of vulnerability data with IDS alerts An attacker originating from China used a Conficker worm exploit (CVE 2008-4250). The attacker used a botnet using the						

What was the attack?

Who was responsible?

Was it successful?

Magnitude		User	Karen
Description	202.153.48.66	Asset Name	Unknown
Vulnerabilities	0	MAC	Unknown
Location	China	Asset Weight	0

Where do I find them?

How valuable are they to the business?

Name	Magnitude	Local Target Count
Buffer Overflow		8
Misc Exploit		3
Network Sweep		716

How many targets involved?

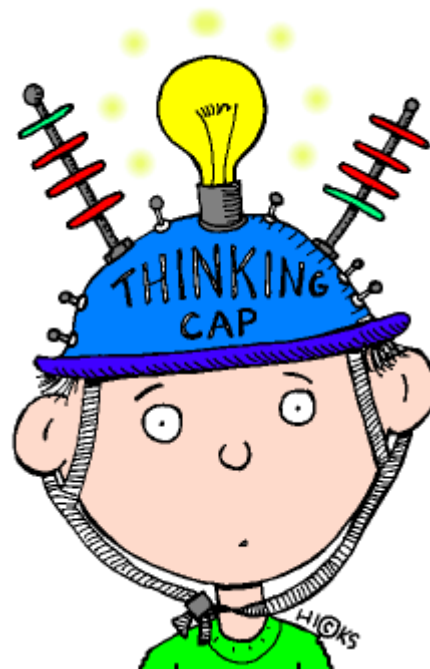
IP/DNS Name	Mag...	Vulnerability	Contained	User	MAC	Location	Weight
Windows AD Server		Unknown	No	Unknown	Unknown	main	8
10.101.3.3		Unknown	No	Unk...		main	0
10.101.3.4		Unknown	No	Unk...		main	0
DC106		Yes	No	Adm...	a7	main	10
10.101.3.11		Unknown	No	DC...	a7	main	0

Are any of them vulnerable?

Event Name	Magnitude	Log Source	Category	Destination	Dst Port	Time
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar		10.101.3.15	445	09-29 16:06:33
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5		10.101.3.10	445	09-29 16:06:28
NETBIOS-DG SMB v4 srvsvc NetrpPathCo...		Snort @ 10.1.1.5		10.101.3.15	445	09-29 16:06:33
Misc Exploit - Event CRE		Custom Rule Engine-8 :: qradar		10.101.3.13	445	09-29 16:06:31
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: q		10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.10	445	09-29 16:05:01
Network Sweep - QRadar Classify Flow		Flow Classification Engine-5 :: qradar-vm	Network Sweep	10.101.3.15	445	09-29 16:05:01

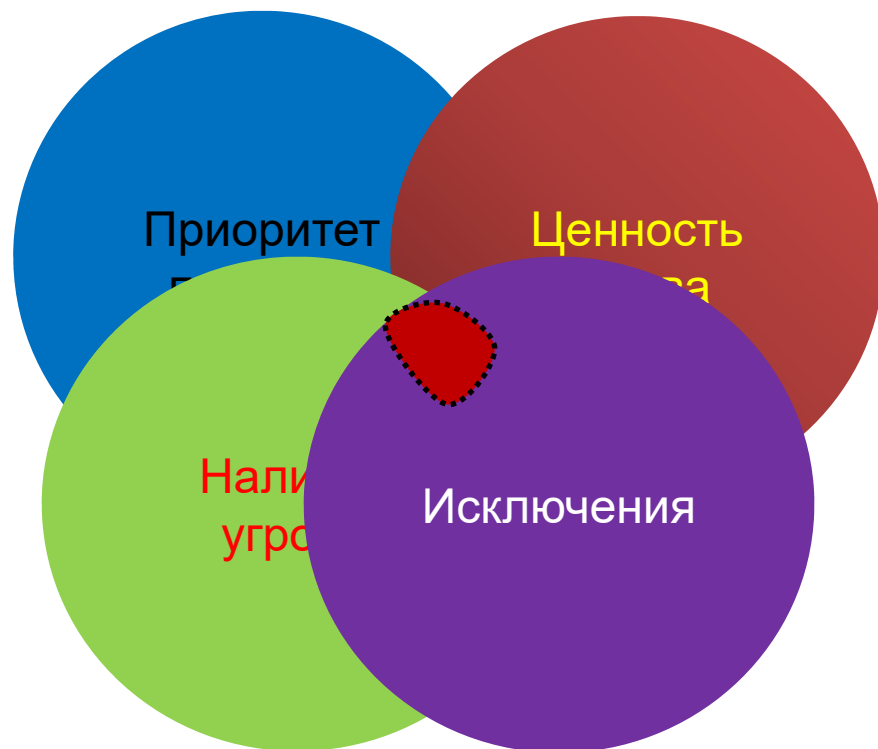
Where is all the evidence?

Приоритет угрозы
==
влияние на бизнес-процессы





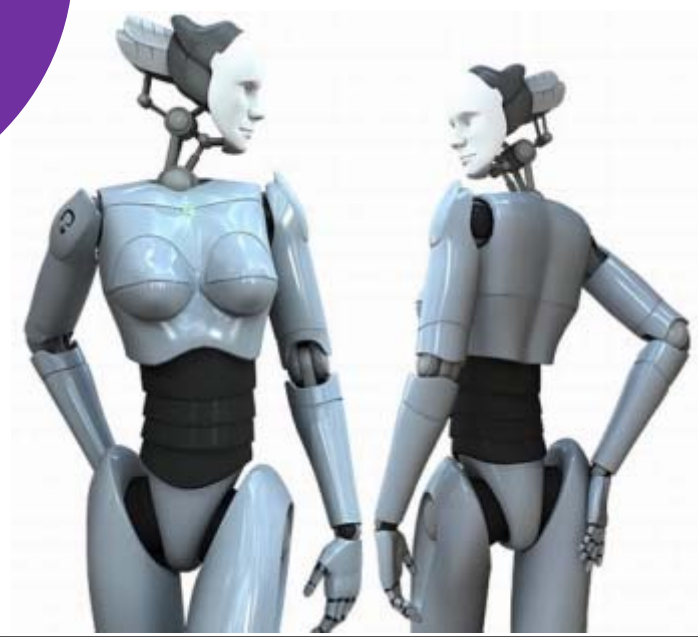






А что дальше?





Когда необходимо решение SIEM

- Высокие риски утечки и стоимость информации
- Дорогие простои информационных систем
- Документальная и юридическая база для расследования инцидентов
- Требования стандартов и регуляторов (Compliance)
- Автоматизация процессов (выявления, обнаружения, контроля)
- Снижение времени реакции на возникающие угрозы
- Сокращения затрат (персонал, операционные риски)
- Создание эмпирических показателей
- Обоснование затрат
- Повышение эффективности работы
- Поддержка принятых решений и их эффективности



Оправданные ожидания

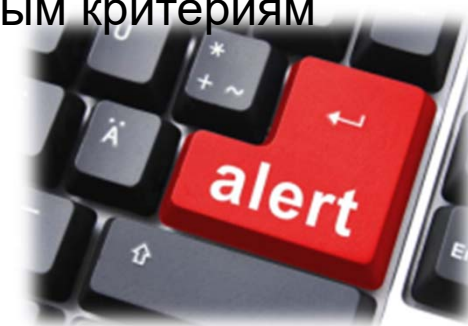


Criteria	Organization	Hard dollar benefits	Time to back	Soft benefits
Prevent Personnel Expansion	Healthcare Insurance and Services Provider	Savings of \$3.5 million over three years from staff reallocation	3 months, 12 days	Better enterprise visibility; Faster incident response; Less employee turnover.
Reduce Critical Incident Rate	Managed Security Services Provider (MSSP)	Annual savings of \$1 million from staff reduction and reallocation	6 months, 20 days	Better incident prioritization; Focused alert resolution; Improved customer service.
Reduce SOX Compliance Reporting Effort	Regional Electric Utilities Company	Savings of \$4.6 million over three years from elimination of 7,600 work-hours	39 days	Fewer compliance violations; Proactive compliance program; More consistency in controls and processes.
Extend Useful Life of Legacy Applications	Credit Union	Savings of \$8 million by deferring software rewrite	3 weeks	Audit violations removed; Avoided risk of technology replacement; Gained visibility into user activity.
Prevent Internal Resource Abuse	Global Telecommunications Company	Savings of \$3.6 million over three years from office supplies usage reduction	2 months, 15 days	Increased call center productivity; Improved recruiting processes; New visibility into user activity.
Prevent Funds Transfer Fraud	Regional Financial Institution	Prevent fraud worth \$900K	Less than 1 week	Increased visibility into transfer operations; Proactive, not reactive, fraud prevention; Additional use cases.

*(ArcSight ROI)

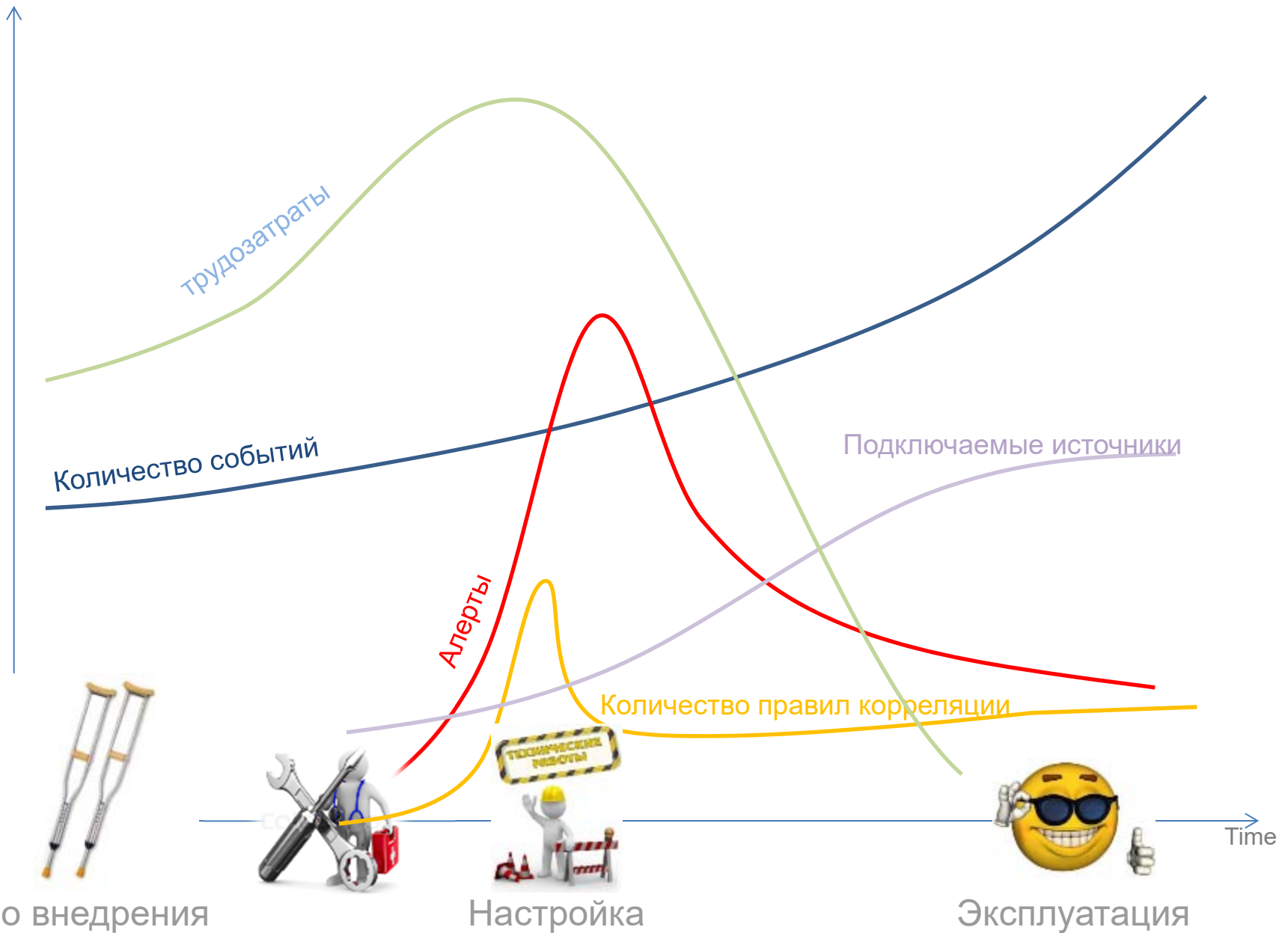
За счет чего достигаются результаты?

- Автоматизация сбора
- Корреляция по событиям
- Автоматический контроль непрерывности сбора
- Интерпретация событий в понятный формат
- Инструменты поиска по событиям
- Графические представления
- Baseline
- Автоматическое оповещение и регистрация инцидентов
- Оперативность решения инцидентов
- Корректное определение приоритета по множественным критериям
- Гибкие отчеты
- Оценка влияния на бизнес-процессы



Проблемы при внедрении





Конец рассказа

Спасибо за внимание

Олеся Шелестова

системный аналитик

Positive Technologies

oshelestova@ptsecurity.ru





POSITIVE TECHNOLOGIES