SOCAAS, ИЛИ СЕРВИСЫ MANAGED PROTECTION

Сергей Солдатов,
Руководитель Центра мониторинга

KASPERSKY lab

КОРОТКО О СЕБЕ

- С 2016: Руководитель SOC в ЛК
  - Внутренний SOC
  - Коммерческие сервисы MDR*
- 2012 – 2016: Главный менеджер в РН-Информ
  - Инсорсинг сервисов безопасности Роснефти
- 2002 – 2012: ТНК-ВР
  - Интеграция ИБ в бизнес - и ИТ-процессы
  - Контроли безопасности в ИТ-проектах
  - Операционная безопасность
- 2001-2002: Разработчик ПО в РосНИИРОС

* Managed Detection and Response

О ЧЕМ РЕЧЬ

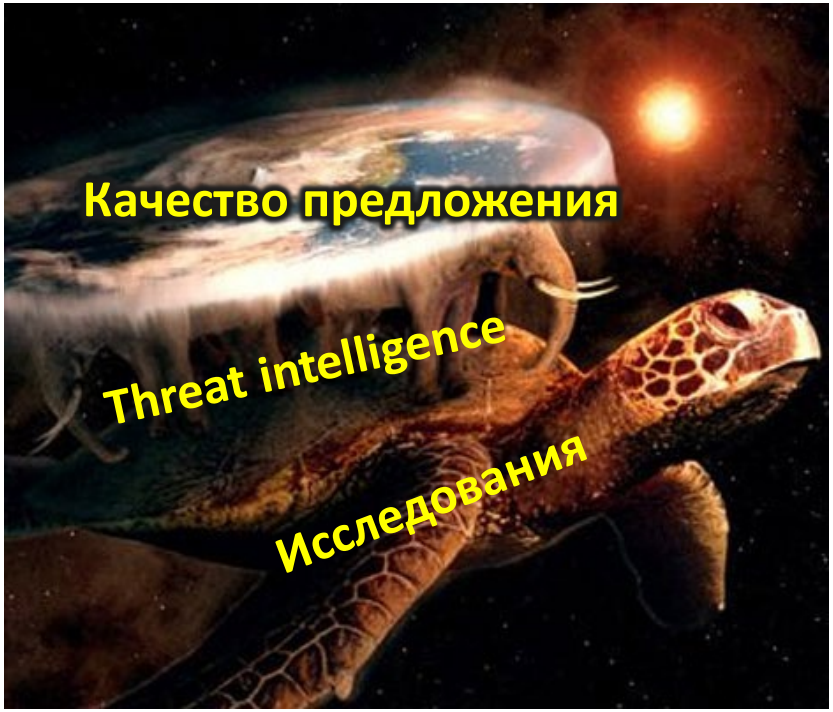
- Что нужно провайдеру для качественного сервиса SOC
  - Почему это важно
- Совместная работка команд провайдера
- Перспективы
- Что делать самому, а что поручить

ИНГРЕДИЕНТ №1: THREAT INTELLIGENCE

KASPERSKY

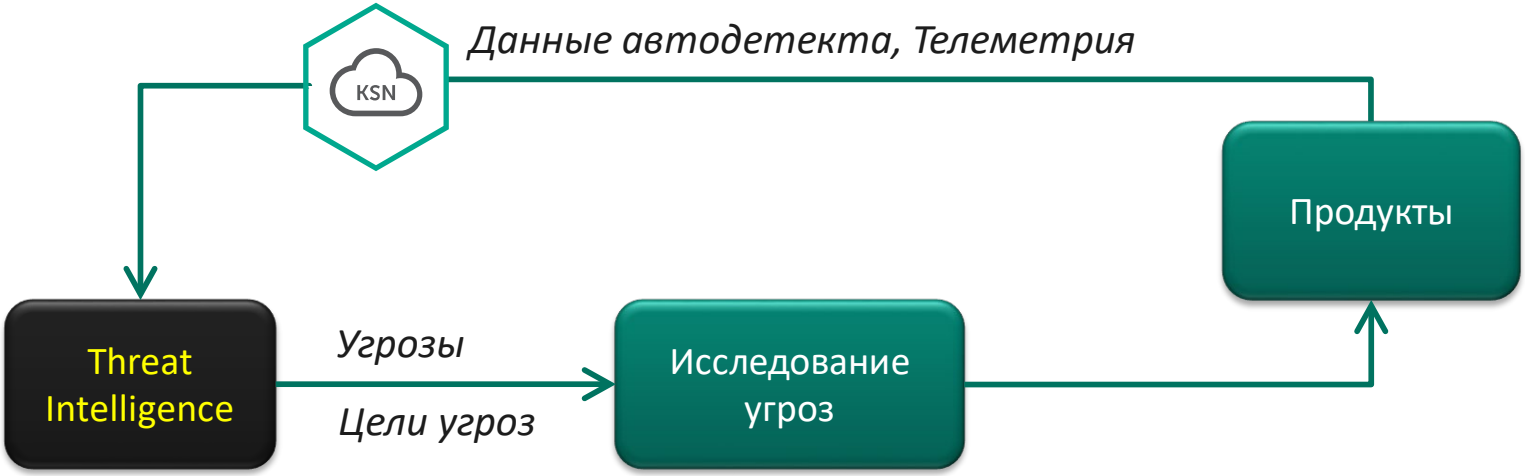
ОПЕРАЦИОННЫЕ ИССЛЕДОВАНИЯ VS AD-HOC

«… хочется отметить, что **системные операционные исследования** имеют мало общего с **ad-hoc ресерчами**, возможно, даже выстрелившими в какие-либо громкие публикации, так как **приоритет operations-исследований - неизменно высокое качество детекта во времении**, а не "вау-эффект" от ad-hoc»



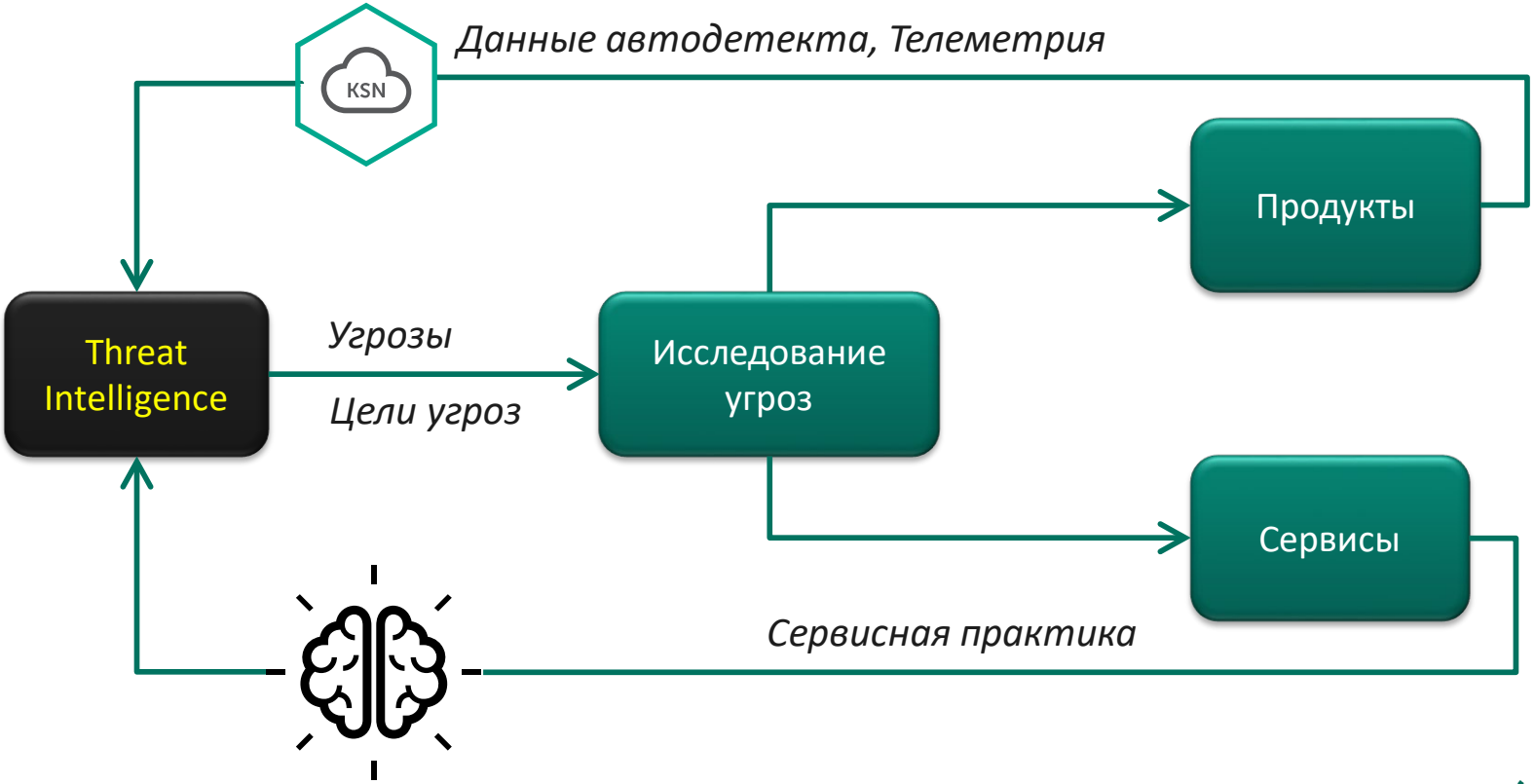
https://reply-to-all.blogspot.com/2017/10/blog-post_20.html

ЦИКЛ ДАННЫХ ОБ УГРОЗАХ

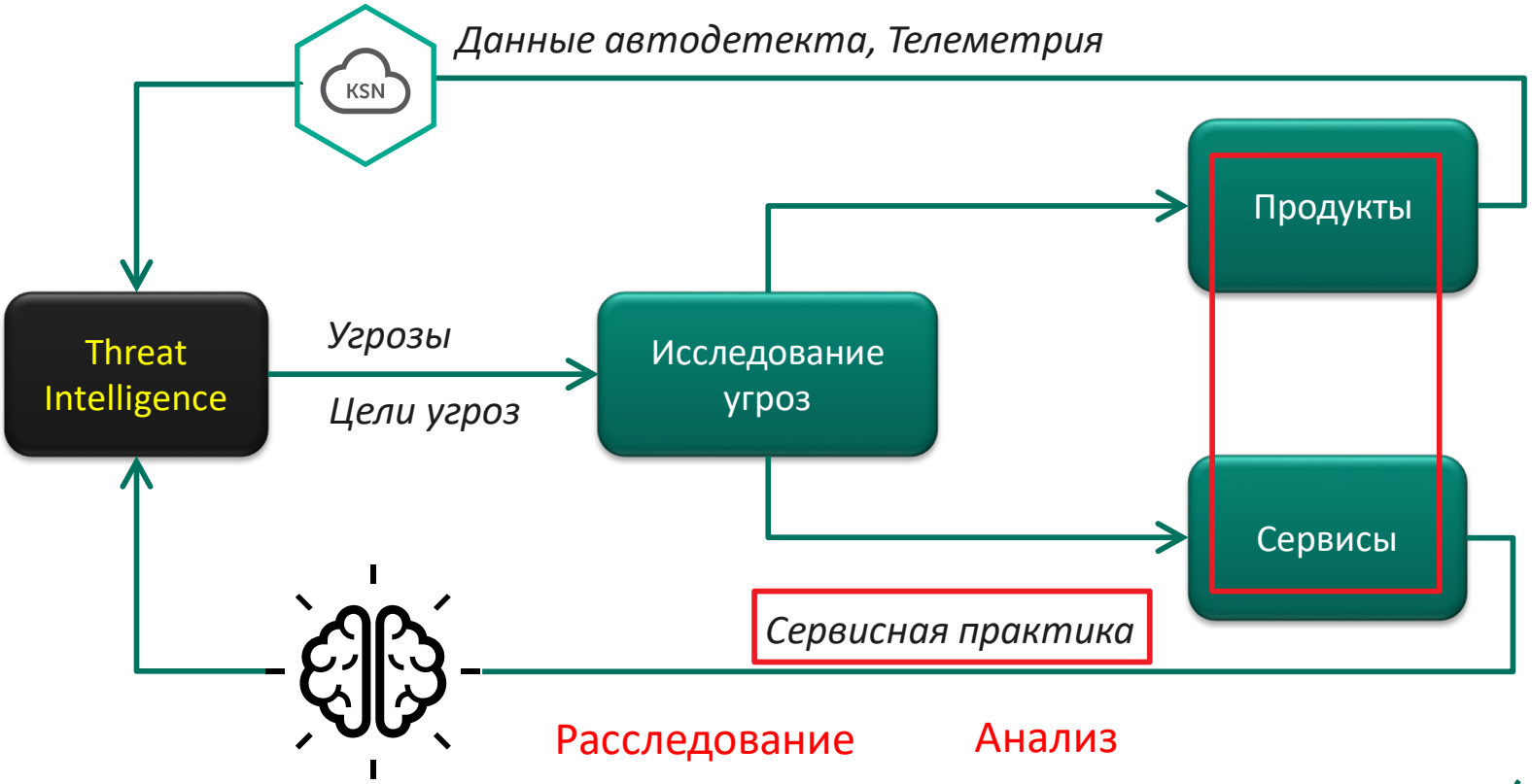


KASPERSKY lab

ЦИКЛ ДАННЫХ ОБ УГРОЗАХ



ЦИКЛ ДАННЫХ ОБ УГРОЗАХ

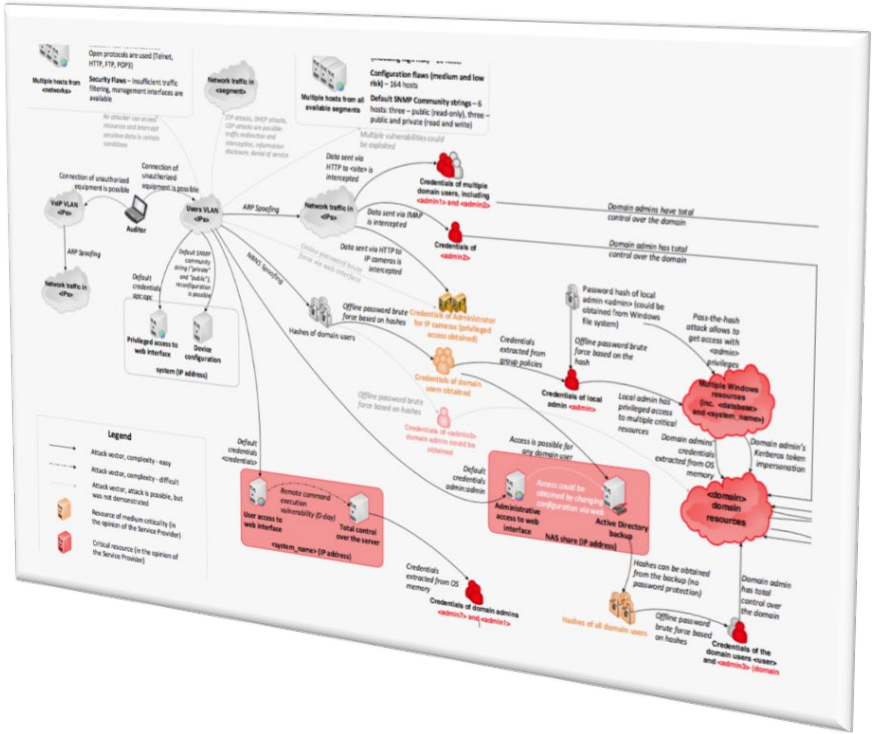


Расследование инцидентов

Анализ защищенности

ИМИТАЦИЯ ДЕЙСТВИЙ АТАКУЮЩЕГО («RED TEAMING»)

- Цель: Оценка операционной готовности SOC и обучение
- Тщательно готовится
- На выходе – полный список артефактов для оценки работы SOC
  - Детальное пошаговое описание атаки
  - С временными метками, инструментами
  - IoCs & IoAs
  - TTPs
- Опциональный семинар
  - Работа «Фиолетовой команды»



АНАЛИЗ ЗАЩИЩЕННОСТИ → КРАСНЫЕ КОМАНДЫ

How To Test Your MSSP/MDR?

by **Anton Chuvakin** | October 11, 2017 | Submit a Comment

As customary in our beloved domain of "cyber", I will start with a depressing quote:

> *"If you really knew how to test an MSSP properly, you likely didn't need an MSSP."* (source: in this thread somewhere, if the author reads this, I am happy to ack by name)

On a more serious note, *clients must test* their Managed Security Services (MSS) or Managed Detection and Response (MDR) provider! In fact, there are two different things to discuss:

- **TEST BEFORE CONTRACT SIGNING** in order to pick the partner with the quality of security you a/ need and b/ are willing to pay for.
- **TEST DURING ONGOING OPERATION** in order to …*and this is tricky!*… test for ongoing value, check for degradation of service effectiveness, and even check to remind the MSSP that you care about the quality of delivery.

Before we talk more, we need to get this out of the way: we all know that some clients who sign up with an MSSP do NOT want quality. They need a checkbox, a party to scream at (and possible to sue) when they are hacked. We are not going to discuss this case…today.

While we want a framework to emerge eventually, here are some ideas, from heavy/deep to light/shallow tests:

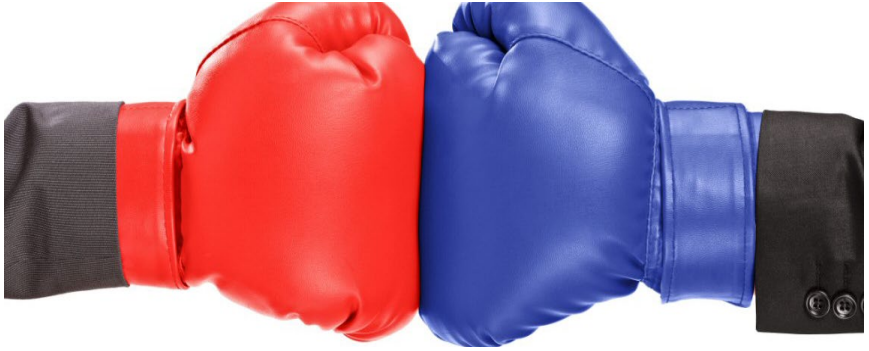
- **HEAVY** (and expensive): A full red team test or a quality pentest [without telling the MSSP/MDR]; your partner should catch them reliably and early in their process.
- **MEDIUM**: some people reported using *threat simulation tools* that generate [hopefully] realistic attack or exfiltration traffic and other "bad-looking" activities; you can probably just vuln scan a box too…
- **LIGHT**: A basic test can be as easy as unplugging an MSSP hardware sensor or blocking its network access (or log flow) and checking how fast they notice 🙂

Pentesting and Red Teams

by **Augusto Barros** | March 31, 2017 | 3 Comments

A red team should be a continuous operation to keep the blue team on its toes. With continuous operations the red team can pick opportunities and scenarios that best fit the threat landscape of the organization at each moment and also work together with the blue team to force it into a continuous improvement mode. This also answers a common question about when to implement a red team: continuous improvement is often a defining factor of the highest maturity level in any maturity scale. So, it makes sense to assemble a red team (a continuous one, not a single "red team exercise", which is just another pentest) when you already on a reasonably high maturity and wants to move into the continuous improvement territory.

https://blogs.gartner.com/augusto-barros/2017/03/31/pentesting-and-red-teams/

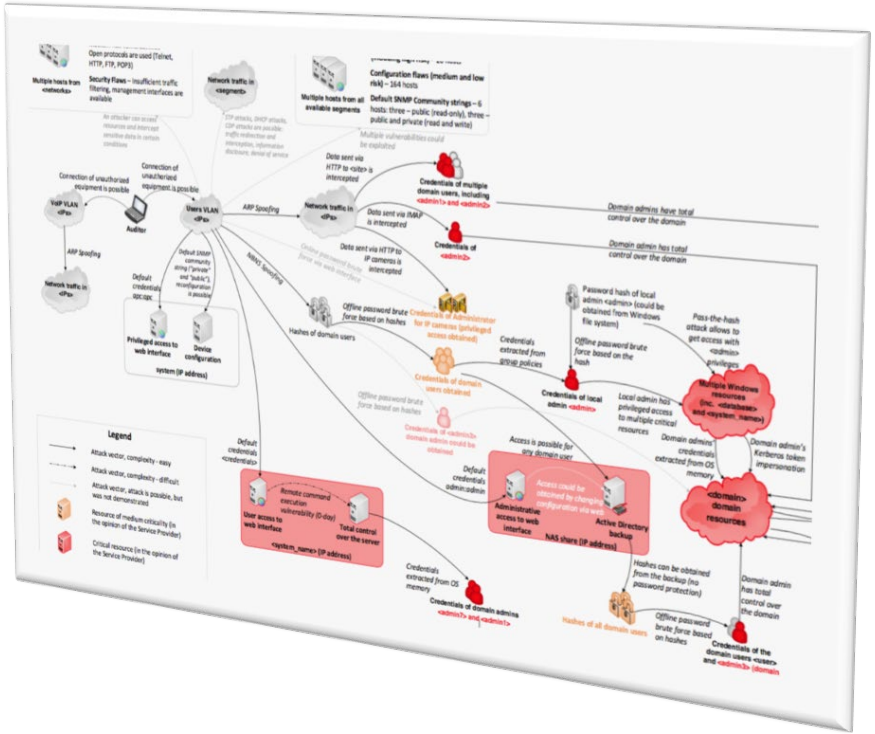


https://blogs.gartner.com/anton-chuvakin/2017/10/11/how-to-test-your-msspmdr/

KASPERSKY lab

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

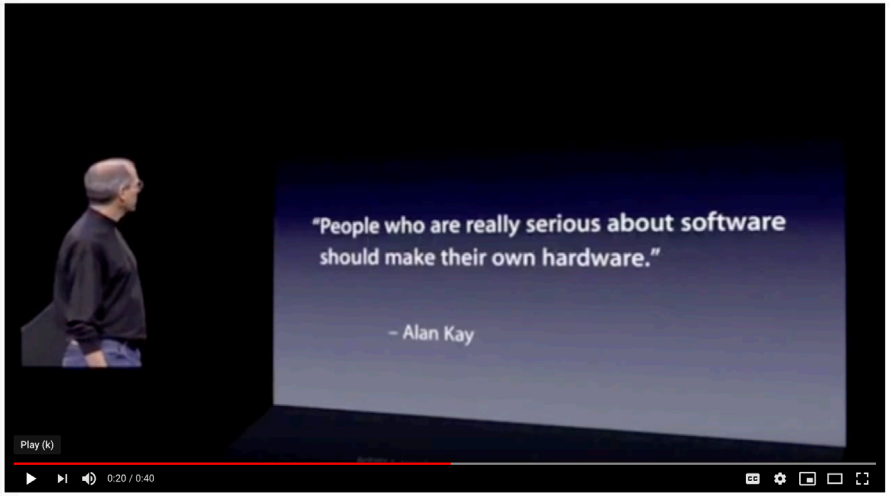
- Цель: Проследить все этапы атаки и установить корневые причины
- Цифровая криминалистика и анализ ВПО
- На выходе – полный список артефактов атаки, для взятия в работу SOC
  - Описание выявленных образцов ВПО
  - Подробное описание этапов атаки
  - Рекомендации по обнаружению и предотвращению


Legend
Attack vector, complexity - easy
Attack vector, complexity - difficult
Attack vector, attack is possible, but was not demonstrated
Resource of medium criticality (in the opinion of the Service Provider)
Critical resource (in the opinion of the Service Provider)
Open protocols are used (Telnet, HTTP, FTP, POP3)
Security flaws – insufficient traffic filtering, management interfaces are available
Configuration flaws (medium and low risk) – 164 hosts
Default SNMP Community strings – 6 hosts: three – public (read-only), three – public and private (read and write)
Credentials of multiple domain users, including <admin1> and <admin2>
Credentials of <admin2>
Credentials of Administrator for IP cameras (privileged access obtained)
Credentials of domain users obtained
Credentials of local admin <admin>
Credentials of <admin3> domain admin could be obtained
Credentials of domain admins <admin3> and <admin1>
Credentials of the domain users <user> and <admin3> domain
Domain admins have total control over the domain
Domain admin has total control over the domain
Password hash of local admin <admin> (could be obtained from Windows file system)
Pass-the-hash attack allows to get access with <admin> privileges
Offline password brute force based on the hash
Multiple Windows resources (inc. <database> and <system_names>)
Local admin has privileged access to multiple critical resources
Domain admins' credentials extracted from OS memory
Domain admin's Kerberos token impersonation
<domain> domain resources
Domain admin has total control over the domain
Credentials extracted from group policies
Offline password brute force based on hashes
Hashes of domain users
Hashes of all domain users
Hashes can be obtained from the backup (no password protection)
Offline password brute force based on hashes
Access is possible for any domain user
Access could be obtained by changing configuration via web
Administrative access to web interface
Active Directory backup
NAS share (IP address)
Remote command execution vulnerability (0-day)
User access to web interface
Total control over the server
<system_name> (IP address)
Credentials extracted from OS memory
Credentials of domain admins <admin3> and <admin1>
Default credentials <credential>
Default credentials admin:admin
Privileged access to web interface
Device configuration
system (IP address)
Default credentials spc:spc
Default SNMP community string "private" and "public"; reconfiguration is possible
Connection of unauthorized equipment is possible
Auditor
VoIP VLAN <IPv>
Users VLAN <IPv>
Network traffic in
Network traffic in <IPv>
Multiple hosts from all available segments
Multiple hosts from <network>
ARP Spoofing
DNS Spoofing
Data sent via HTTP to <site> is intercepted
Data sent via HTTP to IP cameras is intercepted
Data sent via FMU is intercepted
Multiple vulnerabilities could be exploited
An attacker can exceed resources and intercept sensitive data in certain conditions
CDP attacks, DHCP attacks, CDP attacks are possible: traffic redirection and interception, information disclosure, denial of service

КОМПЛЕКСНЫЙ ПОДХОД

- Сервис получает эффективные инструменты, наибольшим образом отвечающие запросам

- Инструменты получают бесценный опыт использования → план развития, основанный на практике



Steve Jobs Quoting Alan Kay

Алан Кей, 1982
Стив Джобс, 2007

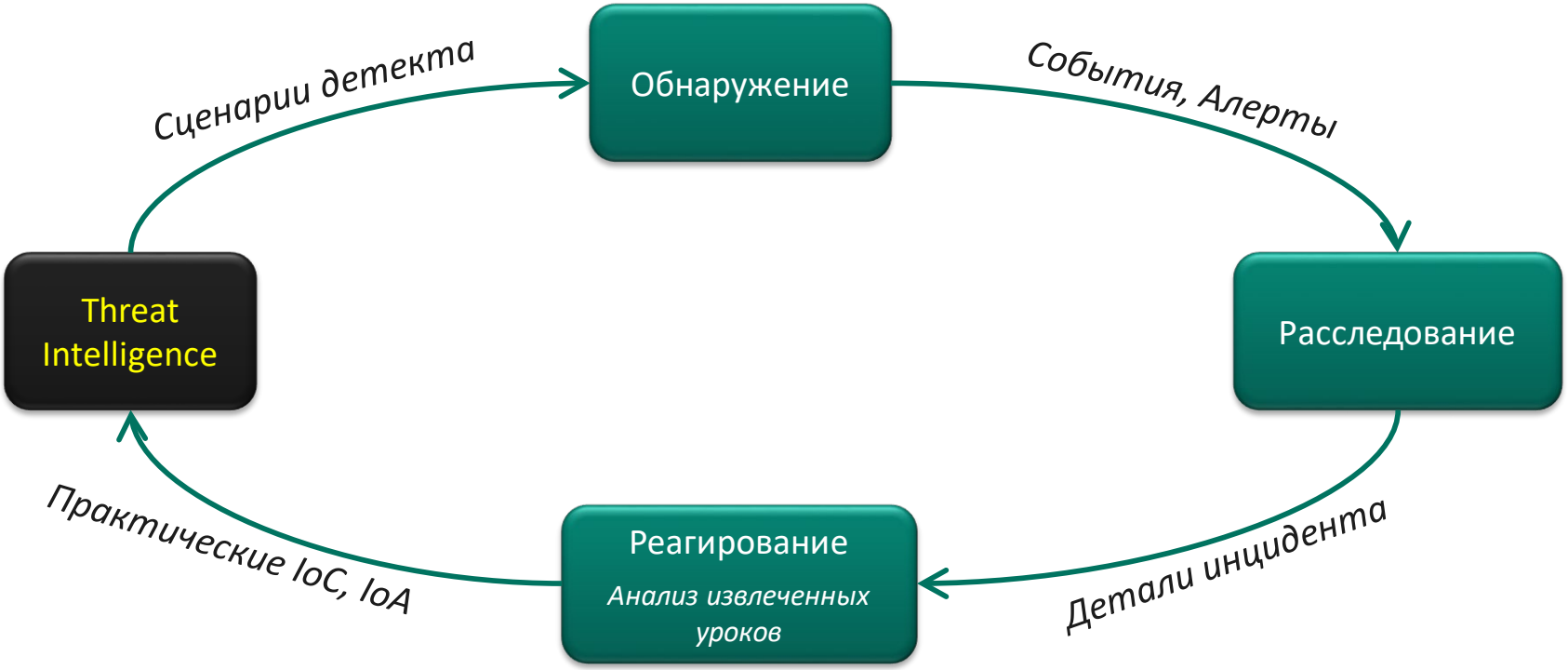
«Компания, выпускающая инструменты, должна предоставлять сервисы на их основе»

«Только комбинация инструментов и услуг дают результат»

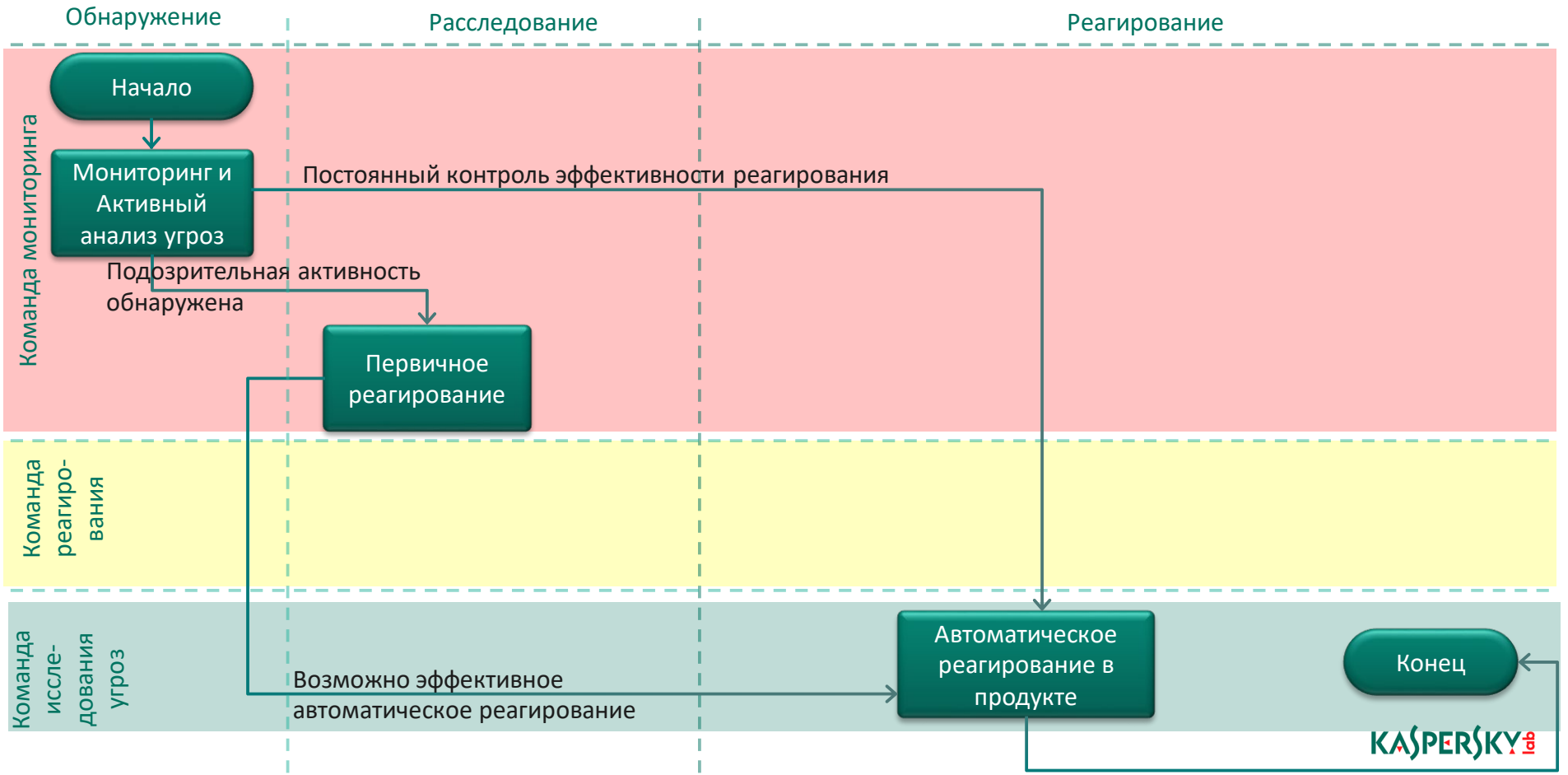
https://reply-to-all.blogspot.com/2015/04/blog-post.html

ИНГРЕДИЕНТ №2: ПРОЦЕСС

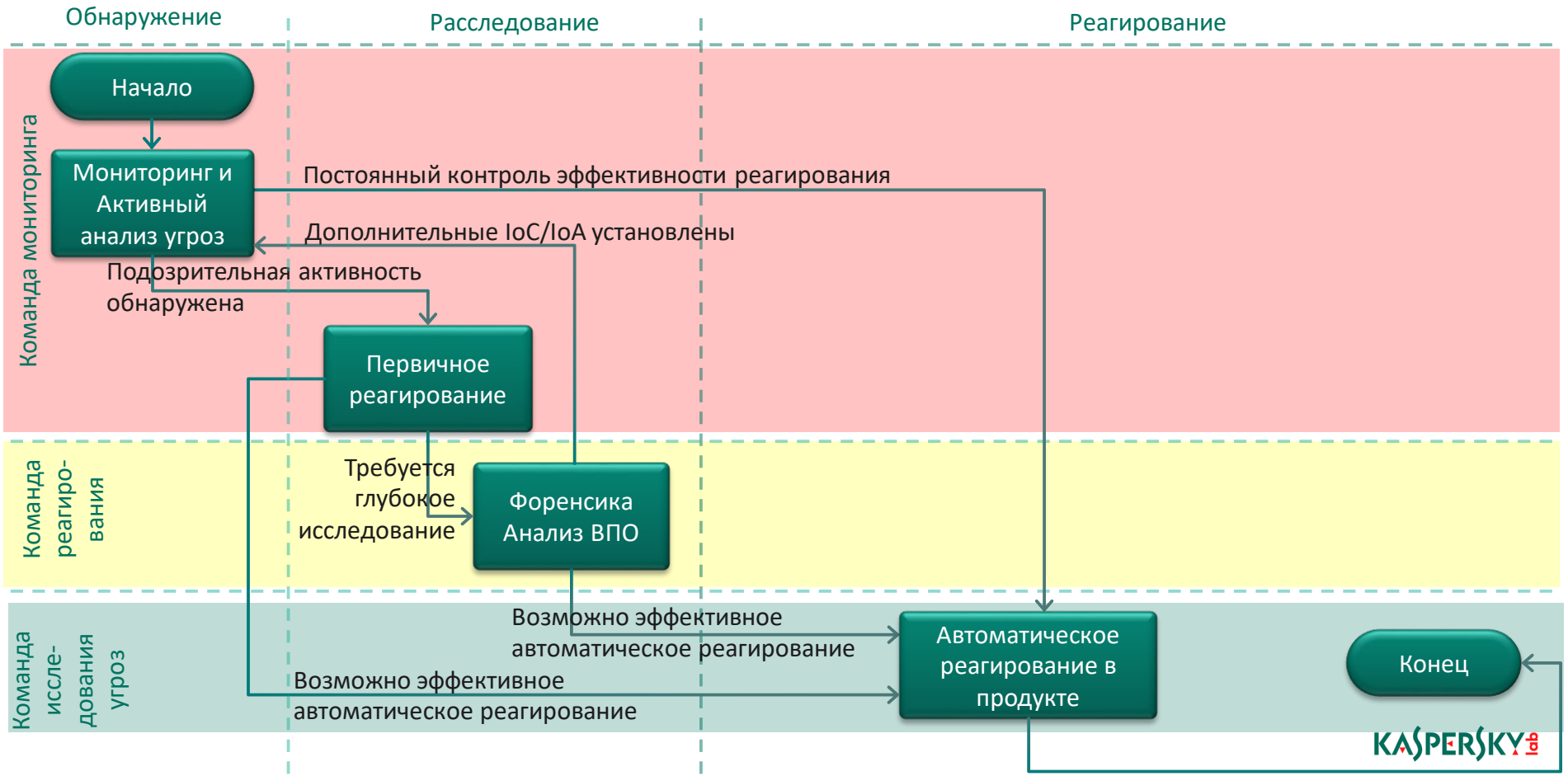
ОПЕРАЦИОННАЯ ИБ НА ПРЕДПРИЯТИИ (ПРОСТО)



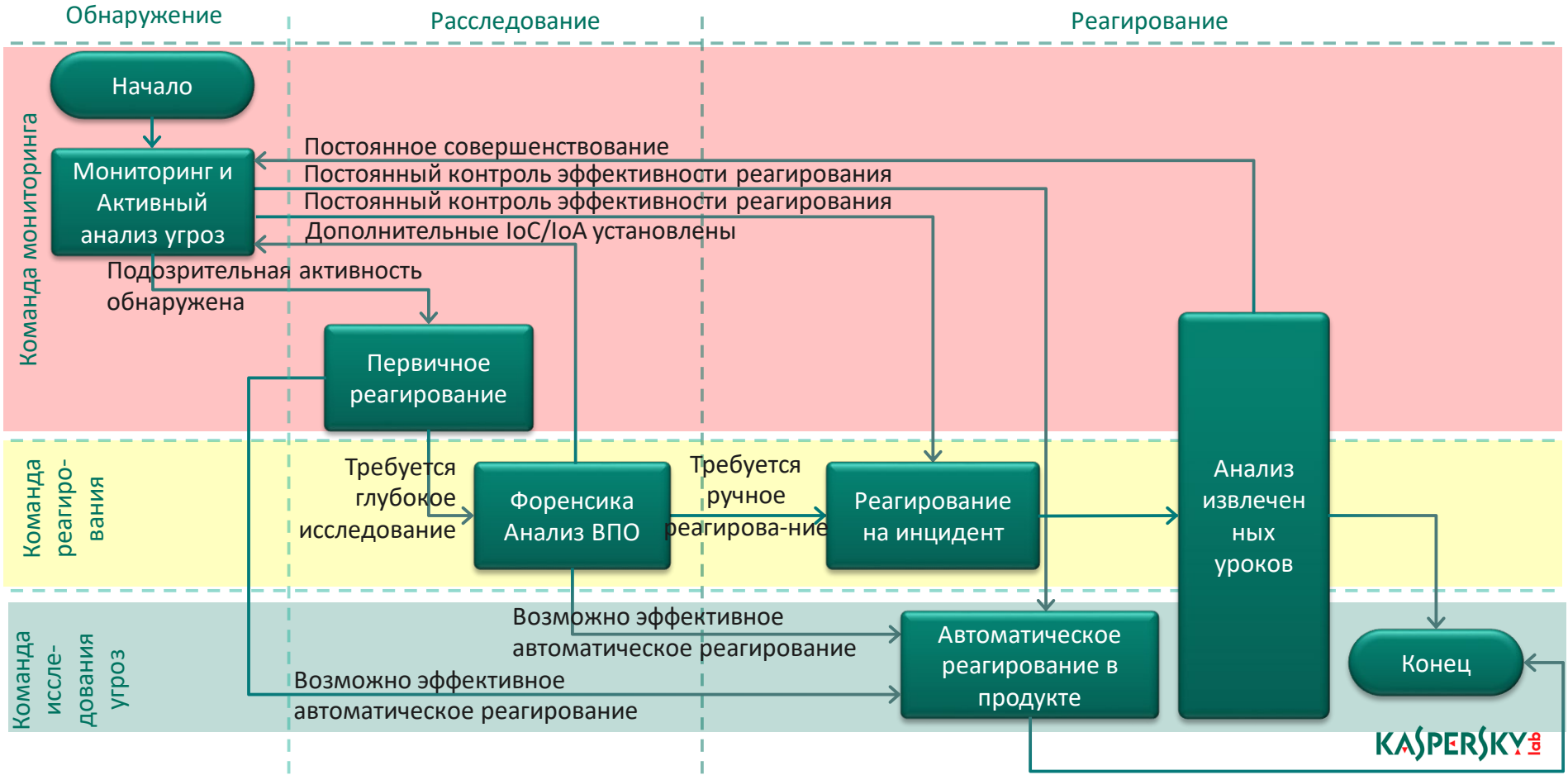
ОПЕРАЦИОННАЯ ИБ И ПРОДУКТЫ



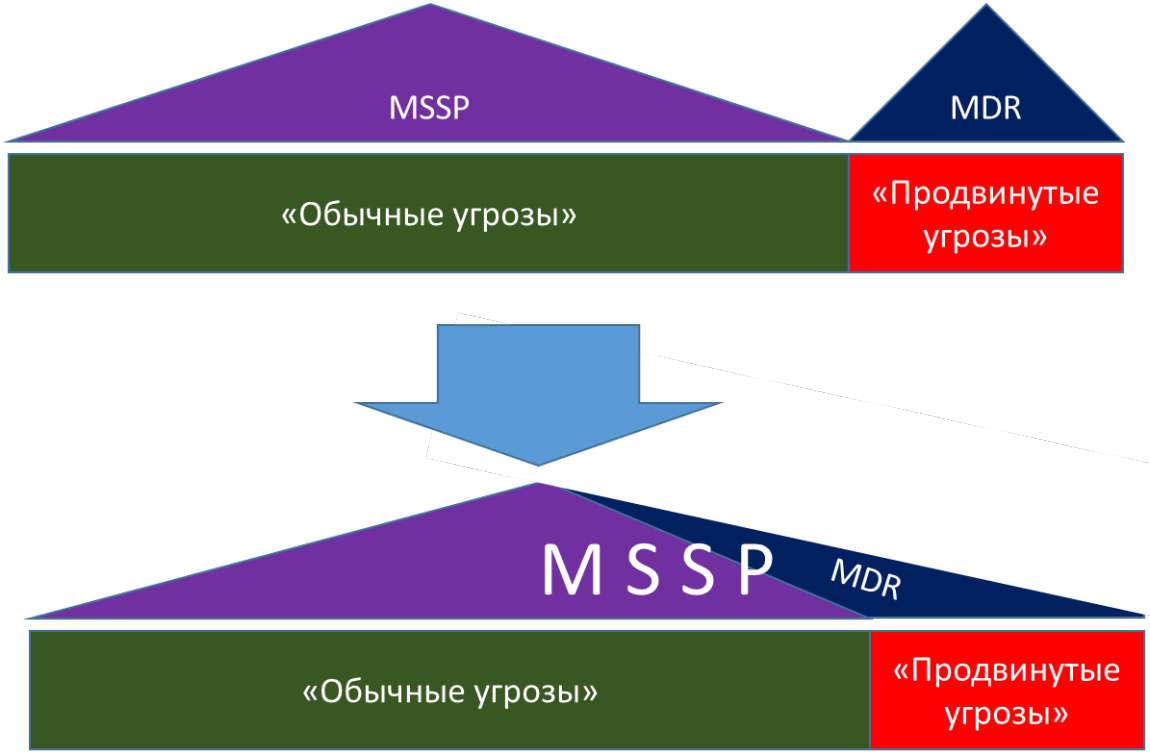
ОПЕРАЦИОННАЯ ИБ И ПРОДУКТЫ



ОПЕРАЦИОННАЯ ИБ И ПРОДУКТЫ



MDR*? MEDR**?? MSSP???



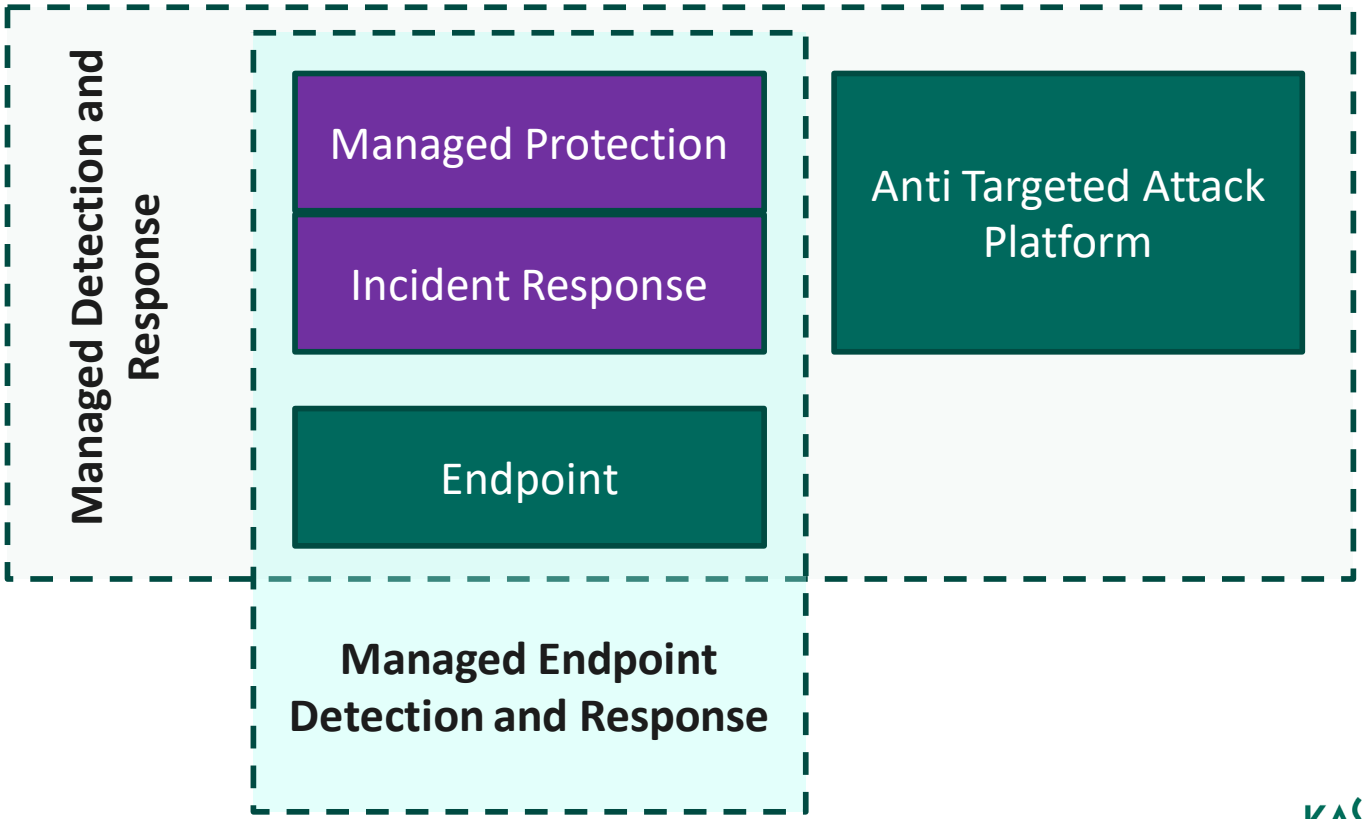
Высокая эффективность MSSP обеспечивается **жесткой формализованностью его бизнес-процессов**, зарегулированностью и алгоритмизацией деятельности участников

* Managed Detection and Response
** Managed Endpoint Detection and Response

http://reply-to-all.blogspot.com/2018/07/managed-defence-and-response.html

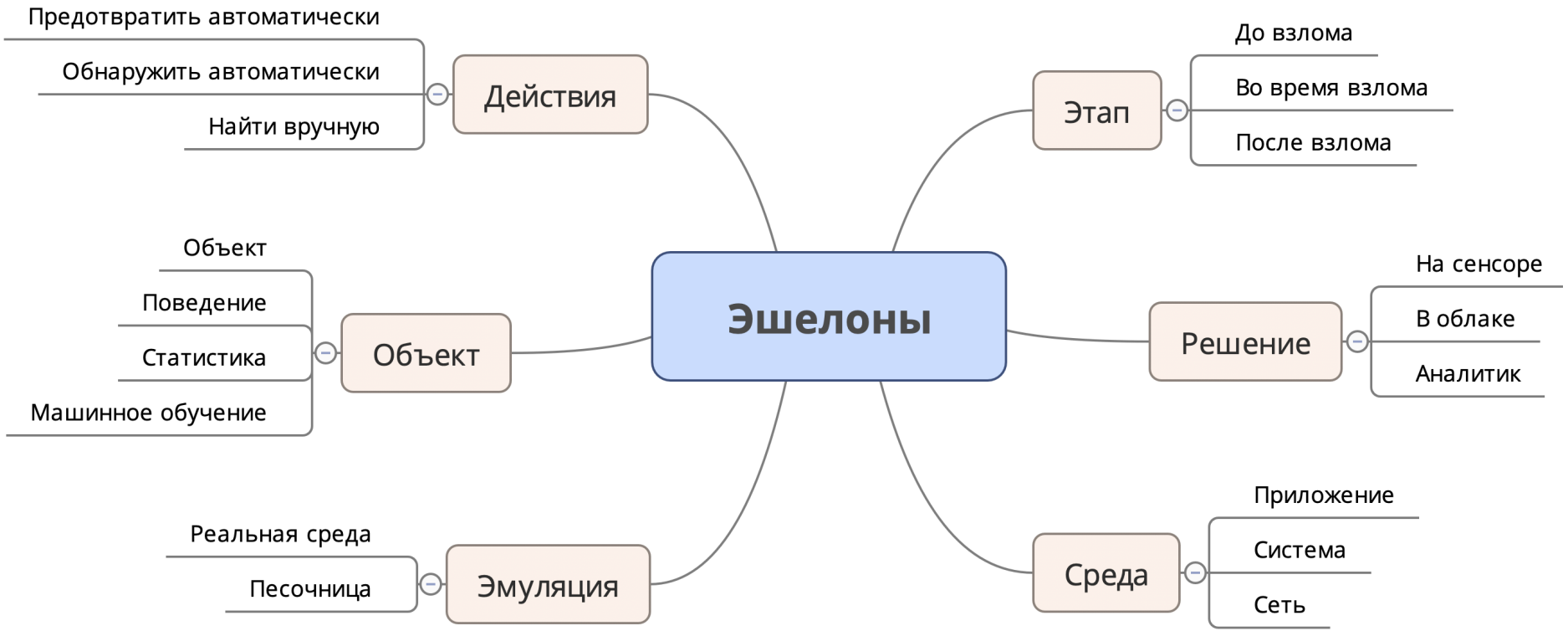
ИНГРЕДИЕНТ №3: ТЕХНОЛОГИИ

MDR И MEDR



KASPERSKY lab

ПЕРСПЕКТИВЫ: ПО ВСЕМ ФРОНТАМ



https://www.youtube.com/watch?v=5-CoJNjtAmY

KASPERSKY lab

АУТСОРСИНГ?

Я сам	Умный консультант
Знаю чего боюсь	Не знает что для Компании актуально
Знаю свою инфраструктуру и приложения	Не знает ИТ-комплекс Заказчика
Знаю своих работников	Не знает персонал Заказчика
Вижу только себя	**Видит глубже и шире**
Не проф. в спец. областях: реверс, форенсика, пентест, threat hunting и т.п.	**Проф. в спец. областях**

Развивайте свои **сильные** стороны,
а слабые – компенсируйте сервисом тех,
у кого это – **сильная** сторона!

http://reply-to-all.blogspot.ru/2016/04/blog-post.html

СПАСИБО ЗА ВНИМАНИЕ!

Сергей Солдатов, CISA, CISSP

Обязательно приходите на «MITRE ATT&CK в повседневной работе SOC»

KASPERSKY