IBM Security

Обработка инцидента после его выявления

ПЛАТФОРМА И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПОМОЩЬ АНАЛИТИКУ

Эльман Бейбутов
Представитель по продвижению IBM Security

18 мая 2017 г.

IBM

IBM Security

СЛАЙД ДЛЯ ПРОВЕРКИ КЛИКЕРА

И ДЛЯ НЕБОЛЬШОГО СПИЧА МИНУТ НА СОРОК

18 мая 2017 г.

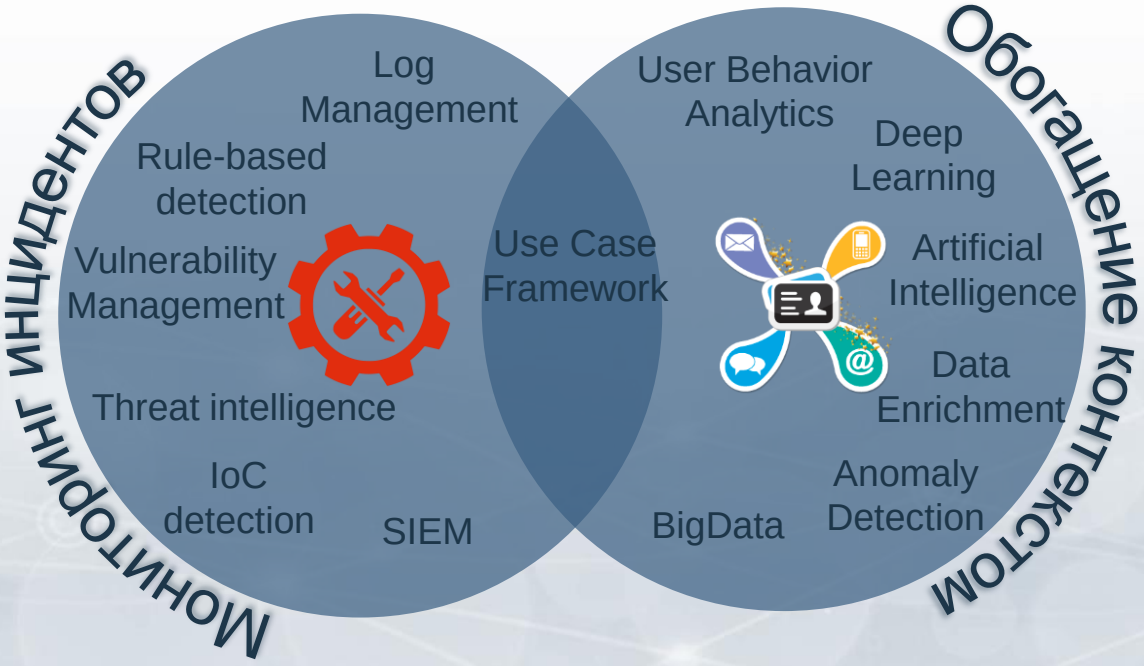
IBM

Когнитивный SOC

- Цели SOC
- Задачи SOC
- **Когнитивные технологии**
- Реагирование
- Выводы

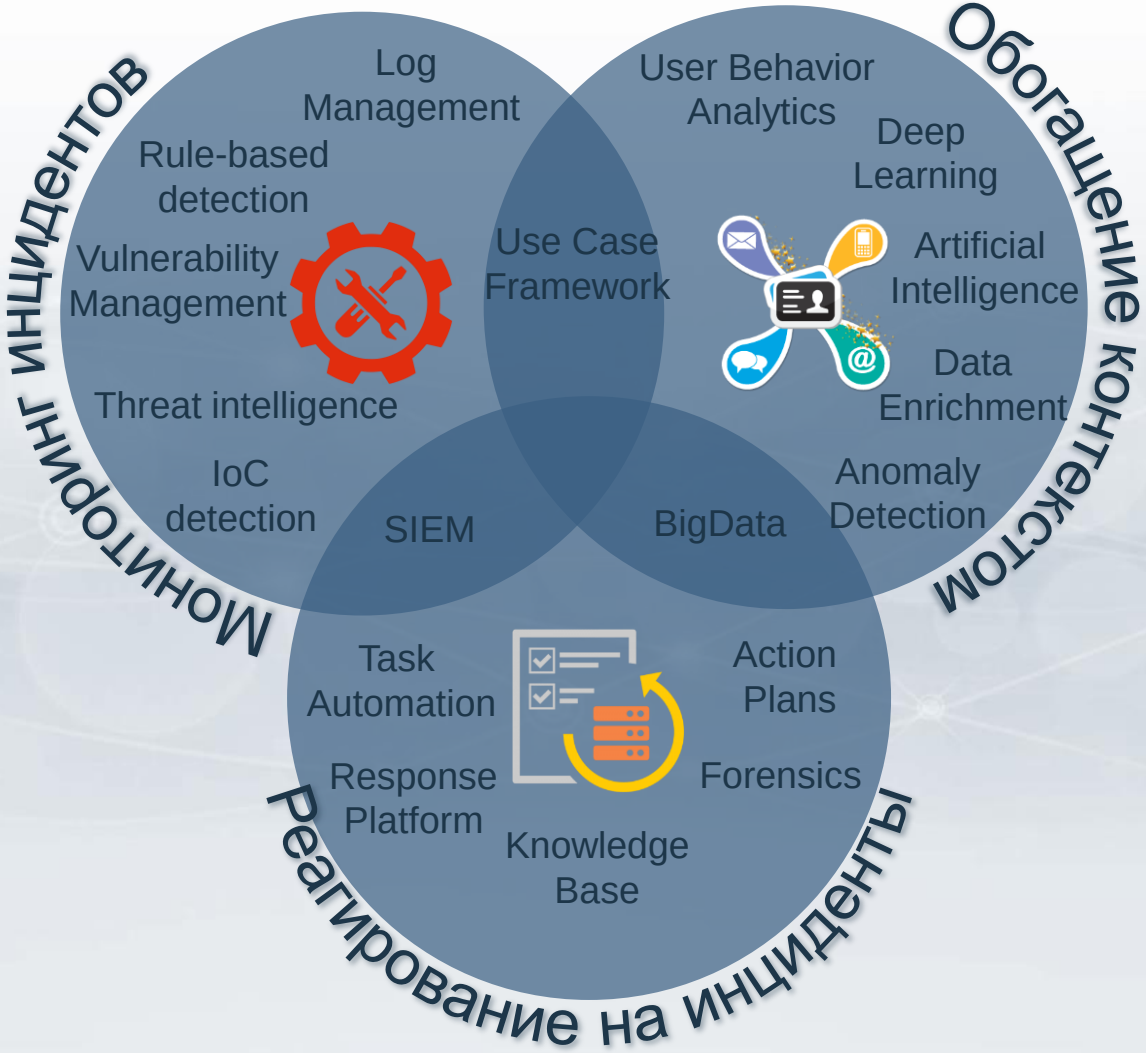
Когнитивный SOC

- Цели SOC
- Задачи SOC
- **Когнитивные технологии**
- Реагирование
- Выводы



Когнитивный SOC

- Цели SOC
- Задачи SOC
- **Когнитивные технологии**
- Реагирование
- Выводы

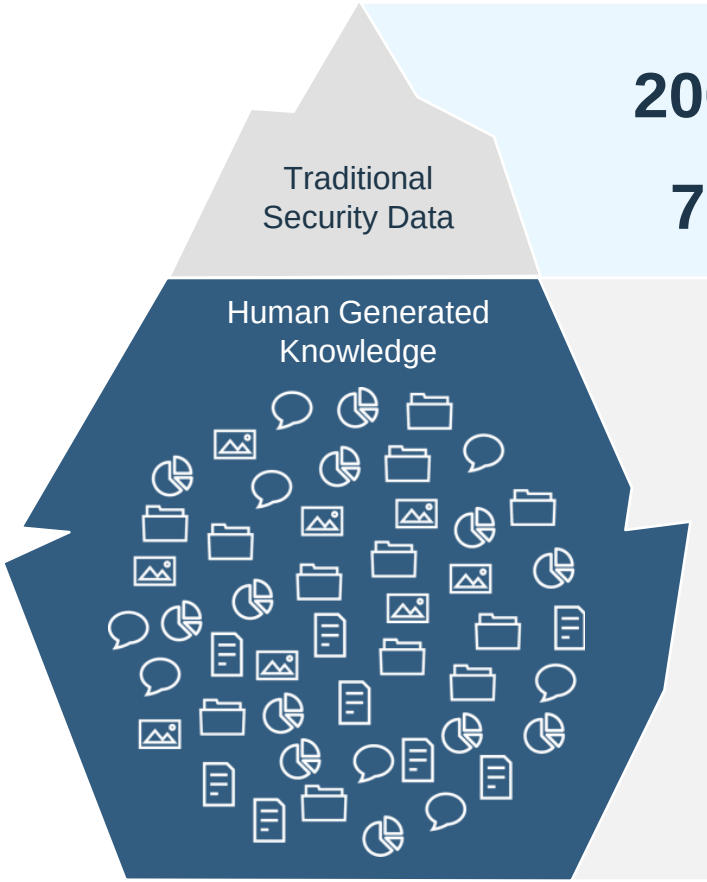


Когнитивный SOC

- Цели SOC
- Задачи SOC
- **Когнитивные технологии**
- Реагирование
- Выводы

Искусственный интеллект в помощь аналитику

Огромный объем данных об ИБ создается, но потребляется только его малая часть



200K+ security events viewed each day

75K+ reported software vulnerabilities

- Security events and alerts
- Logs and configuration data
- User and network activity
- Threat and vulnerability feeds

A universe of security knowledge Dark to your defenses

Typical organizations leverage only 8% of this content*

720K security blogs / year

180K security related news articles / year

10K security research papers / year

- Industry publications
- Forensic information
- Threat intelligence commentary
- Analyst reports
- Conference presentations
- News sources
- Newsletters
- Tweets
- Wikis

[1] Forrester Research : Can You Give The Business The Data That It Needs? , 2013

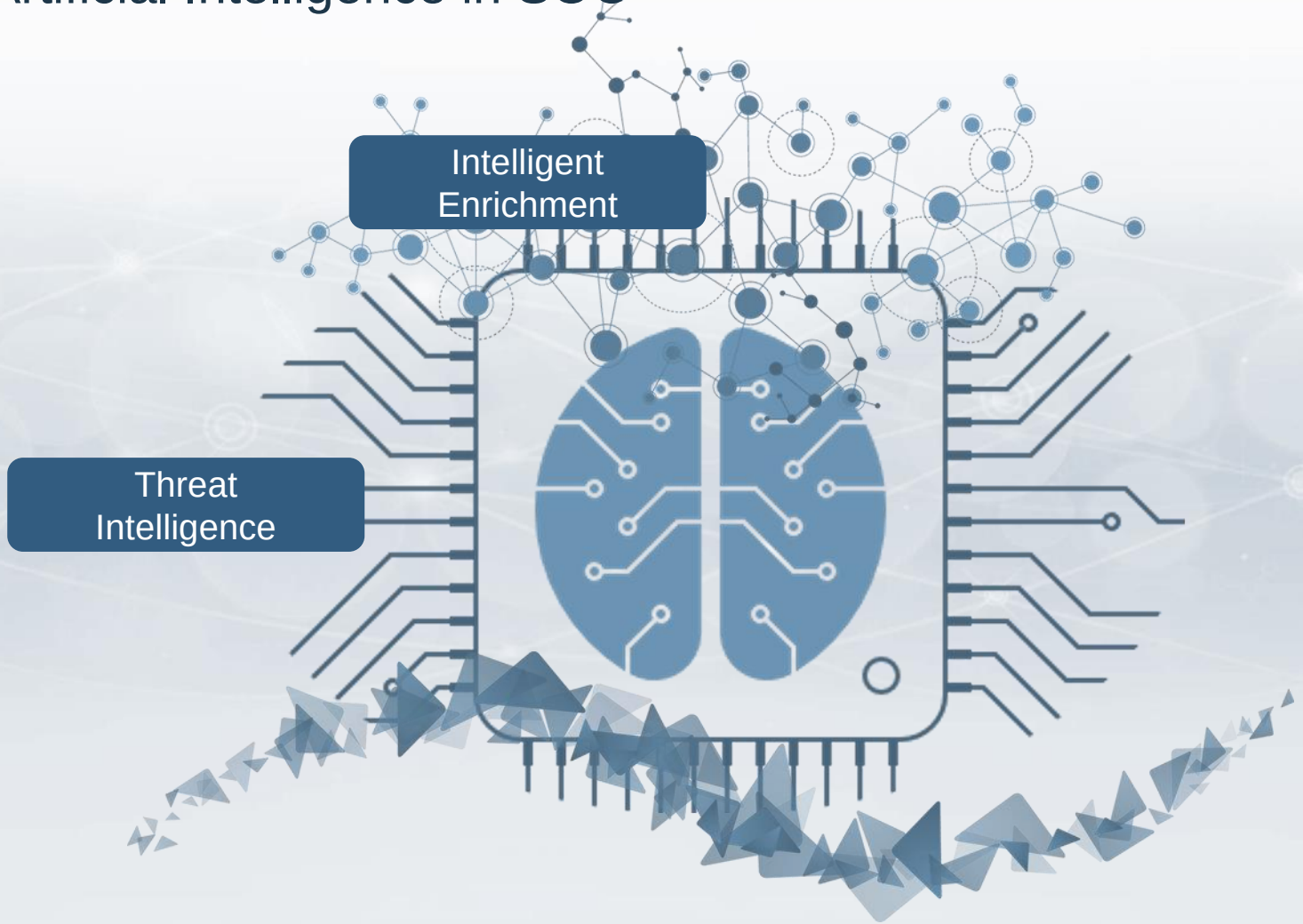
Насколько реально знать все?

”There is a massive amount of noise out there; the human brain can’t process everything on a day-to-day basis. We need something to help, something like AI or cognitive technologies.”

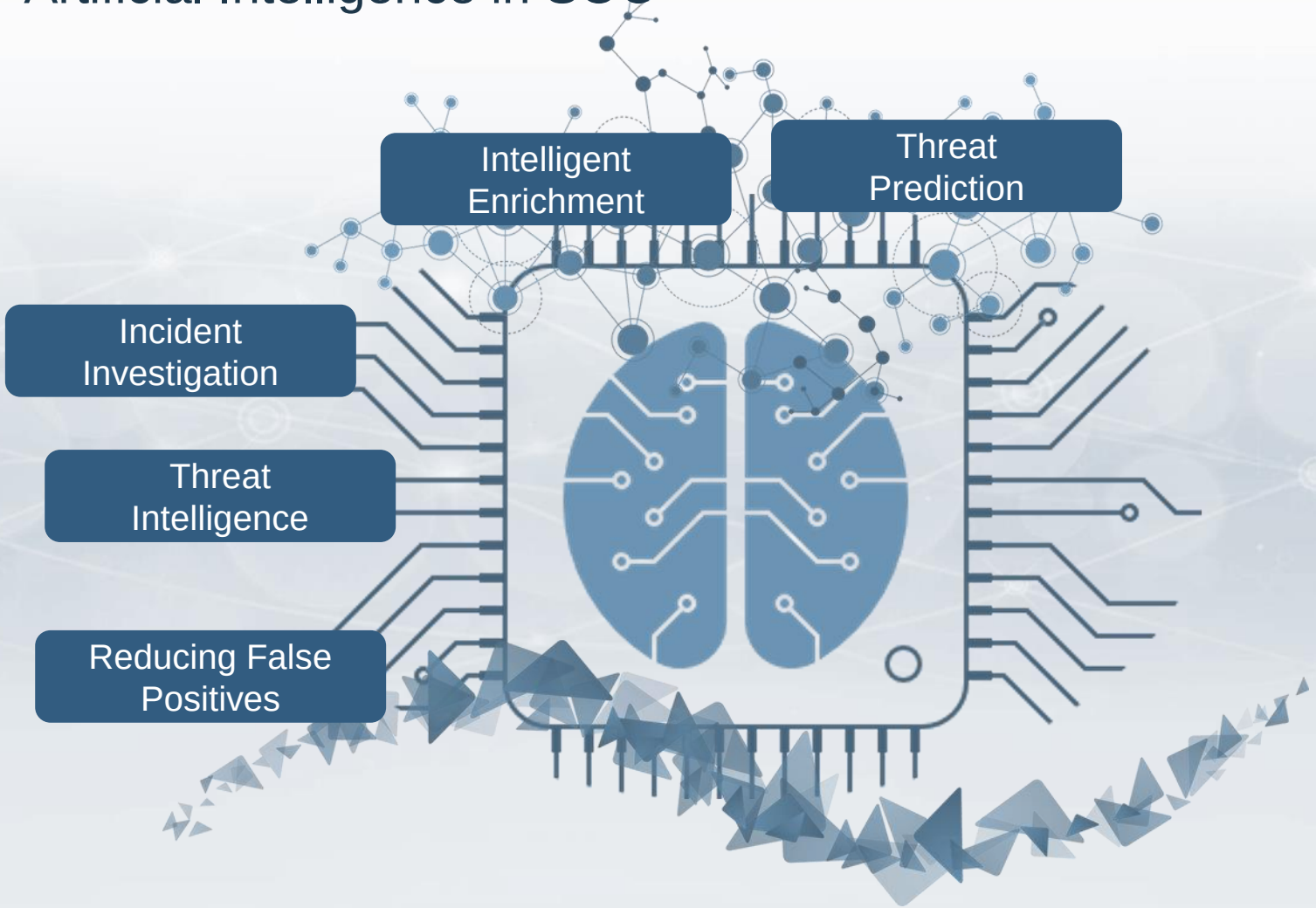
Chad Holmes – Principal and Cyber-Strategy, Technology and Growth Leader (CTO) at Ernst & Young LLP

- Цели SOC
- Задачи SOC
- **Когнитивные технологии**
  - User Behavior Analytics
  - Fast Data
  - **Artificial Intelligence**
- Реагирование
- Выводы

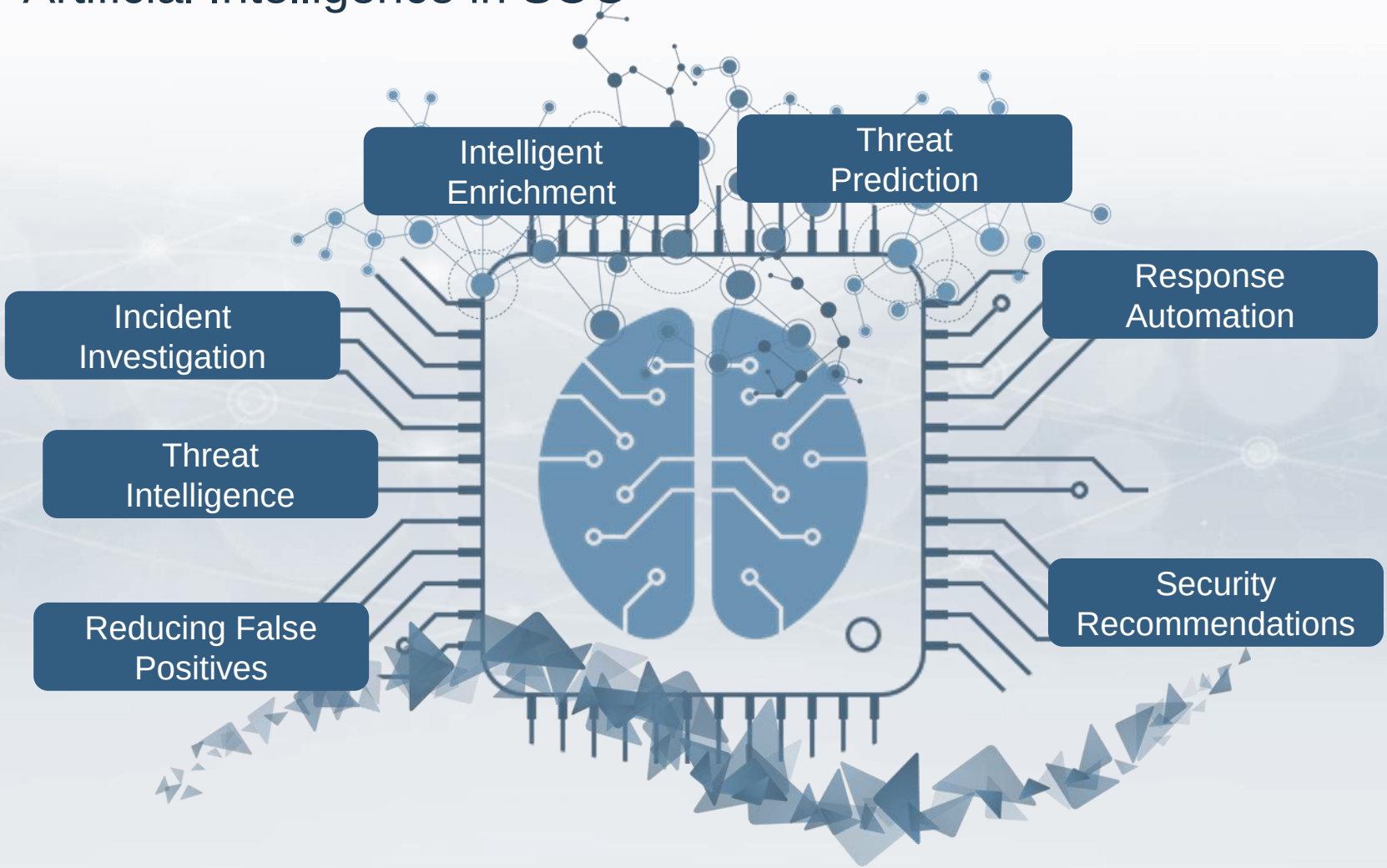
Artificial Intelligence in SOC



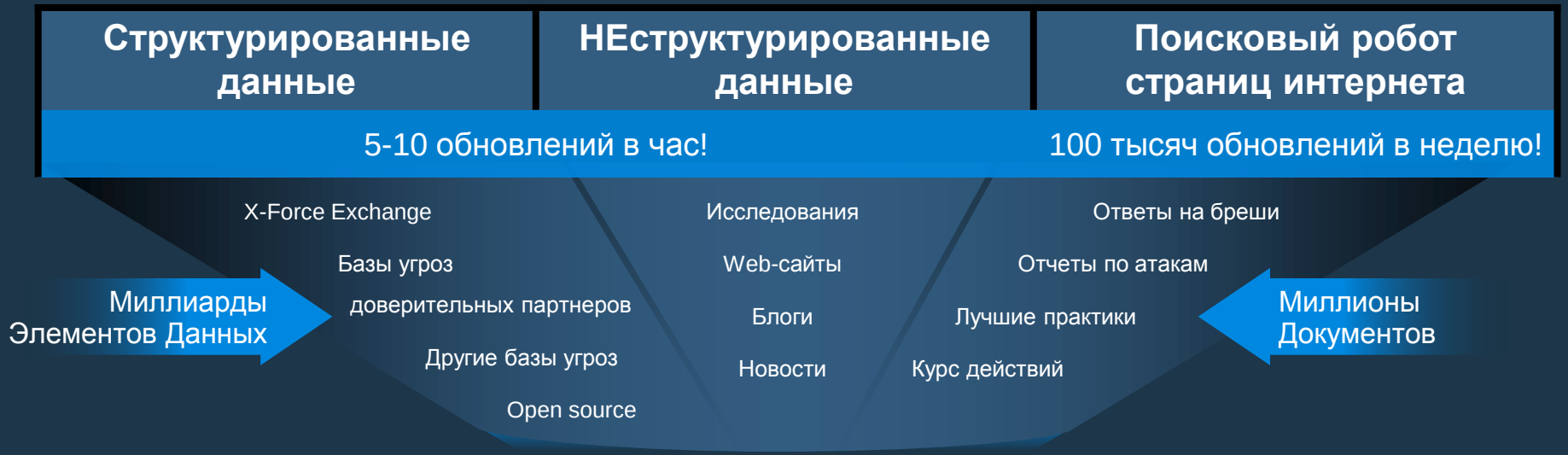
Artificial Intelligence in SOC



Artificial Intelligence in SOC



IBM Watson for Cyber Security в помощь аналитикам ИБ

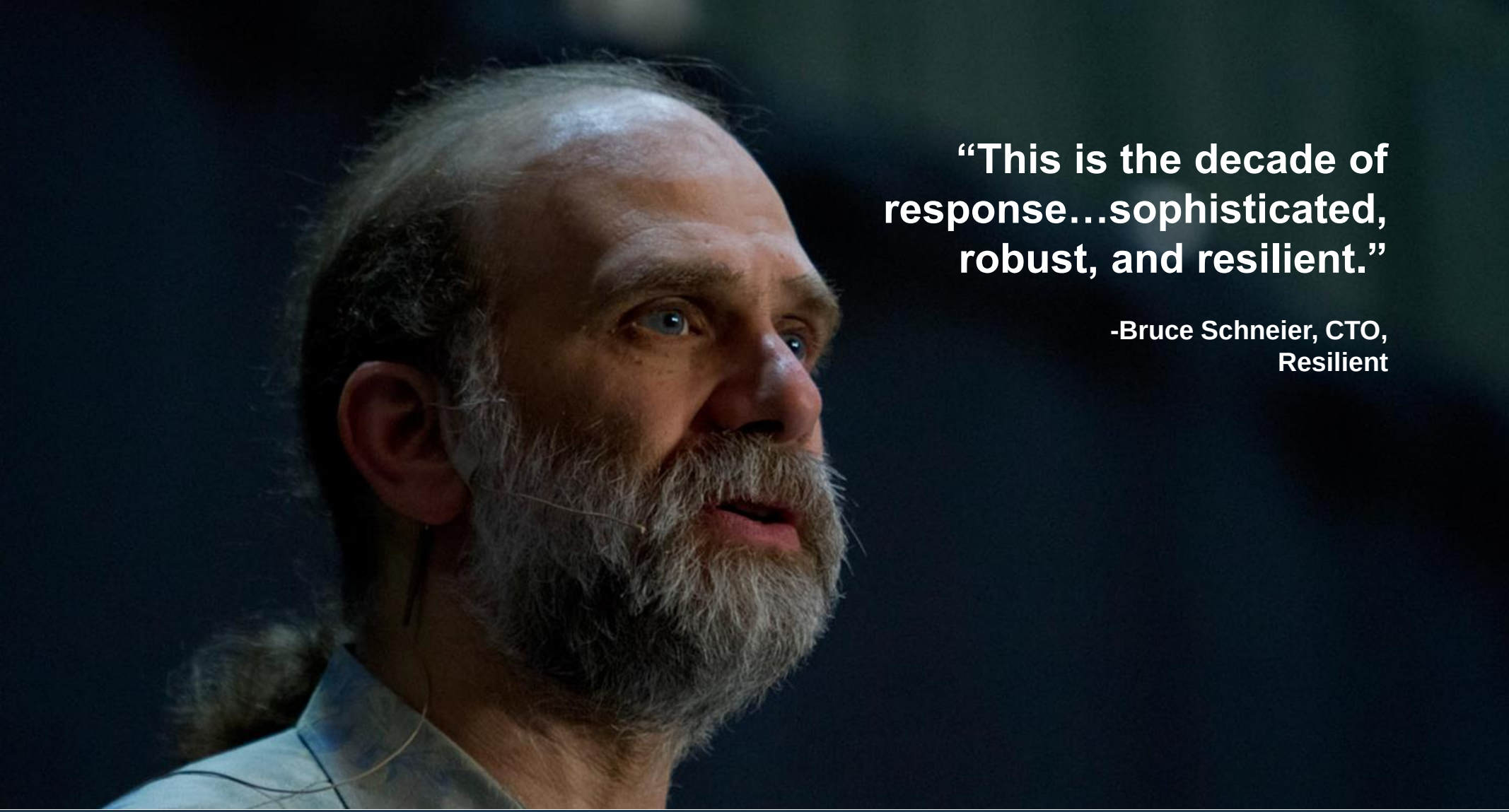


10 Млрд элементов плюс
4 Млн добавляется ежечасно

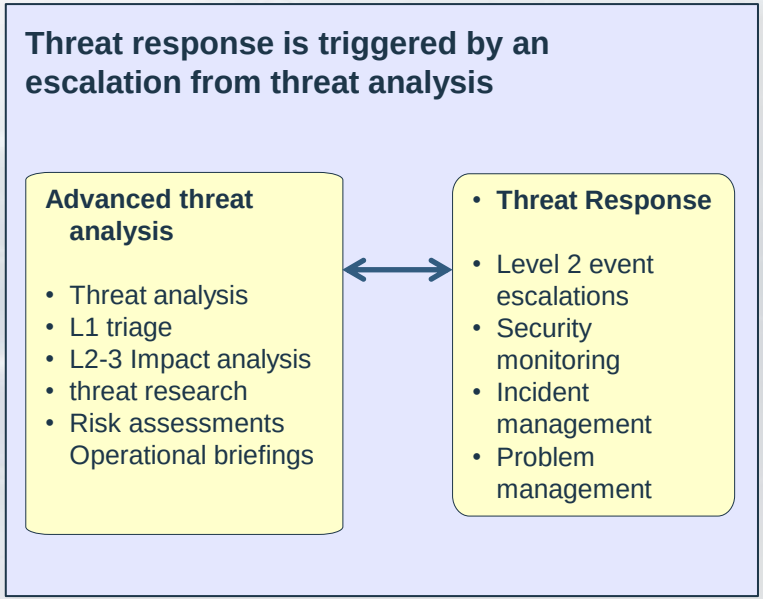
1,25 Млн документов плюс
15 Тысяч добавляется ежедневно

Крупнейшее собрание знаний в области кибербезопасности

Процесс и платформа реагирования на инциденты


“This is the decade of response…sophisticated, robust, and resilient.”
-Bruce Schneier, CTO, Resilient

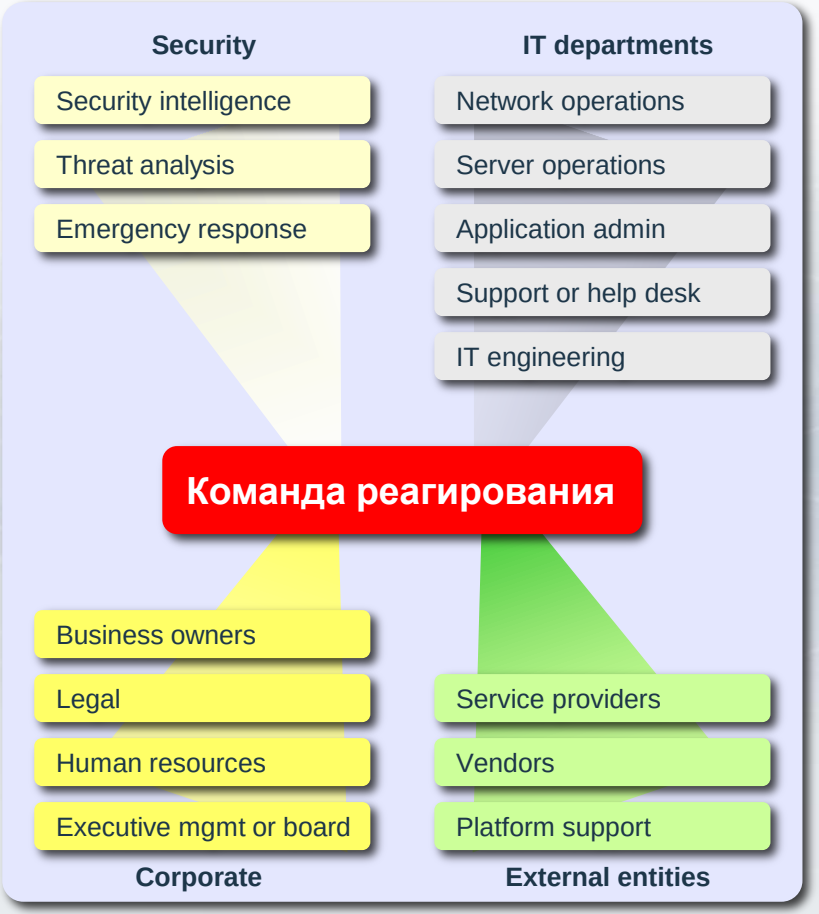
- **Знание - сила**
  As with threat analysis, threat response requires a complete understanding of the security landscape and the business impacts.
- **Изучение угроз безопасности**
  These include the external intelligence feeds that provide insight into the most recent developments in the global security landscape. It should provide the nature and severity of threats as well as actionable recommendations and advice.
- **Изучение специфики бизнеса**
  Internal awareness and documentation of the risks associated with key business processes and the underlying supporting infrastructure underpinned by current corporate security policies, legal obligations, and compliance requirements by the industry or the regulatory bodies or both.



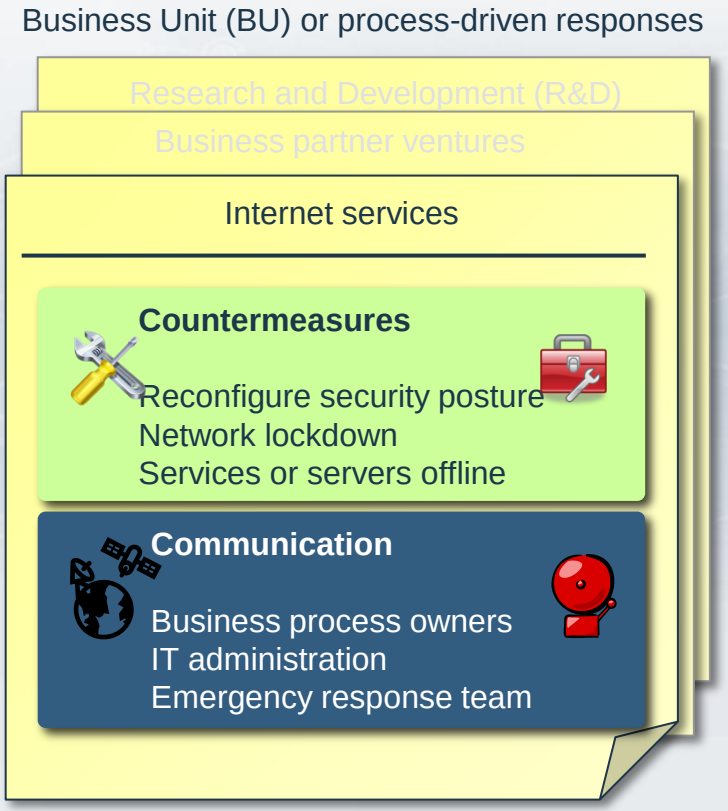
Когнитивный SOC

- Цели SOC
- Задачи SOC
- Когнитивные технологии
- **Реагирование**
  - Intelligence
  - **Coordination**
  - Mitigation
  - Remediation
  - Resolution
- Выводы

- **(Де)Централизованная реакция**
  The response to a threat or incident may be centrally coordinated by a single dedicated organization or it may be distributed around the enterprise. A centralized approach provides a mechanism for accountability and oversight that is more difficult in distributed models.
- **Координация и слаженность**
  An organized and effective response to an incident requires a collaborative effort both within the enterprise and in cooperation with external organizations.
- **Спланированные и отточенные действия**
  Using IT Business Continuity (BC) or Disaster Recovery (DR) plans as a model, threat response plans should be well-defined, regularly reviewed and maintained. It should also have executive approval and, where appropriate, tested to ensure efficacy.



- **Быстрые первые ответные действия**
  The first steps of any security incident response are comprised of actions designed to contain the threat and mitigate further risk exposure. First response actions require advanced planning and ideally include testing to ensure effective results.
- **Учитывайте специфику бизнеса**
  Containment and mitigation techniques will vary for every business process as actions that prove to be effective in one environment may not be effective enough in another environment.
- **Поддерживайте связь с руководством**
  A lack in communication to key stakeholders in the moments following a major security incident is commonly cited as a "lesson learned" in the post-mortem reports.



- **Определение и устранение факторов угрозы**
  It might take some time to eradicate the underlying vulnerability or weakness that allowed the incident to occur may take. The remediation component of threat response installs an enterprise-wide framework holding stakeholders accountable to correct core faults and prevent future activity.
- **Анализ причин возникновения инцидента**
  Research and discovery of the root causes of an incident are paramount to improving an enterprise's security posture. Root causes are rarely a failure in technology alone, rather those typically include procedural and human failure components as well.
- **Проведение расследования инцидента**
  Enlisting the assistance of a forensic or emergency response specialist may be required to preserve the chain of evidence and ensure eradication.

Threat response

Ликвидация – реактивна

component of threat response and …

Исправление - проактивно

component of threat response and includes patching, architectural redesign, and process improvement.

Исправление должно предотвратить появление повторных аналогичных инцидентов в будущем.

- **Описание инцидента и принятых действий**
  The final stage of every incident response is documentation. All relevant aspects of the incident impact are documented including estimate of loss in terms of time, reputation or brand, and financial loss; containment and remediation steps taken; root-cause analysis; and outstanding tasks with accountable owners.
- **Обратная связь от бизнес-блоков**
  Post-escalation, it is imperative for the threat response team to receive feedback on it's response. This feedback closes the circuit on the investigation and provides invaluable material for both threat analyst and threat response education and process improvement.
- **Систематизация знаний, полученных при расследовании инцидента**
  Every security investigation and escalation becomes input to all future investigations and creates a clean chain of evidence of monitoring activities.

SIEM + Incident Response

SIEM
Приоритезация информации из Logs, Flows, Vulns, User, Config Data и т.п.

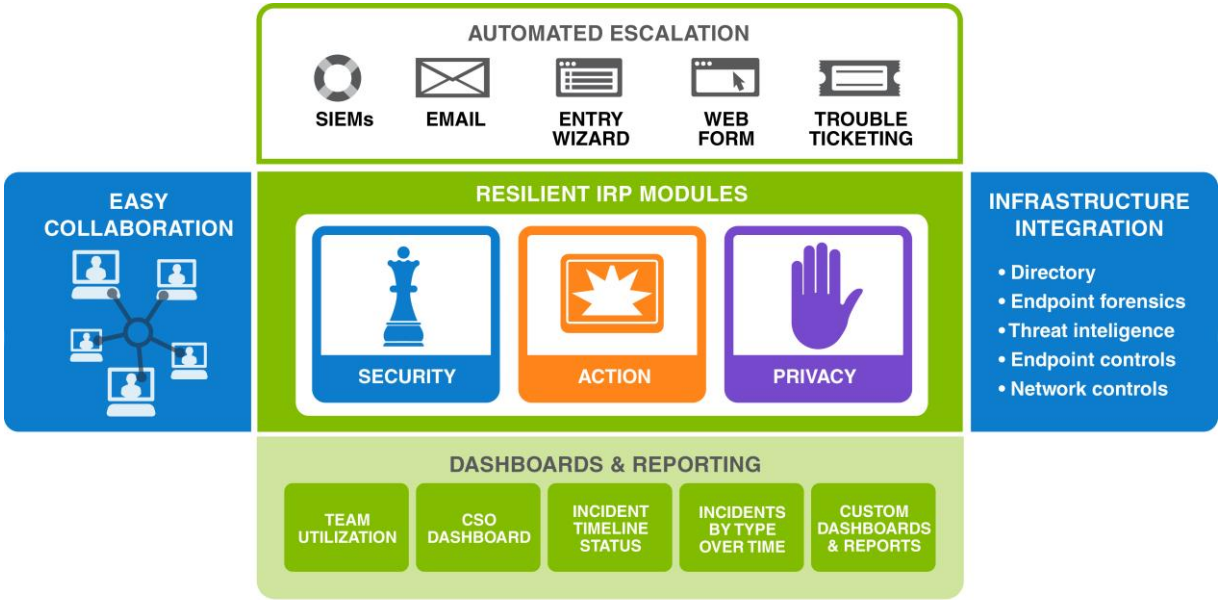
Процесс реагирования SOC на инцидент ИБ для ответа на угрозы, дыры, уязвимости

Постоянная аналитика ИБ

Три этапа инцидента ИБ

Улучшение процесса выявления инцидентов

Платформа Resilient Incident Response Platform (IRP)



Модуль SECURITY

- Стандарты workflows по индустрии (NIST, SANS)
- Подключение внешних баз знаний/угроз ИБ
- Стандарты организации
- Лучшие практики компании

Модуль ACTION

- Автоматизация процессов
- Обогатить детали инцидента
- Сделать расследование
- Снизить нагрузку

Модуль PRIVACY

- База регуляторов
- Требования нормативов
- Требования контрагентов
- Стандартные операции организации
- Лучшие мировые практики

Новое! *Resilient Standard IRP создан для постепенного помодульного внедрения полной версии Resilient Enterprise IRP – более 140 внедрений в мире.*

Особенности и подводные камни

- Попытки построить Security Operations Center без поддержки высшего менеджмента компании не принесут желаемого результата
- Обязательно нужны цели запуска SOC и поэтапный план их достижения
- Разбейте цели на задачи, определите границы, рассчитайте минимальный и максимальный бюджет SOC
- Согласуйте деятельность SOC со смежными подразделениями
- На самых ранних этапах начинайте создавать команду SOC
- Документируйте процессы, чтобы упростить ротацию в команде
- Определите KPI и согласуйте их с руководством, будьте понятны для высшего менеджмента компании

IBM Security

СПАСИБО

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM