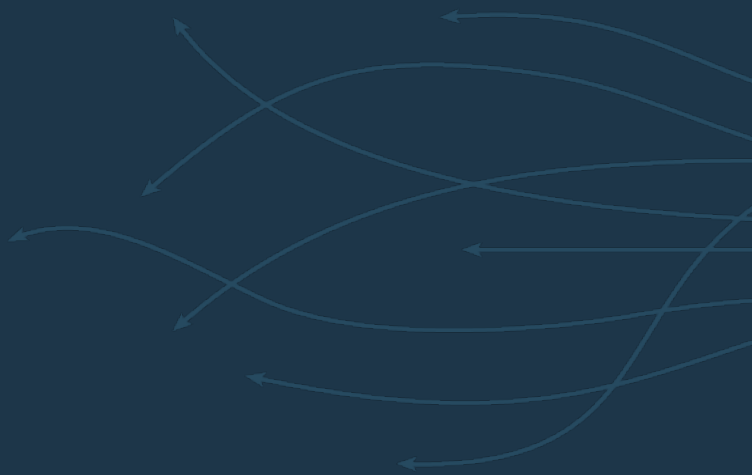
Эволюция корреляции -

КОГНИТИВНЫЕ КЕЙСЫ

Эльман Бейбутов



VB-Trend 2017

СЛАЙД ДЛЯ ПРОВЕРКИ КЛИКЕРА

COGNOSCERE (лат.)

ЗНАТЬ, УЗНАВАТЬ, РАССЛЕДОВАТЬ

- Обозначает знание, мыслительную способность, способность к изучению, сохранению знания и обмену им с другими

Когнитивные кейсы

- **Задачи SOC**
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Понимание задач SOC как функций безопасности

	Известно аналитику SOC	Не известно аналитику SOC
Известно атакующему	-1- Типовые фазы реализации атаки и соответствующие контроли Известные способы обхода User Access Control Детектируемое вредоносное ПО Детектируемые по сигнатурам атаки Отклонения от best practice частных политик ИБ И др., что можно описать в правилах корреляции SIEM и т.п.	
Не известно атакующему		

Когнитивные кейсы

- **Задачи SOC**
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Понимание задач SOC как функций безопасности

	Известно аналитику SOC	Не известно аналитику SOC
Известно атакующему	-1- Типовые фазы реализации атаки и соответствующие контроли Известные способы обхода User Access Control Детектируемое вредоносное ПО Детектируемые по сигнатурам атаки Отклонения от best practice частных политик ИБ И др., что можно описать в правилах корреляции SIEM и т.п.	
Не известно атакующему	-2- Архитектура сети Используемые системы ИБ и их настройки Расстановка HoneyPot в сети Стандарты конфигурации узлов сети Профили работы узлов Профили сетевого взаимодействия сегментов сети Регламенты и инструкции работы рядовых и привилегированных пользователей	

Когнитивные кейсы

- **Задачи SOC**
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Понимание задач SOC как функций безопасности

	Известно аналитику SOC	Не известно аналитику SOC
Известно атакующему	-1- Типовые фазы реализации атаки и соответствующие контроли Известные способы обхода User Access Control Детектируемое вредоносное ПО Детектируемые по сигнатурам атаки Отклонения от best practice частных политик ИБ И др., что можно описать в правилах корреляции SIEM и т.п.	-3- Факт эксплуатации известных уязвимостей инфраструктуры Факт эксплуатации известных уязвимостей приложений Использование методик заражений и атак, не оставляющих следов в журналах аудита ИБ Применение социальной инженерии
Не известно атакующему	-2- Архитектура сети Используемые системы ИБ и их настройки Расстановка HoneyPot в сети Стандарты конфигурации узлов сети Профили работы узлов Профили сетевого взаимодействия сегментов сети Регламенты и инструкции работы рядовых и привилегированных пользователей	

Когнитивные кейсы

- **Задачи SOC**
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Понимание задач SOC как функций безопасности

	Известно аналитику SOC	Не известно аналитику SOC
Известно атакующему	-1- Типовые фазы реализации атаки и соответствующие контроли Известные способы обхода User Access Control Детектируемое вредоносное ПО Детектируемые по сигнатурам атаки Отклонения от best practice частных политик ИБ И др., что можно описать в правилах корреляции SIEM и т.п.	-3- Факт эксплуатации известных уязвимостей инфраструктуры Факт эксплуатации известных уязвимостей приложений Использование методик заражений и атак, не оставляющих следов в журналах аудита ИБ Применение социальной инженерии
Не известно атакующему	-2- Архитектура сети Используемые системы ИБ и их настройки Расстановка HoneyPot в сети Стандарты конфигурации узлов сети Профили работы узлов Профили сетевого взаимодействия сегментов сети Регламенты и инструкции работы рядовых и привилегированных пользователей	-4- Весь доступный арсенал эксплойтов 0-day уязвимостей Перекрытие используемыми в SOC репутационными базами всех возможных C&C серверов и зараженных хостов в Интернет

Когнитивные кейсы

- Задачи SOC
- **Контексты**
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Дополнительные контексты

Тип контекста	Пример источника информации
О пользователе	Identity and Access Management, AD, HR
О бизнес ролях пользователя	Орг. структура, приложения, полномочия, регламенты
Об ИТ-активах и системах	CMDB, AD, Applications and SAST reports
Об уязвимостях	Vulnerability Scanners, DAST/SAST
О конфигурации ИТ-активов	CMDB, Vulnerability Scanners (audit), Network map
О известных угрозах	TI feeds: bad IP, DNS, URL, file HASHes
О внешних связях	Lists of partners, maintainers, deliverers
О данных	DLP, Data Management Systems
О компании во внешнем мире	Private TI feeds, Social media monitoring
О пользователе во внеш. мире	Social networks monitoring
О местонахождении	Business travel systems, Physical Access Control
О коммуникациях	Выгрузки по SIM картам, по корп. WiFi сетям

Когнитивные кейсы

- Задачи SOC
- Контексты
- **Когнитивный SOC**
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Когнитивные кейсы

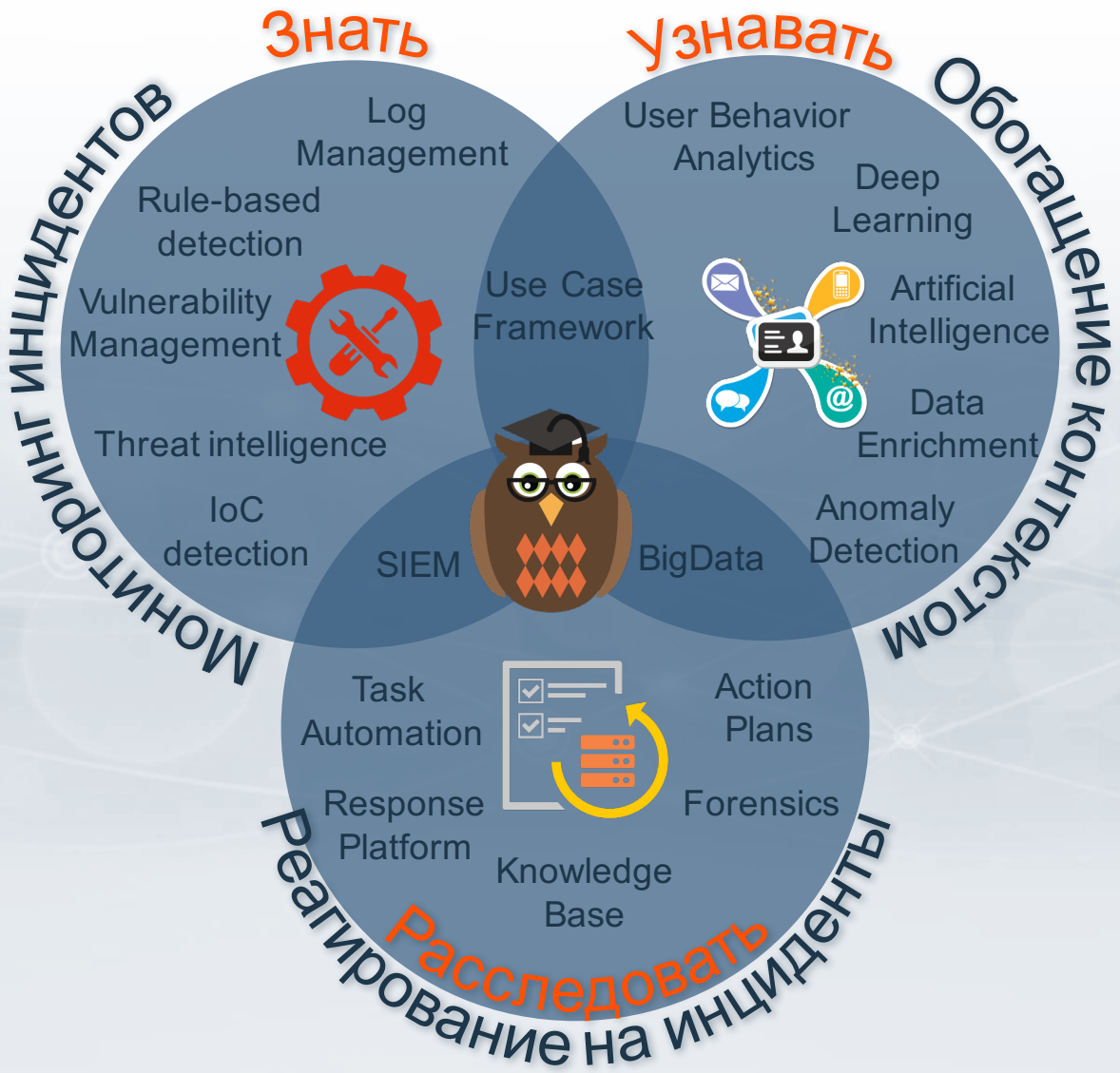
- Задачи SOC
- Контексты
- **Когнитивный SOC**
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Когнитивные кейсы

- Задачи SOC
- Контексты
- **Когнитивный SOC**
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Когнитивные кейсы

- Задачи SOC
- Контексты
- **Когнитивный SOC**
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- **Use Cases**
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

SOC: Цель определяет средства

Глобальные цели ИБ

- Сокращение потерь от инцидентов
- Оптимизация расходов ИБ
- Соответствие требованиям ИБ
- Безопасность продуктов и услуг
- Повышение доступности бизнес-функций

Remember **“Logs don’t lie”**

Когнитивные кейсы

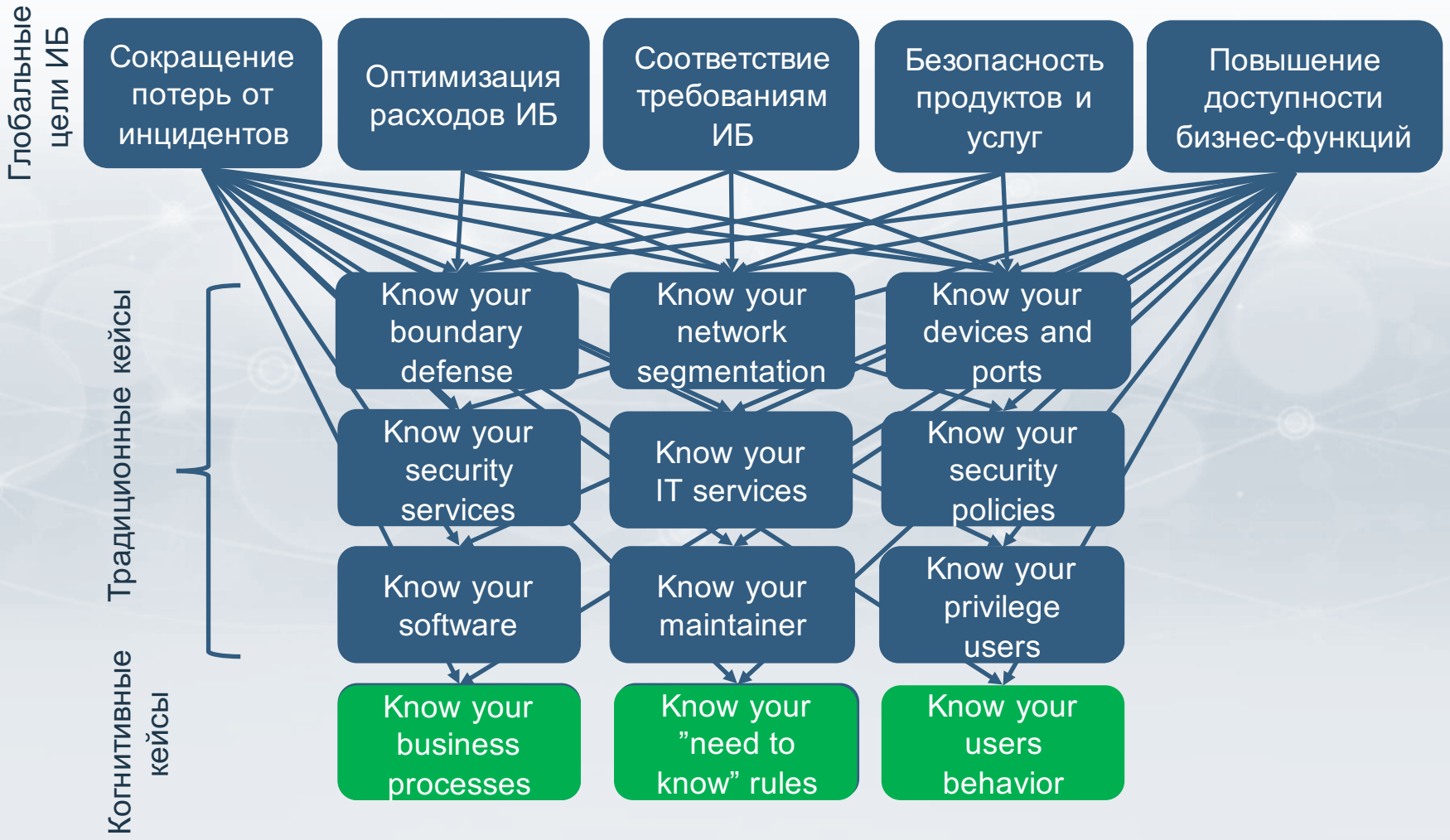
- Задачи SOC
- Контексты
- Когнитивный SOC
- **Use Cases**
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

SOC: Цель определяет средства

Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- **Use Cases**
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

SOC: Цель определяет средства



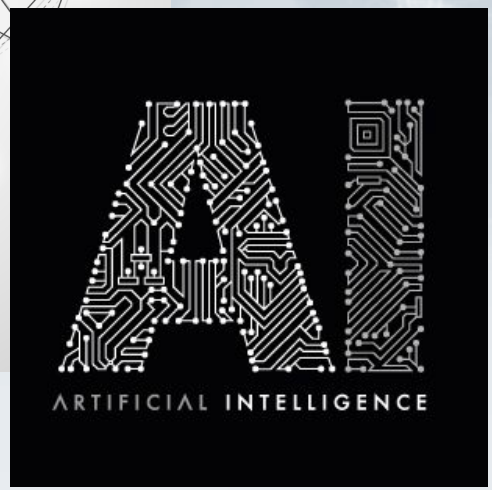
Традиционные vs Когнитивные кейсы

	Традиционные кейсы	Когнитивные кейсы
Выявление угроз ИБ	Использование правил «из коробки» SIEM для детектирования распространенных инцидентов Следование логике Kill Chain первых стадий (разведка, заражение, проникновение) Выявление скомпрометированных учетных записей через корреляцию событий Поиск обращений на подозрительные внешние IP-адреса Применение подписок на feeds для выявления инцидентов Выстраивание процесса реагирования на инциденты внутри SIEM на основе сырых событий	Использование визуализации для выявления скрытых инцидентов Применение подходов Data Mining для обнаружения дополнительных инцидентов Профилирование действий пользователей и поиск аномалий Использование контекстов при составлении корреляционных правил и применении данных из TI feeds Анализ сетевых потоков, данных об уязвимостях и событий с End Point систем ИБ Применение техник Threat Hunting на исторических данных за длительные периоды

Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- **Когнитивные технологии**
  - Fast Data
  - ML
  - UBA
  - AI
- Выводы

Когнитивные технологии



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - **Fast Data**
  - ML
  - UBA
  - AI
- Выводы

Big and Fast Data Analytics in SOC

Deep Machine Learning

Deep Anomaly Detection

Fast Data Enrichment

Gold Data Mining

Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - **Fast Data**
  - ML
  - UBA
  - AI
- Выводы

Big and Fast Data Analytics in SOC

Deep Machine Learning

Deep Anomaly Detection

Fast Data Enrichment

Gold Data Mining

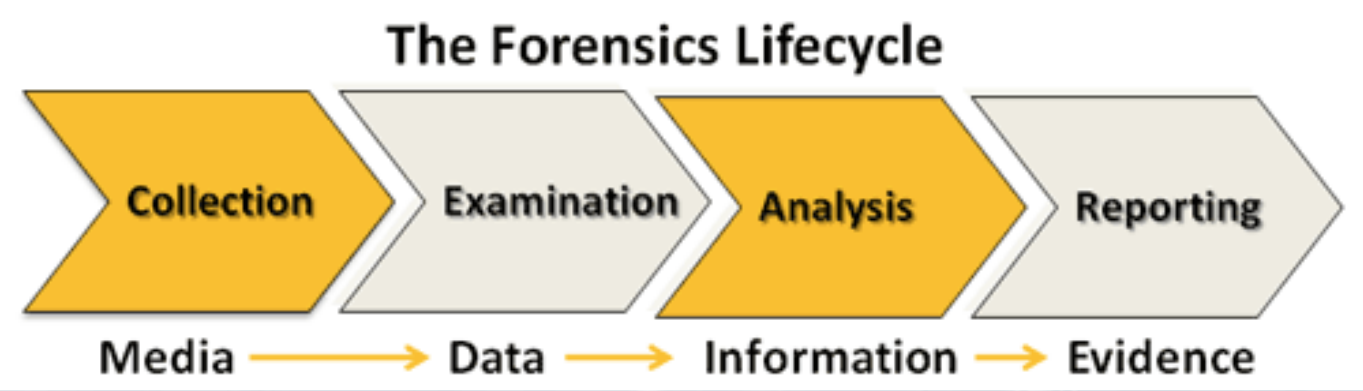
10 часов на отчет из SIEM?

Поток NetFlow зашкаливает?

Корреляция данных за 1 год?

Нужна реакция в миллисекундах?

Big and Fast Data for Network Forensics

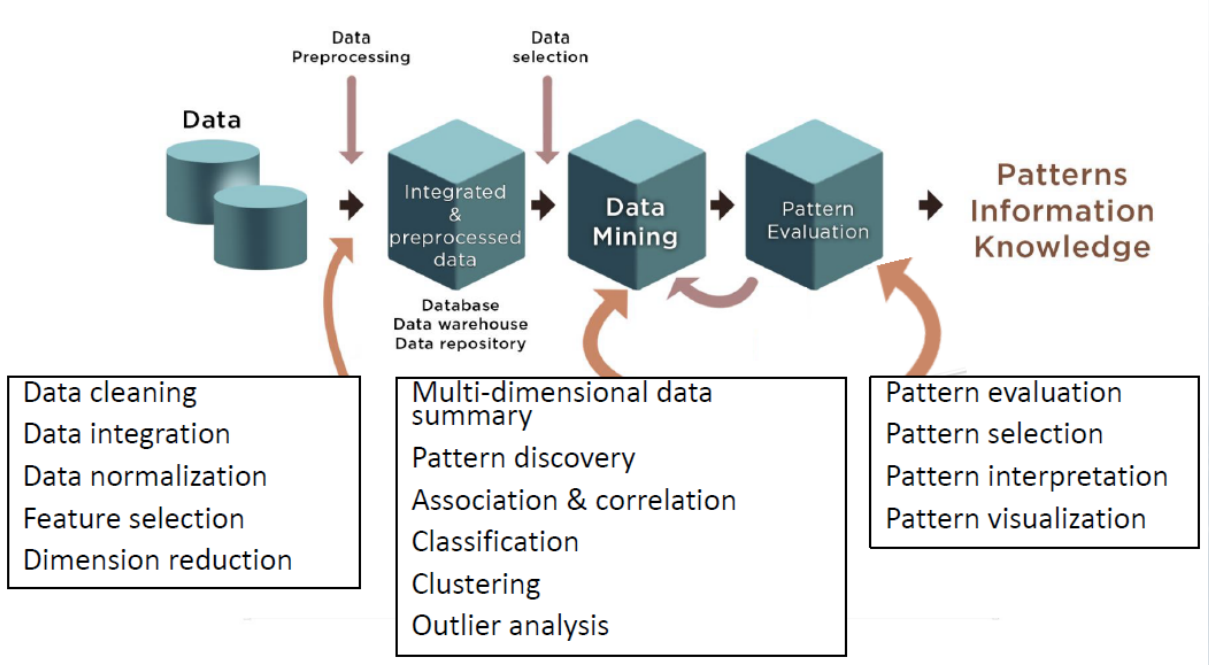


Data Sources:
Full packet capture (PCAP)
Flow data
Logs
IDS Alerts

BigData Software Tools:
MapReduce
Spark, Hadoop
Yarn, Mesos
Storm, Beam, Flink
Ignite, Hazelcut
Apache Drill, Kylin
HBase, MongoDB, Cassandra
Pheonix, Pig

Network Forensics Cases:
Full session reconstruction
Searching for data
Searching for communications
Visualization to discover issues

Big and Fast Data for Unknown Data Mining



Data Mining Cases:

Using unusual ports on group of hosts

Indicate fraudsters carrying out automated card validation procedures

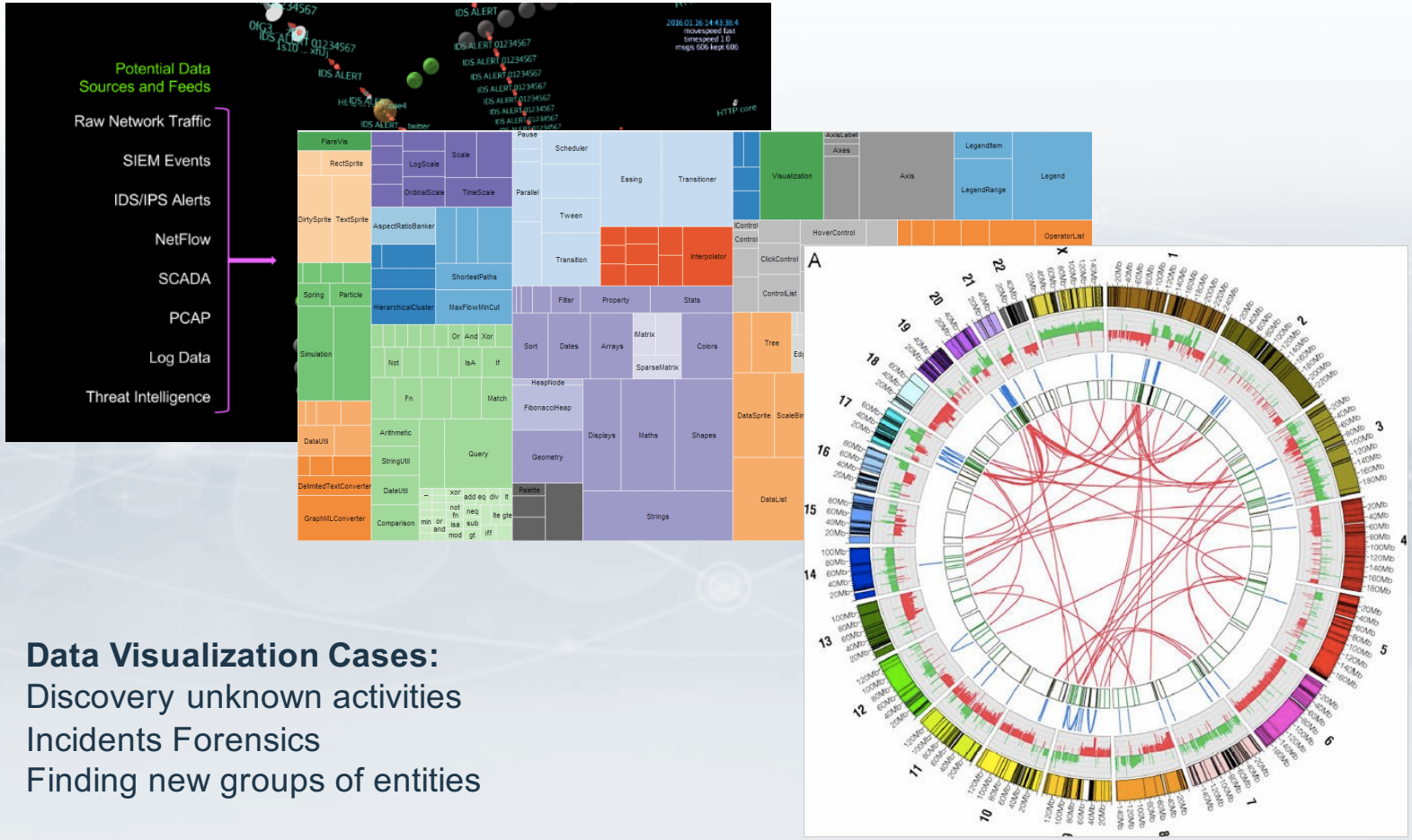
Compare patterns between servers that should be identical

Detect traffic activity patterns between different network zones

Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - **Fast Data**
  - ML
  - UBA
  - AI
- Выводы

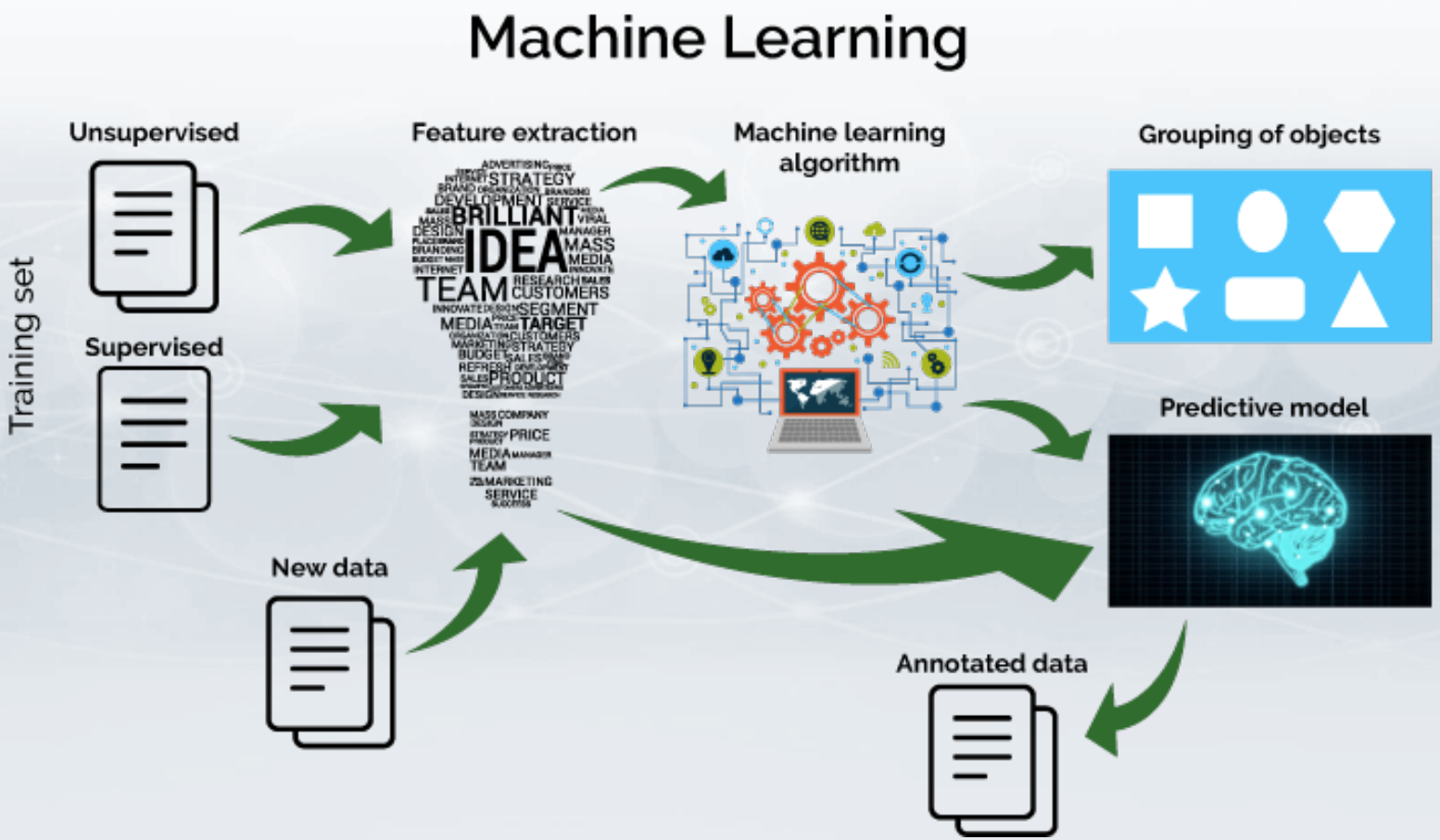
Big and Fast Data for Data Visualization



Data Visualization Cases:
Discovery unknown activities
Incidents Forensics
Finding new groups of entities

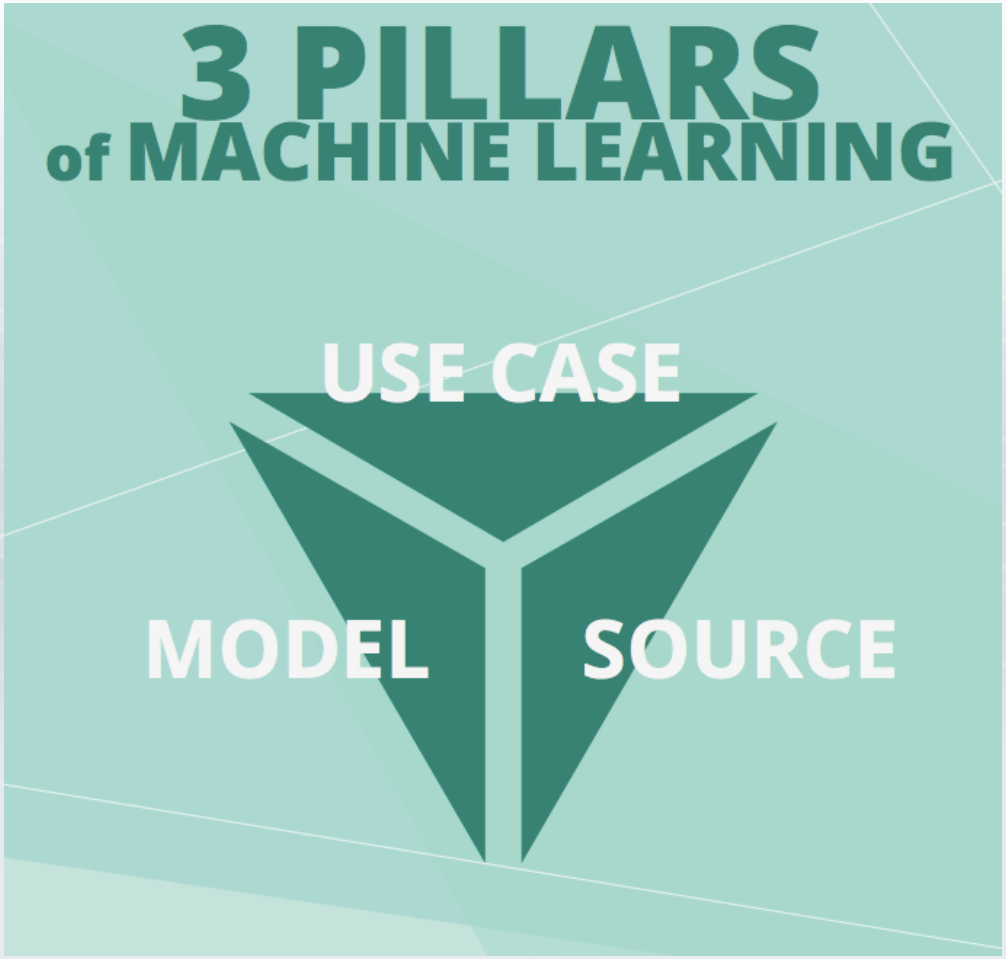
Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - **ML**
  - UBA
  - AI
- Выводы



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - **ML**
  - UBA
  - AI
- Выводы



Use Case:
Какой тип атаки пытаемся найти и на какой стадии Kill Chain он находится

Model:
Какой наиболее подходящий алгоритм обучения следует применить

Source:
Какой тип информации следует подать на вход для изучения

Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - **ML**
  - UBA
  - AI
- Выводы

Supervised vs UNsupervised ML

	TRAINING DATA	APPROACH	EXAMPLE MODEL TYPES	DETECTION TYPE & FOCUS	ATTACK STAGES	EXAMPLE USE CASES
UNSUPERVISED	Unlabeled	Training onsite Classification onsite	SVD K-means clustering Neural network	**TYPE** Anomaly **FOCUS** Unknown threats	Lateral movement Exfiltration	Abnormal server access, lateral attack spread, flight risk, data exfiltration etc.
SUPERVISED	Labeled	Training offsite Classification onsite	Naïve bayes Logistic regression SVM	**TYPE** Maliciousness **FOCUS** Known threats	Infection Command & control	Malicious object download, email phishing/spam, DNS DGA, etc.

Индуктивное обучение
Метод самообучения системы, основанный на выявлении эмпирических закономерностей в данных

Дедуктивное обучение
Метод обучения системы экспертом, основанный на его опыте и знаниях о закономерностях в данных

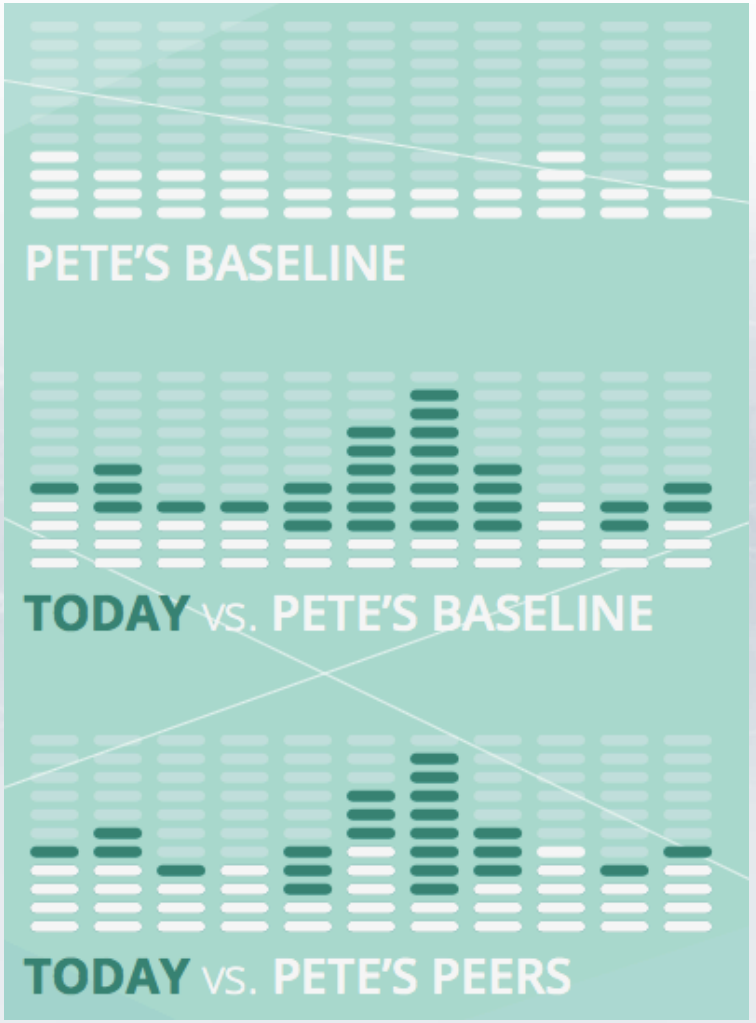
Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - **ML**
  - UBA
  - AI
- Выводы

Baselining with Machine Learning

Одна из задач ML – составление профиля
Изучение данных для составления «схемы» нормального состояния системы/пользователя:

- используемые ресурсы и приложения
- время подключений и длительность сессий
- география подключений
- хосты, с которых идут подключения
- вводимые типы и форматы данных
- используемые порты и протоколы
- цепочка переходов между ресурсами
- и т.п.

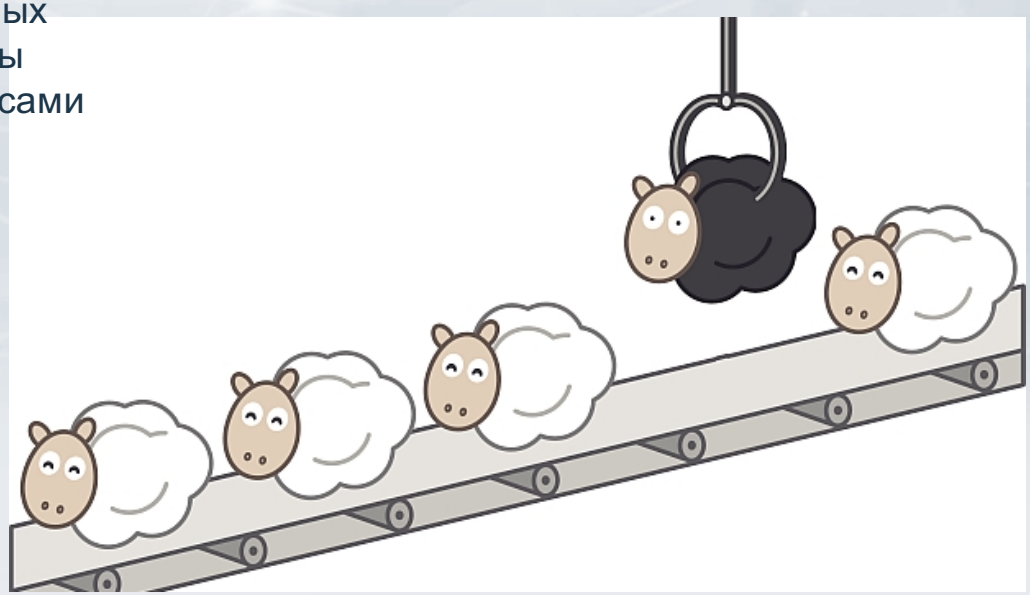


Categorization with Machine Learning

Одна из задач ML – определение схожих групп

Изучение данных для группировки объектов/субъектов по признакам:

- используемые ресурсы и приложения
- время подключений и длительность сессий
- география подключений
- хосты, с которых идут подключения
- вводимые типы и форматы данных
- используемые порты и протоколы
- цепочка переходов между ресурсами
- и т.п.



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - **UBA**
  - AI
- Выводы

SIEM vs ML-UBA

	SIEM	UBA
Логика детектирования	Четкие сценарии инцидентов, использование базовой статистики и порогов	Машинное обучение
Акцент на угрозы	Широкий круг детектируемых угроз	Угрозы, связанные с действиями пользователей
Типы анализируемых данных	Logs, NetFlow	Данные из SIEM + дополнительные контекстные справочники
Средний интервал анализа данных	В режиме реального времени, исторический анализ за короткий интервал времени (3-5 дней)	Анализ исторической информации за длительный период (3-6 мес)
Типы детектируемых угроз	Known, Known-Unknowns	Unknown, Unknown-unknowns
Дополнительные контексты	Используются базовые данные для обогащения	Зачастую сами становятся новым контекстом

Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - **UBA**
  - AI
- Выводы

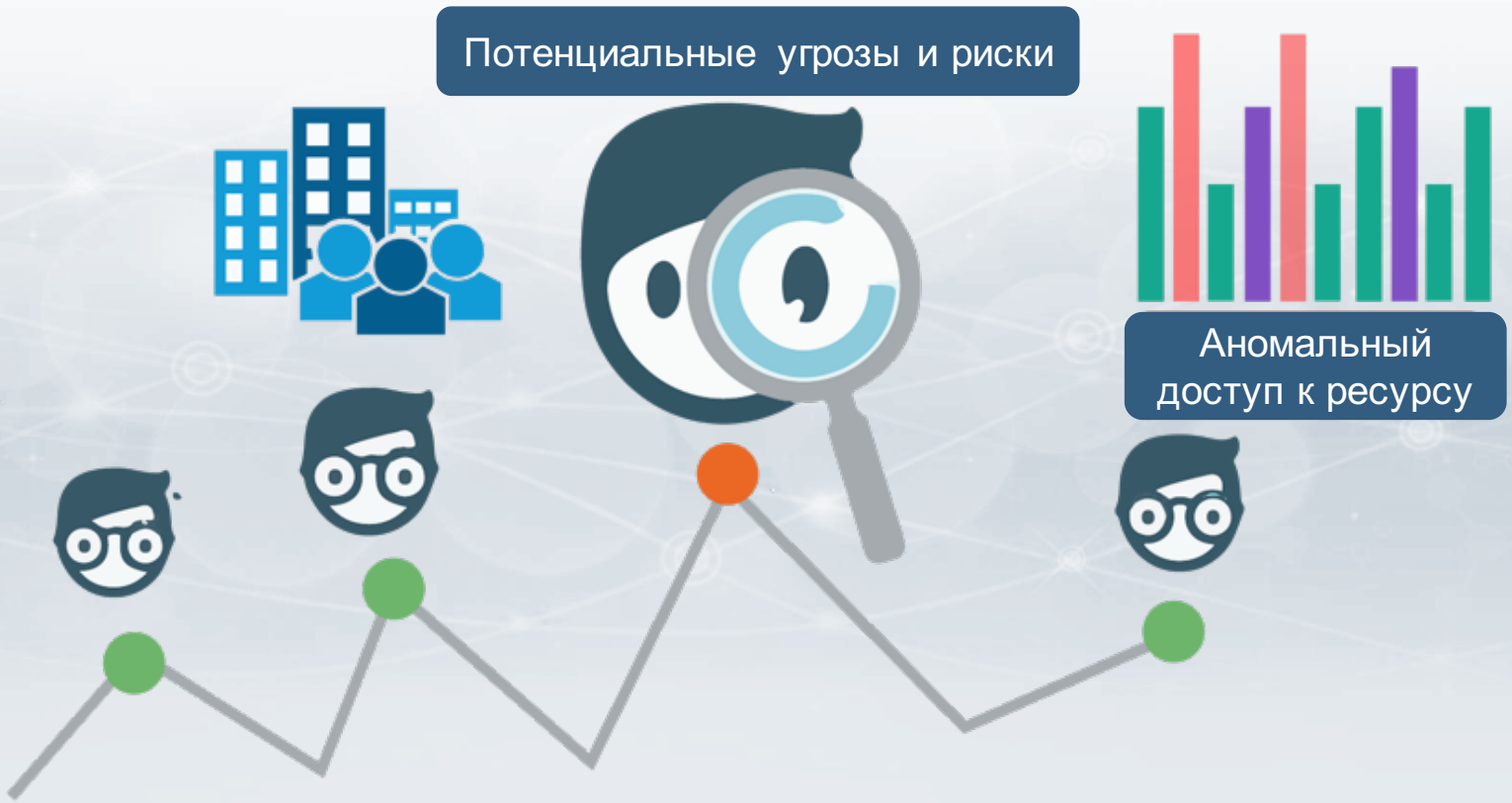
Примеры UBA Use Cases

Use Case	Details
Compromised user account detection	The UEBA tool identifies situations where user credentials have been stolen and are being used by someone other than the authorized user (who can be a person or an application). Detecting shared account usage and generic account abuse falls under this use case as well. Note that this use case should not be reduced to privileged accounts only, and is focused on threat detection, not IAM optimization.
Compromised endpoint detection	The UEBA tool is used to identify network endpoints that have been compromised, infected by malware or are otherwise behaving suspiciously. This is different than the use case above in the sense that malicious activity might be detected on a host, but not necessarily tied to a specific user account (e.g., command and control [C&C] traffic can be identified from a system where no user is currently logged on).
Data exfiltration detection	UEBA is used to identify data exfiltration. Unauthorized or malicious data exfiltration may occur even by action of authorized users. As a result, this use case is focused on identifying this type of activity, which is necessary even when the ability to detect compromised accounts and endpoints is in place. This use case often focuses on data loss prevention (DLP) alerts, cloud access security broker (CASB) logs and/or network traffic data.
Insider access abuse, including privilege abuse	All users in an enterprise environment should restrict their actions on systems and on the network to their authorized entitlements and privileges. UEBA tools can be used to identify users (both employees and trusted third parties) abusing those access privileges, which in many cases is linked to malicious intent. Examples of this type of activity would be excessive or unauthorized access to data (e.g., accessing too many records from a database with personally identifiable information [PII]) or even abuse of system privileges (e.g., creating new user accounts or assigning additional privileges not in line with security policies).
Providing additional context and information for investigations	UEBA technologies have to learn a lot about users and entities in the organization in order to identify anomalies that could be linked to threats. This information is extremely useful for analysts performing alert triage and incident investigations. If an analyst suspects that an endpoint has been compromised, for example, he can use the UEBA tool to learn about the users of that desktop, their regular behavior and even the role of that endpoint in the network. For example, is it a server or a workstation? Is it used for system administration or business functions?

Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - **UBA**
  - AI
- Выводы

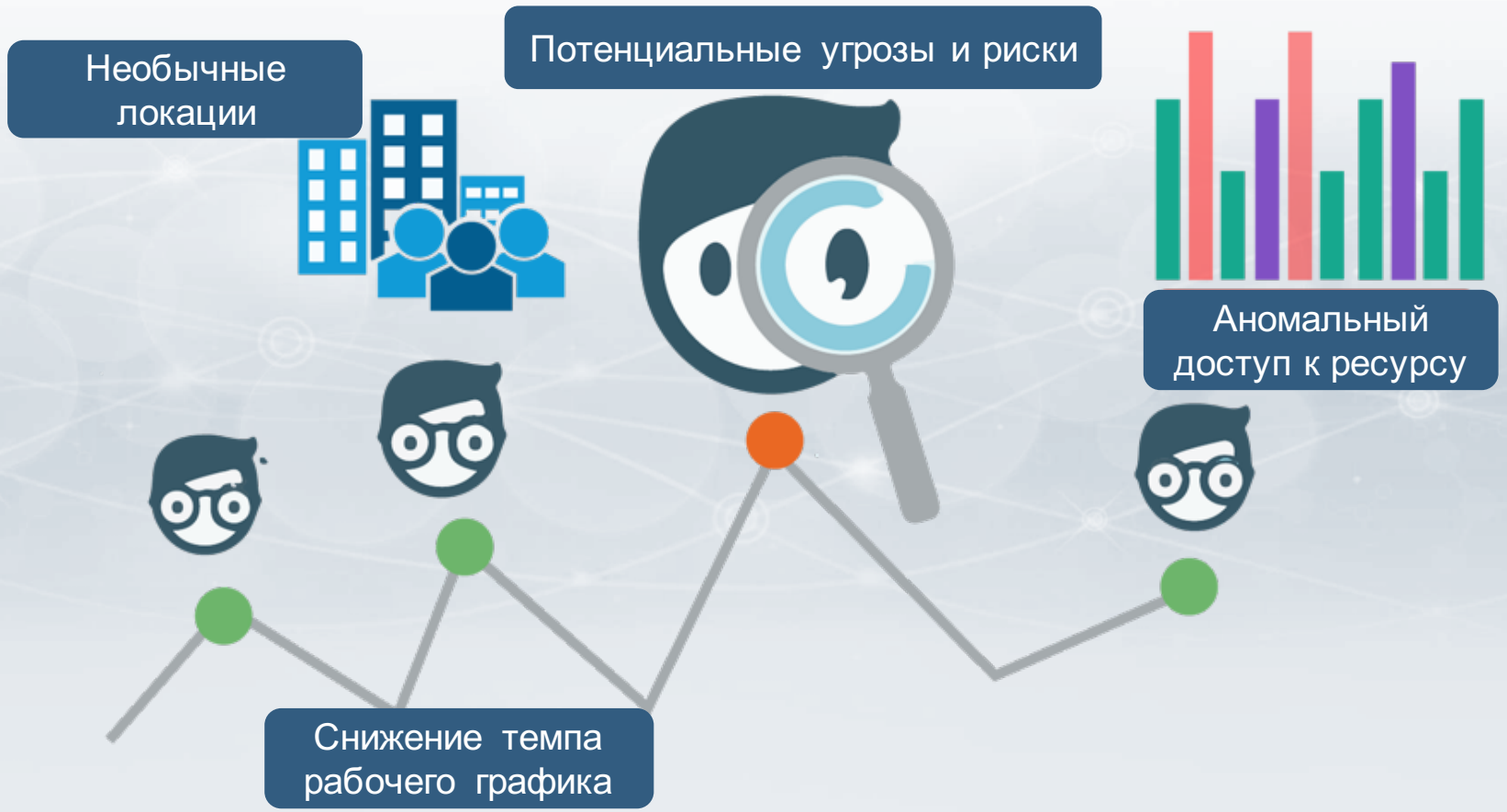
User Behavior Analytics



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - **UBA**
  - AI
- Выводы

User Behavior Analytics



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - **UBA**
  - AI
- Выводы

User Behavior Analytics

Когнитивные кейсы

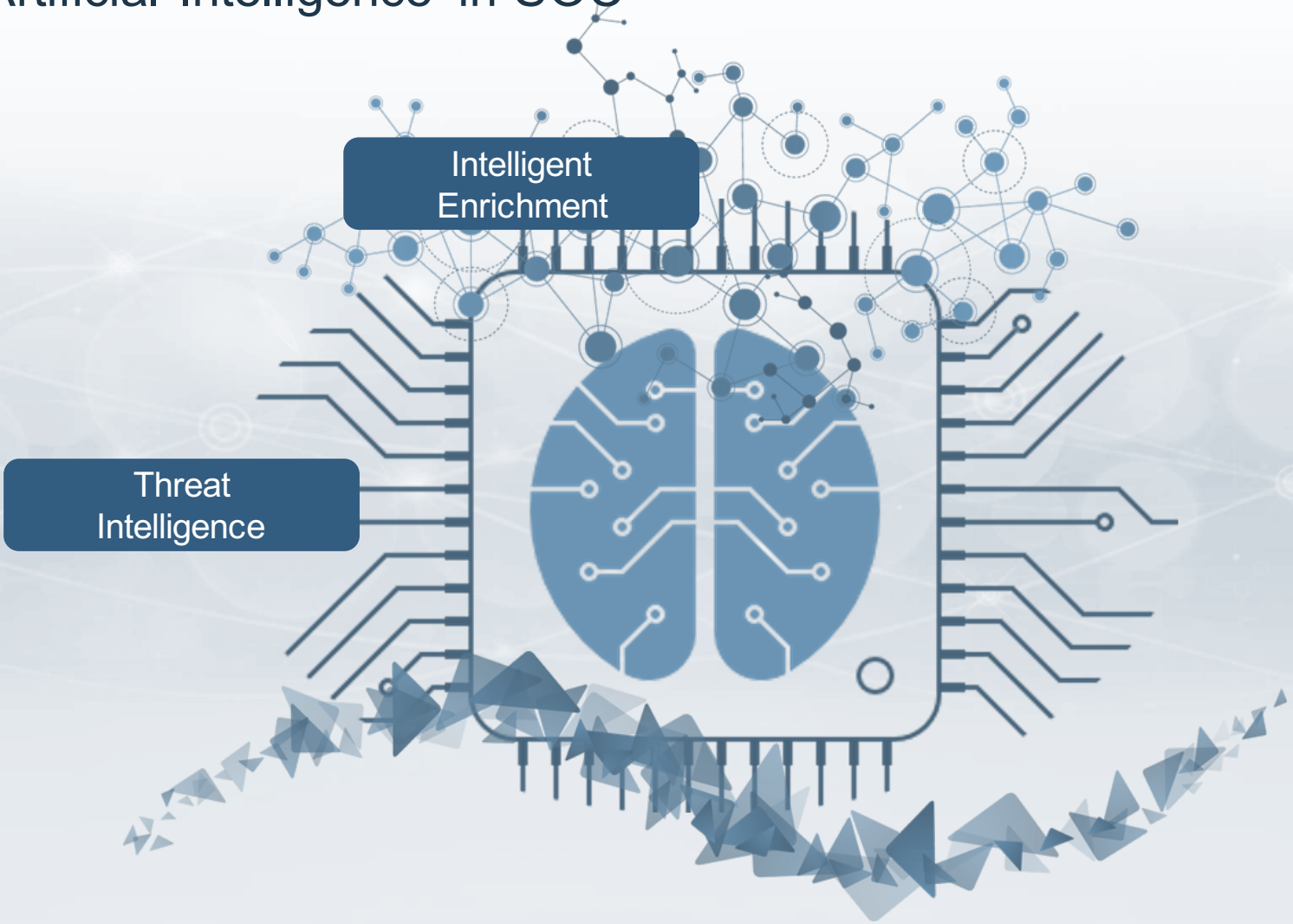
- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - **UBA**
  - AI
- Выводы

User Behavior Analytics

Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - **AI**
- Выводы

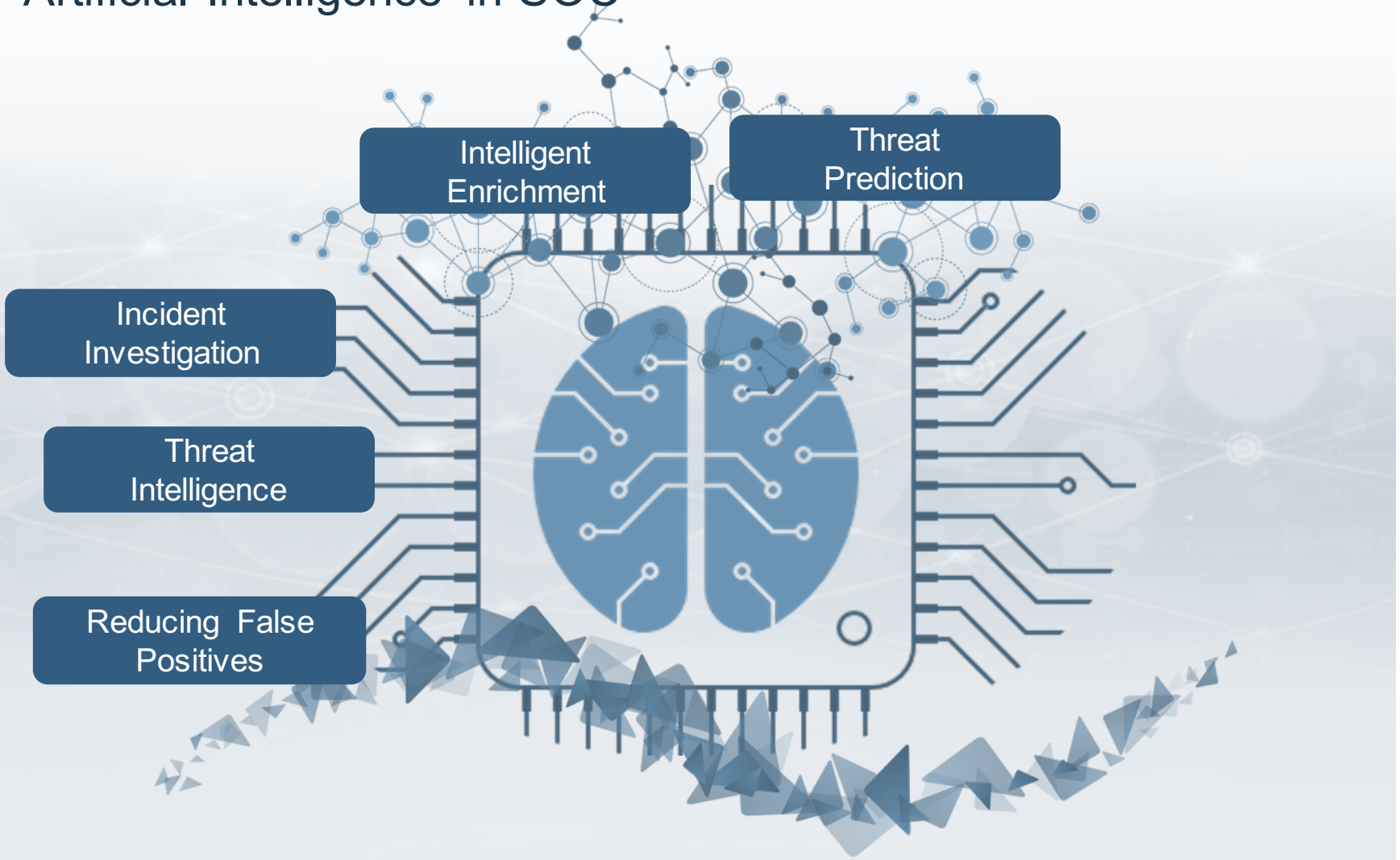
Artificial Intelligence in SOC



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - **AI**
- Выводы

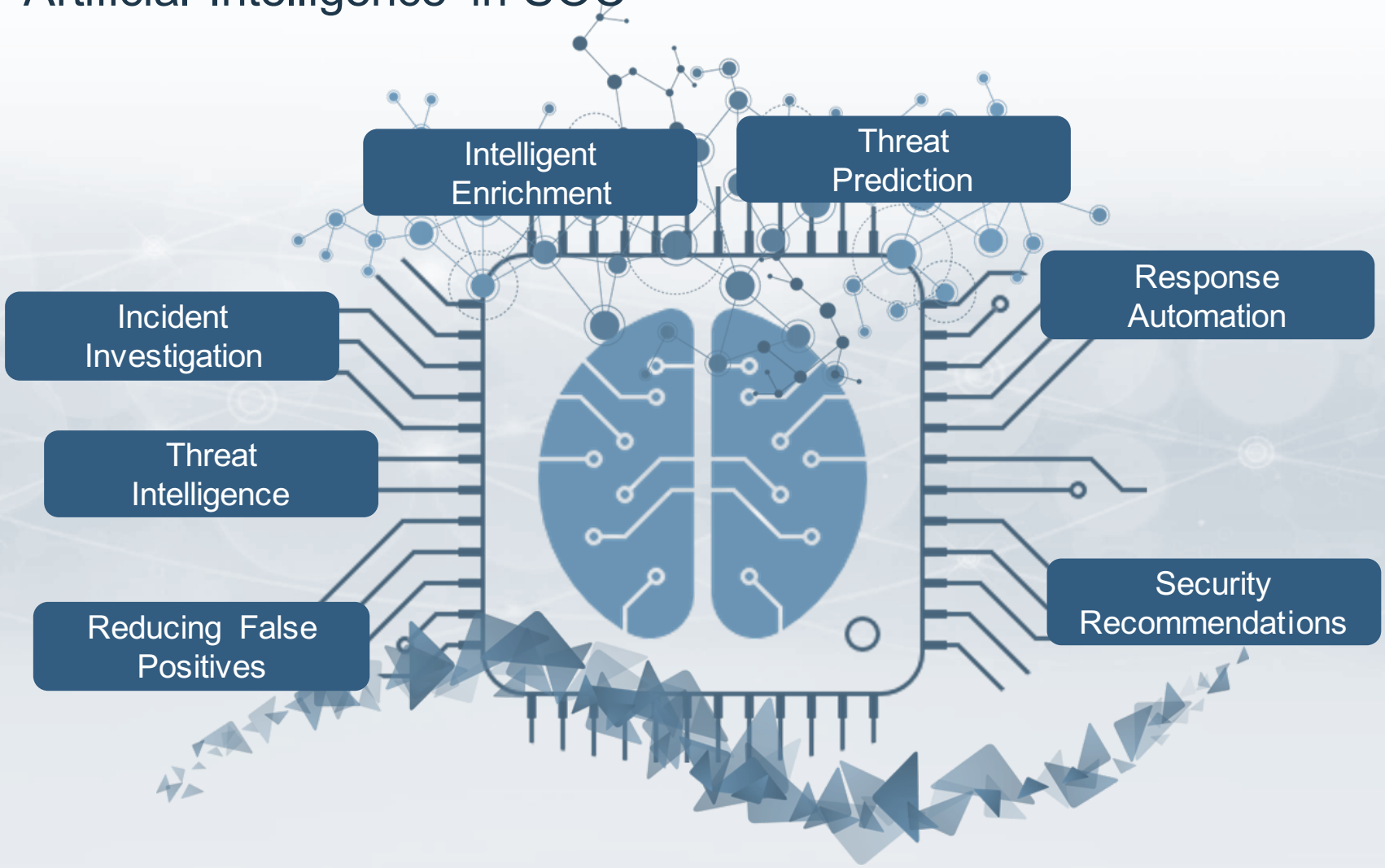
Artificial Intelligence in SOC



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - **AI**
- Выводы

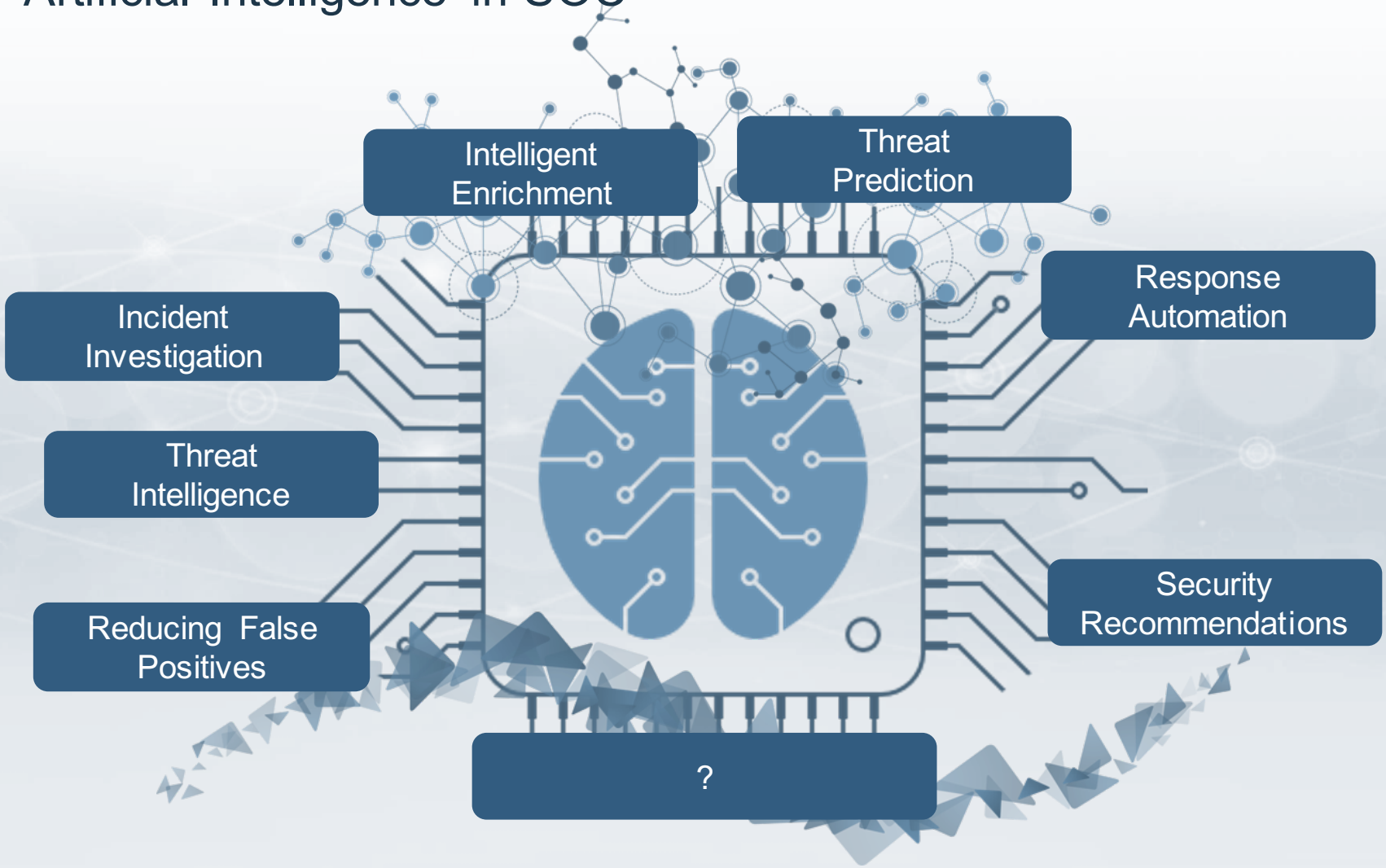
Artificial Intelligence in SOC



Когнитивные кейсы

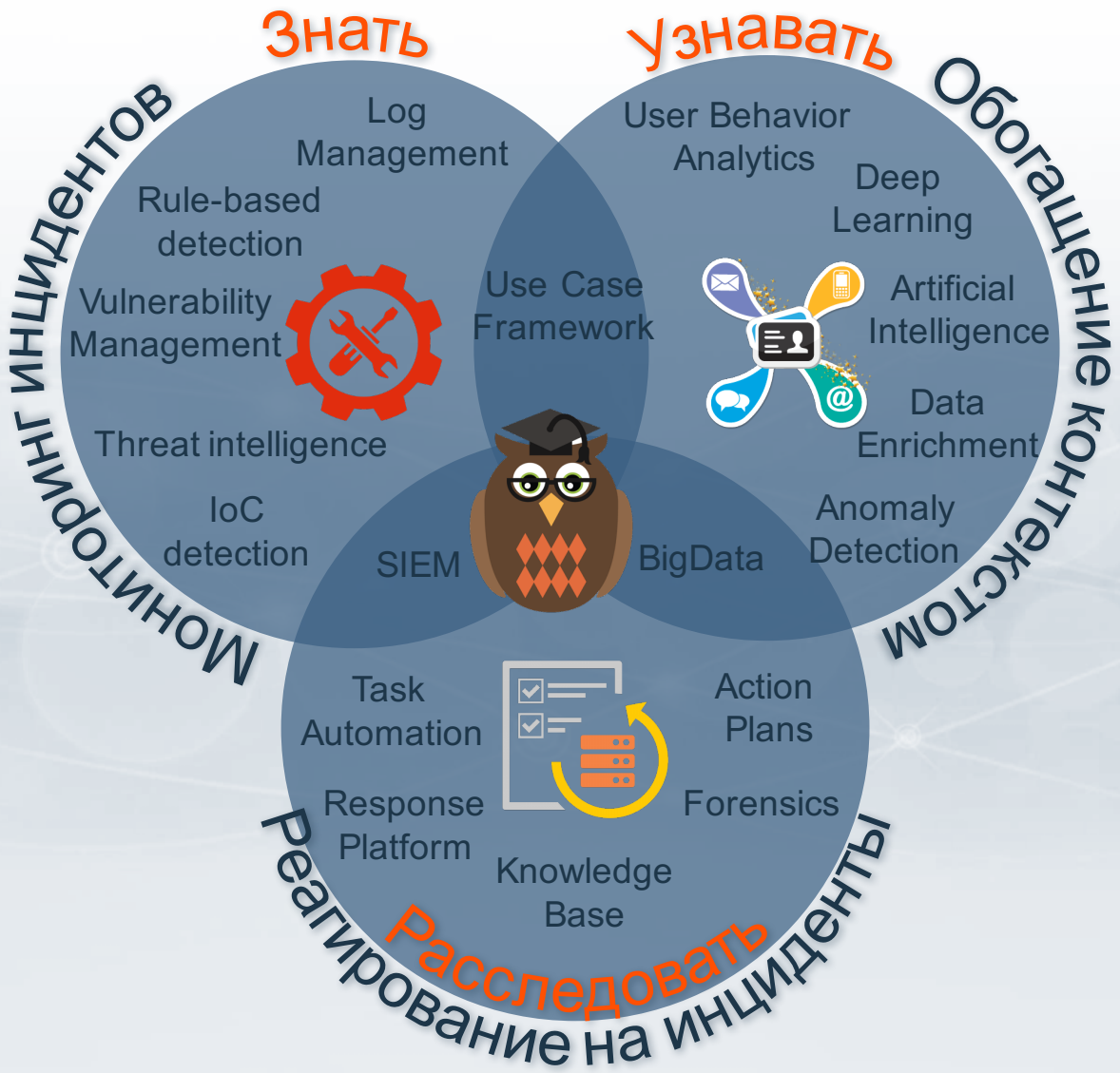
- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - **AI**
- Выводы

Artificial Intelligence in SOC



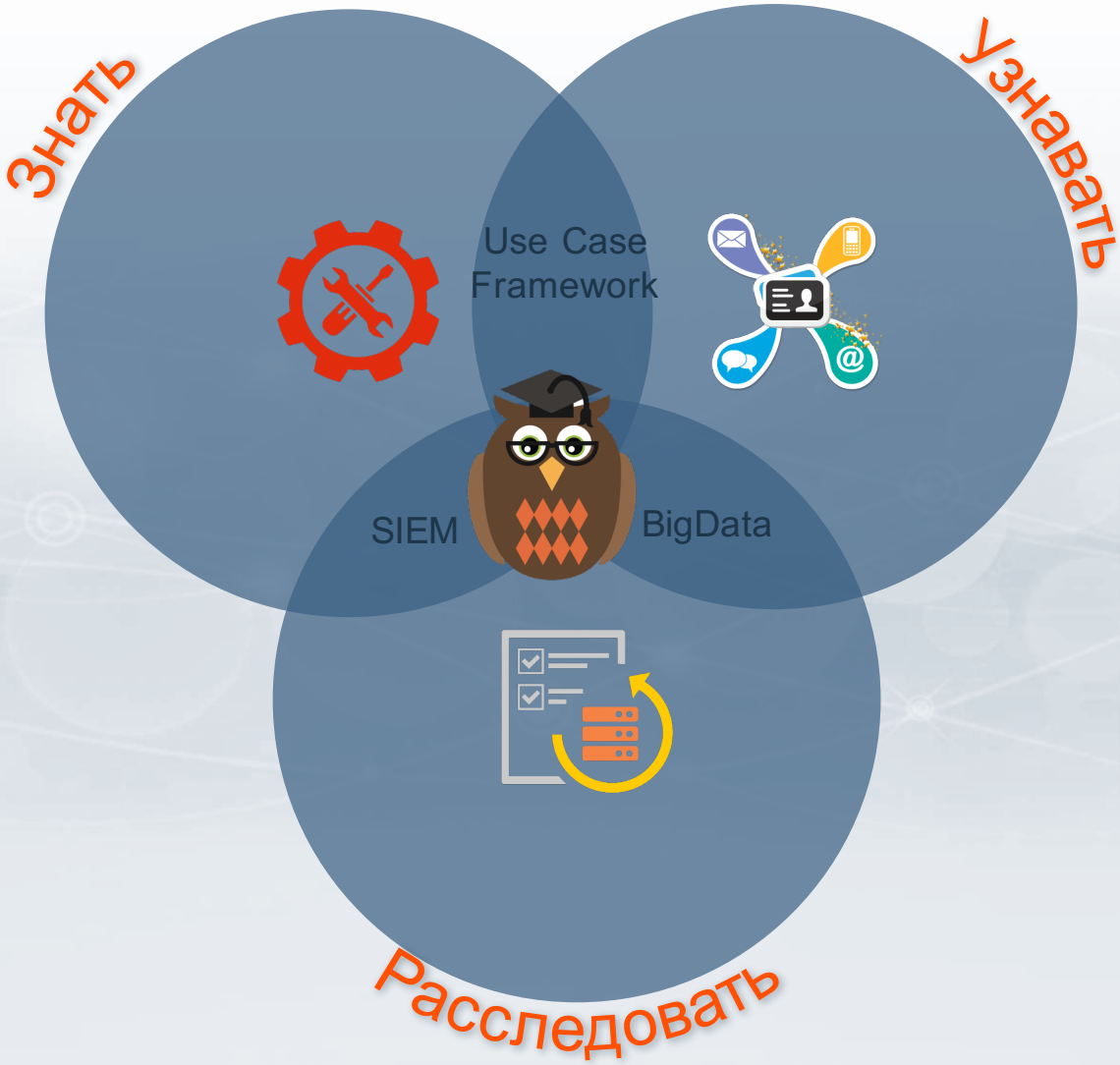
Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- **Выводы**



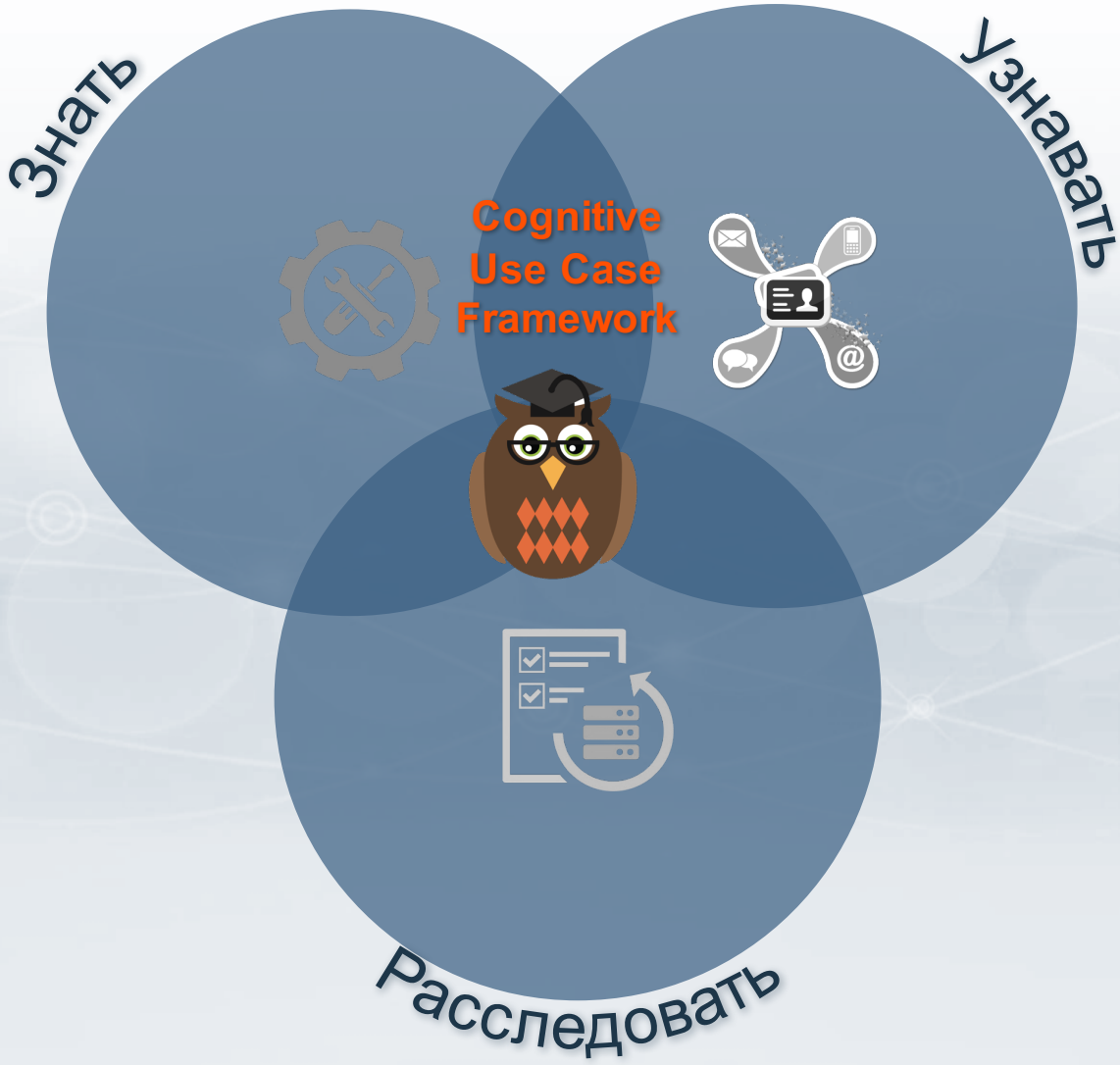
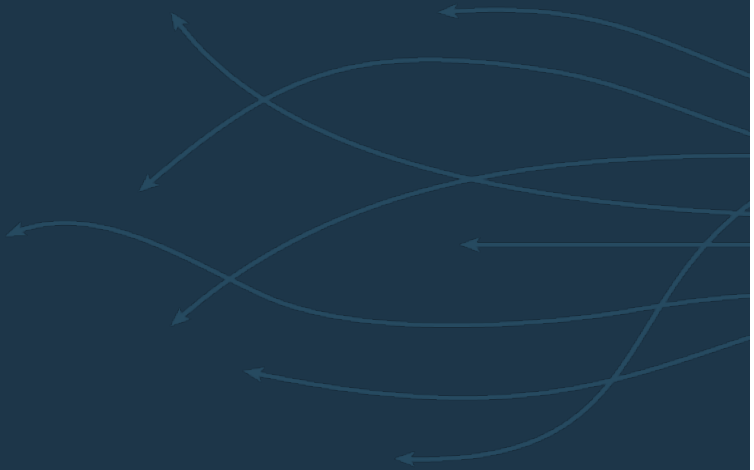
Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- **Выводы**



Когнитивные кейсы

- Задачи SOC
- Контексты
- Когнитивный SOC
- Use Cases
- Когнитивные технологии
  - Fast Data
  - ML
  - UBA
  - AI
- **Выводы**



СПАСИБО