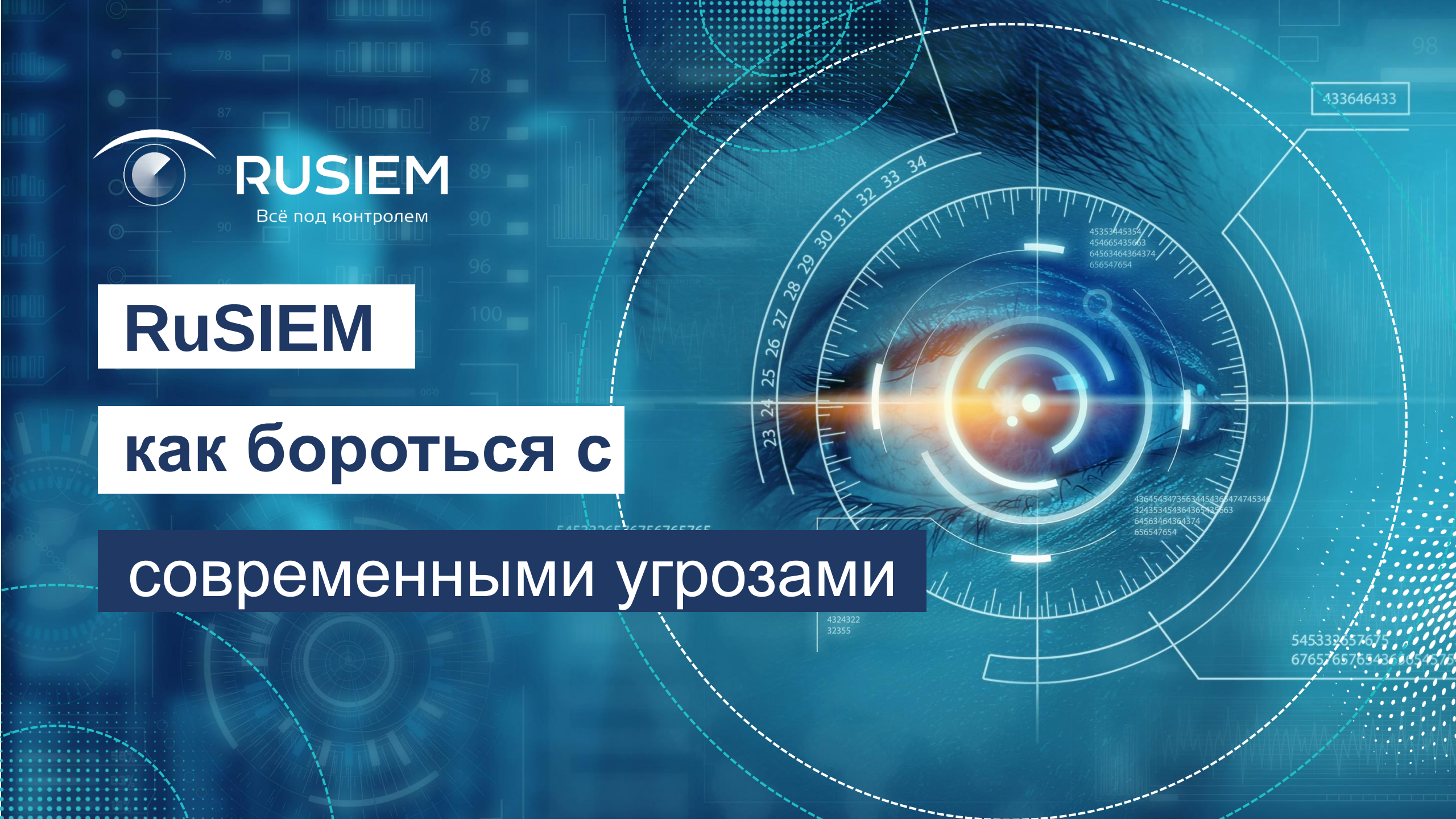
RUSIEM

Всё под контролем

RuSIEM

как бороться с современными угрозами



О КОМПАНИИ RUSIEM

программный код создан российскими экспертами

>300

пилотных внедрений

резидент Сколково

>50

партнеров в странах СНГ

2014

с этого года ведется активная разработка

продукт включен в реестр отечественного ПО

10000

установок free-версии в мире в 2017-18 годах

ЧТО ТАКОЕ SIEM И ЗАЧЕМ ОНА НУЖНА

SIEM представляет собой улучшенную систему обнаружения вредоносной активности и различных системных аномалий. Работа SIEM позволяет увидеть более полную картину активности сети и событий безопасности. Когда обычные средства обнаружения по-отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников.

Сотни и тысячи устройств живут своей жизнью и генерируют миллионы событий, сообщая о том, что происходит с ними и вокруг. При этом необходимо реагировать только на часть из них

Отдельные устройства, операционные системы только предоставляют события без детального анализа

Для полной картины происходящего необходимо собрать воедино состояния с отдельных устройств

Для этого и нужна SIEM-система

SIEM – система, которая собирает, анализирует и представляет информацию из сетевых устройств, средств защиты информации и информационных систем

Также в систему входят приложения для контроля идентификацией и доступом, инструменты управления уязвимостями

ГДЕ МОЖЕТ ПРИМЕНЯТЬСЯ SIEM?

Везде, где из журналов событий можно извлечь полезную информацию

ПРИМЕРЫ СОБЫТИЙ

- Сетевые атаки
- Фрод и мошенничество
- Откуда и когда блокировались учетные записи
- Изменение конфигураций «не админами»
- Повышение привилегий
- Выявление несанкционированных сервисов
- Обнаружение НСД (вход под учетной записью уволенного сотрудника)
- Отсутствие антивирусной защиты на новом установленном компьютере
- Изменение критичных конфигураций с VPN-подключений
- Контроль выполняемых команд на серверах и сетевом оборудовании
- Аудит изменений конфигураций (сетевые устройства, приложения, ОС)
- Выполнение требований законодательства и регуляторов (PCI DSS, СТО БР, ISO 27xx)
- Аномальная активность пользователя (массовое удаление/копирование)
- Обнаружение вирусной эпидемии
- Обнаружение уязвимости по событию об установке софта
- Оповещение об активной уязвимости по запуску ранее отключенной службы
- Обнаружение распределенных по времени атак
- Влияние отказа в инфраструктуре на бизнес-процессы

РЕШЕНИЕ

RUSIEM

система мониторинга и управления событиями информационной безопасности на основе симптомов и анализа данных в реальном времени, для крупных и средних компаний

RvSIEM (free)
классическое
решение класса LM

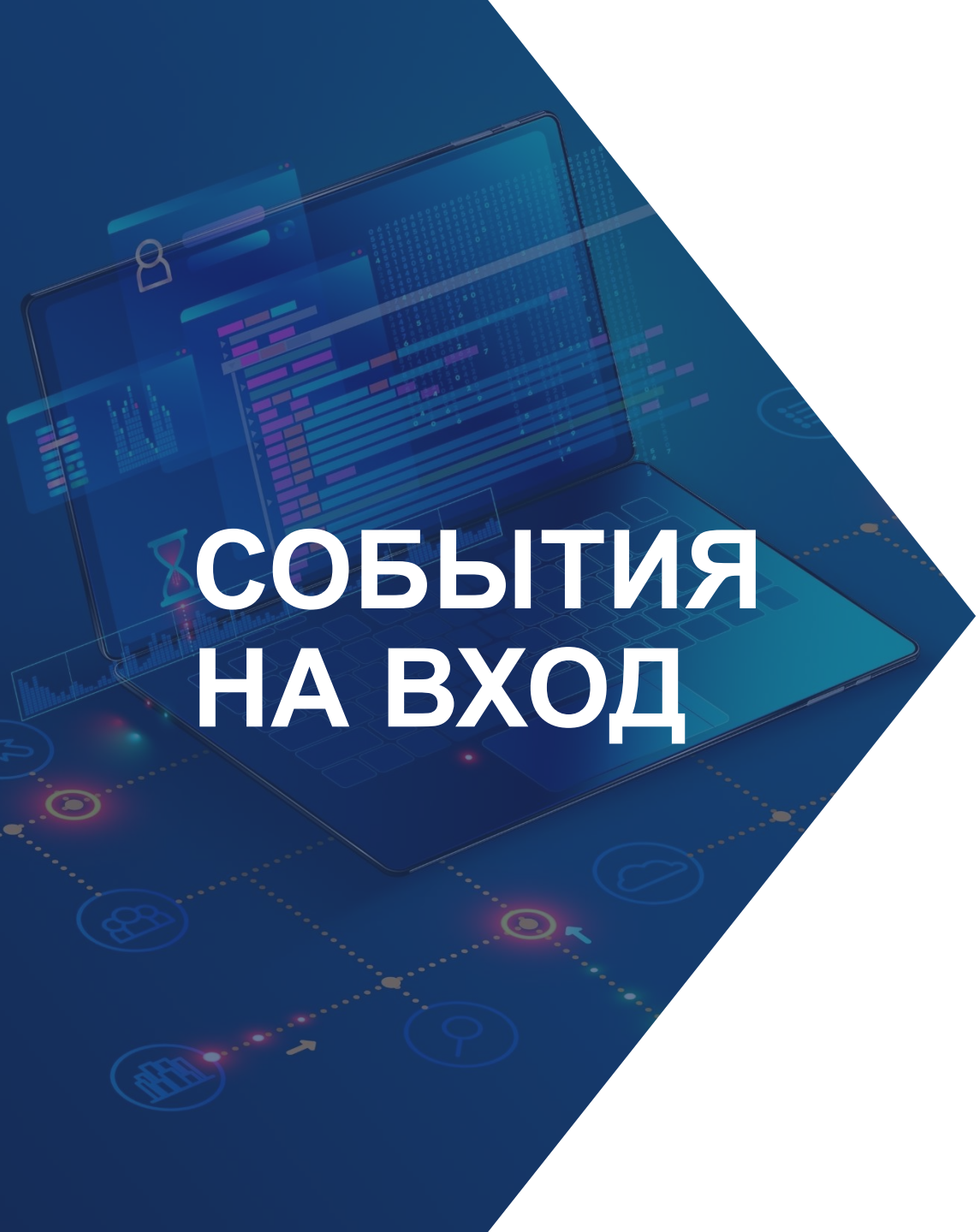
RuSIEM
коммерческая
версия

RuSIEM
Analytics
обнаружение
аномалий

RuSIEM Agent
агент под
Windows OS

RuSIEM Replicator
утилита для
массовой установки
и управления агентами

Линейка продуктов

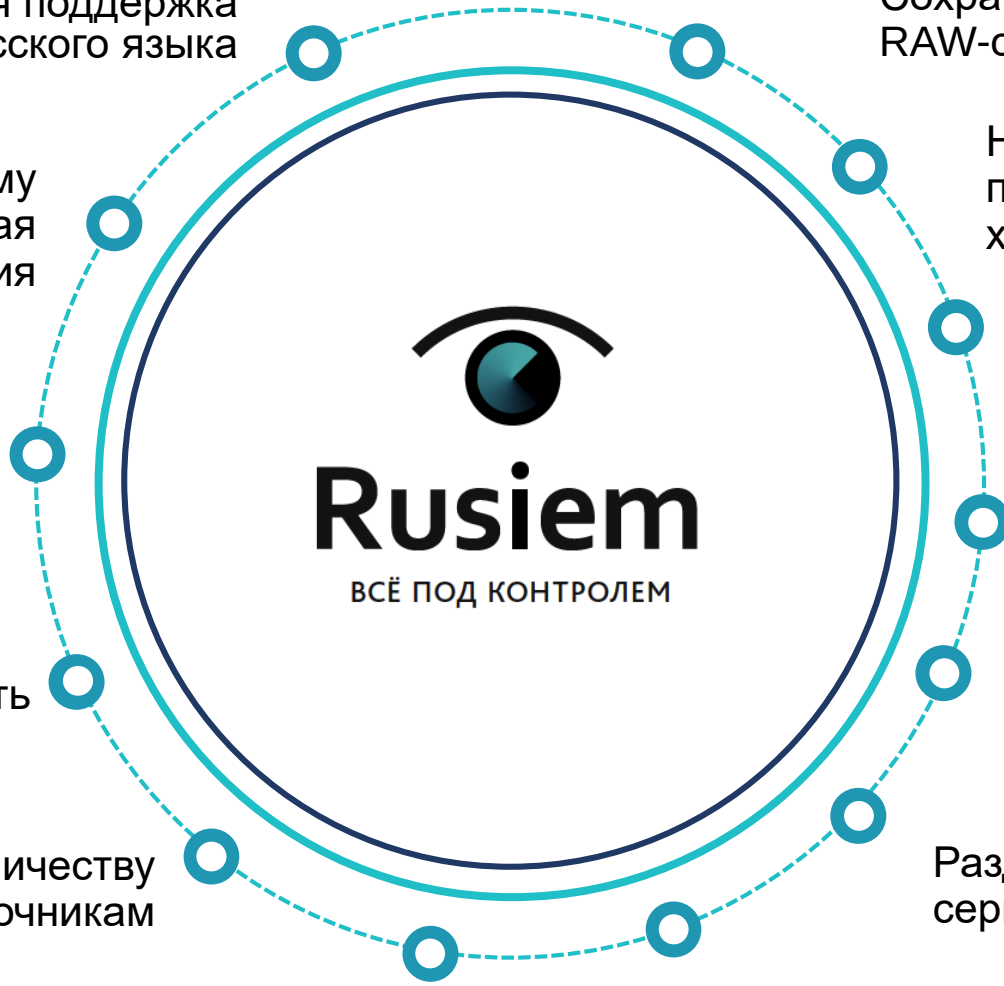


СОБЫТИЯ НА ВХОД

ЛЮБЫЕ

- Межсетевые экраны
- IPS
- DNS logs
- АСУТП
- СКУД
- Различные датчики
- Спам-фильтры
- Антивирусные системы
- Сетевые устройства
- Бизнес-приложения
- Windows event log
- Web servers
- App servers
- Load balancing
- Network flow
- Network payload
- Транзакции
- Почтовые системы

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА



Полная поддержка русского языка

Сохранение исходных RAW-событий

Приведенная к общему формату объектная нормализация

Нет ограничений по размеру архивного хранилища

Встроенная управляемая и редактируемая корреляция

Коннекторы от производителя

Высокая производительность

Real-time и историческая корреляция

Нет ограничений по количеству событий и источникам

Наличие собственных модульных агентов

Вертикальная масштабируемость

Разделение нагрузки на несколько серверов или виртуальных машин

Горизонтальная масштабируемость

АЛГОРИТМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

МАШИННОЕ ОБУЧЕНИЕ

КЛАССИФИКАЦИЯ ИИ

Система поддержки принятия решений

Система принятия решений на основе входящей информации

СИСТЕМЫ ИБ

Технологии машинного обучения давно используются в различных отраслях

Системы безопасности – это одна из малого количества современных, наукоемких отраслей, где технологии ИИ появились относительно поздно

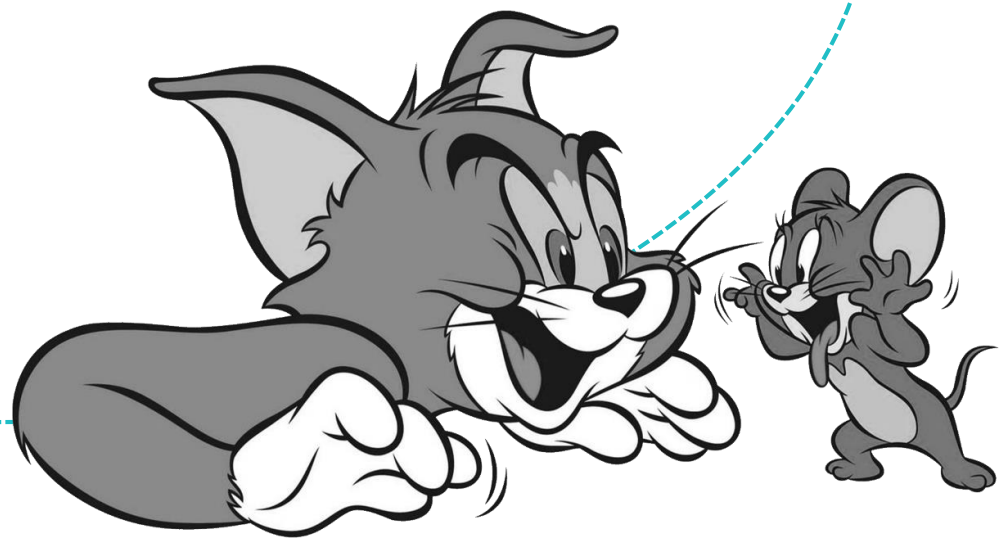
ВОПРОС:

А вы знаете, в чем отличие между СИСТЕМАМИ БЕЗОПАСНОСТИ и МЕТЕОРОЛОГИЕЙ?

RUSIEM
Всё под контролем

Киберпреступники и Защитники информации - вечная борьба добра и зла!

Кто окажется более оснащеным и технологичным!?



АЛГОРИТМ DGA

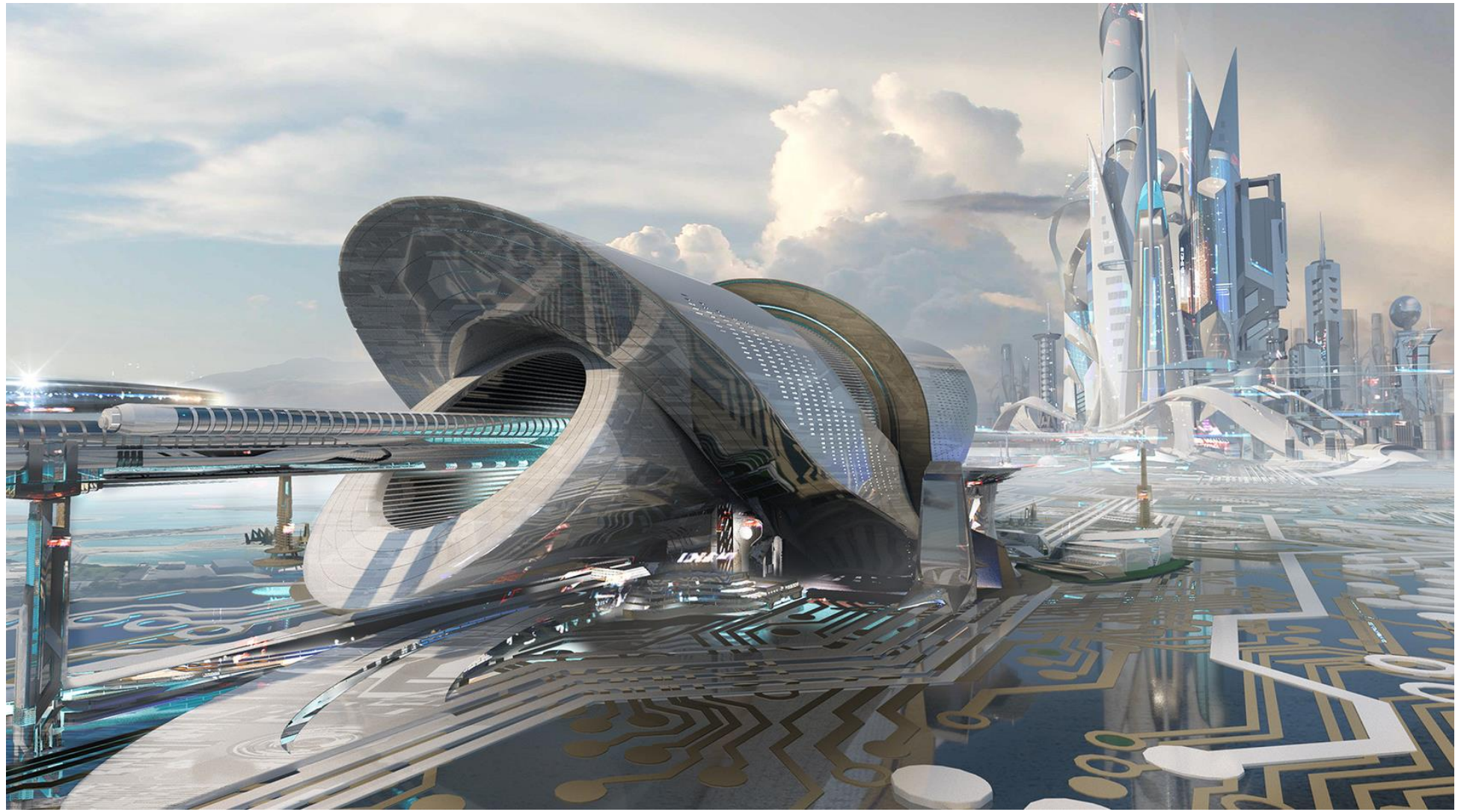
СЕМЕЙСТВА DGA

bamital	banjori	bigviktor	blackhole	ccleaner	chinad
conficker	cryptolocker	dircrypt	dyre	emotet	enviserv
feodo	fobber	gameover	gspy	locky	madmax
matsnu	mirai	murofet	mydoom	necurs	ngioweb
nymaim	omexo	padcrypt	proslikefan	pykspa	qadars
ramnit	ranbyus	rovnix	shifu	shiotob	simda
suppobox	symmi	tempedreve	tinba	tinynuke	tofsee
vawtrak	vidro	virut	xshellghost		

ПРИМЕНЕНИЕ UEBA В ИБ

- DLP
- IAM
- EM
- EDR
- NTA

- Data-Centric Audit and Protection
- Cloud Access Security Broke
- PAM
- Application security testing



ЧТО ЭТО НАМ ДАЕТ?

Актуальность искусственного интеллекта в информационной безопасности

Результат внедрения технологий искусственного интеллекта (поведенческий анализ и предиктивная аналитика)

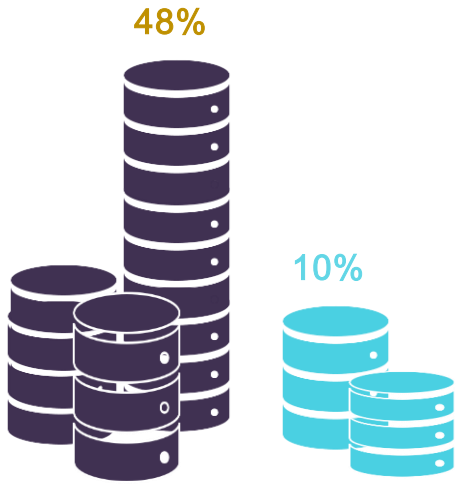
- ✓ повышение эффективности обнаружения атак
- ✓ сокращение времени реагирования
- ✓ сокращение затрат на организацию безопасности

СОКРАЩЕНИЕ ЗАТРАТ

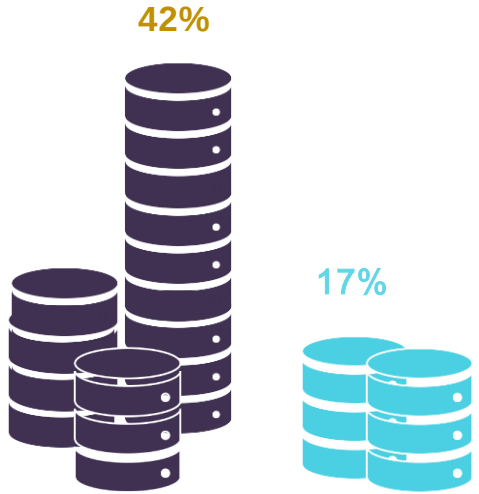
Статистика* сокращения расходов на детектирование и реагирование на инциденты при использовании технологий ИИ

- снижение на 1-15%
- снижение более, чем на 15%

*По данным Capgemini Research Institute



Затраты на обнаружение нарушения

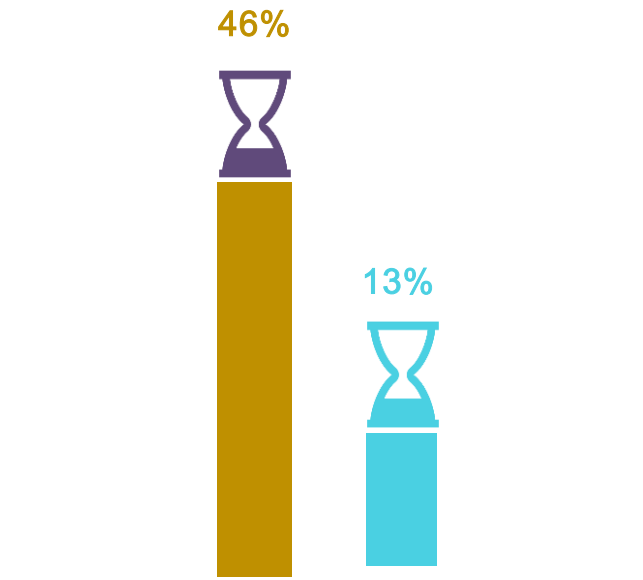


Затраты на восстановление после нарушения с точки зрения ИТ-систем

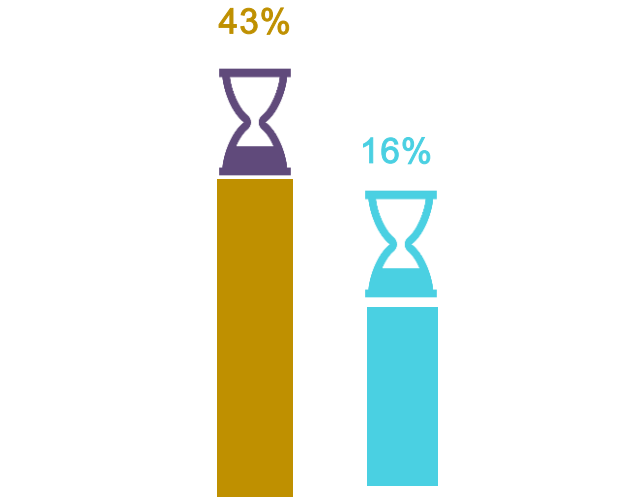
СОКРАЩЕНИЕ ВРЕМЕНИ

Статистика* сокращения времени обнаружения угроз при использовании технологий ИИ

- снижение на 1-15%
- снижение более, чем на 15%



Время, затраченное на обнаружение нарушения



Время, затраченное на устранение нарушения

*По данным Capgemini Research Institute

Ответим на все вопросы ОБРАЩАЙТЕСЬ!

Контактная информация:

Антон Фишман, технический директор RuSIEM

Сайт : www.rusiem.com

Почта: info@rusiem.com

Телефон: +7(495)748-83-11