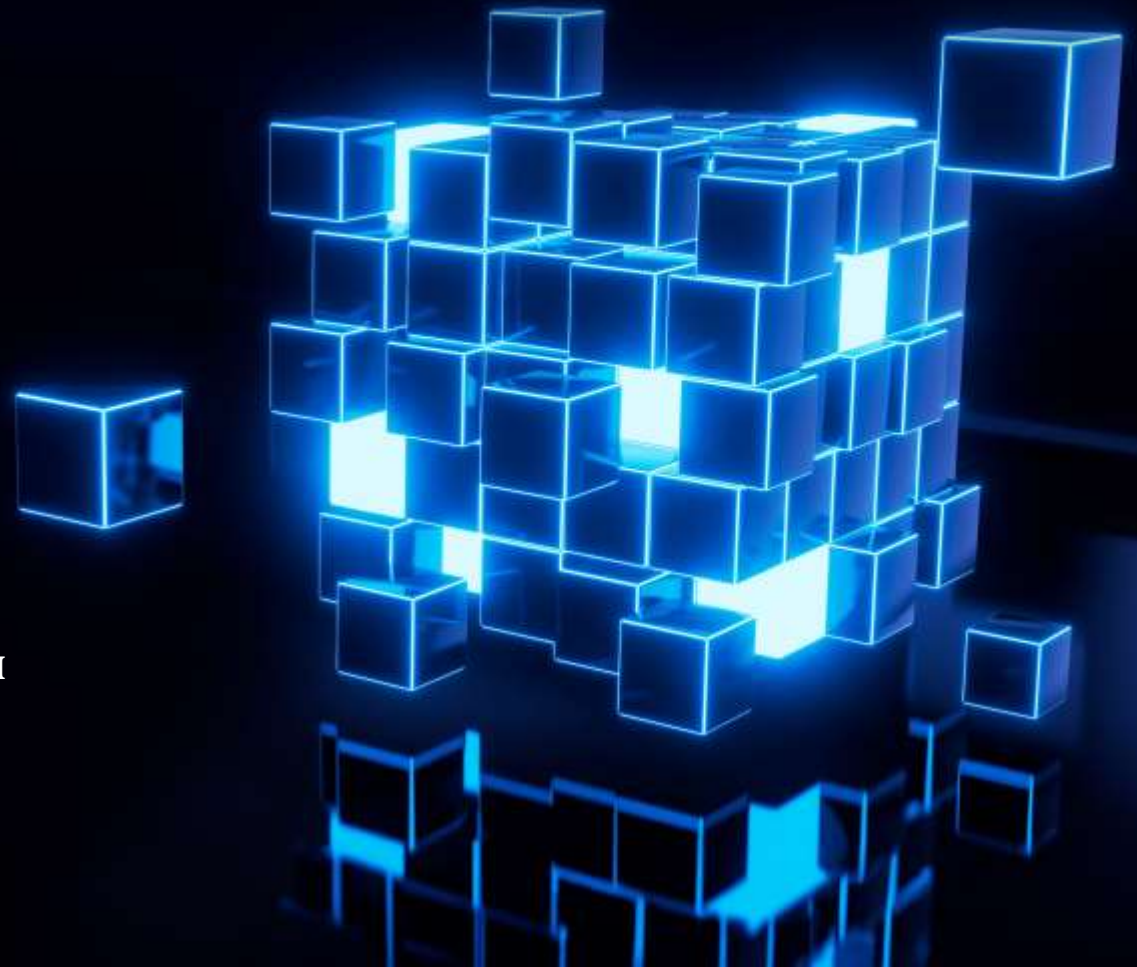
BI.ZONE

Импортозамещение SIEM

Танец на граблях

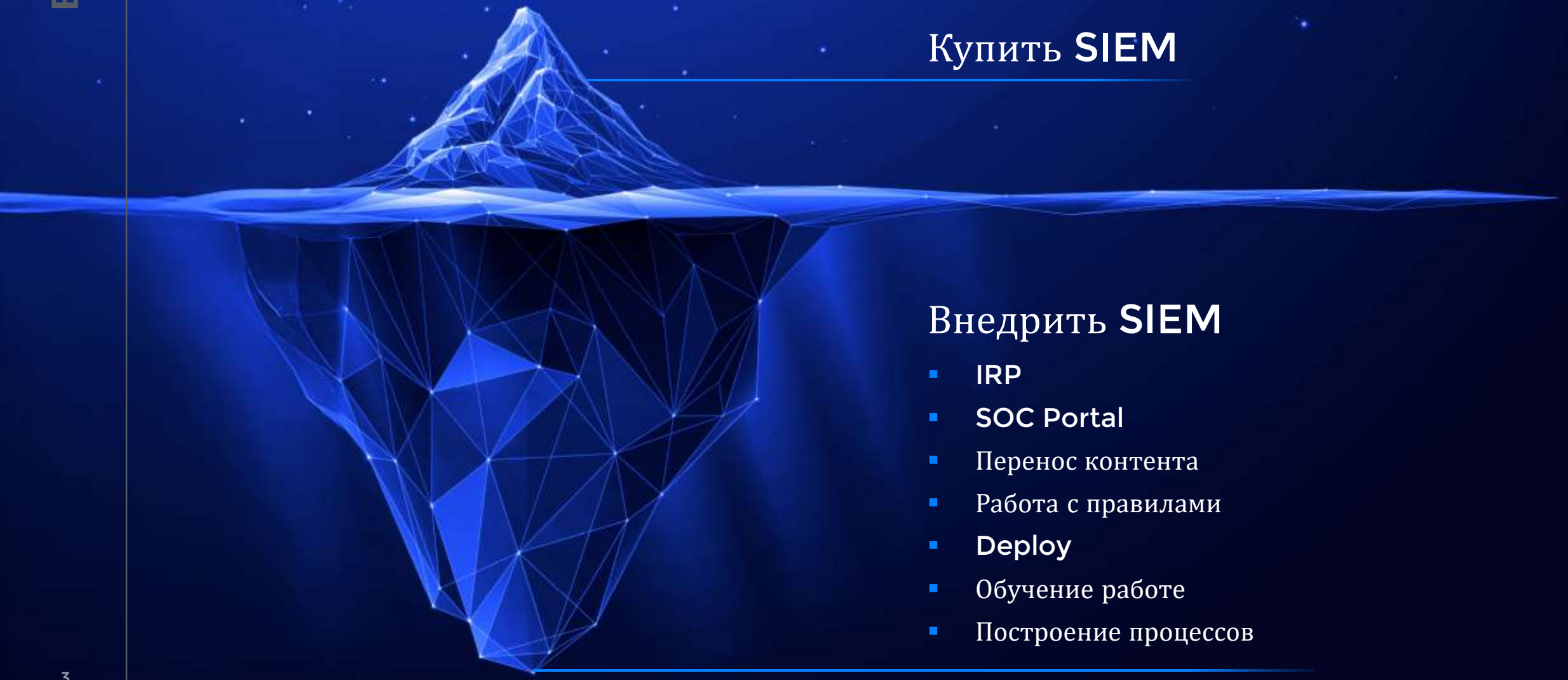


Геннадий Мухамедзянов

Руководитель группы поддержки и развития систем мониторинга кибербезопасности

- Лауреат премии **Positive Awards 2023**
- Маинтейнер
  - **mpsiemlib**
  - **mpsiem_exporter**
  - **VSCodeXP-Workspace** для **Apple ARM**
- Руководитель группы поддержки и развития систем мониторинга кибербезопасности, **BI.ZONE**
- Архитектор **SOC, ex-JSOC**
- Спикер **PHDAYS**

BI.ZONE



Купить **SIEM**

Внедрить **SIEM**

- **IRP**
- **SOC Portal**
- Перенос контента
- Работа с правилами
- **Deploy**
- Обучение работе
- Построение процессов

BI.ZONE

О чем мы говорим

Контентная часть

- Алгоритмы действий
- Методология разработки
- Модели данных
- Создание исключений
- Актуализация контента

BI.ZONE

О чем мы говорим

Архитектурная часть

- Архитектура **SIEM**
- Сетевые доступы
- Интеграций со сторонними системами
- Доставка контента
- Мониторинг системы и ее модель здоровья

BI.ZONE

Контентная часть

01

BI.ZONE

Когда в первый раз увидел контент новой **SIEM**

Когда понял контент **SIEM**

BI.ZONE

Алгоритм действий

Анализ существующего контента

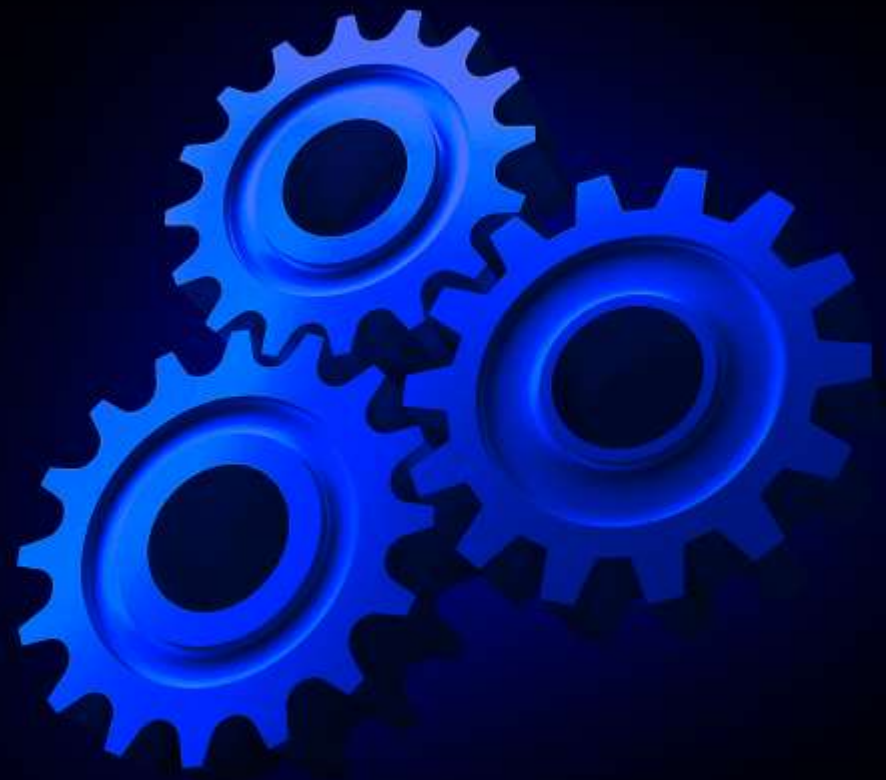
- Выявление устаревших и тестовых правил
- Выявление типов правил и табличных списков
- Группировка по правилу **20/80**
- Персонализированный контент
- Приоритеты контента
- Работа с исключениями и профилирование

BI.ZONE

Методология разработки

Правила работы

- Стиль написания контента
- Правила наименования сущностей
- Шаблоны правил
- Работа с исключениями
- Активное использование макросов
- Формирование пакетов экспертизы
- Правила актуализации контента



BI.ZONE

Макросы

Редактирование макроса BB_common_Powershell_without_ScriptBlock_Windows

```
filter BB_common_Powershell_without_ScriptBlock_Windows() {
            filter::NotFromCorrelator()
            and event_src.vendor == "microsoft"
            and event_src.title == "windows"
            and ((event_src.title == "windows" and msgid == "400")
            or regex(lower(subject.process.original_name), "powershell.exe|syncappvpublishingserver.exe", 0)
!= null
            or regex(lower(object.process.cmdline), ".*
(powershell|syncappvpublishingserver|pwsh\.exe|pwsh).*", 0) != null)
}
```

Редактирование макроса BB_eventtype_ServiceInstall

```
filter BB_eventtype_ServiceInstall() {
        event_src.vendor == "microsoft"
        and event_src.title == "windows"
        and in_list(["4697", "7045"], msgid)
    }
```

BI.ZONE


Кто мы?
Аналитики SOC
Чего мы хотим?
Свою модель данных в любой SIEM
Когда мы это хотим?
Всегда

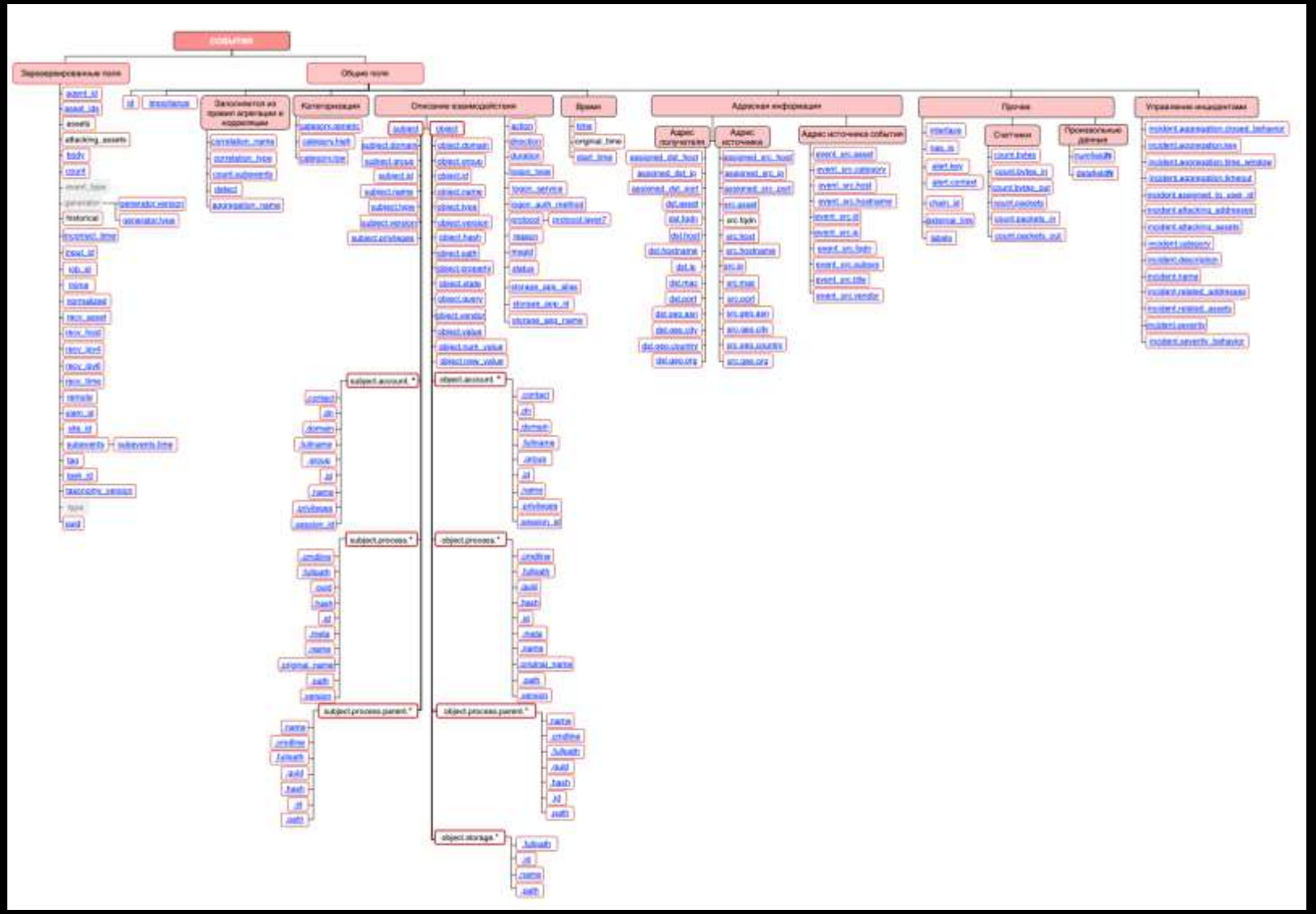
BI.ZONE

Синхронизация моделей данных

- Формирование маппинга полей
- Приведение типов
- Доработка моделей данных

BI.ZONE

Таксономия



BI.ZONE

Маппинг полей

Таблица маппинга

BDM = Начните набирать... MP SIEM DM = Начните набирать...

BDM	MP SIEM DM	Условие
		Общие поля события
__payload	body	`"__payload": c.item("body", default=None)`
event_category	event_src.category	`"event_category": c.item("event_src.category", default=None)`
event_description	text	`"event_description": c.item("text", default=None)`
event_id	msgid	`"event_id": c.item("msgid", default=None)`
event_log_name	event_src.subsys	`"event_log_name": c.item("event_src.subsys", default=None)`
event_reason	reason	`"event_reason": c.item("reason", default=None)`
event_reason_code	reason	`"event_reason_code": c.item("reason", default=None)`
event_result	status	`"event_result": c.item("status", default=None)`
event_time	time	`"event_time": c.item("time", default=c.call_func(dt_now))`
event_type	object.type	`"event_type": c.item("object.type", default=None)`
event_utc_time	original_time	`"event_utc_time": c.item("original_time", default=None)`
logSourceType	event_src.title	`"logSourceType": c.item("event_src.id", default=None)`
rule_name	correlation_name	`"rule_name": c.item("correlation_name", default=None)`
		Источник активности

dev_action	action	`"dev_action": c.if_(`
		`  c.item("event_category", default=None).in_(["Firewall", "IDS/IPS"]),`
		`  if_true=c.item("action", default=None),`
		`  if_false=None`
		`)`

BI.ZONE

Алгоритм действий

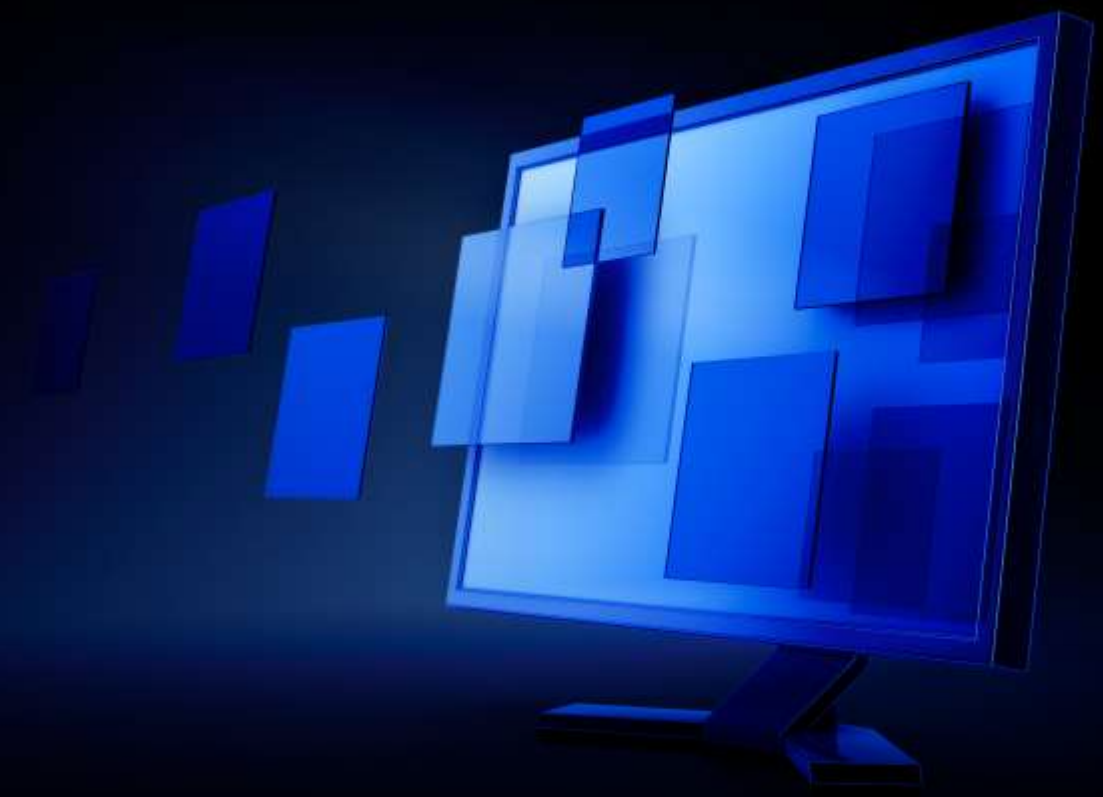
Работа с контентом

- Тестирование своих правил в новом **SIEM**
- Определение узких мест
- Переработка логики правил
- Переработка плейбуков

BI.ZONE

Актуализация контента

- Автоматизированное тестирование правил
- Версионирование контента
- Перенос обновлений в измененные формулы нормализации
- Подготовка пакета логов для тестов



BI.ZONE

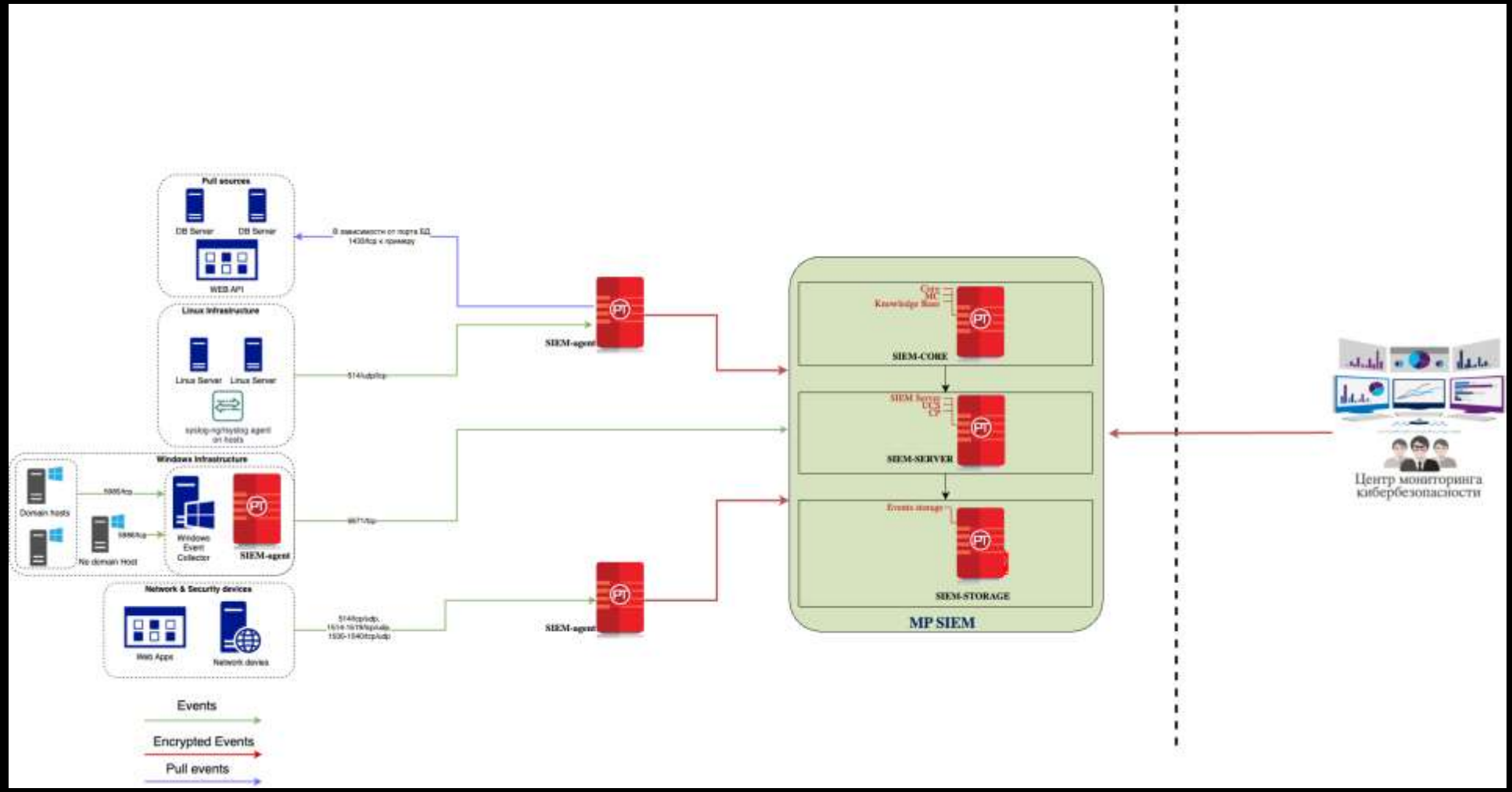
Архитектурная часть

02

BI.ZONE

Архитектура SIEM

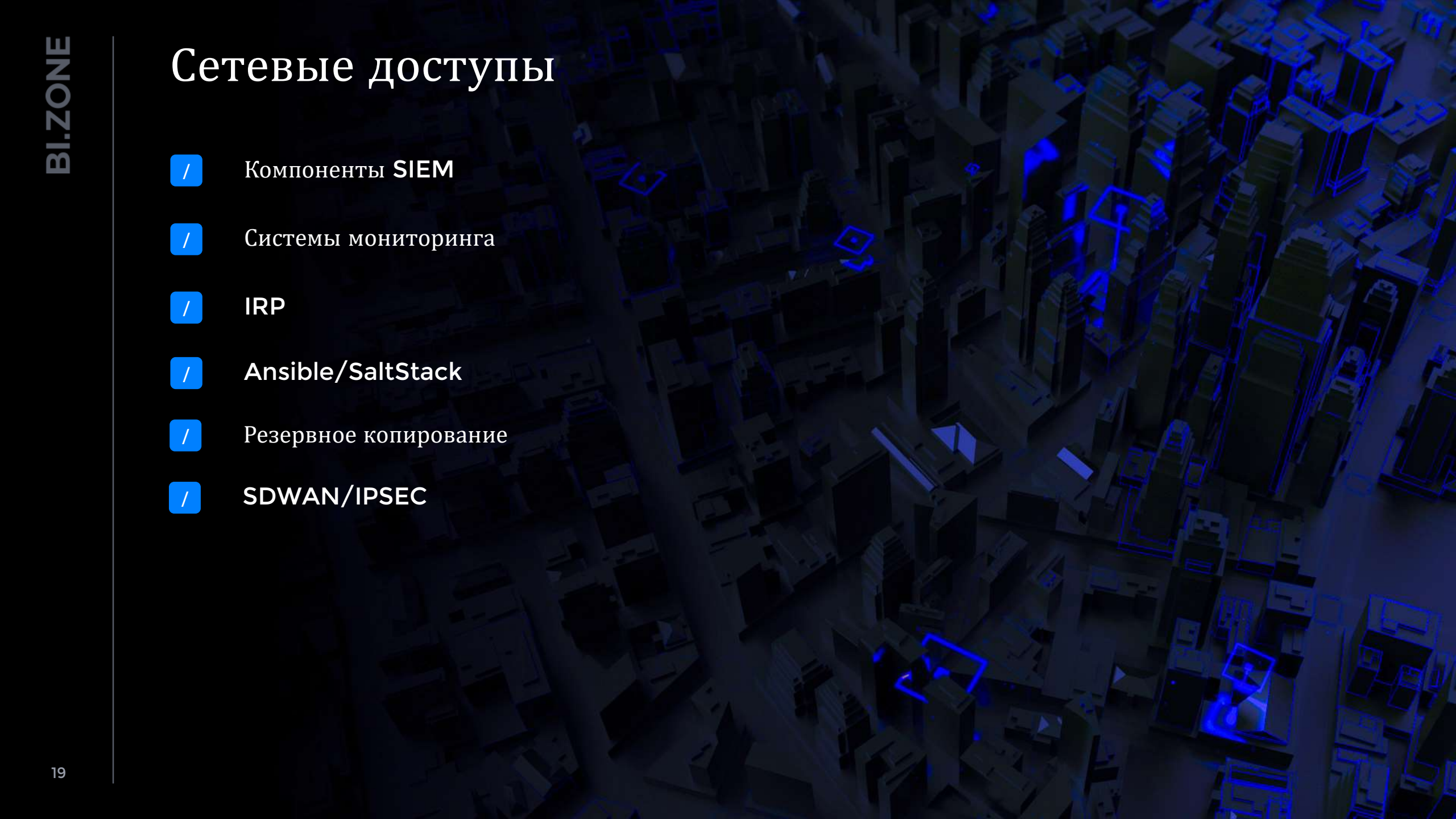
Гибридный вариант



BI.ZONE

Сетевые доступы

- Компоненты **SIEM**
- Системы мониторинга
- **IRP**
- **Ansible/SaltStack**
- Резервное копирование
- **SDWAN/IPSEC**



BI.ZONE

Интеграций со сторонними системами

- Threat Intelligence Platform
- Incident Response Platform
- Retro Correlation Platform
- Клиентский портал

BI.ZONE

Доставка контента

- Ручная доставка контента
- Методология GitOPS
- Специальные сборки контента

BI.ZONE


Кто мы?
Инженеры SOC
Чего мы хотим?
Унификации настройки
и мониторинга любой SIEM
Когда мы это хотим?
Всегда

BI.ZONE

Мониторинг системы и ее модель здоровья

- Мониторинг оборудования
- Мониторинг операционной системы
- Мониторинг компонентов **SIEM**
- Мониторинг сущностей **SIEM**
- Мониторинг источников
- Мониторинг доступности

BI.ZONE

Мониторинг системы и ее модель здоровья

Алерты MP SIEM (Общие)					
- alert: MPSIEMLicenseExpires 10d expr: siem_lic_expiration_days{service="MP_SIEM"} < 10 for: 30m labels: severity: medium team: MPSIEM annotations: summary: License expires description: "Days before license expiration: {{ print \"%.0f\" $value }}\nHost: {{ .Labels.instance }}"	До окончания срока лицензии меньше 10 дней	MEDIUM	Узнать о статусе обновления лицензии		
- alert: MPSIEMLicenseExpires 3d expr: siem_lic_expiration_days{service="MP_SIEM"} < 3 for: 30m labels: severity: high team: MPSIEM annotations: summary: License expires description: "Days before license expiration: {{ print \"%.0f\" $value }}\nHost: {{ .Labels.instance }}"	До окончания срока лицензии меньше 3 дней	HIGH	Узнать о статусе обновления лицензии		
- alert: MPSIEMHealthStatusRed expr: last_over_time(mpsiem_lights_color{service="MP_SIEM",color="red"}[5m]) == 3 for: 10m	В MP SIEM обнаружена ошибка в работе системы или ее компонента	HIGH	Для просмотра ошибки нужно залогиниться в MP SIEM и в интерфейсе прочитать сообщение		

BI.ZONE

Мониторинг системы и ее модель здоровья

Алерт	Объяснение	Severity	Реагирование
	• Порт 8091 и порт 9081 недоступны • Порт 9200 недоступен		
Алерты MP SIEM (Общие)			
Лицензия истечет менее чем через 10 дней	До окончания срока лицензии меньше 10 дней	MEDIUM	
Превышение EPS - поток событий превысил норму более чем в 2 раза	EPS увеличился более чем в 2 раза за последние 10 минут	MEDIUM	
Светофор красный	В MP SIEM обнаружена какая-то ошибка.	HIGH	Для просмотра ошибки ну MP SIEM и в интерфейсе п
Светофор желтый		MEDIUM	
Алерты MP SIEM (Задачи)			
Задача {Taskname} не запущена	Задача {Taskname} не запущена	HIGH	
Светофор задачи {Taskname} красный	Ошибки в задаче, которые нужно исправлять	HIGH	
Светофор задачи {Taskname} желтый	Часть подзадач в задаче не работаю. К примеру, собираются логи только с 3 серверов, а не с 5	MEDIUM	
Алерты MP SIEM (EPS)			
Превышение EPS - поток событий превысил норму более чем в 2 раза	EPS увеличился более чем в 2 раза за последние 10 минут	MEDIUM	
Поток ниже минимального	EPS системы ниже минимального. Возможно у заказчика отвалились какие-то информационные системы	MEDIUM	
Алерты (Источники)			
Сутки нет данных с {#SOURCE}			
Час нет данных с {#SOURCE}			

BI.ZONE

Спасибо
за внимание

Геннадий Мухамедзянов

Руководитель группы поддержки и развития систем
мониторинга кибербезопасности