КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОНЛАЙН

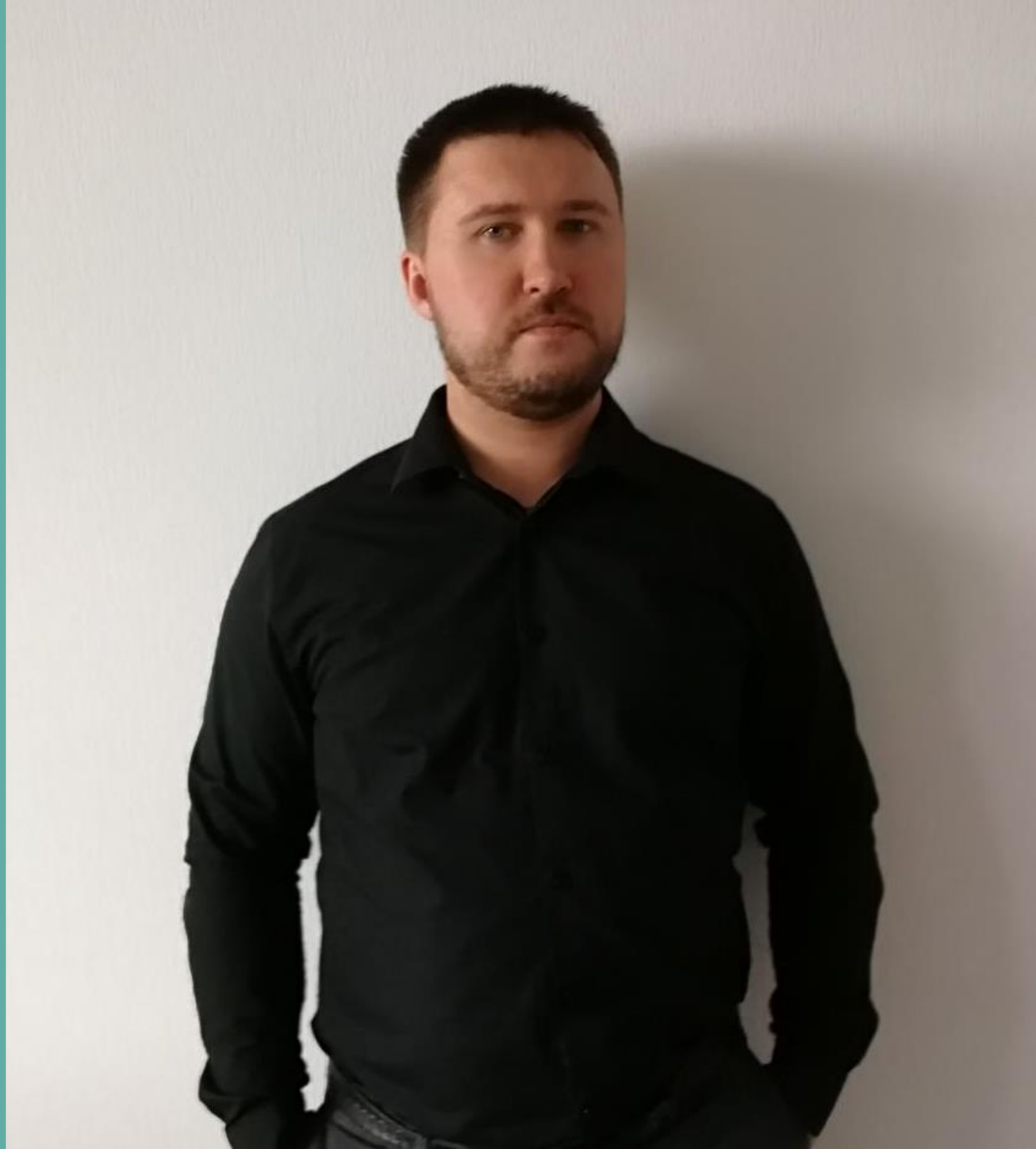
Жизнеспособность SOC, построенного на базе опенсорсного SIEM

Игорь ПИТЕРСКИХ
Независимый эксперт по ИБ

МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

18.00 МСК

29 - 30 ЯНВ'20



Выбор стека под SIEM

1. AlienVault OSSIM
2. Graylog
3. Apache Metron
4. MozDef (ELK)
5. Wazuh (ELK)
6. Sentinel (ELK)

Общие плюсы и минусы

-

- Большинство не поддерживаются большим сообществом
- У части, отсутствует управление логами, визуализация
- У большинства отсутствует интеграция со сторонними сервисами
- Часть не имеют агентов и средств доставки логов
- Сложность внедрения
- Требуют значительной доработки напильником
- Отсутствие техподдержки
- Скудный инвентарь средств по сравнению с энтерпрайзными решениями

+

- Низкая стоимость
- Гибкость (при наличии разработчика в команде)

Обязанности линий

1 мониторинг поступающих событий

2 расследование инцидентов поступивших от первой линии

3 анализ иницидентов, отслеживание актуальных угроз, настройка правил корреляции

Уровень развития SOC

1

1*5 - начальный - заведение начального перечня событий, простая корреляция, система менеджмента инцидетов

2

8*5 - средний - заведение расширенного перечня событий, сложная корреляция, обогащение событий, плейбуки, отслеживаемое время реакции в зависимости от критичности

3

24*7 - зрелый - отслеживание поступления событий, автоматический контроль перечня хостов, контроль и тестирование работоспособности компонентов и средств, активлисты, тренды, автоматизированные плейбуки, ARP

Жизнеспособность SOC на каждом этапе предъявляет разные требования.

Для вашей компании может быть совсем не нужен зрелый SOC

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

piterskih@inbox.ru