КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОНЛАЙН

Построение "инхаус" SOC.
Цели, этапы, ошибки

Игорь ПИТЕРСКИХ
Независимый эксперт по ИБ

МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

18.00 МСК

29 - 30 ЯНВ'20

Уровень развития SOC

1

1*5 - начальный - заведение начального перечня событий, простая корреляция, система менеджмента инцидетов (численность:1-2 сотрудника, сочетающих в себе 1, 2, 3 линии + администрирование)

2

8*5 - средний - заведение расширенного перечня событий, сложная корреляция, обогащение событий, плейбуки, отслеживаемое время реакции в зависимости от критичности (численность: 2 сотрудника 1 линии, 2 сотрудника 2 лини, аналитик +администрирование)

3

24*7 - зрелый - отслеживание поступления событий, автоматический контроль перечня хостов, контроль и тестирование работоспособности компонентов и средств, активлисты, тренды, автоматизированные плейбуки, ARP (численность: 5 сотрудников 1 линии, 2-3 сотрудника 2 лини, 1-2 аналитика, сотрудник редтима, 1-2 сотрудника под администрирование)

Цели

1. Снизить время обнаружения проникновения в сеть злоумышленников и обеспечить реакцию
2. Обнаружить и предотвратить небезопасные действия сотрудников
3. Недопустить/купировать утечки информации

Задачи

1. Покрыть необходимый перечень источников (антивирусы, IDS/IPS, логи домена, локальные логи машины, логи сетевых устройств)
2. Реализовать простые правила обеспечивающие ранее выявление проникновения злоумышленников в сеть
3. Реализовать правила по выявлению действий сотрудников, несогласованных или недобросовестных
4. Обеспечить утилизацию поступающих кейсов сотрудниками 1 и 2 линии, установить SLA
5. Построить процесс создания и отладки новых правил, поддержки существующих
6. Построить процесс выявления и оперативного устранения неполадок на системах и в поступлении логов и событий

Распространенные ошибки

1. Неправильно поставленные цели
2. Перекосы в развитии
3. Отсутствие связи между линиями
4. Отсутствие контроля за системами исключения в правилах обнаружения (над действиями сотрудников SOC)
5. Отсутствие контроля поступления логов от источников (за оборудованием)

Краткие выводы

Необходимо ставить корректные цели, не допускать перекосов, обеспечивать горизонтальные и вертикальные связи между сотрудниками и процессами

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

piterskih@inbox.ru