ОТ ПОДХОДОВ К СОЗДАНИЮ СИТУАЦИОННОГО ЦЕНТРА К ПОСТРОЕНИЮ ЭФФЕКТИВНЫХ МЕТОДОВ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИБ

Ксения Засецкая
Старший консультант Отдела консалтинга
АО «ДиалогНаука»

Роман Ванерке
Технический директор
АО «ДиалогНаука»

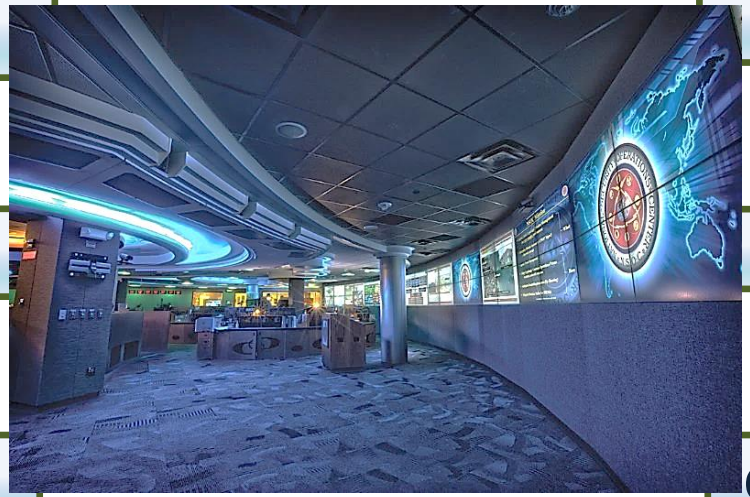
ДиалогНаука

Ситуационные центры ИБ (SOC)

- Уровень зрелости компании и готова ли компания к построению SOC?
- Какая форма организации SOC предпочтительнее?
- Какой целевой уровень зрелости SOC?

SANS

NIST



ISO

ГОСТ

HPE, IBM

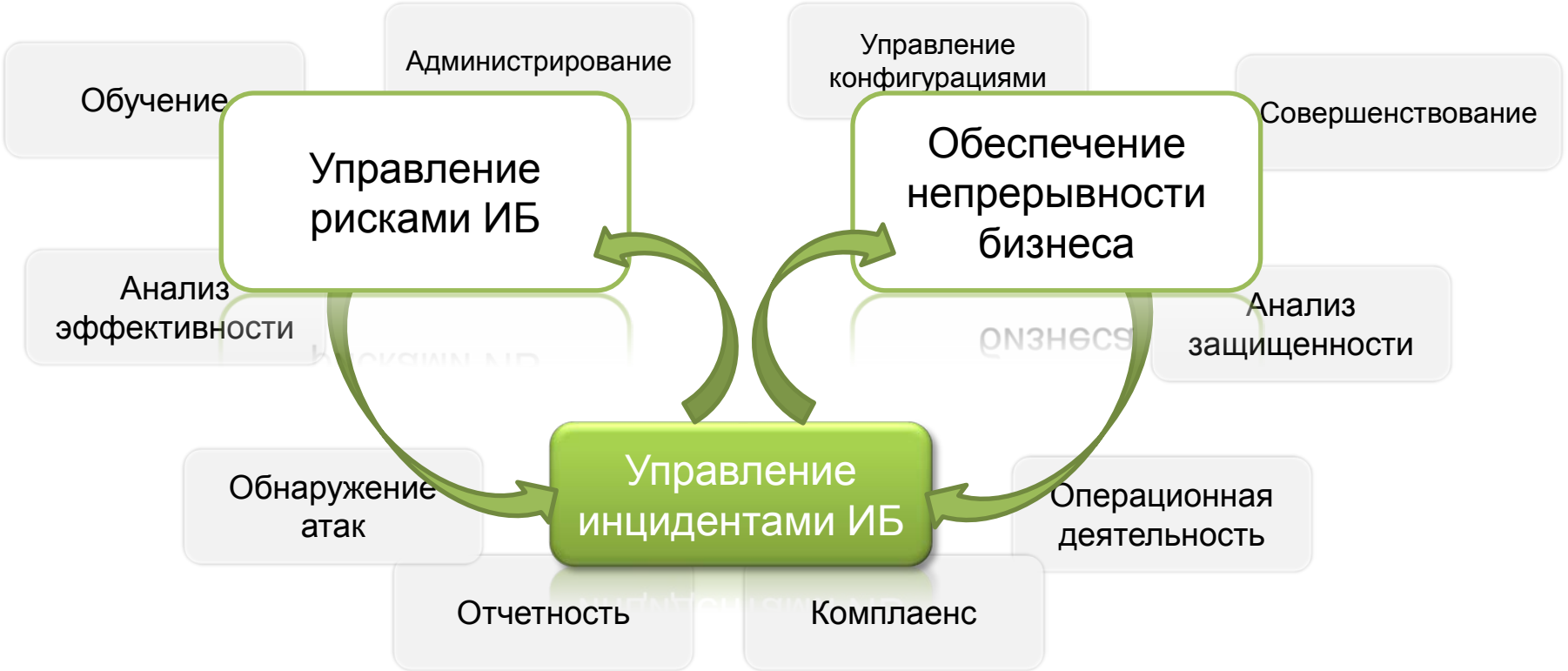
СТО БР ИББС

Критичные параметры для SOC

- Определенность в целях и режиме работы
- Документированность
- Взаимодействие участников
- Оценка эффективности
- Анализ и совершенствование

Управляемые процессы - в основе успеха!

Взаимосвязанные процессы

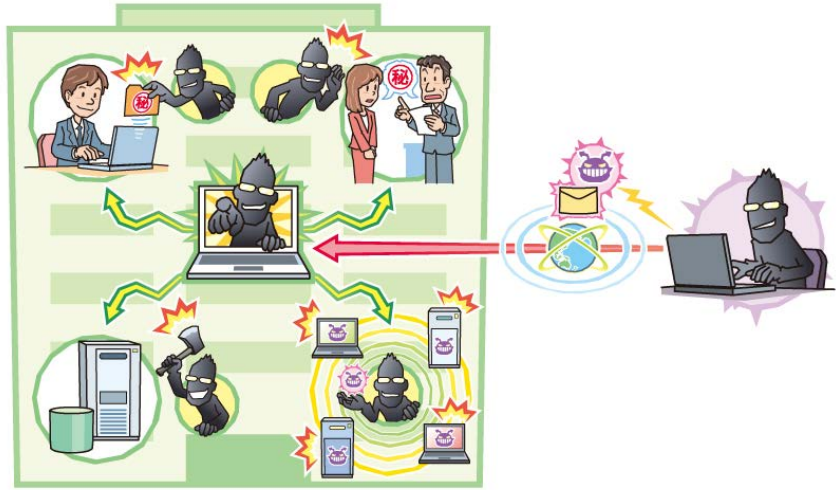


Обмен информацией

Взаимодействие с внешними SOC

Оценка угроз в основе управления

- Для организации успешного процесса управления инцидентами:
  - выделить критичные информационные ресурсы
  - провести оценку угроз информационной безопасности, актуальных для критичных ресурсов
  - использовать полученные результаты при реализации механизмов выявления инцидентов



Угрозы ИБ и методы реализации угроз

- Три основных параметра, на которые направлены угрозы

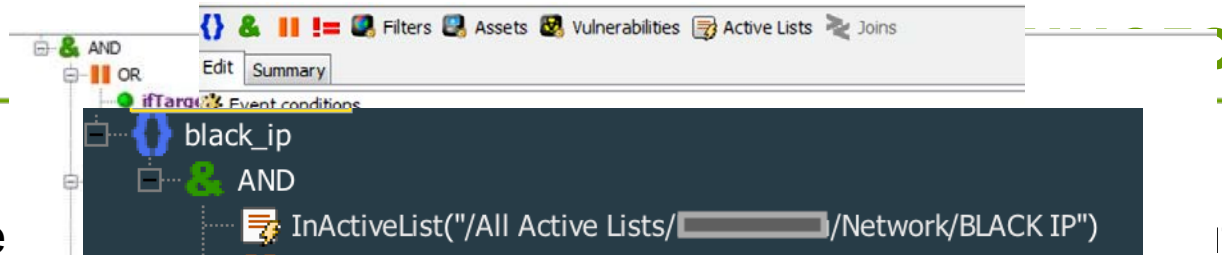
Конфиденциальность | Целостность | Доступность

- 8 типов угроз информационной безопасности, охватывающих все варианты
- 14 комплексных методов реализации угроз безопасности

Методы и сценарии

Описание угрозы	Описание метода	Связанные сценарии	Описание уровня среды обработки	Код сценария выявления	Сценарий выявления
хищение информации (получение доступа к информации)	Несанкционированный доступ	Доступ к информационным ресурсам с использованием скомпрометированных аутентификационных данных	прикладной уровень	1.04.26.05.00001	«Спящие» учетные записи сотрудников и хостов - по которым не было активности в заданный период (30 дней)
хищение информации (получение доступа к информации)	Несанкционированный доступ	Доступ к информационным ресурсам с использованием скомпрометированных аутентификационных данных	Общесистемный уровень (ОС)	1.04.26.03.00001	«Спящие» учетные записи сотрудников и хостов - по которым не было активности в заданный период (30 дней)
блокирование информации	Несанкционированный доступ	Подбор аутентификационной информации	Общесистемный уровень (ОС)	7.04.27.03.00012	Блокировка X учетных записей за Y минут
утрата (неумышленная потеря) информации и/или средств ее обработки	Ошибки персонала	Нарушение процесса путем удаления критичных объектов	Уровень баз данных	3.14.17.04.00015	Удаление критичных объектов (таблиц, файлов)
модификация (искажение) информации	Ошибки персонала	Нарушение процесса путем внесения изменений в критичные объекты	Уровень баз данных	4.14.18.04.00016	Изменение критичных объектов (таблиц, файлов)

Тип нарушителя может быть классифицирован только в ходе расследования и аналитики

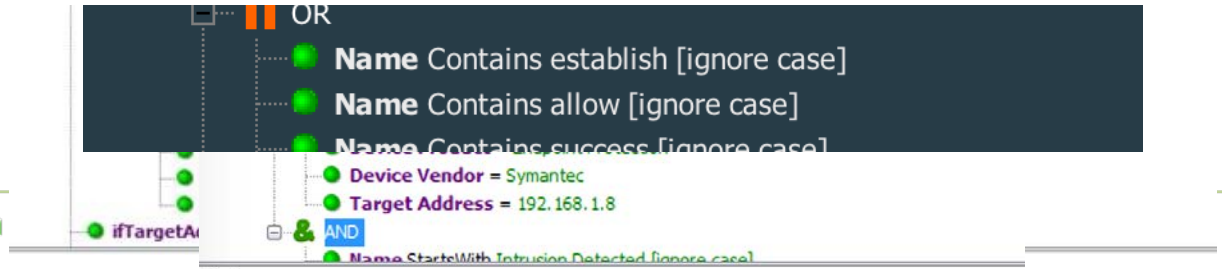


- Сложные
- покине
- Необхс
- данны
- Отсутс
- Сложн
- Отсутс

11/20/17 11:08:00 AM to 11/21/17 11:08:00 AM

Success authenticaton[Preview]

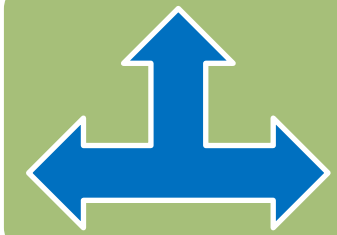
Category Behavior	Category Outcome	Device Vendor	Count(Category Behavior)
/Authentication/Verify	/Success	Microsoft	56472268
/Authentication	/Success	Microsoft	24966
/Authentication/Modify	/Success	Microsoft	942
/Authentication/Verify	/Success	ArcSight	148
/Authentication/Verify	/Success	CISCO	102
/Authentication/Add	/Success	Microsoft	22
/Authentication/Modify	/Success	ArcSight	12



От сценариев выявления к сценариям реализации

L2 - инцидент

- Срабатывание на L0 или L1, использование списков
- Унификация подхода к созданию сценариев



L1 - обогащение

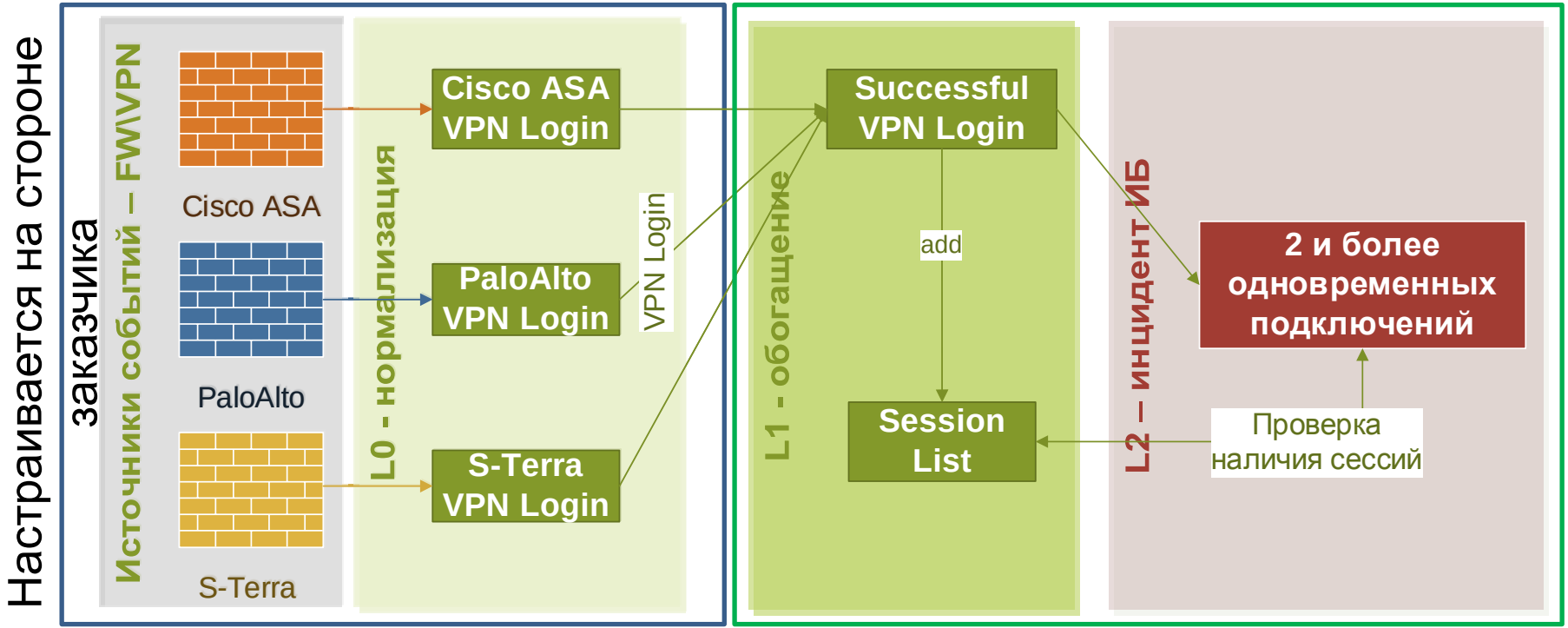
- Дополнительная обработка и обогащение
- Использование Active List\Session List

L0 – нормализация

- Приведение к единой таксономии однотипных событий
- Упрощение условий
- Возможность использования в разных сценариях

Как это работает в ArcSight

- Рассмотрим настройку следующего сценария выявления «2 и более подключений через VPN под одним пользователем»



Вопросы

Спасибо за внимание!

АО «ДиалогНаука»
Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: k.zasetskaya@DialogNauka.ru
rv@DialogNauka.ru