УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИБ. СОЗДАНИЕ ЭФФЕКТИВНЫХ МЕТОДОВ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИБ

Ксения Засецкая
Старший консультант
АО «ДиалогНаука»

Никита Цыганков
Руководитель направления
АО «ДиалогНаука»

ДиалогНаука

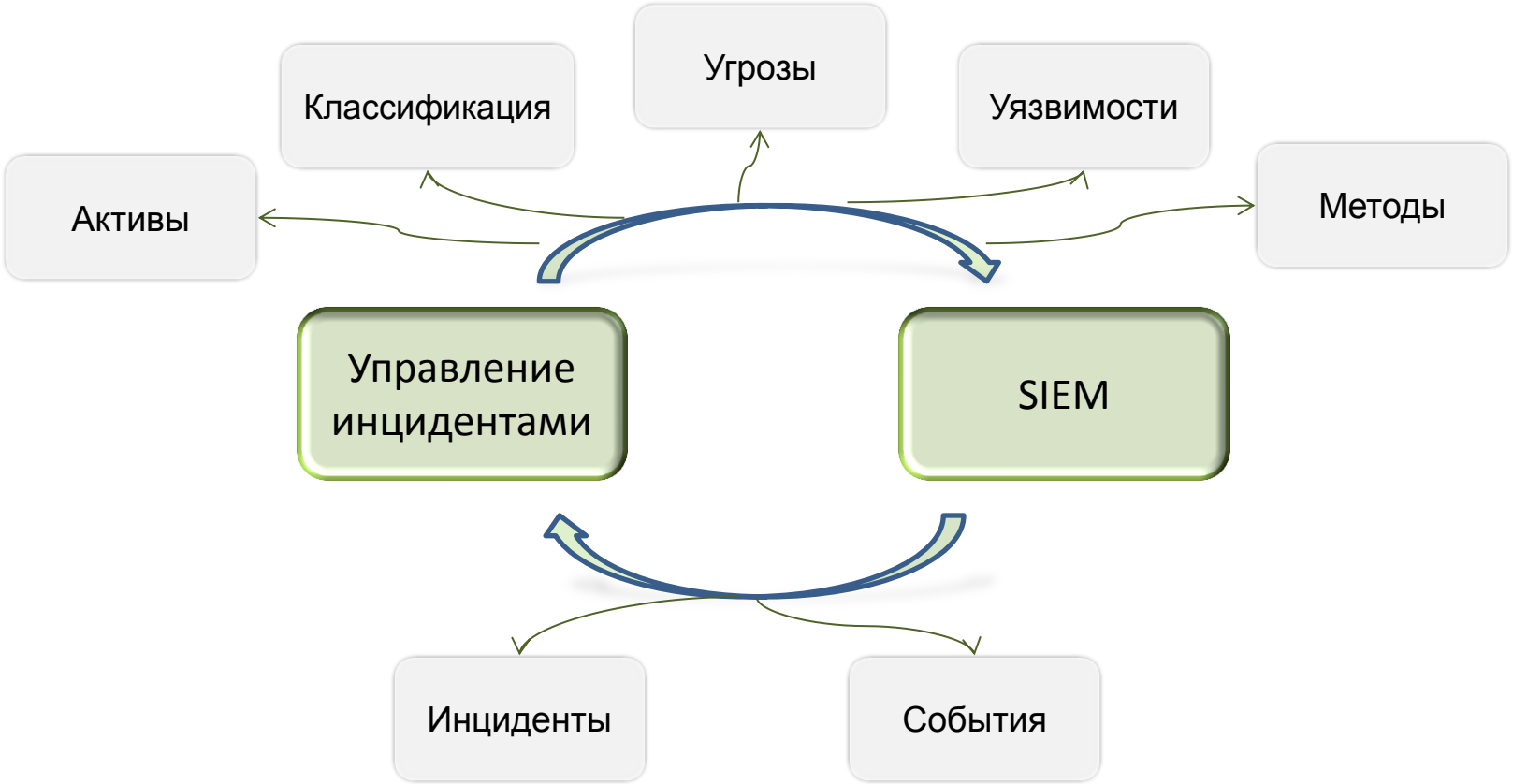
О чем мы говорим?

Управление инцидентами

SOC

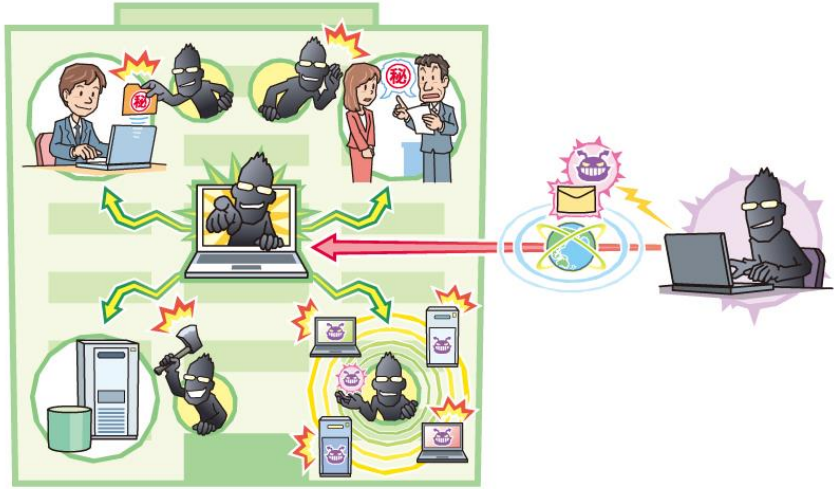
SIEM

Взаимное влияние



Оценка угроз в основе управления

- Критичные информационные ресурсы
- Оценка угроз
- Результаты для 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

Угрозы ИБ

- хищение и утрата информации и средств обработки → ✓ Нарушение конфиденциальности
- модификация, отрицание подлинности информации → ✓ Нарушение целостности
- блокирование, уничтожение → ✓ Нарушение доступности

Методы реализации угроз ИБ

- Выполнение вредоносных программ
- Сетевое сканирование и прослушивание
- Несанкционированный доступ
- Сбои и отказы каналов связи
- Ошибки в обеспечении безопасности информации
- Социальный инжиниринг

Уровень среды обработки

- Физический уровень (линии связи, аппаратные средства)
- Уровень сетевой инфраструктуры
- Общесистемный уровень (ОС)
- Уровень баз данных
- Прикладной уровень
- Уровень бизнес-процессов

Методы и сценарии

Описание угрозы	Описание метода	Связанные сценарии	Описание уровня среды обработки	Код сценария выявления	Сценарий выявления
Хищение информации (получение доступа к информации)	Сетевое сканирование и прослушивание	Использование уязвимостей доступных ресурсов	Прикладной уровень	01.02.37.02.00043	Обнаружение попыток SQL инъекции
Хищение информации (получение доступа к информации)	Несанкционированный доступ	Доступ к информационным ресурсам с использованием скомпрометированных аутентификационных данных	Общесистемный уровень (ОС)	01.04.26.03.00028	Интерактивная аутентификация сотрудника без регистрации в СКУД
Навязывание ложной информации	Внедрение ложных доверенных объектов в КИВС	Несанкционированное создание нелегитимного узла	Уровень сетевой инфраструктуры	06.03.54.02.00039	Появление новых хостов в критичном/пользовательском/серверном сегменте
Утрата (неумышленная потеря) информации и/или средств ее обработки	Ошибки персонала	Нарушение процесса путем удаления критичных объектов	Уровень баз данных	03.14.17.04.00015	Удаление/изменение критичных объектов (таблиц, файлов)
Хищение информации (получение доступа к информации)	Несанкционированный доступ	Подбор аутентификационной информации	Уровень баз данных	01.04.27.04.00195	Обнаружение успешного подбора пароля к СУБД

Тип нарушителя может быть классифицирован только в ходе расследования и аналитики

Корреляция

- Correlation rule предназначено для выявления **инцидентов ИБ**
- Типы правил – обычное правило, «легкие» правила, предобработка
- Правила – realtime или «по расписанию»
- Используются Filters и Variables
- Учитывать активы (инвентаризация, категоризация событий, категории)
- Агрегация, Time Frame
- Active list/Session List
- Trends, Data Monitor
- Actions/Threshold
- Реагирование (CounterACT)

похода

- Сложные ... ита покинет к...
- Необхо... данные ...)
- Отсутс...
- Сложн...
- Отсутс...

Filters Assets Vulnerabilities Active Lists Joins

Edit Summary

AND

OR

ifTarg... Event conditions

black_ip

AND

InActiveList("/All Active Lists/[redacted]/Network/BLACK IP")

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

OR

Name Contains establish [ignore case]

Name Contains allow [ignore case]

Name Contains success [ignore case]

Device Vendor = Symantec

Target Address = 192.168.1.8

ifTargetA...

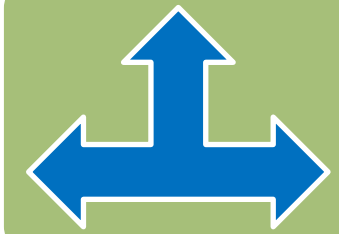
AND

Name StartsWith Intrusion Detected [ignore case]

От сценариев выявления к сценариям реализации

L2 - инцидент

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



L1 - обогащение

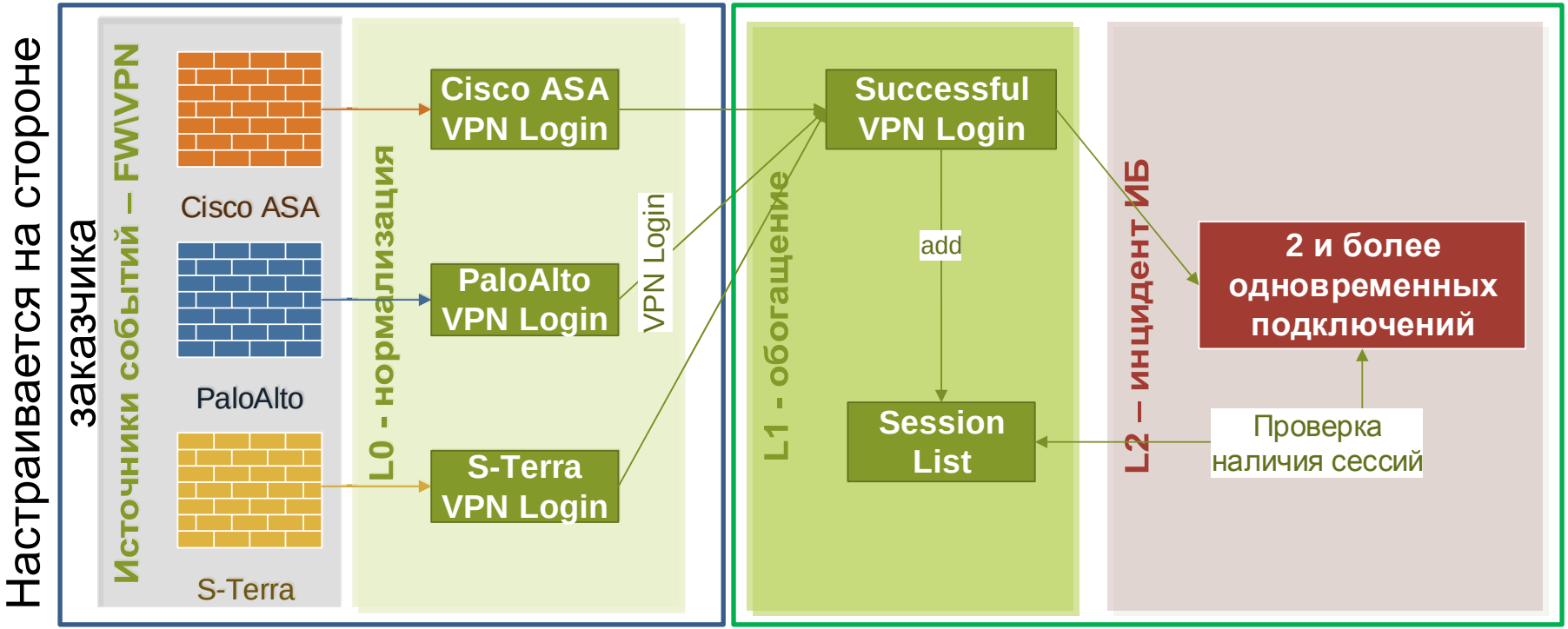
- Дополнительная обработка и обогащение
- Использование Active List\Session List

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»



Пакет правил корреляции АО «ДиалогНаука»

- Пакет включает в себя набор готовых правил корреляции и отчетов, позволяющих выявлять инциденты информационной безопасности
- Может поставляться в месте с стандартной или расширенной технической поддержкой
- Пакет постоянно развивается и пополняется новыми правилами корреляции
- Внедрение пакета позволяет значительно повысить эффективность существующей ИБ ArcSight, а также существенно сократить временные затраты на создание новых правил корреляции собственными силами

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

tsygankov@DialogNauka.ru