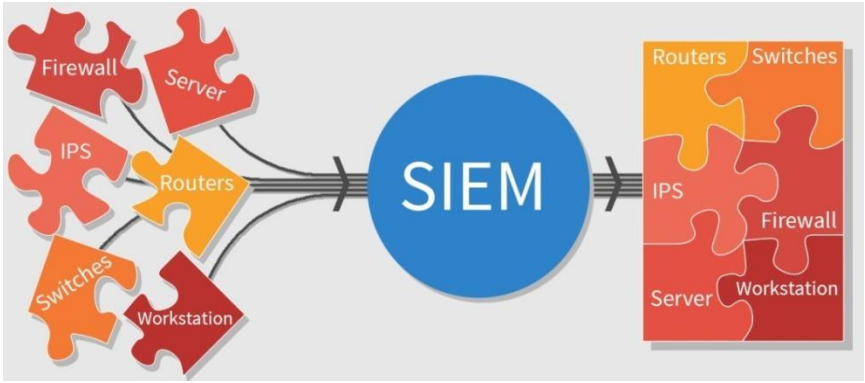
Бардак с выявлением инцидентов?
Покажем!
Научим!
Внедрим!

Никита Цыганков
Руководитель направления
АО «ДиалогНаука»

ДиалогНаука

Темы презентации

Многоуровневый подход **пакета SOC**
Выявление сложных инцидентов по **Kill Chain**
Классификация **инцидентов**
Выявление **атак**, отслеживание стадий и классификация

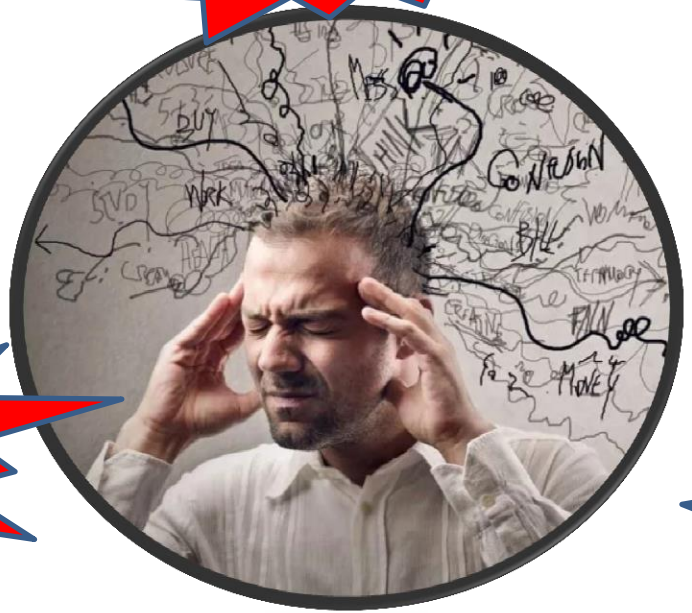


Болит голова от несвязных инцидентов?

DB instance droped

Virus Detection

SQL injection

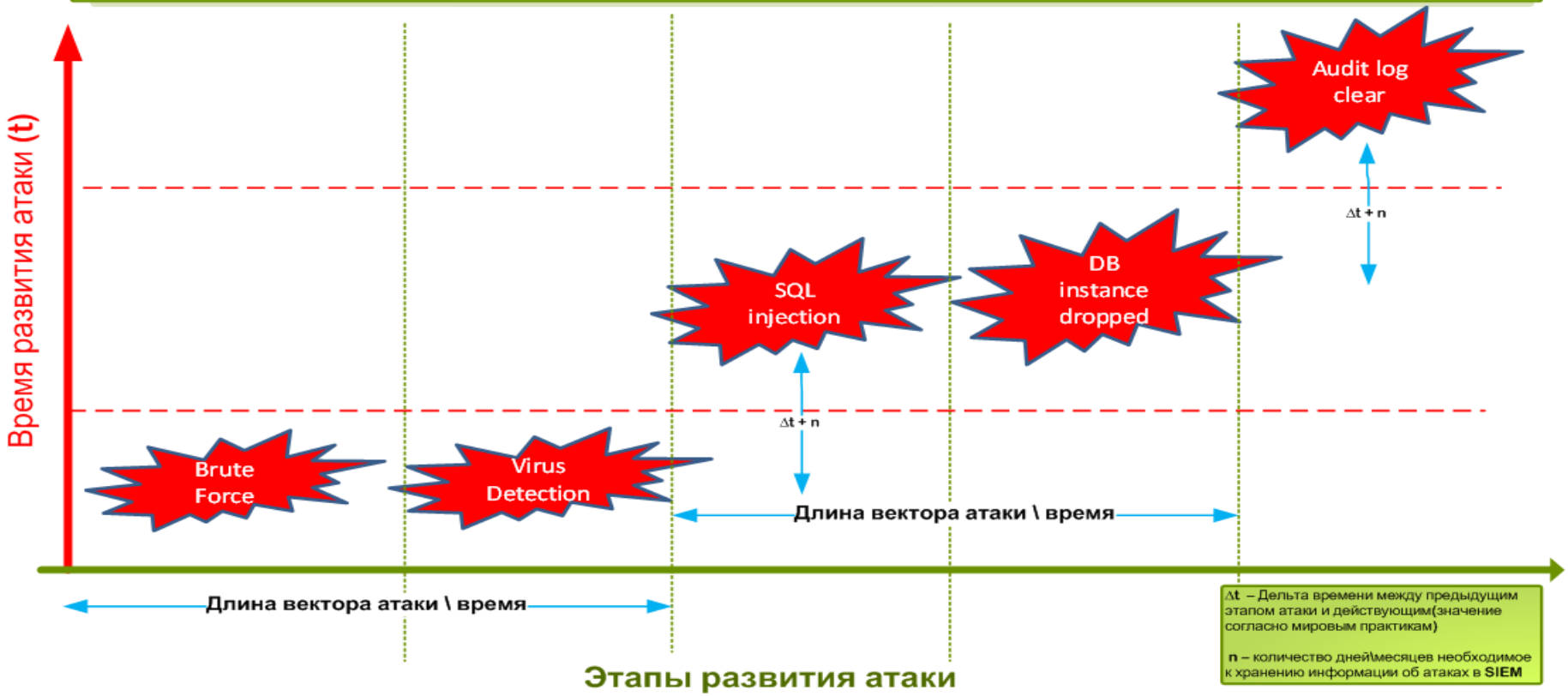


Brute Force

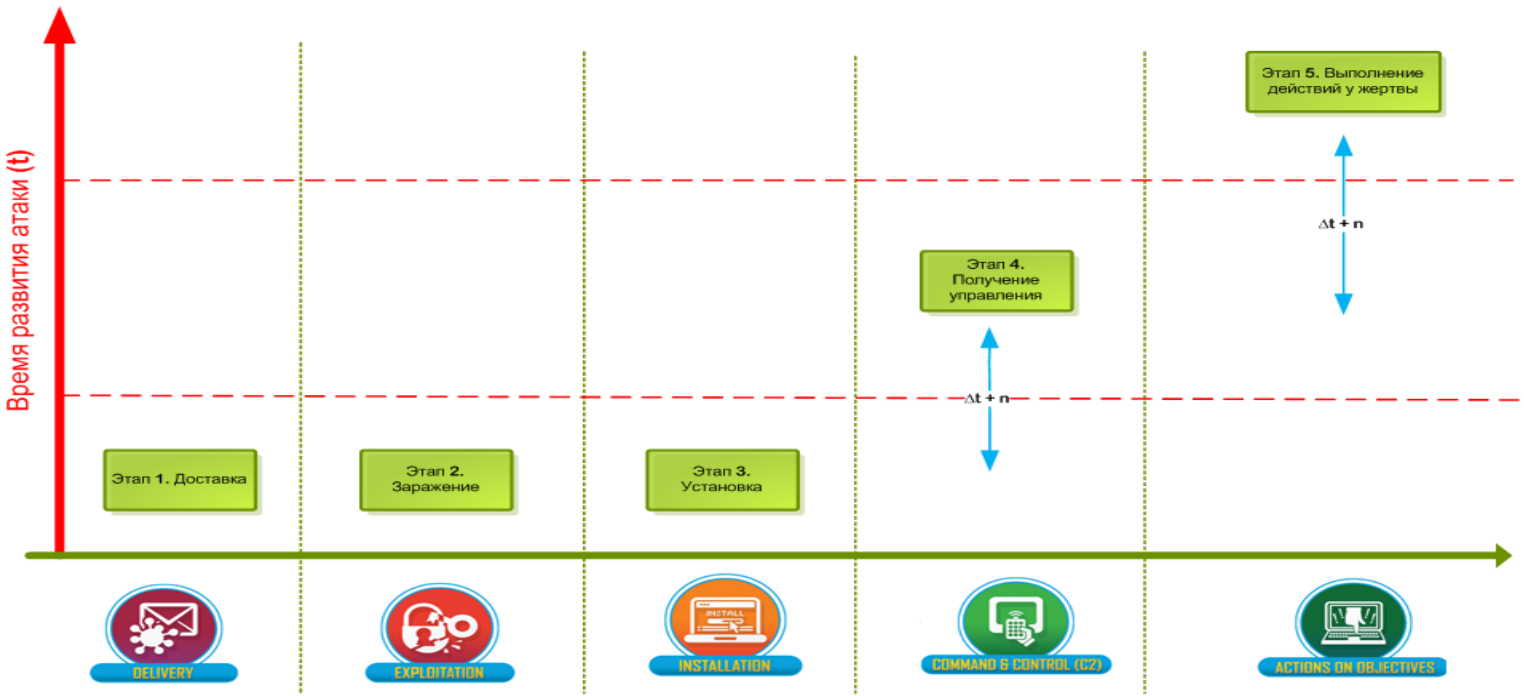
Audit log clear

Мы знаем что делать!

Практическая реализация в нашем пакете



Контроль за всеми этапами атак на стороне клиента



Этапы развития атаки

Δt – Дельта времени между предыдущим этапом атаки и действующим(значение согласно мировым практикам)

n – количество дней\месяцев необходимое к хранению информации об атаках в **SIEM**

Инвентаризация

Определение **типов источников** событий в режиме real-time

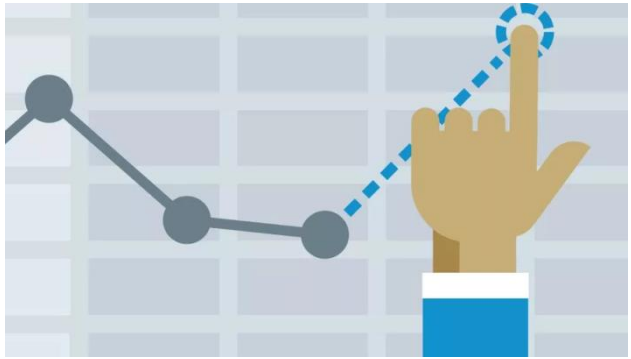
Автоматическое детектирование появления **новых источников** и их классификация

Источник достоверной информации для работы всех последующих уровней

Категоризация

Категоризация поступающих базовых событий от источников событий

Обогащение базовых событий дополнительными данными



Дополнительная обработка и обогащение

Сбор **дополнительной информации** необходимой для выявления инцидента

Работа только с категорированными событиями, поступающими с уровня **L0-Level**

Обеспечение работы по выявлению инцидентов следующих уровней

Выявление инцидентов

Выявление **инцидентов ИБ** на основе результатов работы всех предыдущих уровней
Динамическая категоризация инцидентов в соответствии с поставляемой матрицей классификации инцидентов

Выявление **таргетированных атак** на клиента

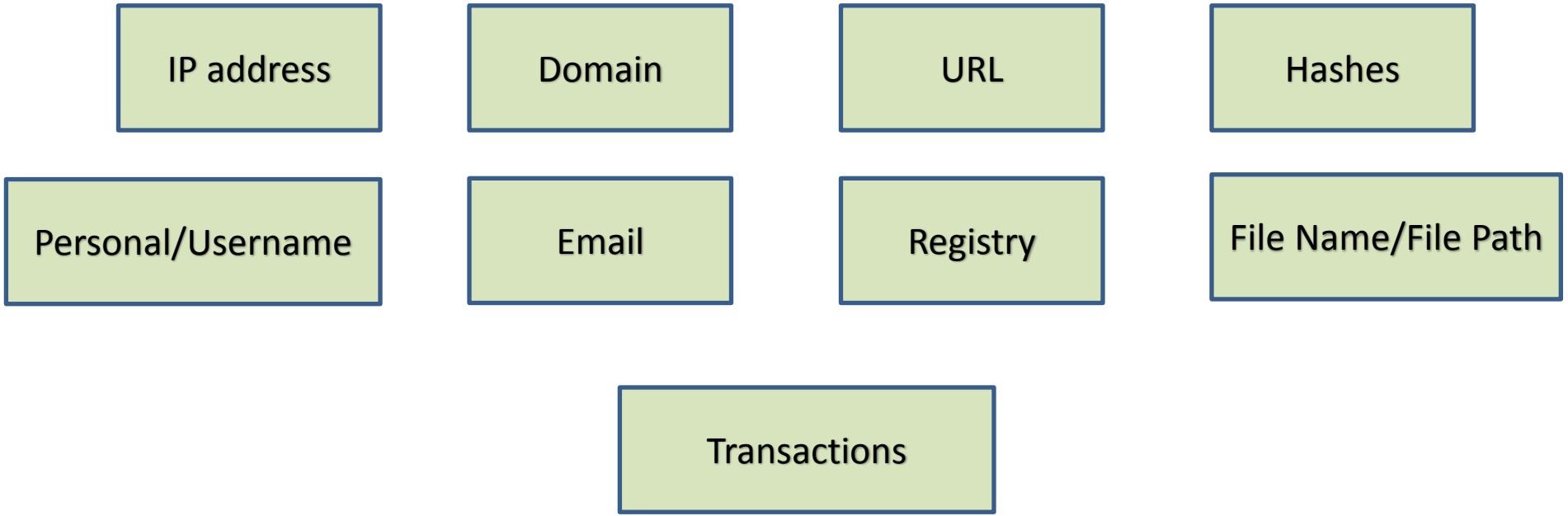
Индикаторы компрометации (IoC)

Скоринговая модель выявления инцидентов

Дашборды контроля вектора атак

Виджеты стадий и развития атаки

Indicator of Compromise (IoC)



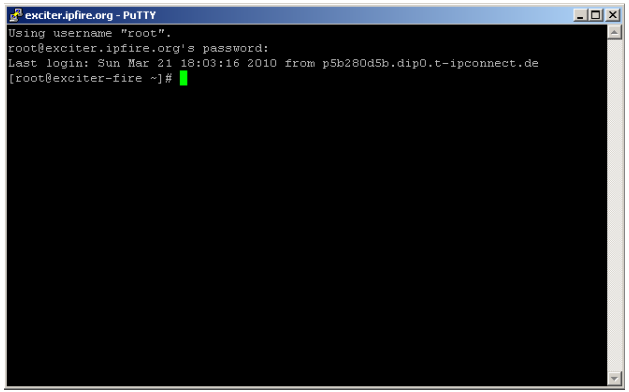
Скоринг

Total Score

John 20

192.168.1.2 80

Credential Access -> Execution 80



Brute Force

Log rate diminish

Settings changing

CISCO

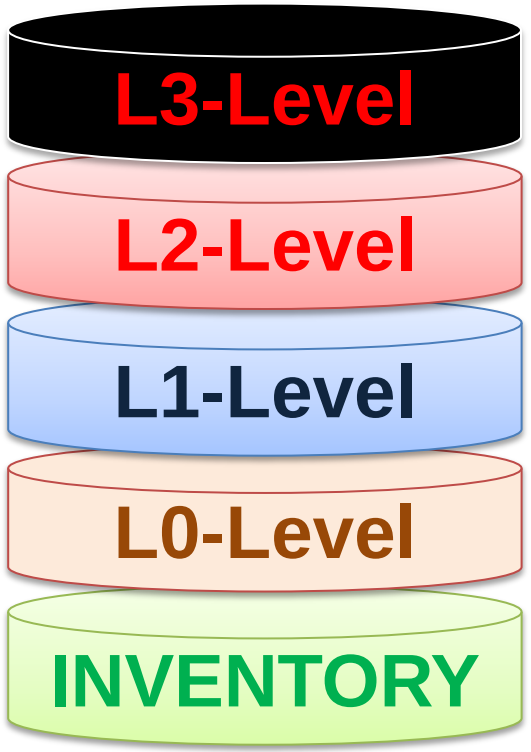
Классификация по мировым стандартам

ATT&CK Matrix for Enterprise

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture
Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection
Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data
AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged
AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories
Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System
Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive
BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media

Наш SOC пакет ЭТО

Многоуровневая система **выявления инцидентов** и **атак** с отслеживанием всех стадий
Скоринг инцидентов и «вес атаки»
Полная прозрачность работы
Возможность молниеносного изменения логики работы выявления инцидентов
Динамическая **категоризация** выявленных инцидентов
Автоматическое выявление и **инвентаризация** существующих или новых устройств и систем
Инструменты визуализации и контроля



Сложности обычного похода

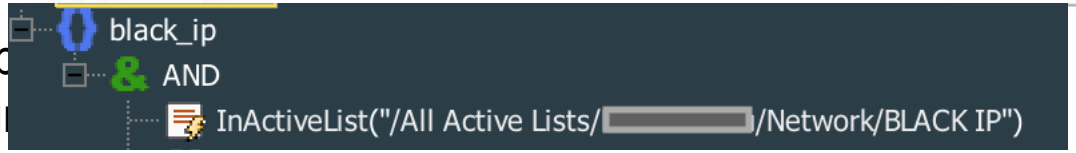
Сложные, тр нта
покинет ком

Необх
данны а)

Отсутс

Сложн

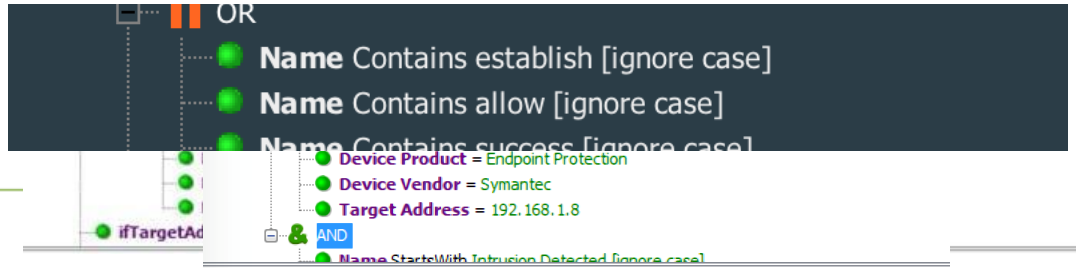
Отсутс



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

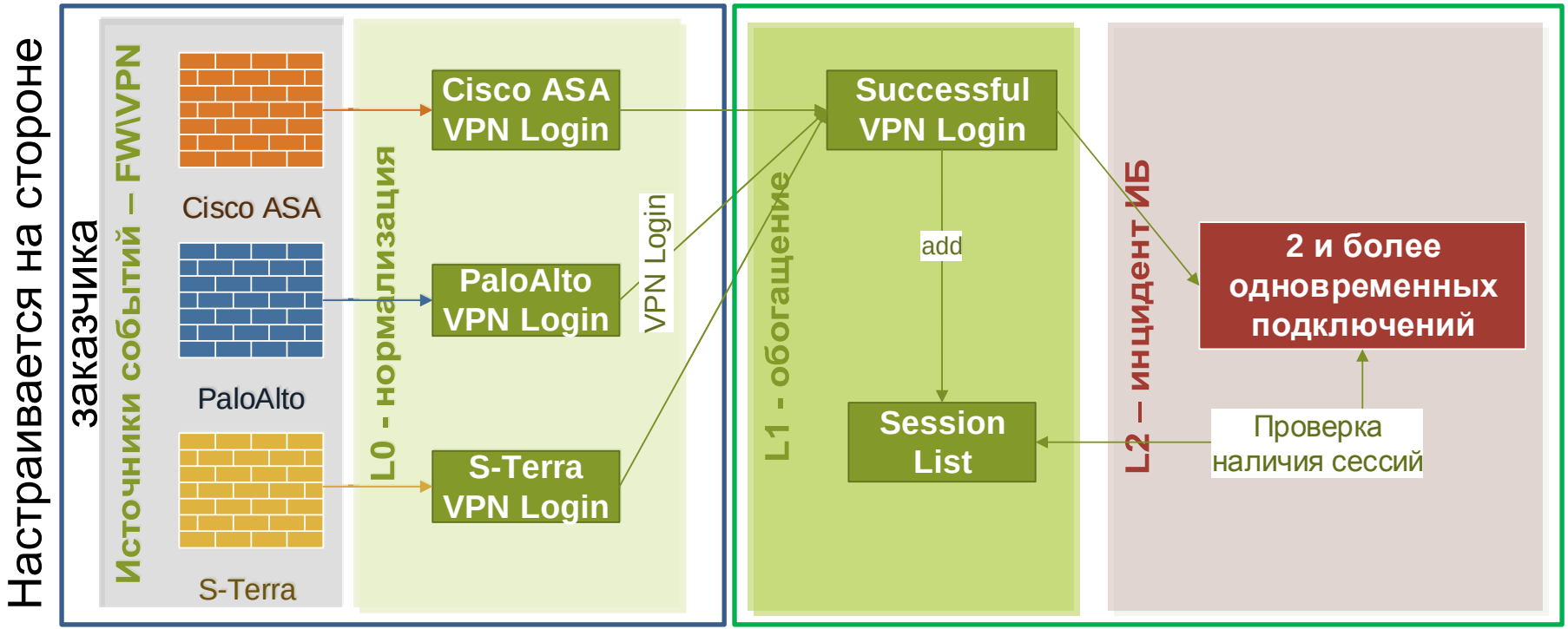
Success authenticaton[Preview]

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



Как это работает в ArcSight

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

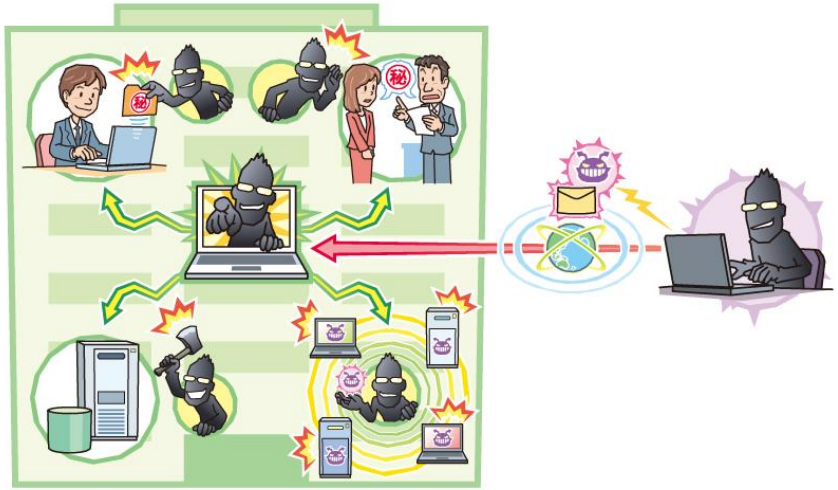


Оценка угроз в основе управления

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

Пакет правил корреляции АО «ДиалогНаука»

Пакет включает в себя набор готовых правил корреляции, отчетов и инструментов визуализации

Может поставляться вместе с стандартной и 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

Спасибо за внимание!

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

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