Защита

Сценарии

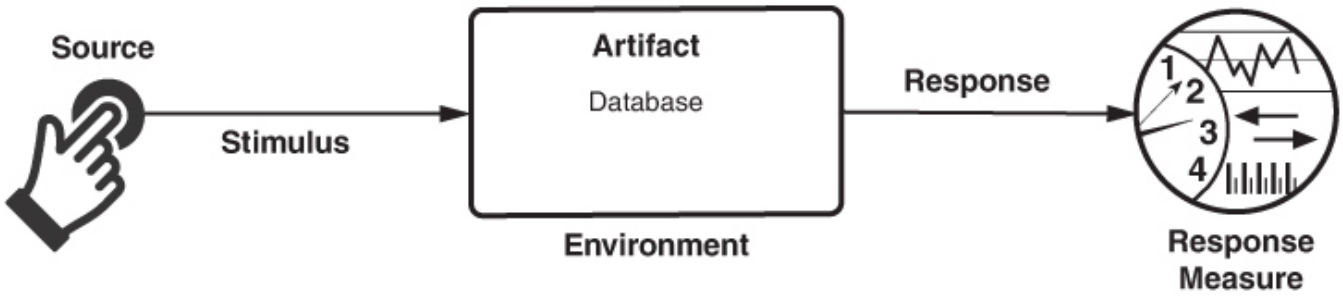
Часть сценария	Описание	Возможные значения

Источник стимула	Атака может исходить извне или изнутри организации. Источником атаки может быть как человек, так и другая система. Он мог быть ранее идентифицирован (как правильно, так и неправильно) или в настоящее время неизвестен.	• Человек
		• Другая система, которая может быть:
		  ○ Внутри организации
		  ○ Вне организации
		  ○ Ранее идентифицированна
		  ○ Неизвестно

Стимул	Стимулом является сама атака.	Несанкционированная попытка: • Отображать данные • Собирать данные • Изменять или удалять данные • Получать доступ к системным службам • Изменять поведение системы • Уменьшать доступность
Артефакт	Какова цель атаки?	• Системные службы • Данные внутри системы • Компонент или ресурсы системы • Данные, производимые или потребляемые системой
Окружение	В каком состоянии находится система в момент атаки?	Состояние системы: • В сети или офлайн • Подключена к сети или отключена от нее • Защищена брандмауэром или открыта для сети • Полностью работоспособна • Частично работоспособна • Неработоспособна

Реакция	Система обеспечивает сохранение конфиденциальности, целостности и доступности.	Транзакции выполняются таким образом, что: • Данные или услуги защищены от несанкционированного доступа • Данные или услуги не подвергаются несанкционированному манипулированию • Участники транзакции гарантированно идентифицированы • Участники транзакции не могут отказаться от своего участия • Данные, ресурсы и системные услуги будут доступны для законного использования. Система отслеживает действия внутри себя путем: • Регистрации доступа или изменения данных • Регистрации попыток доступа к данным, ресурсам или услугам; • уведомления соответствующих субъектов (людей или систем) о возникновении очевидной атаки.
Мера реакции	Показатели реакции системы связаны с частотой успешных атак, временем и затратами на отражение и устранение атак, а также с ущербом, наносимым этими атаками.	• Объем скомпрометированного или защищенного ресурса • Точность обнаружения атак • Сколько времени прошло до обнаружения атаки • Сколько атак было отражено • Сколько времени требуется для восстановления после успешной атаки • Какой объем данных уязвим для конкретной атаки

Пример



A disgruntled employee at a remote location	Attemps to improperly modify the pay rate table	Normal operations	The unauthorized access is detected and the system maintains an audit trail	Correct data is restored within one day