DAAC digital

Оценка готовности Организации

к реагированию на инциденты IT
и информационной безопасности

daacdigital.com

В момент кибернетической атаки специалисты Организации должны принимать оперативные решения, направленные на прекращение инцидента и минимизацию причинённого ущерба.

В процессе оценки готовности Организации к реагированию на инциденты IT и информационной безопасности выявляются пробелы, существующие на каждом из этапов процедуры реагирования на 3 предложенные сценария реагирования на инциденты (либо любого другого, предложенного Заказчиком), оценивается результативность распределения ролей внутри команды реагирования, наличие технических и практических возможностей для выявления и анализа артефактов, а также контроль соответствия ожидаемых параметров допустимого времени простоя и потери данных.

Оцените Вашу готовность реагировать

С помощью данной услуги Организация может проверить готовность собственных систем, команды и процессов к реагированию на инциденты IT и информационной безопасности и составить либо откорректировать план действий для мимнимизации негативного воздействия.

Вы получите ответы на следующие вопросы:.

- Как выяснить заранее, готова ли Организация отреагировать и восстановиться после инцидента в установленное бизнес процессом время?
- Как найти уязвимость и прекратить злоумышленникам доступ к системе?
- Есть ли возможность собрать информацию, необходимую для расследования?

Сценарии реагирования на инциденты

1

Атака типа Ransomeware

выявлены файлы с неизвестными расширениями на нескольких пользовательских хостах – задача предотвратить шифрование критических данных и идентифицировать источник проникновения зловредного кода.

2

Несанкционированное использование торговой марки (бренда) Организации

злоумышленниками на торговых площадках в Internet в мошеннических целях – задача остановить действия злоумышленников и минимизировать ущерб для репутации Организации.

3

Выявление чувствительных данных клиентов Организации,

опубликованных в общедоступных хранилищах – задача идентификация источников утечки информации и минимизация негативного воздействия на бизнес процессы.

Результаты оценки

ЗАКЛЮЧЕНИЕ О ПРИГОДНОСТИ

содержания планов либо концепций обеспечения непрерывности функционирования информационных систем и их аварийного восстановления для идентификации критически важных информационных активов и ожидаемых параметров допустимого времени простоя и потери данных.

ПРАКТИЧЕСКАЯ ТРЕНИРОВКА

команды реагирования на воздействие инцидентов информационной безопасности

СОЗДАНИЕ РЕКОМЕНДАЦИЙ

по корректировке содержания планов непрерывности функционирования информационных систем и их аварийного восстановления либо их разработка (при необходимости).

Ориентировочная стоимость услуги: $6700

Опционально: $3000 на разработку планов BCP & DRP (срок до 2-х месяцев)

Для более подробной информации свяжитесь с нами и мы применим все наши знания и опыт, чтобы помочь Вам повысить уровень безопасности в Вашей организации.

DAAC digital

Moldova
www.daacdigital.com
info@dsi.md

Uzbekistan
www.daacdigital.uz
info@daacdigital.uz

Romania
www.daacsystems.ro
info@daacsystems.ro