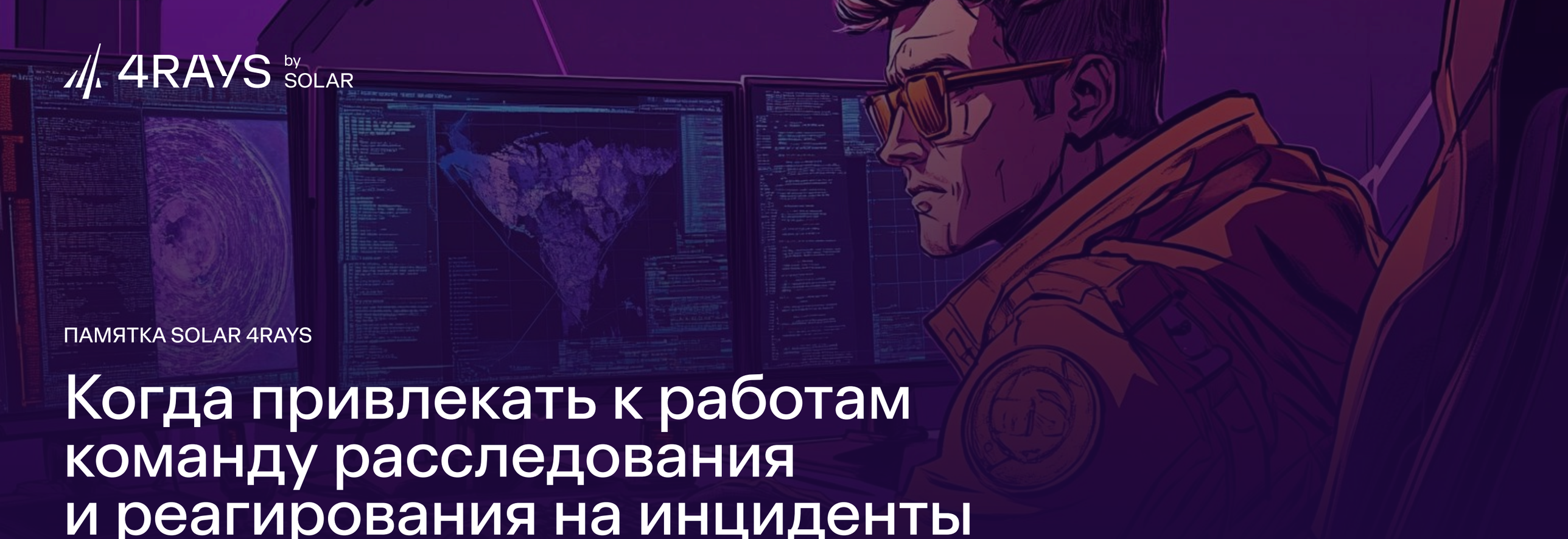
4RAYS by SOLAR



ПАМЯТКА SOLAR 4RAYS

Когда привлекать к работам команду расследования и реагирования на инциденты

СТАТУС ИНЦИДЕНТА И ЗАДАЧИ	ПРИМЕРЫ ВОЗМОЖНЫХ ПРЕДПОСЫЛОК	РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ DFIR →	ВЫЯВЛЕНИЕ СЛЕДОВ КОМПРОМЕТАЦИИ COMPROMISE ASSESSMENT →
Подозрение на инцидент Задача проверить, не скомпрометирована ли ИТ-инфраструктура сейчас или в прошлом	Появление неизвестных процессов, аномалии в сетевом трафике		✓
	Отклонения в профилях поведения пользователей и технических средств		✓
	Множественные срабатывания систем защиты информации	✓	✓
	Потеря доступа к информационным ресурсам	✓	✓
	Появление неучтенных административных записей	✓	✓
Инцидент подтвержден Локализовать инцидент и предотвратить его повторение в будущем	Заражение ВПО	✓	
	Целенаправленные атаки	✓	
	Хищение данных	✓	
	Компрометация учетных данных	✓	
	Компрометация инфраструктурных сервисов (СУБД, почта, домен)	✓	
Подозрение на инцидент Задача проверить поглощаемый актив в рамках подготовки или завершения M&A сделок	Снижение рисков наступления инцидента (уничтожения данных, шифрования инфраструктуры и т. д.)		✓

Запросить консультацию

Узнать, как команда Solar 4RAYS поможет остановить скрытую атаку или отразить активную стадию атаки

W: RT-SOLAR.RU/SOLAR-4RAYS
T: 8 (800) 302-85-23