

Мониторинг информационной безопасности и реагирования на компьютерные инциденты

ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ – РЕАЛЬНЫЕ УГРОЗЫ

Современная киберпреступность – это бизнес-индустрия с оборотом денежных средств в миллионах долларов.

Использование новейших техник в проведении компьютерных атак позволяет обходить стандартные средства защиты, получать полное управление над устройством и выполнять несанкционированные действия. Атаки совершаются с различными целями, например, получение финансовой выгоды, остановка сервисов и служб, промышленный шпионаж, кибертерроризм и др.

Для эффективного противодействия современным угрозам безопасности необходим комплексный подход, включающий в себя:

- Эффективные средства защиты информации, обеспечивающие обнаружение, предупреждение и ликвидацию последствий компьютерных атак
- Квалифицированный персонал, обладающий достаточным уровнем экспертизы для противодействия киберпреступникам
- Непрерывный мониторинг, обеспечивающий своевременное обнаружение компьютерных атак и инцидентов, оперативную локализацию атак и сдерживание их дальнейшего развития
- Всесторонний ретроспективный анализ компьютерных атак и нарушений, разработку и осуществление комплекса превентивных мер
- Получение перечня уязвимостей сетевой инфраструктуры (в том числе недостатков конфигурации) при помощи автоматизированных средств и дополнительных ручных проверок



СПЕЦИАЛИЗИРОВАННЫЙ СЕРВИС CyberART

Имея за плечами многолетний успешный опыт обеспечения информационной безопасности для широкого круга предприятий и организаций из различных отраслей экономики, команда CyberART предлагает комплексные услуги по обнаружению и предотвращению компьютерных нарушений - мониторинг информационной безопасности и реагирования на компьютерные инциденты.



Для должного уровня защиты необходим комплексный подход, включающий в себя технологии, процессы и людей. Сервисный подход CyberART решает эти задачи.

ОСНОВНЫЕ НАПРАВЛЕНИЯ УСЛУГ

- Мониторинг событий информационной безопасности, выявление подозрительных событий, регистрация инцидентов и оповещение ответственных специалистов, контроль и координация расследования компьютерных атак
- Аудит и контроль состояния защищенности информационных ресурсов и систем, позволяющий получить максимально полную картину уязвимостей сетевой инфраструктуры
- Предоставление средств обнаружения компьютерных атак, средств защиты информации и средств мониторинга как сервис (HaaS/SaaS)
- Взаимодействие с Государственной системой обнаружения и предотвращения компьютерных атак (ГосСОПКА)



СООТВЕТСТВИЕ НОРМАТИВНЫМ ТРЕБОВАНИЯМ

- Приказ ФСТЭК № 239 от 25 декабря 2017
- Положение Банка России № 382-П от 9 июня 2012;
- Стандарт безопасности данных индустрии платежных карт (PCI DSS)
- Приказ ФСТЭК № 17 от 11 февраля 2013

ПРЕИМУЩЕСТВА ОТ СОТРУДНИЧЕСТВА

- Внедрение и обслуживание систем безопасности
- Доступный экспертный сервис
- Выстраивание и контроль процессов реагирования на компьютерные угрозы
- Консультативная и непосредственная помощь в расследовании и ликвидации атак
- Аудит информационной системы и рекомендации по повышению защищенности
- Круглосуточный мониторинг событий безопасности и уведомление ответственных специалистов по удобным каналам связи

КОНТАКТЫ

Телефон: +7 (843) 567-42-90
E-mail: soc@cyberart.ru

Казань: 420015, ул. Подлужная, 60



innostage-group.ru



cyberart.ru