CROC CLOUD SERVICES

Сервис	Описание	Решения и вендоры	Уровень CSS
Мониторинг событий и инцидентов ИТ-безопасности (SIEM, log management) Управление и реагирование на инциденты (IRP/SOAR)	Централизованный сбор, нормализация, хранение журналов регистрации, корреляция событий безопасности, оповещение об обнаруженных угрозах. События поступают от типовых и нетиповых источников.	SOC MSSP K2 Кибербезопасность, Kaspersky KUMA, R-Vision, Security Vision	II
Межсетевой экран (пакетный фильтр)	Фильтрация трафика	Cloud Firewall	I, II
Защита каналов связи. Межсетевые экраны (NGFW)	Снижение уровня рисков безопасности при передаче информации между зонами безопасности	Код Безопасности Континент, Check Point, Ideco UTM, Sangfor, Infotecs ViPNet X-Firewall, UserGate, Смарт-Софт Traffic Inspector Next Generation	II
Обнаружение и предотвращение вторжений (IPS)	Предотвращение в автоматическом режиме несанкционированного доступа к корпоративным информационным системам как на границе, так и внутри сети	Детектор атак Континент, Check Point, UserGate, ViPNet IDS	II
Криптографическая защита каналов связи	Организация шифрованного канала связи между площадками (зонами доступности) предприятия	Код Безопасности Континент, С-Терра, Check Point, ViPNet	II
VPN. Пользовательский сегмент	Организация удаленного подключения сотрудников к сервисам предприятия	Код Безопасности Континент, КриптоПро NGate, С-Терра, ViPNet	II
Анализ сетевого трафика (NTA)	Обнаружение вредоносной активности на периметре и внутри сети, в том числе в зашифрованном трафике	F.A.C.C.T Threat Hunting Framework	II
Система обнаружений от комплексных целевых атак	Передовая защита от комплексных угроз и целевых атак	Athena, F.A.C.C.T Sandbox, Kaspersky Anti Targeted Attack (KATA)	II
Антивирус	Защита от вредоносного кода	Kaspersky	I, II
Защита от вредоносных программ – (X/E/M)DR решение	Комплексное решение на базе новейших технологий для защиты конечных устройств Windows/Linux и данных на них	CheckPoint Harmony, Kaspersky EDR/EDR Optimum, Group-IB XDR	II
Контентная фильтрация (Proxy Server)	Защита HTTP-, HTTPS- и FTP-трафика, проходящего через прокси-сервер	Kaspersky Web Traffic Security, UserGate UTM	II
Защита веб-приложений и API (WAF, WAAP)	Защита веб-приложений от вредоносных атак и нежелательного интернет-трафика, в том числе ботов, инъекционных атак и атак типа «отказ в обслуживании» (DoS) на уровне приложений	Вебмониторэкс, SolidWall WAF, Radware AppWall	II
Anti-DDoS	Снижение рисков DDOS-атак	Mitigator, Телеком Биржа Complete DDoS Protection, Qrator	II
Управление уязвимостями (Vulnerability management)	Оценка реального уровня защищенности ИТ-инфраструктуры, построение процесса управления уязвимостями, разработка регламентов сканирования и устранения уязвимостей	Алтэкс Софт RedCheck	II
Защита виртуализации	Защита виртуальной инфраструктуры, реализация механизмов безопасности по требованиям регуляторов	Код Безопасности vGate, Конфидент Dallas Lock ВИ	II
Идентификация и управление доступом (IDM/IAM)	Централизованное управление учетными записями и правами пользователей всех информационных систем предприятия	Avanpost, 1IDM	I, II
Многофакторная аутентификация (MFA)/SSO	Компонент системы идентификации и управления доступом, который требует от пользователей подтверждения личности с использованием как минимум двух различных факторов проверки, прежде чем предоставить им доступ к ИТ-активам предприятия	Aladdin, Avanpost, Indeed, Multifactor	II
Защита баз данных (DAM, Database Firewall)	Обеспечение безопасности СУБД и независимый аудит операций с базами данных	Гарда БД	II
Зоны безопасности	Организуются на межсетевом экране для выделения продуктивной зоны, зоны серверов с конфиденциальной информацией (в облаке)	Cloud VPC	I
Фильтрация почтового трафика	Защита от атак, распространяемых при помощи электронных сообщений	CyboNet Mail SeCure, F.A.C.C.T Atmosphere, Kaspersky Secure Mail Gateway	II
Контроль привилегированных пользователей на серверах (PAM)	Отслеживание действий удаленных и локальных пользователей корпоративной сети. Применяется для контроля за привилегированными пользователя и пользователями третьей стороны	АйТи Бастион СКДПУ, Indeed PAM, Infrascope NGR Softlab, Solar Safeinspect	II
Предотвращение утечек конфиденциальной информации (DLP)	Защита предприятия от утечек информации	InfoWatch Traffic Monitor, Zecurion DLP	II
VLAN	Мера безопасности, позволяющая делить корпоративную сеть на логические сегменты независимо от физической топологии (в облаке)	Cloud VLAN	I
Киберразведка (TI)	Информация об актуальных угрозах и группировках киберпреступников, позволяет SOC улучшить качество мониторинга	F.A.C.C.T Threat Intelligence, Kaspersky Threat Intelligence	II
Повышение осведомленности персонала (Security Awareness)	Обучение, фишинговые рассылки и тестирование по актуальным темам ИТ-безопасности	Kaspersky ASAP, Phishman	II
Защита контейнеров	Комплексное решение для защиты сред контейнеризации, единый интерфейс ко всем известным способам защиты контейнеров	Kaspersky Container Security, Luntry	II
Защищенный обмен файлами (VDR)	Создание безопасного пространства для хранения и совместной работы с документами с возможностью предоставления разных уровней доступа к ним	mFlash, MitraSoft Vaultize, Secret Cloud Enterprise	II
Усиление защищенности системы с целью снижения рисков от возможных угроз	Процесс реализуется путем более тонкой настройки ОС/ИС. Используем практики от Center for Internet Security (CIS)	Экспертиза КРОК Облачные сервисы и К2 Кибербезопасность	II
Анализ угроз (Threat Hunting)	Проактивный поиск следов взлома или функционирования вредоносных программ в обход существующих средств защиты информации	Экспертиза КРОК Облачные сервисы и К2 Кибербезопасность	II
Управление обновлениями	Помогаем тестировать и устанавливать обновления на ПО предприятия	Экспертиза КРОК Облачные сервисы и К2 Кибербезопасность	II
Политики, регламенты, процедуры (разработка документов)	Помогаем внедрять процессы ИТ-безопасности. Разрабатываем пакеты документов: от концепций развития ИТ-безопасности до процедур	Экспертиза КРОК Облачные сервисы и К2 Кибербезопасность	II

Преимущества работы с КРОК Облачные сервисы

На рынке **с 2009 года**

Персональный подход к каждому проекту

24/7
SLA 10 минут

750+
клиентов

400+
экспертов реализуют проекты любой сложности