???? ?????????????? ????????? (???????????? ????)

СОВ.0 Разработка политики предотвращения вторжений (компьютерных атак)

Для реализации данной меры разрабатываются внутренние нормативные документы.

СОВ.1 Обнаружение и предотвращение компьютерных атак

KICS for Nodes

Мера реализуется в части проверки входящего сетевого трафика на узле на предмет действий, характерных для сетевых атак, с помощью задачи «Защита от сетевых угроз».

KICS for Linux Nodes

Мера реализуется в части проверки входящего сетевого трафика на узле на предмет действий, характерных для сетевых атак, с помощью задачи «Защита от сетевых угроз».

Мера реализуется в части проверки входящего сетевого трафика, передаваемого по протоколам HTTP, HTTPS и FTP, веб-сайтов и IP-адресов с целью предотвращения загрузки вредоносных файлов из Интернета, а также блокирования доступа к фишинговым, рекламным и прочим опасным веб-сайтам с помощью компонента «Защита от веб-угроз».

KICS for Networks

Мера реализуется в части обнаружения вторжений с использованием встроенных и пользовательских правил обнаружения вторжений.

Также применяются следующие дополнительные методы для обнаружения вторжений:

- обнаружения признаков подмены адресов в ARP-пакетах (ARP-спуфинг);
- обнаружения аномалий в протоколе TCP;
- обнаружения аномалий в протоколе IP;
- Обнаружение атак подбора и сканирования.

СОВ.2 Обновление базы разрешающих правил

KICS for Nodes

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

KICS for Linux Nodes

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

KICS for Networks

Мера реализуется в части получения обновлений собственных баз и программных модулей KICS for Nodes от серверов АО «Лаборатория Касперского», серверов Kaspersky Security Center или через утилиту Kaspersky Update Utility.

Kaspersky Security Center

Мера реализуется в части:

- централизованного автоматизированного обновления баз и модулей программного обеспечения АО «Лаборатория Касперского»;
- централизованного автоматизированного поиска обновлений программ сторонних производителей; при этом любые сторонние обновления программного обеспечения, которые вы устанавливаете с помощью Системного администрирования, автоматически проверяются на наличие вредоносных программ с помощью технологий АО «Лаборатория Касперского». Эти технологии используются для автоматической проверки файлов и включают антивирусную проверку, статический анализ, динамический анализ, поведенческий анализ "песочницы" и машинное обучение

Revision #2
Created 29 December 2025 19:04:06 by Olga Sinotova
Updated 29 December 2025 20:36:25 by Olga Sinotova