Kaspersky ICS EDR

> Данная статья является информационной и описывает решение Kaspersky ICS EDR

??? ????? EDR?

Технология EDR или Endpoint Detection and Response - это технология кибербезопасности, которая предназначена для мониторинга активности на устройствах (рабочие станции, сервера и тд), выявления подозрительных действий и быстрого реагирования на потенциальные инциденты.

??? ????? Kaspersky ICS EDR?

Kaspersky ICS EDR (Industrial CyberSecurity Endpoint Detection and Response) - это решение, предназначенное для защиты промышленных объектов и АСУ ТП. В отличии от обычного EDR, который используется в IT сегменте, ICS EDR используется только в OT сегменте и позволяет защищать важные компоненты промышленных предприятий от кибеугроз. Kaspersky ICS EDR является дополнением к решение Kaspersky Industrial CyberSecurity.

?????????????? ??????????? Kaspersky ICS EDR

Функции	**KICS for Nodes 4.5**		**KICS for Linux Nodes 2.0**	
	EDR	**без EDR**	**EDR**	**без EDR**
YARA-проверка	+	-	N/A	N/A
KSC: Сетевая изоляция узла	+	-	N/A	N/A
KSC: Запретить запуск	+	-	N/A	N/A
KSC: Обнаружение аномалий с помощью Sigma-правил	+	-	N/A	N/A
KSC: Поиск IOC	+	-	+	-
KSC: Завершить процесс	+	-	+	-
KSC: Запустить процесс	+	-	+	-

KSC: Поместить файл на карантин	+	-	+	-
KSC: Удалить файл	+	-	+	-
KSC: Получить файл	+	-	+	-
KSC: Аудит безопасности	+	+	N/A	N/A
Интеграция с KICS for Networks: передача сведений об узле	+	+	+	+
Интеграция с KICS for Networks: аудит безопасности, анализ уязвимостей, контроль конфигурации	+	+	+	+
Интеграция с KICS for Networks: передача событий	+	+	+	+
Интеграция с KICS for Networks: передача сетевых сессий	+	+	+	+
Интеграция с KICS for Networks: передача графа атаки на узле	+	-	+	-
Реагирование из KICS for Networks: изоляция узла	+	-	+	-
Реагирование из KICS for Networks: запрет запуска	+	-	+	-
Реагирование из KICS for Networks: поместить на карантин	+	-	+	-
Реагирование из KICS for Networks: удалить файл	N/A	N/A	+	-

Функции	KICS for Nodes 4.0		KICS for Linux Nodes 1.5	
	EDR	без EDR	EDR	без EDR

YARA-проверка	+	-	N/A	N/A
KSC: Сетевая изоляция узла	+	-	N/A	N/A
KSC: Запретить запуск	+	-	N/A	N/A
KSC: Обнаружение аномалий с помощью Sigma-правил	+	-	N/A	N/A
KSC: Поиск IOC	+	-	N/A	N/A
KSC: Завершить процесс	+	-	+	-
KSC: Запустить процесс	+	-	+	-
KSC: Поместить файл на карантин	+	+	-	-
KSC: Удалить файл	+	-	+	-
KSC: Получить файл	N/A	N/A	+	-
KSC: Аудит безопасности	+	+	N/A	N/A
Интеграция с KICS for Networks: передача сведений об узле	+	+	+	+
Интеграция с KICS for Networks: аудит безопасности, анализ уязвимостей, контроль конфигурации	+	+	+	+
Интеграция с KICS for Networks: передача событий	+	+	+	+
Интеграция с KICS for Networks: передача сетевых сессий	+	-	+	+
Интеграция с KICS for Networks: передача графа атаки на узле	+	-	N/A	N/A
Реагирование из KICS for Networks: изоляция узла	+	-	N/A	N/A
Реагирование из KICS for Networks: запрет запуска	+	-	N/A	N/A

Реагирование из KICS for Networks: поместить на карантин	+	-	N/A	N/A
Реагирование из KICS for Networks: удалить файл	N/A	N/A	N/A	N/A

Revision #5
Created 26 December 2025 11:44:44 by Alexander Somonov
Updated 6 April 2026 13:01:49 by Alexander Somonov