Nozomi Networks вызвалась разместить первый сервер ETHOS для бета-тестирования и уже разработала возможности интеграции для обмена данными между машинами.

ETHOS (Emerging THreat Open Sharing)
ETHOS предназначен для обмена информацией в режиме реального времени для разработки механизмов раннего предупреждения для расследования аномального поведения в широком диапазоне сред операционных технологий (OT) и промышленных систем управления (ICS), а не для обмена данными после оповещения об известных обнаружениях и сигнатурах вредоносного ПО.
ETHOS автоматизирует частотный анализ новых угроз и действий и позволяет быстрее реагировать на новые тактики, методы и процедуры по мере их появления.
Преимущества включают сокращение сроков уточнения данных для выявления и классификации новых угроз и предотвращение более серьезных путей атаки из-за успешного использования.
Созданный для среды OT, любой субъект или поставщик средств безопасности может внести свой вклад в проект и разместить свой собственный сервер для:

- Сравнения общей информации
- Предоставления анонимных данные
- Получения уведомлений о корреляциях.

Nozomi Networks вызвалась разместить первый сервер ETHOS для бета-тестирования и уже разработала возможности интеграции для обмена данными между машинами.
В будущем любая компания или государственное учреждение сможет самостоятельно разместить сервер ETHOS, используя проект с открытым исходным кодом.

Хост может разрешить выбранным участникам и клиентам подключаться и обмениваться информацией.
Чтобы участвовать в сервере ETHOS и получать уведомления, организация также должна иметь клиент ETHOS, созданный с возможностями интеграции для отправки данных.
Каждый сервер ETHOS будет выполнять корреляцию данных, совместно используемых участвующими клиентами, или встроенным инструментом мониторинга и обнаружения.
Каждому клиенту будет предоставлен уникальный идентификатор для сервера, и аутентификация будет проходить без идентификации каких-либо данных клиента поставщика.
Уведомление о том, что нужно расследовать, будет отправлено непосредственно конечным пользователям, где ответственность за более глубокий анализ и расследование на основе уведомлений ETHOS лежит на клиентах, которые выбрали получение сводных и коррелированных уведомлений с сервера.

Необходимость активного обмена информацией С точки зрения правительства США, руководящие документы в настоящее время находятся на пути к обновлению для сбора OT/ICS.
Несколько агентств рассматривают новые способы обеспечения обмена информацией и создания предупреждений в секторах и между ними, когда они могут стать мишенью или иметь недавно обнаруженные уязвимости в своих системах.
Однако ни один источник информации не может информировать всю отрасль. В случае широкого распространения ETHOS может служить надежным сторонним средством для раннего предупреждения о надвигающихся атаках на объекты критической инфраструктуры на основе множества объектов, работающих независимо и анонимно обменивающихся информацией.

Участились киберинциденты с использованием как ИТ-, так и OT-специфических векторов и вредоносных программ, как финансово мотивированных, так и направленных на физическое разрушение.
Детерминированный, специально созданный характер киберфизических систем и операций до сих пор гарантировал, что нет двух одинаковых атак на OT/ICS, а это означает, что обнаружение, созданное в ответ на известные атаки, никогда не может быть достаточным для предотвращения новых атак.
Инициатива CISA Shields Up имеет свой собственный фон геополитической напряженности в то время, когда кибер-возможности и государственное управление вызывают споры и оспариваются.
Эта динамика создала реальность, в которой инфраструктура кажется не укомплектованной, оборона часто реакционна.
Сообщество ETHOS создало необходимую основу для стороннего, независимого от поставщика, обмена анонимной информацией в режиме реального времени для любого количества соответствующих субъектов критической инфраструктуры и заинтересованных сторон.