# Kaspersky ICS Threat Intelligence Reporting

kaspersky АКТИВИРУЙ БУДУЩЕЕ

# Отчеты об угрозах для АСУ ТП

**В рамках отчетов об угрозах для АСУ ТП** «Лаборатория Касперского» предоставляет подробные аналитические данные о вредоносных кампаниях, нацеленных на промышленные организации, и об уязвимостях, обнаруженных в наиболее популярных АСУ ТП и их технологиях. Поскольку отчеты размещаются на интернет-портале, достаточно зарегистрироваться в сервисе, чтобы получить к ним доступ.

## Что входит в сервис?

**Отчеты об APT-атаках.** Отчеты о новых APT-атаках и масштабных кампаниях против промышленных организаций и обновленные данные об активных угрозах.

**Обнаруженные уязвимости.** Отчеты об уязвимостях, обнаруженных «Лабораторией Касперского» в наиболее популярных продуктах для АСУ ТП, промышленном интернете вещей и IT-инфраструктуре различных отраслей.

**Ландшафт угроз.** Отчеты о значительных изменениях в ландшафте угроз для АСУ ТП и новых критических факторах, которые влияют на уровень безопасности и уязвимости таких систем, с разделением по регионам, странам и отраслям.

**Анализ и минимизация уязвимостей.** Эксперты «Лаборатории Касперского» дают практические рекомендации по выявлению и минимизации уязвимостей в инфраструктуре предприятия.

## Данные анализа угроз позволяют

### Выявлять и предотвращать

угрозы для критически важных устройств, включая программное и аппаратное обеспечение, чтобы обеспечить безопасность и непрерывность производственного процесса.

### Сопоставлять

вредоносную и подозрительную активность, обнаруженную в промышленной среде, с результатами исследований «Лаборатории Касперского», чтобы связать эту активность с вредоносными кампаниями, определить угрозы и оперативно отреагировать на них.

### Оценивать

уязвимости производственной среды и устройств на основе точных сведений о масштабах и серьезности обнаруженных проблем и принимать обоснованные решения по установке исправлений и другим рекомендованным профилактическим мерам.

### Использовать

Информацию о тактиках, техниках и процедурах атак, недавно обнаруженных уязвимостях и других важных изменениях ландшафта угроз, чтобы:

- выявлять и оценивать риски, связанные с обнаруженными угрозами и их аналогами;
- планировать и внедрять изменения в производственную инфраструктуру для обеспечения безопасности и непрерывности производственного процесса;
- повышать осведомленность сотрудников о киберугрозах, разрабатывая тренинги с участием red team и blue team на основе анализа реальных случаев;
- принимать обоснованные стратегические решения об инвестициях в кибербезопасность и прочих мерах, повышающих защищенность процессов.

# Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave™: External Threat Intelligence Services, Q1 2021)

**«Лаборатория Касперского» предлагает сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.**

**Наша компания обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT. Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах.**

Kaspersky Threat Intelligence

Подробнее

**www.kaspersky.ru**