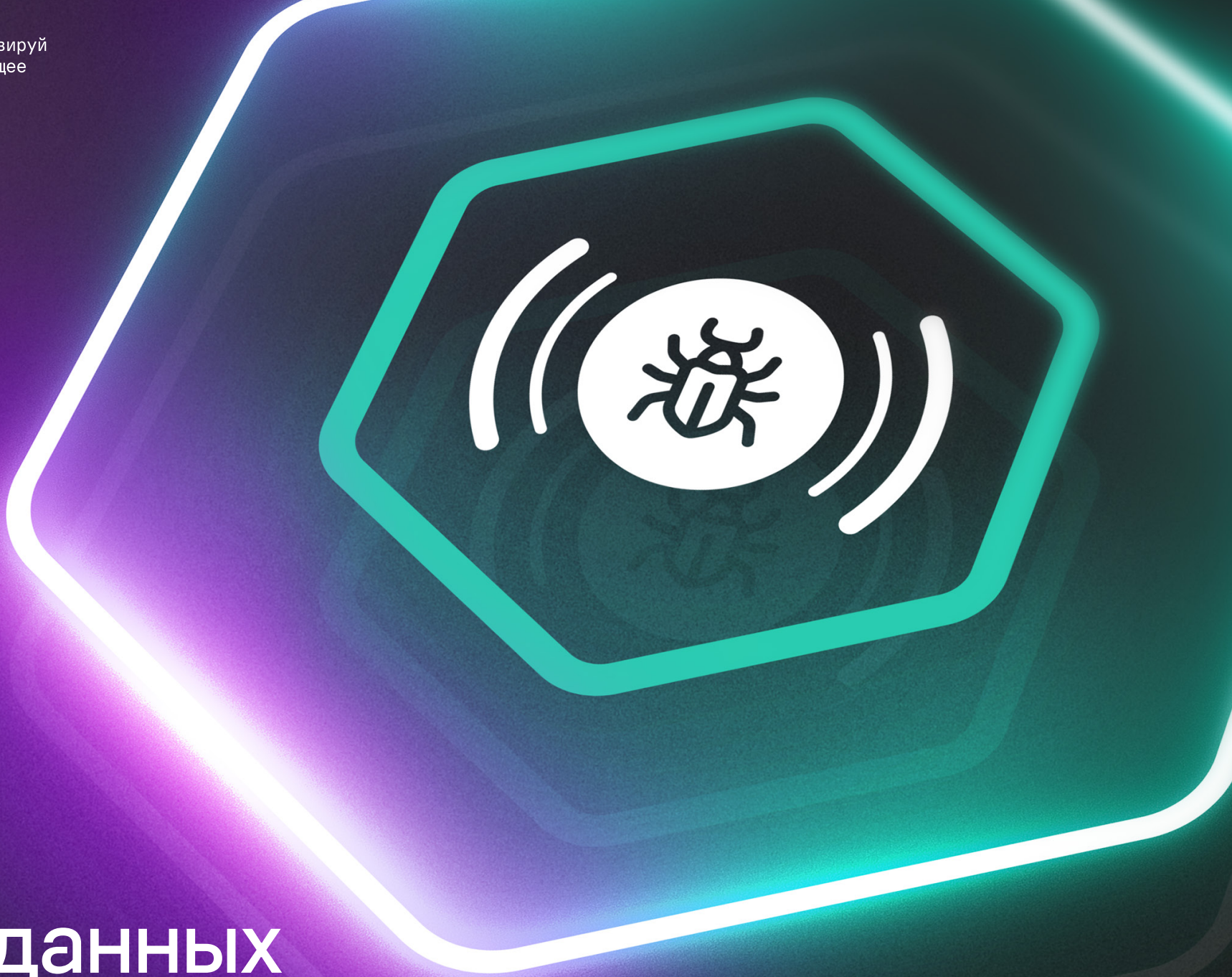
kaspersky активируй будущее



Kaspersky
Threat Intelligence

Потоки данных об угрозах

Введение

Что содержится в потоках

Записи в потоках, предоставляемых «Лабораторией Касперского», содержат контекстные данные, которые позволяют быстро подтвердить и приоритизировать угрозы:

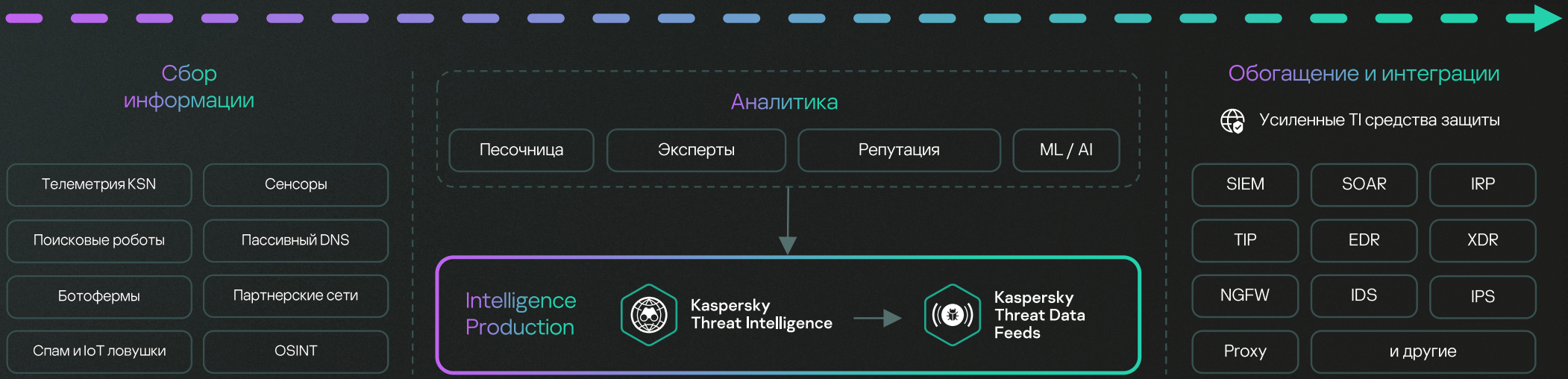
- Имена угроз
- Установленные IP-адреса и доменные имена вредоносных веб-ресурсов
- Хеши вредоносных файлов
- Идентификаторы уязвимых и скомпрометированных объектов
- Тактики, техники и процедуры атак в соответствии с классификацией MITRE ATT&CK
- Метки времени
- Географическое положение
- Популярность и прочее

Потоки данных об угрозах — это сервис «Лаборатории Касперского», предоставляющий компаниям информацию об угрозах для защиты их инфраструктуры. В рамках данного решения предоставляется информация об известных вредоносных программах, фишинговых веб-сайтах, последних уязвимостях и эксплойтах, а также других типах киберугроз. Эта информация может использоваться организациями для блокировки вредоносного трафика, обновления своих средств обеспечения безопасности и принятия других мер защиты от кибератак.

Данные собираются из множества разнообразных надежных источников, включающих Kaspersky Security Network, и наши собственные поисковые роботы, сервис мониторинга ботнет-угроз (круглосуточное слежение за ботнетами, их целями и активностями), ловушки для спама, данные исследовательских групп и партнеров.

Вся собранная информация тщательно проверяется и очищается в режиме реального времени при помощи различных методов предварительной обработки: с применением сетевых песочниц, средств статистического и эвристического анализа, инструментов для определения сходств, профилирования моделей поведения и проверки аналитиками.

Потоки данных об угрозах помогают составить общее представление о событии или провести дополнительные проверки по нему. Также они помогают найти ответы на вопросы «Кто? Что? Где? Когда?» и выявить источники атак для принятия своевременных решений и защитить компанию от угроз любой сложности.



Как можно использовать потоки данных

Перечень потоков данных «Лаборатории Касперского» непрерывно расширяется

Название потока	Предотвращение	Обнаружение	Расследование
Malicious URL Data Feed	•	•	•
Ransomware URL Data Feed	•	•	•
Phishing URL Data Feed	•	•	•
Botnet C&C URL Data Feed	•	•	•
Mobile Botnet C&C URL Data Feed	•	•	•
Malicious Hash Data Feed	•	•	•
Mobile Malicious Hash Data Feed	•	•	•
IP Reputation Data Feed	•	•	•
IoT URL Data Feed	•	•	•
Vulnerability Data Feed	•	•	•
ICS Vulnerability Data Feed	•	•	•
ICS Vulnerability Data Feed в формате OVAL		•	
ICS Hash Data Feed	•	•	•
pDNS Data Feed			•

Название потока	Предотвращение	Обнаружение	Расследование
Suricata Rules Data Feed		•	
Cloud Access Security Broker (CASB) Data Feed		•	
APT Hash Data Feed		•	•
APT IP Data Feed		•	•
APT URL Data Feed		•	•
APT Yara Data Feed		•	•
Open Source Software Threats Data Feed	•	•	•
Crimeware Hash Data Feed		•	•
Crimeware URL Data Feed			•
Crimeware Yara Data Feed			•
Sigma Rules Data Feed	•		
Network Security IP Data Feed	•	•	
Network Security URL Data Feed	•	•	
Network Security Web Filtering Data Feed	•	•	

Описание данных об угрозах от «Лаборатории Касперского»

Коммерческие потоки

Коммерческие потоки предоставляют доступ к наиболее полным коллекциям информации, доступной в рамках сервиса. Обновление информации происходит на постоянной основе. В зависимости от типа потока регулярность может варьироваться от нескольких минут до нескольких часов.

Название потока	Описание потока	Тип индикатора	Сценарии использования потока
Malicious URL Data Feed	Веб-ресурсы, с которых распространяется вредоносное программное обеспечение	Маска	• Системы управления ИБ предполагают возможность обогащения внешними источниками информации. Подключение данных потоков к SIEM / SOAR / IRP позволяет своевременно реагировать на актуальные угрозы, создавать дополнительный контекст при расследовании инцидента. • Интеграция с системами сетевой и почтовой безопасности (например, NGFW / IDS / IPS / Mail / Web Security) позволяет предотвращать киберинциденты, дополняя нативную базу индикаторов компрометации данными об актуальных угрозах.
Ransomware URL Data Feed	Веб-ресурсы, с которых распространяются программы-вымогатели		
Phishing URL Data Feed	Фишинговые веб-ресурсы		
Botnet C&C URL Data Feed	C&C серверы ботнетов и связанные с ними вредоносные объекты (боты)		
Mobile Botnet C&C URL Data Feed	C&C серверы мобильных ботнетов с связанные с ними вредоносные объекты (боты)		

#Предотвращение

#Обнаружение

#Расследование

Название потока	Описание потока	Тип индикатора	Сценарии использования потока	
Malicious Hash Data Feed	Хэши распространенных вредоносных файлов	Hash	• Интеграция с инфраструктурными системами безопасности (Endpoint Security, Server Security) для предотвращения загрузки и запуска вредоносного ПО, а также детектирования уже запущенного вредоносного ПО. • Интеграция с системами класса SIEM / SOAR / IRP позволяет своевременно реагировать на актуальные угрозы, создавать дополнительный контекст при расследовании инцидента.	#Предотвращение #Обнаружение #Расследование
Mobile Malicious Hash Data Feed	Хэши распространенных вредоносных файлов для мобильных операционных систем (Android и iOS)			
IP Reputation Data Feed	Различные категории подозрительных и вредоносных IP-адресов	IP	• Интеграция с системами сетевой и почтовой безопасности (NGFW / IDS / IPS / Mail / Web Security) позволяет предотвращать киберинциденты, дополняя нативную базу индикаторов компрометации данными об актуальных угрозах. • Интеграция с системами класса SIEM / SOAR / IRP позволяет своевременно реагировать на актуальные угрозы, создавать дополнительный контекст при расследовании инцидента.	#Предотвращение #Обнаружение #Расследование
IoT URL Data Feed	Веб-ресурсы, с которых распространяется вредоносное программное обеспечение для IoT-устройств (IP-камер, RFID датчиков, умных ценников и освещения и пр.)	Маска		
Vulnerability Data Feed	Уязвимости корпоративного программного обеспечения	CVE	• Выявление уязвимых элементов инфраструктуры через интеграцию со сканерами уязвимостей и Asset Management-системами. • Интеграция с Endpoint Protection системами, с целью предотвращения запуска ПО с критичными уязвимостями. • Детектирование запуска уязвимого ПО. • Помощь при проведении расследований. • Предоставление рекомендаций по закрытию уязвимостей.	#Предотвращение #Обнаружение #Расследование
ICS Vulnerability Data Feed	Уязвимости программного и аппаратного обеспечения АСУ ТП, а также корпоративного программного обеспечения, используемого в инфраструктуре управления технологическим процессом			

Название потока	Описание потока	Тип индикатора	Сценарии использования потока	
ICS Vulnerability Data Feed в формате OVAL	Правила для автоматизированного поиска уязвимостей программного обеспечения АСУ ТП	OVAL check	• Обогащение популярных сканеров уязвимостей программного обеспечения с целью обнаружения уязвимого программного обеспечения АСУ ТП.	#Обнаружение
ICS Hash Data Feed	Распространенные вредоносные файлы, представляющие угрозу для АСУ ТП	Hash	• На периметре OT-сетей аналогично сценариям использования Malicious Hash Data Feed. • Внутри OT-сетей для детектирования потенциально опасных файлов.	#Предотвращение #Обнаружение #Расследование
pDNS Data Feed	Записи, содержащие результаты DNS преобразований для доменов в соответствующие IP-адреса за период времени	IP, FQDN	• Интеграция с системами сетевой и почтовой безопасности (NGFW / IDS / IPS / Mail / Web Security) позволяет предотвращать киберинциденты, дополняя нативную базу индикаторов компрометации данными об актуальных угрозах. • Интеграция с системами класса SIEM / SOAR / IRP позволяет своевременно реагировать на актуальные угрозы, создавать дополнительный контекст при расследовании инцидента.	#Расследование
Suricata Rules Data Feed	Правила обнаружения различных категорий угроз в сетевом трафике, таких как APT, Botnet C&C, Ransomware и др.	Suricata-правило	• Интеграции в системы класса NGFW / IDS / IPS / NTA / NDR для обогащения правил детектирования вредоносной активности.	#Обнаружение
Cloud Access Security Broker (CASB) Data Feed	Домены и хосты, относящиеся к популярным облачным сервисам	Маска	• Построение CASB решения, в частности, для настройки политик доступа к облачным сервисам.	#Обнаружение

Название потока	Описание потока	Тип индикатора	Сценарии использования потока	
APT Hash Data Feed	Хэши файлов, используемых участниками APT группировок для проведения целевых атак	Hash	• Интеграция с инфраструктурными системами безопасности (Endpoint / Server Security) для предотвращения загрузки и запуска вредоносного ПО, а также детектирования уже запущенного вредоносного ПО. • Интеграция с системами сетевой и почтовой безопасности (NGFW / IDS / IPS / Mail / Web Security) позволяет предотвращать киберинциденты, дополняя нативную базу индикаторов компрометации данными об актуальных угрозах. • Интеграция с системами класса SIEM / SOAR / IRP позволяетсоздавать дополнительный контекст при расследовании инцидента, а также своевременно реагировать на актуальные угрозы, связанные с проведением целевых атак или имеющие отношение к участникам APT-группировок.	#Обнаружение #Расследование
APT IP Data Feed	Сведения об элементах инфраструктуры, имеющих отношение к проведению целевых атак	IP		
APT URL Data Feed		Маска		
APT Yara Data Feed	YARA-правила для идентификации файлов, используемых в целевых атаках	YARA-правило	• Проактивный поиск признаков целевых атак в организации за счёт интеграции с инфраструктурыми системами безопасности (Endpoint / Server Security) • Полезен при расследовании киберинцидентов.	#Обнаружение #Расследование
Open Source Software Threats Data Feed	Программные пакеты с открытым исходным кодом (open source), содержащие уязвимости, вредоносную функциональность либо политически мотивированную компрометацию функциональности (блокировку в определенных регионах, политические лозунги и тд.)	Имя и версия пакета	• Предназначен для компонентного анализа разрабатываемого программного обеспечения в рамках процесса безопасной разработки (DevSecOps) с целью защиты программного продукта от атак на цепочку поставок (supply chain attack), раннего обнаружения и устранения уязвимостей, а также предотвращения использования пакетов, содержащих политически ориентированные недекларированные возможности (НДВ).	#Предотвращение #Обнаружение #Расследование

Название потока	Описание потока	Тип индикатора	Сценарии использования потока	
Crimeware Hash Data Feed	Хэши файлов, используемых в мошеннических кампаниях, описанных в Crimeware отчетах «Лаборатории Касперского»	Hash	• Интеграция с инфраструктурными системами безопасности (Endpoint / Server Security) для предотвращения загрузки и запуска вредоносного ПО, а также детектирования уже запущенного вредоносного ПО. • Интеграция с системами сетевой и почтовой безопасности (NGFW / IDS / IPS / Mail / Web Security) позволяет предотвращать киберинциденты, дополняя нативную базу индикаторов компрометации данными об актуальных угрозах. • Интеграция с системами класса SIEM / SOAR / IRP позволяетсоздавать дополнительный контекст при расследовании инцидента, а также своевременно реагировать на актуальные угрозы, связанные с мошенническими действиями злоумышленников.	#Обнаружение #Расследование
Crimeware URL Data Feed	Сведения об элементах инфраструктуры, имеющие отношение к мошенническим кампаниях, описанным в Crimeware-отчетах «Лаборатории Касперского»	Маска		
Crimeware Yara Data Feed	Правила YARA для идентификации файлов, используемых в мошеннических кампаниях, описаны в Crimeware отчетах «Лаборатории Касперского»	YARA-правило	• Активно ищет признаки мошеннических кампаний в инфраструктуре организации. • Полезно при расследовании киберинцидентов.	#Расследование
Sigma Rules Data Feed	Правила в формате YAML для обнаружения вредоносных действий в журналах безопасности	SIGMA-правило	• Интеграция с SIEM/EDR решениями для обнаружения вредоносных действий в журналах безопасности	#Обнаружение
Network Security IP Data Feed	Перечень IP-адресов для обновления списков оповещения/блокировки NGFW	IP	• Интеграция с системами контроля сетевой безопасности (NGFW) для повышения уровня их защиты	#Обнаружение #Предотвращение

Название потока	Описание потока	Тип индикатора	Сценарии использования потока	
Network Security URL Data Feed	Перечень URL-адресов для обновления списков оповещения / блокировки NGFW	URL	• Интеграция с системами контроля сетевой безопасности (NGFW) для повышения уровня их защиты	#Обнаружение #Предотвращение
Network Security Web Filtering Data Feed	Перечень категоризированных доменов для обновления списков оповещения / блокировки NGFW	URL	• Интеграция с системами контроля сетевой безопасности (NGFW) для повышения уровня их защиты	#Обнаружение #Предотвращение

Демонстрационные потоки

Демонстрационные потоки предназначены для ознакомления. Данные содержат ограниченные выборки с существенно сокращённым количеством информации и более редкими обновлениями. Структура потоков похожа на формат коммерческих, но в некоторых случаях может отличаться.

- Demo IP Reputation Data Feed
- Demo Botnet C&C URL Data Feed
- Demo Malicious Hash Data Feed
- Demo APT IP Data Feed
- Demo APT URL Data Feed
- Demo Sigma Rules Data Feed
- Demo APT Hash Data Feed
- Demo Suricata Rules Data Feed
- Demo Suricata Rules Data Feed
- Demo ICS Vulnerability Data Feed
- Demo ICS Vulnerability Data Feed в формате OVAL
- Demo Crimeware Hash Data Feed
- Demo Crimeware URL Data Feed

Запросить потоки

Kaspersky Threat Intelligence

Подробнее

Подробная информация об угрозах

Потоки данных об угрозах от «Лаборатории Касперского» расширяют возможности существующих элементов управления безопасностью, включая системы SIEM, системы обнаружения вторжений, прокси-серверы безопасности и т. д. Благодаря достоверным данным, содержащим контекст, процессы предотвращения, обнаружения и расследования инцидентов информационной безопасности будут более эффективными и быстрыми.

www.kaspersky.ru