ПЯТЬ ОШИБОК АНАЛИТИКИ БЕЗОПАСНОСТИ И КАК ИХ ИЗБЕЖАТЬ

VARONIS

СОДЕРЖАНИЕ

> Организациям зачастую не удается выявить утечку данных на ранних этапах, при этом в целом утечки данных раскрываются менее чем в 20% случаев [1].

Gartner

VARONIS

ВВЕДЕНИЕ

Многие организации рассматривают вопрос внедрения аналитики безопасности, чтобы расширить возможности обнаружения угроз.

Накопив некоторые данные аналитики безопасности и журналов, аналитики информационной безопасности отправляют журналы на центральный сервер для анализа, полагая, что для обнаружения угрозы этого достаточно. Конечно, данные журналов необходимы, однако для их правильной интерпретации требуется более глубокая проработка, чем принято считать.

Ниже мы расскажем о пяти ошибках, которые совершают организации в попытке *превентивного* анализа журналов и расследования инцидентов безопасности.

1. Большой объем данных журналов. В большинстве организаций регистрируют сотни миллионов событий в день. Сетевые устройства, конечные точки, системы безопасности, приложения, устройства хранения, прокси-серверы — все регистрируют события в огромном количестве. При этом журналы разных типов устройств и от разных поставщиков могут быть организованы каждый по-своему.

2. Данные журналов нельзя использовать в исходном виде. Чтобы использовать журналы, необходимо их проанализировать или распознать описываемые в них объекты. Вот пользователь, вот устройство, а это событие входа в систему и т. д. Без должного анализа журналов невозможно связать объекты одного журнала с объектами другого, а ведь именно это требуется как для расследования уже случившихся инцидентов, так и для превентивной аналитики. Это более сложная задача, поскольку не существует единого стандарта журнала (они все отличаются), но проанализировать нужно каждый. Кроме того, в некоторых журналах для описания одного «события» используется несколько строк, и они не всегда идут по порядку. Такие журналы лучше обрабатывать с помощью систем автоматизации аналитики с участием человека.

3. Адекватного анализа журналов недостаточно, требуется контекст. Специалистам по аналитике безопасности необходимо расставить приоритеты и исследовать записи журналов с предупреждениями. Кто этот пользователь и чем он занимается? Это его рабочая станция? В каком офисе находится пользователь? Специалисты по аналитике безопасности тратят немало времени на отслеживание такой информации, чтобы определить, является ли то или иное событие угрозой безопасности и какова его природа.

4. Отдельные события не значимы без контекста. Без контекста не отслеживается связь с предшествующими событиями и событиями разных систем, в то время как инциденты безопасности могут длиться в течение недель, месяцев и даже дольше. Без контекста непонятна роль пользователя, поступает ли запрос с его обычной рабочей станции, из привычного местоположения, являются ли данные запроса конфиденциальными, есть ли что-то необычное в этом событии. Специалисты по аналитике просматривают тысячи событий, чтобы ответить на эти вопросы. Так они накапливают достаточный контекст для понимания каждого инцидента и подготовки ответных действий.

5. Зачастую расследование инцидентов заходит в тупик, когда дело доходит до критически важного вопроса: *«Находятся ли данные в безопасности?»* Это важно, потому что обращения к данным зачастую не регистрируются, не собирается по ним статистика, не анализируются. Например, во многих организациях не собирают и не хранят какую-либо информацию о том, как пользователи взаимодействуют с файлами и электронными письмами, а ведь это распространенные пути утечки данных.

Описанные ошибки помогают объяснить, почему исходные данные журналов представляют относительно мало значимых оповещений, а их изучение требует опыта, навыков и времени. Из настоящего документа вы узнаете о том, как избежать ошибок при работе с аналитикой безопасности, сократить количество ложных результатов, ускорить расследование и быстрее предотвращать атаки.

> Система управления информацией о безопасности и событиями безопасности (SIEM) — это не просто накопление и хранение данных всех журналов со всех устройств и приложений без разбора. Однако существует распространенное и ошибочное представление, что накопленные данные легко обработать, как только они загружены в SIEM. Предсказуемый итог такого подхода — данные для тренировки системы по удалению «шума» фактически усиливают и приумножают его. Иголка в стоге сена не найдется быстрее оттого, что сена станет больше.[1]

Gartner

VARONIS

ИНТЕЛЛЕКТУАЛЬНЫЙ СБОР ДАННЫХ

Подготовка журнала часто заканчивается простой регистрацией событий устройств в системном журнале на сервере. Однако в журналах регистрируется большое количество «шума», а для описания одного «события» может использоваться несколько строк.

Такие строки не всегда хранятся в правильном порядке, и не каждая из них несет полезную с точки зрения безопасности информацию. Иногда регистрация ведется в нескольких файлах журнала, которые впоследствии приходится объединять. Задачу усложняет наличие разных устройств с разными форматами журналов, которые могут отличаться даже у разных версий одного устройства. В зависимости от поставщика устройства в журнале регистрируются различные данные и используются разные форматы имен пользователей, хостов, доменов.

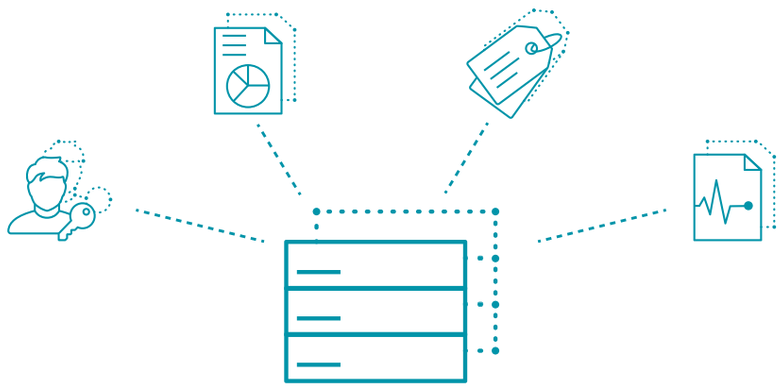
Например, начало удаленного сеанса VPN будет зарегистрировано в форме 10–20 отдельных событий журнала, которые зачастую сохраняются не по порядку, так как в системе одновременно работает сразу несколько пользователей.

Вот как выглядят исходные данные журнала одного подключения VPN от одного поставщика VPN:

```
Dec  6 13:07:52 127.0.0.1  2017-12-06T11:08:09Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:09 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Key Exchange number 1 occurred for user with NCIP 172.16.248.93

Dec  6 13:07:52 127.0.0.1  2017-12-06T11:08:09Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:09 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: User with IP 172.16.248.93 connected with ESP tran
sport mode.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Starting dsagentd session.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: User with IP 172.16.248.93 connected with SSL tran
sport mode.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - VPN Tunneling: Session started for user with IPv4 address 172.16.
248.93, hostname OSHEZAF-LT

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[Varonis-User, PM] - Agent login succeeded for oshezaf/VaronisCertificate from 84.229.
120.164 with Pulse-Secure/8.3.3.1021 (Windows 10) Pulse/5.3.3.1021.

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[] - Host Checker realm restrictions successfully passed for oshezaf/VaronisCertificat
e , with certificate 'CN=Ofer Shezaf, OU=Herzliya, OU=IL, OU=Users, OU=Varonis, DC=varonis, DC=com'

Dec  6 13:07:48 127.0.0.1  2017-12-06T11:08:05Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:05 - ive - [84.229.12
0.164] oshezaf(VaronisCertificate)[] - Primary authentication successful for oshezaf/CertificateServer from 84.229.120.1
64

Dec  6 13:07:46 127.0.0.1  2017-12-06T11:08:03Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:03 - ive - [84.229.12
0.164] oshezaf()[] - Host Checker policy 'Varonis' passed on host '84.229.120.164' address 'a4-34-d9-ec-4d-66'  for user
 'oshezaf'.

Dec  6 13:07:46 127.0.0.1  2017-12-06T11:08:03Z  vpn-isr.varonis.com PulseSecure: 2017-12-06 11:08:03 - ive - [84.229.12
0.164] oshezaf()[] - Host Checker policy 'Domain' passed on host '84.229.120.164' address 'a4-34-d9-ec-4d-66'  for user
 'oshezaf'.
```

Исходные данные постепенно копятся в системном журнале на сервере и начинают занимать все больше дискового пространства. Для операций с ними потребуются большие вычислительные мощности, и в конечном счете эти данные не принесут вам ожидаемой пользы. Журналы подключений VPN имеют немалый размер, а журналы DNS и Proxy и того больше.

Эффективнее и выгоднее обработать, обрезать лишнее и провести предварительный анализ, особенно если журналы в конечном итоге передаются на обработку в сервис с оплатой по мегабайтам. Решения Security Analytics позволяют обрезать необработанные журналы в момент сбора данных, потенциально сокращая объем данных на 70–80%. После предварительной обработки и сортировки записей (вход пользователя в систему, подключение хоста и т. д.) журналы можно отправлять на центральный сервер для быстрого анализа. Интеллектуальное средство сбора данных анализирует, сокращает и объединяет исходные данные событий, способно выполнять базовую аналитику и создавать предупреждения в момент сбора данных. Например, оно может создать оповещения при попытке пользователя подключиться по VPN в режиме, приближенном к реальному времени, еще до того, как будет выполнена проверка и анализ необработанных данных журналов на центральном сервере.



> “Во время исследования большинство поставщиков SIEM-систем сообщили Gartner, что их клиенты в основной массе (около 85 %) не используют современные технологии обнаружения угроз или аналитики данных [2].

Gartner

VARONIS

ОБОГАЩЕНИЕ ДАННЫХ И АНАЛИТИКА

Предположим, вы настроили интеллектуальный сбор данных, обрезали и проанализировали данные и привели журналы в лучшую форму. На этом этапе у вас на руках куда более совершенный инструмент для расследования по сравнению с методом прочесывания исходных данных журналов вручную. Однако для того, чтобы получить осмысленные выводы о превентивных мерах с помощью аналитики, вам еще предстоит проделать определенную работу. Для эффективного анализа требуется контекст — информация о пользователях, системах и обращении с данными.

В качестве пользователя может выступать руководитель с открытым доступом к конфиденциальным данным, администратор с доступом к ключевой инфраструктуре или недавно уволившийся сотрудник. Системой может быть критически важный сервер, рабочая станция или тестовая система. Некоторые файлы могут содержать личную информацию или важные IP-адреса. А другие файлы — это просто фотографии котиков.

Без контекста крайне трудно определить разницу между чем-то важным и чем-то бессмысленным. Если пользователь без прав администратора использует инструменты администратора, например анализатор (и создает при этом множество DNS-запросов), вероятно, следует немедленно заблокировать его учетную запись и рабочую станцию. Если тот же анализатор (с огромным набором DNS-запросов) использует известный системе администратор, в ответ можно отправить электронное письмо или позвонить для уточнения обстоятельств. Массовая загрузка данных из необычного местоположения будет иметь важное значение, если пользователь или рабочая станция недавно обращались к личным данным или критическим IP-адресам. А если обращения были к личным фотографиям пользователя, это не так важно.

События для эффективной обработки не только должны быть обогащены контекстом, но и сам контекст необходимо дополнять и уточнять с течением времени. Пользователи получают доступ к различным наборам данных в разных системах с разных рабочих станций в разные часы из разных мест. Именно для этой задачи действительно эффективно использовать машинное обучение — создание и поддержание базовых показателей нормального поведения пользователей при обращении с системами и данными.

И последнее замечание по аналитике безопасности: она работает хорошо, только если накоплено достаточно актуальных данных или метаданных для анализа. Если данные для вас — это актив, о безопасности которого вы заботитесь больше всего, необходимо понять, действительно ли у кого-то был доступ к вашим данным. Если вы храните критически важные данные в файловых и почтовых системах, следует обратить внимание на активность файловой и почтовой систем. Без этого вы не сможете ответить на самый важный вопрос безопасности: «Находятся ли данные в безопасности?»

К сожалению, исходные данные журналов в отношении файлов и электронной почты часто недоступны. А если и доступны, то хранятся в необработанном виде и занимают много места (например, телеметрия защиты внешнего периметра). Если для вас безопасность данных действительно важна, то огромным преимуществом станет применение технологии, которая ориентирована на работу с данными и предоставляет контекст об их использовании и конфиденциальности во всех хранилищах данных.

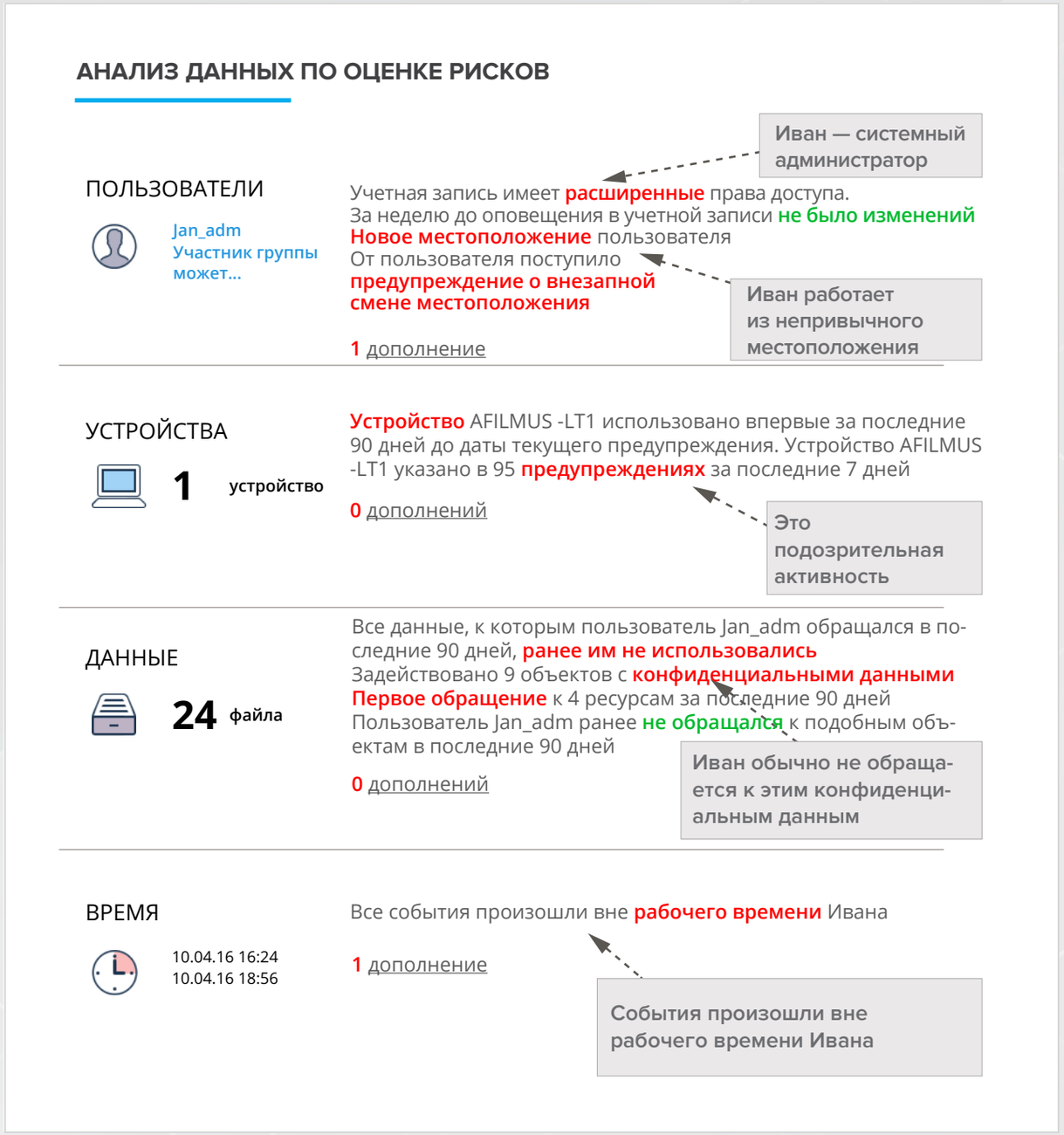
РЕАГИРОВАНИЕ

Специалисты по аналитике безопасности в своей работе постоянно сталкиваются с оповещениями: на рабочей станции обнаружено вредоносное ПО, заблокирована учетная запись, совершен успешный вход с Южного полюса. При этом исходные необработанные события создают больше оповещений, а для расследования каждого из них требуется гораздо больше времени. Чтобы удостовериться в необходимости ответных действий, специалистам по аналитике приходится сопоставлять события вручную: это сложный, трудоемкий процесс.

Предположим, аналитик получает следующее предупреждение от системы обнаружения вредоносных программ: «обнаружен вредоносный файл по адресу: 10.10.150.12.». Первым делом нужно идентифицировать рабочую станцию, связаться с ее владельцем и проверить, действительно ли она была заражена вредоносным ПО. Если это так, то следует сделать запрос в журнал прокси-сервера, чтобы выявить источник вредоносного ПО, проверить подключения к необычным местоположениям и (или) события загрузки крупных файлов. Если описанное соответствует действительности, то беспокойство об утечке конфиденциальных данных начинает вызывать неприятные ощущения в животе, а расследование затянуться.

Аналитика безопасности значительно ускоряет описанный процесс. Специалисты по аналитике просматривают меньше оповещений с действительно значимой информацией, их легче анализировать, особенно учитывая, что все связи и контекст события доступны в одном месте..

Чтобы определить график расследования и масштаб инцидента, аналитикам необходима информация об учетной записи пользователя, устройстве, данных и времени создания предупреждения. Аналитика безопасности показывает, обращался ли пользователь к сети из своего обычного местоположения, имеет ли учетная запись расширенные права доступа, имел ли место доступ к конфиденциальным данным и произошло ли это событие в рамках привычного для пользователя рабочего времени. Такой контекст помогает определить, представляет ли оповещение реальную угрозу или это лишь незначительная аномалия.



Event Time	Event Type	SAM Accou	Event Statu	Blacklisted.	Country	Connection Type	Upload Siz.	Download .	Session Du	IP Address	External IP Addr.
12/05/2017 4:15 PM	VPN login request		✔			Unkonwn					192.168.200.89
12/05/2017 4:15 PM	VPN login request		✔			Tunneling				172.16.212.150	192.168.200.89
12/05/2017 4:18 PM	VPN logout request		✔			Tunneling	265349	41638	158	172.16.212.150	192.168.200.89
12/07/2017 9:48 AM	VPN login request	dpnini	✔	–	Israel	AccessApplica...					89.139.198.93
12/07/2017 10:02 AM	VPN logout request	dpnini	✔	–	Israel	Unkonwn					89.139.198.93

Если специалист по безопасности, используя этот контекст, решит предпринять дальнейшие действия, он получит доступ к исходным данным событий, связанным с инцидентом.

ЗАКЛЮЧЕНИЕ

Аналитика безопасности сочетает в себе интеллектуальный сбор правильных метаданных, интеллектуальный анализ и обогащение данных средствами машинного обучения. Она позволяет сократить количество оповещений и время расследования. С меньшим количеством более значимых оповещений у специалистов по аналитике гораздо больше шансов быстрее отследить реальные угрозы, ведь в вопросах безопасности данных важна каждая секунда.

Если пользователь из списка наблюдения загружает конфиденциальные данные на веб-сайт сразу после получения доступа к нему в нерабочее время, он попадет на верхнюю строчку списка подозреваемых вместе с администратором, который читает электронные письма генерального директора и по VPN-подключению помечает их как непрочитанные. Если учетная запись, пользователь которой обычно работает в вашей базе данных, внезапно получит доступ к данным пациента, это вызовет подозрение. А если пользователь, как обычно, обновляет десятки файлов в конце месяца в стандартные рабочие часы со своей рабочей станции, никаких оповещений не последует, потому что это рядовая операция.

Независимо от того, хотите вы объединить журналы или вы можете попробовать решение по аналитике безопасности. Увеличивая ваши шансы на обнаружение важных угроз безопасности, решение для аналитики безопасности ускорит расследование инцидентов, сократит расходы на обработку данных и дисковое пространство (и связанные расходы на электропитание), а также облегчит выполнение нормативных требований.

О КОМПАНИИ VARONIS

Varonis — пионер в области защиты данных и аналитики. Компания применяет нестандартные методы обеспечения информационной безопасности. Varonis специализируется на защите корпоративных данных, хранящихся локально и в облаке. Это файлы с конфиденциальными сведениями, электронные письма, конфиденциальные данные клиентов, пациентов и сотрудников, финансовая информация, планы стратегического развития и разработки продуктов, интеллектуальная собственность.

Платформа кибербезопасности Varonis обнаруживает внутренние угрозы и кибератаки, анализируя данные, действия учетной записи и поведение пользователей, и эффективно поддерживает инфраструктуру в защищенном состоянии с помощью средств автоматизации.

Делая акцент на безопасности данных, решения Varonis подходят для множества вариантов использования, включая классификацию данных, соответствие стандартам, классификацию и аналитику угроз. Компания Varonis ведет свою деятельность с 2005 года, и по состоянию на 2020 год нашими клиентами являются более 7000 компаний по всему миру. Это отраслевые лидеры во многих областях, включая технологии, потребительские товары, розничную торговлю, финансовые услуги, здравоохранение, производство, энергетику, средства массовой информации и образование.

Онлайн-демонстрация

Настройте Varonis в своей системе. Быстро и без проблем.

info.varonis.com/demo/ru

Оценка рисков кибербезопасности данных

Получите обзор вашей системы безопасности данных, сократите количество потенциальных рисков и исправьте реальные проблемы безопасности.

https://info.varonis.com/risk-assessment/ru

[1] Gartner, «Использование системы SIEM для целевого обнаружения атак», Оливер Рочфорд и Келли М. Кавана, 12 марта 2014 г.
[2] Gartner, «Выход летнего обновления системы SIEM, 2017 г.», Антон Чувакин, 11 июля 2017 г.

О СИСТЕМЕ DATALERT

DatAlert автоматически анализирует информацию платформы кибербезопасности Varonis (Data Security Platform) для обнаружения, предупреждения и реагирования на угрозы почти в реальном времени. С помощью DatAlert вы можете получать уведомления об инцидентах, требующих срочного внимания. Например, если какой-то пользователь использует или шифрует большое количество конфиденциальных файлов, читает электронную почту руководителя или в непривычное время вносит изменения в групповую политику.

ПОДРОБНЕЕ

“ Varonis —
просто фантастическое решение

Gartner
peerinsights™

VARONIS

О СИСТЕМЕ VARONIS EDGE

Varonis Edge анализирует устройства периметра безопасности, такие как DNS-, VPN- и прокси-серверы, сопоставляя события периметра для обнаружения вредоносных программ, целенаправленного вторжения и переноса файлов. Системы DatAlert и Edge обнаруживают подозрительную активность и предотвращают утечку данных на разных платформах, позволяют визуализировать риски и определять приоритеты расследования.

ПОДРОБНЕЕ

Тысячи ведущих предприятий мира доверяют Varonis управление защитой данных.

VARONIS