

**Выявление
инцидентов ИБ
с помощью SIEM:
типичные
и нестандартные
задачи**

2020

Содержание

Об исследовании	3
Как начать выявлять инциденты ИБ с помощью SIEM-системы	4
Задачи для SIEM-системы: типичные и нестандартные	4
Источники для сбора событий	6
Выявленные инциденты ИБ	8
Предполагаемая атака	9
Обнаружение вредоносного ПО	11
Аномальное поведение пользователей	12
Нарушение политик ИБ	13
Заключение	14

Об исследовании

В инфраструктуре компаний происходит много событий, которые могут свидетельствовать о различных инцидентах информационной безопасности, таких как нарушение политик пользователями или проникновение злоумышленника в локальную сеть. Для централизованного сбора и анализа информации о событиях используют решения класса security information and event management (SIEM). Основная задача SIEM-системы — не просто собрать информацию о событиях с различных источников — сетевых устройств, приложений, журналов ОС, средств защиты, — но и автоматизировать процесс обнаружения инцидентов, а также своевременно информировать о них специалистов по безопасности. Пилотный проект позволяет продемонстрировать работу SIEM-системы в условиях, приближенных к условиям реальной корпоративной инфраструктуры. После таких проектов мы получаем много ценной информации от экспертов, поработавших с системой, и эта обратная связь позволяет совершенствовать продукт.

В этой статье мы расскажем о результатах 23 пилотных проектов по внедрению системы MaxPatrol SIEM, проведенных во второй половине 2019 — начале 2020 года¹, и на их примере покажем, как информация из различных источников при использовании SIEM-системы позволяет выявлять инциденты ИБ в компании. Кроме того, расскажем о решении нетипичных задач с помощью SIEM-системы.

124 дня средняя длительность пилотного проекта

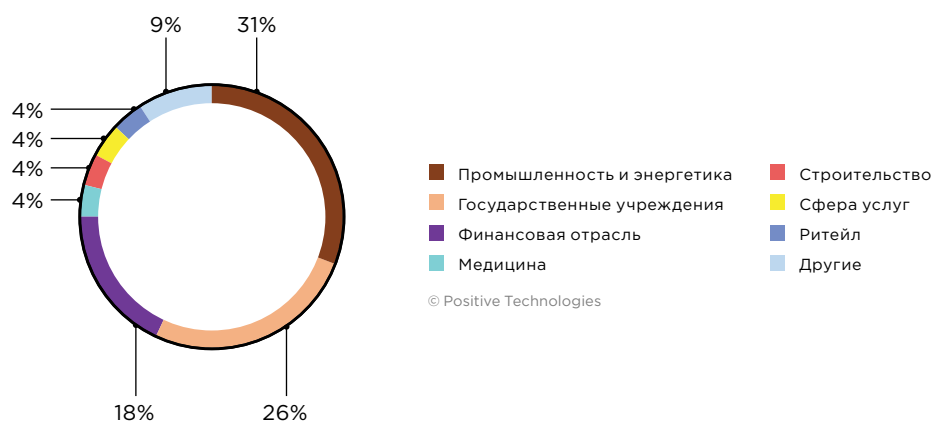


Рисунок 1. Портрет участников исследования

1. В выборку вошли пилотные проекты по внедрению системы мониторинга и корреляции событий MaxPatrol SIEM, в которых объем инфраструктуры, выделенной для проведения пилотных работ, и обрабатываемых данных был достаточен для фиксации реальных инцидентов. Из исследования были исключены компании, которые не дали своего согласия на использование обезличенных результатов пилотного проекта в исследовательских целях.

Как начать выявлять инциденты ИБ с помощью SIEM-системы

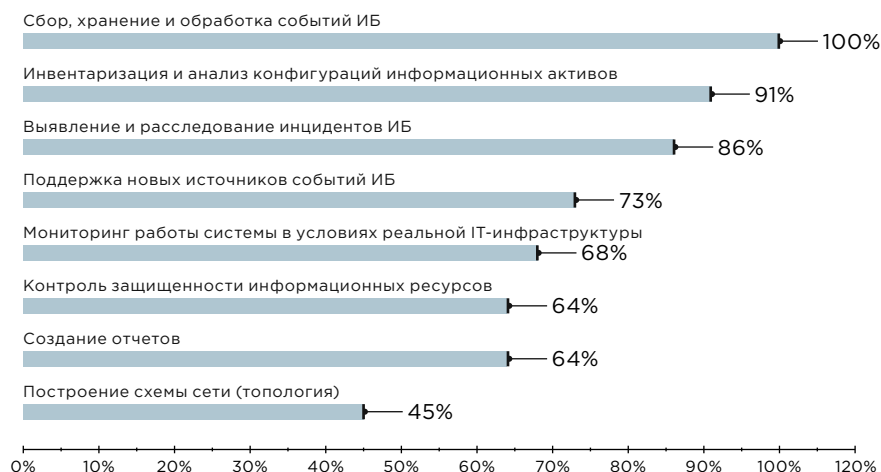
Для того чтобы начать выявлять инциденты ИБ в инфраструктуре компании с помощью SIEM-системы, необходимо сначала тщательно подготовиться:

1. Сформулировать задачи, которые вы планируете решать с помощью SIEM-системы. Следует учитывать особенности инфраструктуры, положения корпоративной политики ИБ, а также требования и рекомендации регулирующих организаций.
2. Определить список источников, которые необходимо подключить к SIEM-системе для решения поставленных задач.
3. Если вы готовитесь к пилотному внедрению, то следует определить четкие границы пилотной зоны. Фрагмент инфраструктуры, попадающий под пилотное внедрение, должен позволить оценить работу SIEM-системы и решить поставленные задачи.

Рассмотрим подробнее, какие задачи решались с помощью SIEM-системы в ходе пилотных проектов, и разберем, какие источники следует подключать для выявления различных типов инцидентов. Также приведем примеры реальных инцидентов и кибератак, выявленных в ходе проведенных работ.

Задачи для SIEM-системы: типичные и нестандартные

SIEM-система традиционно применяется для решения проблемы накопления и оперативной обработки данных о событиях безопасности, поэтому первоочередные задачи, решаемые в рамках каждого пилотного проекта, — это сбор, хранение и обработка событий ИБ. Однако область применения SIEM-решения этим не ограничивается: с помощью SIEM-систем решаются такие важные задачи, как выявление и расследование инцидентов ИБ, инвентаризация активов, контроль защищенности информационных ресурсов. Как правило, список задач для пилотного проекта определяется на основании целей дальнейшего использования SIEM-системы в компании.



© Positive Technologies

Рисунок 2. Список популярных задач для пилотного внедрения MaxPatrol SIEM (доля проектов)

Мы всегда рекомендуем формулировать такие задачи для пилотного проекта, которые важны для компании и учитывают особенности ее инфраструктуры, а также учитывают требования нормативной документации, а не такие, которые просто покажут, что SIEM-система включена и работает. Это позволяет оценить функциональность системы, проверить корректность ее конфигурации, а также определить, какие источники событий необходимо подключить для решения поставленных задач, убедиться в отсутствии «слепых зон».

Пример из практики: несанкционированное появление активов

В одной из компаний SIEM-система была настроена на выявление несанкционированного появления активов внутри сети, когда служба ИТ без согласования со службой ИБ вводила какие-либо новые информационные объекты. Благодаря встроенной функции инвентаризации сети появилась возможность в реальном времени детектировать события в контурах разработки и стандартизировать процесс DevOps.

Задача Реализовать контроль за повышением привилегий учетных записей на Linux-серверах	Решение Правило корреляции отслеживает все случаи повышения привилегий, и если учетная запись, запросившая повышение привилегий, отсутствует в табличном списке допущенных, формируется инцидент
Задача Контролировать несанкционированное подключение ноутбуков к сетевому оборудованию компании	Решение Реализован мониторинг MAC-адресов на портах сетевых устройств. В случае добавления или удаления MAC-адреса формируется инцидент
Задача Контролировать несанкционированное использование программ удаленного доступа	Решение Сформирован список рабочих станций, к которым запрещено подключаться с использованием программы DameWare, применяемой в компании для удаленной техподдержки. При удаленном подключении к рабочим станциям из этого списка формируется инцидент

© Positive Technologies

Рисунок 3. Примеры нестандартных задач, решенных в рамках пилотного внедрения SIEM-системы

Источники для сбора событий

Поиск инцидентов начинается с подключения источников, которые генерируют разнообразные события. Для получения наиболее полного представления о том, что происходит в инфраструктуре компании, рекомендуется подключать все имеющиеся источники ИТ-событий и событий ИБ.



ИТ-источники — общесистемное прикладное программное и аппаратное обеспечение, порождающее ИТ-события. ИТ-источники сообщают о тех или иных явлениях в автоматизированной системе без оценки уровня их защищенности (без оценки — «хорошо» или «плохо»). Примеры: журналы серверов и рабочих станций (для контроля доступа, обеспечения непрерывности, соблюдения политик информационной безопасности), сетевое оборудование (контроль изменений конфигураций и доступа к устройствам).



Источники событий ИБ — специализированное программное и аппаратное обеспечение для информационной безопасности, порождающее события ИБ. Такие источники обладают дополнительными внешними знаниями о том, как трактовать те или иные события с точки зрения безопасности (является ли наблюдаемое явление «хорошим» или «плохим»). Примеры источников событий ИБ: IDS/IPS (для сбора данных о сетевых атаках), средства антивирусной защиты (обнаружение вредоносных программ).

В рамках пилотных проектов внедрение SIEM-системы производится на тестовую площадку, имитирующую фрагмент реальной инфраструктуры компании, либо в выделенную пилотную зону, включающую в себя ряд источников.



© Positive Technologies

Рисунок 4. Наиболее часто подключаемые источники событий (доля проектов)

Для сбора наиболее полных данных со всех источников SIEM-система должна уметь взаимодействовать с широким спектром сетевых протоколов и технологий сетевого взаимодействия: syslog, WMI, RPC, Telnet, SSH, ODBC и другими. Например, для получения сообщений из системных журналов и журналов безопасности Windows (WinEventLog, WindowsAudit) на серверах и рабочих станциях используется протокол syslog. Так в SIEM-систему попадает информация о событиях, определенных политиками аудита Windows (таких как вход в систему, доступ к объектам, изменение привилегий). WMI позволяет собирать информацию с Windows-устройств о таких событиях, как создание, изменение или удаление файлов с определенным расширением; подключение физических устройств; запуск служб в ОС. Также рекомендуется дополнительно использовать инструмент расширенного аудита — Sysmon, поскольку в журналы аудита безопасности Windows попадает не вся информация. Sysmon отслеживает изменения в ветках реестра, видит, когда злоумышленник пытается получить хеш-значения паролей пользователей, а также позволяет отследить вредоносную активность внутри сети, получить информацию об источнике, включая хеш-значение файла, породившего процесс.



Не все инциденты можно выявить, основываясь на данных, полученных с серверов и рабочих станций. Для обнаружения атак в сетевом трафике (например, при использовании злоумышленником туннелей для передачи вредоносного кода или атаки DCSync) рекомендуется дополнить решение класса SIEM системой анализа сетевого трафика (NTA/NDR).

Ниже представлен список основных событий ИБ, выявляемых с помощью SIEM-системы, и соответствующих им источников.

События ИБ	Источники событий
Вредоносный контент , доставленный легальным образом, как правило по электронной почте (спам и фишинговые атаки)	▪ Прокси-серверы с контролем контента ▪ Средства защиты веб-трафика ▪ Средства защиты почты ▪ Средства защиты конечных узлов со встроенными модулями контроля веб-ресурсов и электронной почты
Сбор данных об инфраструктуре компании, определение доступных сервисов, поиск уязвимых узлов	▪ Межсетевые экраны ▪ Средства обнаружения и предотвращения вторжений
Нарушение доступности отдельных сервисов и систем в целом (например, в случае DDoS-атаки)	▪ Межсетевые экраны ▪ Системы обнаружения и предотвращения вторжений ▪ Системы выявления и блокировки сетевых DoS-атак

Эксплуатация уязвимостей в компонентах системы	Средства обнаружения и предотвращения вторжений
Использование хакерских утилит, применяемых для взлома систем или иных противоправных действий	- Средства обнаружения и предотвращения вторжений - Сканеры уязвимостей и средства аудита - Антивирусные средства защиты
Выполнение вредоносного кода	- Антивирусные средства защиты - Средства обнаружения и предотвращения вторжений
Нарушение политик ИБ , невыполнение требований нормативных документов (PCI DSS, приказа ФСТЭК № 21), корпоративных политик безопасности	Сканеры уязвимостей
Утечка конфиденциальных данных по любым коммуникационным каналам	Системы предотвращения утечек данных
Выявление аномалий , существенных отклонений параметров объекта защиты или его поведения от ранее установленной нормы	- Межсетевые экраны нового поколения (NGFW) - Системы предотвращения утечек данных - Системы класса User and Entity Behavior Analytics

Выявленные инциденты ИБ

В рамках пилотных проектов для демонстрации возможностей SIEM-системы часто выполняется моделирование условий, которые приводят к регистрации киберинцидента. Однако, помимо смоделированных, в 100% проектов, вошедших в выборку, MaxPatrol SIEM зафиксировал еще и реальные инциденты ИБ. Во время пилотных проектов были выявлены события ИБ, свидетельствующие о потенциальных кибератаках, заражении вредоносным ПО, нарушении политик ИБ, а также об отклонениях в поведении пользователей.



Рисунок 5. Наиболее часто выявляемые инциденты ИБ (доля проектов)

Предполагаемая атака

Специалисты Positive Technologies в ходе работ по тестированию на проникновение часто выявляют в инфраструктуре заказчика следы кибератак. Это говорит о том, что либо атака осталась незамеченной специалистами по ИБ, либо при расследовании инцидента не удалось выявить все скомпрометированные узлы, а значит, и полностью устранить последствия. Причиной может быть как отсутствие современных технических средств для выявления атак, так и недостаточный объем данных, собираемых с источников событий, и следовательно, невозможность детально отслеживать все происходящие события в инфраструктуре компании.

Во время пилотных проектов были выявлены события, которые свидетельствуют о потенциальных атаках. Многие из этих событий связаны, в частности, с получением злоумышленниками информации о скомпрометированной системе и внутренней сети: после проникновения во внутреннюю сеть жертвы преступникам требуется определить, где в инфраструктуре они находятся, принять решение о дальнейших действиях, получить учетные данные пользователей для подключения к серверам и рабочим станциям. Своевременное обнаружение этих событий может помочь специалистам по ИБ остановить кибератаку на ранней стадии и минимизировать ущерб.

К примеру, в одном из пилотных проектов был обнаружен запрос сеансового билета Kerberos для несуществующего пользователя. Подобные события могут свидетельствовать об ошибочной настройке сервиса (например, учетная запись для запуска службы была удалена, но сама служба продолжает работать) или о попытке перечисления существующих пользователей.

INC-101992

TGS_request_by_non_existent_user

Служба KRBGT на узле [redacted] отклонила запрос от узла [redacted] на выдачу TGS для несуществующего пользователя [redacted]

Содержит данные об 1 срабатывании правила корреляции TGS_request_by_non_existent_user

Параметры

Категория: Не определена

Тип: Не определен

Влияние

Расположение

Статус

Опасность: ↑ Высокая

Статус: ● Новый

Ответственный: Не назначен

Автор

Источник инцидента: SIFM

Обнаружен: 24 декабря 2019, 13:43

Создан: 24 декабря 2019, 13:43

Последнее изменение: Изменено: описание, дата обнаружения, событие, опасность, тип декабря 24, 2019

Задачи   **События**   Активы и сети   Атакующие активы   Комментарии

Время	Событие
24 декабря 13:43	Служба KRBGT на узле [redacted] отклонила запрос от узла [redacted] на выдачу TGS для несущ...
24 декабря 13:43	Служба Kerberos на узле [redacted] не удалось выдать сеансовый билет (TGS) для учетной записи...

Открыть страницу События

Рисунок 6. Инцидент «Обнаружение сеансового билета Kerberos для несуществующего пользователя»

В ходе атак на контроллер домена, в котором используется аутентификация по протоколу Kerberos, злоумышленники могут прибегнуть к атаке Kerberoasting. Любой аутентифицированный в домене пользователь может запросить Kerberos-билет для доступа к сервису (Ticket Granting Service, TGS). Билет TGS зашифрован NT-хешем пароля учетной записи, от имени которой запущен целевой сервис. Злоумышленник, получив значение TGS-REP, может его расшифровать, подобрав пароль от ассоциированной с сервисом учетной записи, который зачастую является простым или словарным. В ходе пилотных проектов в ряде компаний были выявлены подобные атаки.

INC 114214

Kerberoasting

Возможная атака Kerberoasting: пользователь [REDACTED] запросил "TGS Kerberos" со слабым алгоритмом шифрования на узле [REDACTED]

Содержит данные об 1 срабатывании правила корреляции [Kerberoasting](#)

Статус

Опасность ■ Средняя

Статус ● Новый

Ответственный ■ Не назначен

Автор

Источник инцидента SIEM

Обнаружен Сегодня в 14:59

Создан Сегодня в 15:00

Последнее изменение

Изменено: описание, дата обнаружения, событие, тип 15:00

Параметры

Категория

Не определена

Тип

Не определен

Влияние

Расположение

Задачи

События

Активы и сети

Атакующие активы

Комментарии

Время

Событие

22 января 14:59

На узле [REDACTED] службой Kerberos выдан сеансовый билет (TGS) для учетной записи [REDACTED]

22 января 14:59

Возможная атака Kerberoasting: пользователь [REDACTED] запросил "TGS Kerberos" со слабым алгоритмом...

Открыть страницу События

Рисунок 7. Инцидент «Атака Kerberoasting»

Перечисление существующих пользователей через запрос сеансового билета Kerberos, а также Kerberoasting злоумышленники применяют в атаках с использованием тактик «Разведка» (Discovery) и «Получение учетных данных» (Credential Access) по модели MITRE ATT&CK. SIEM-система, обладающая правилами детектирования популярных техник атак, сумеет обнаружить активность злоумышленников еще во время их попыток получить список учетных записей домена и перечень установленных приложений и служб.

Пример из практики: фишинг

В одной компании была выявлена активность злоумышленника, преодолевшего сетевой периметр с помощью фишингового письма. Вредоносное ПО начало собирать информацию о сети. SIEM-система зафиксировала, что на активе пользовательской группы (бухгалтерия) выполняются административные команды, связанные со сбором информации о домене. Таким образом с помощью SIEM-системы был выявлен факт компрометации с использованием фишинга, который пропустило другое средство защиты.

SIEM-система помогает в выявлении и других типов атак. Так, во время проведения одного из пилотных проектов была своевременно обнаружена DDoS-атака. После анализа внешних адресов, с которых обращались злоумышленники, эти адреса были заблокированы на корпоративном межсетевом экране.

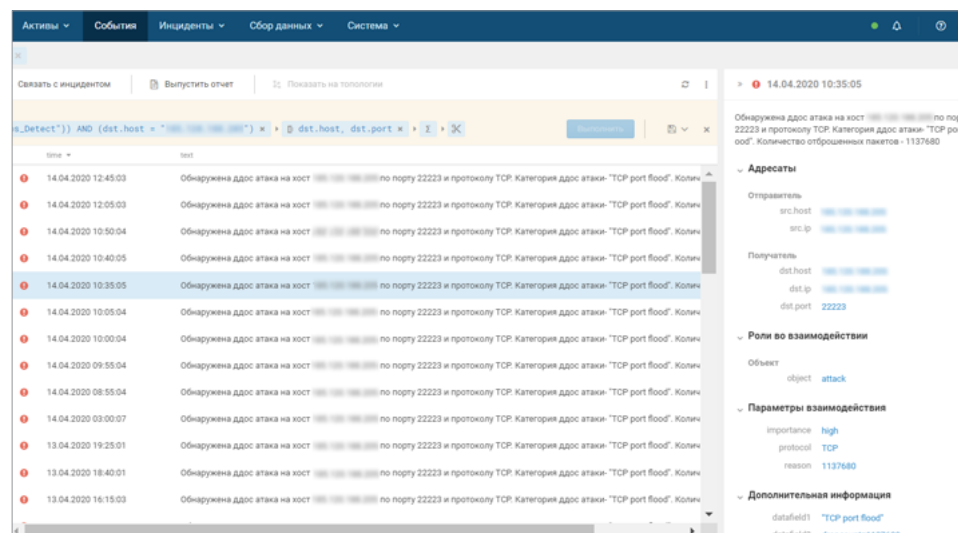


Рисунок 8. Выявление DDoS-атаки с помощью MaxPatrol SIEM

В ряде пилотных проектов выполнялся ретроспективный анализ событий ИБ для выявления атак и фактов компрометации объектов инфраструктуры компании, пропущенных или неверно приоритизированных при реализации штатных мер защиты. Так, например, удалось выявить и пресечь целенаправленную атаку на ресурсы одной компании, которая длилась не менее 8 лет. По результатам анализа журналов регистрации событий SIEM-системы были выявлены следы действий злоумышленников на 195 узлах контролируемой инфраструктуры. Причем, как выяснилось во время расследования, преступники были активны на протяжении всех этих лет, а именно использовали вредоносное ПО:

- для связи с командным сервером,
- удаленного исполнения команд,
- исследования скомпрометированной инфраструктуры,
- извлечения учетных данных пользователей на узлах,
- сжатия данных в архивы,
- передачи файлов на командный сервер и приема с него.

В минимальные сроки были заблокированы командные серверы злоумышленников и ликвидировано их присутствие в инфраструктуре. В ходе расследования специалисты Positive Technologies установили принадлежность атакующих к группировке TaskMasters.

Обнаружение вредоносного ПО

Каждый пятый инцидент, выявляемый в ходе пилотных проектов, связан с обнаружением вредоносного ПО. Причем большинство из них (порядка 85%) связаны с фишинговыми рассылками. Согласно нашему исследованию АРТ-группировок, атаковавших компании по всему миру, 90% группировок начинают атаки именно с целенаправленных фишинговых рассылок по электронной почте.

В одном из пилотных проектов было зафиксировано большое количество вредоносных писем, в частности содержащих Trojan-Banker.RTM, отправленных сотрудникам компании с 592 различных IP-адресов. Операторов этого вредоносного ПО в основном интересуют корпоративные банковские счета, поэтому фишинговые письма адресуют бухгалтерам и финансистам, имитируя переписку с финансовыми структурами. Темой такого письма может быть, например, «Заявка на возврат», «Пакет документов за прошлый месяц» или «Паспортные данные сотрудников».

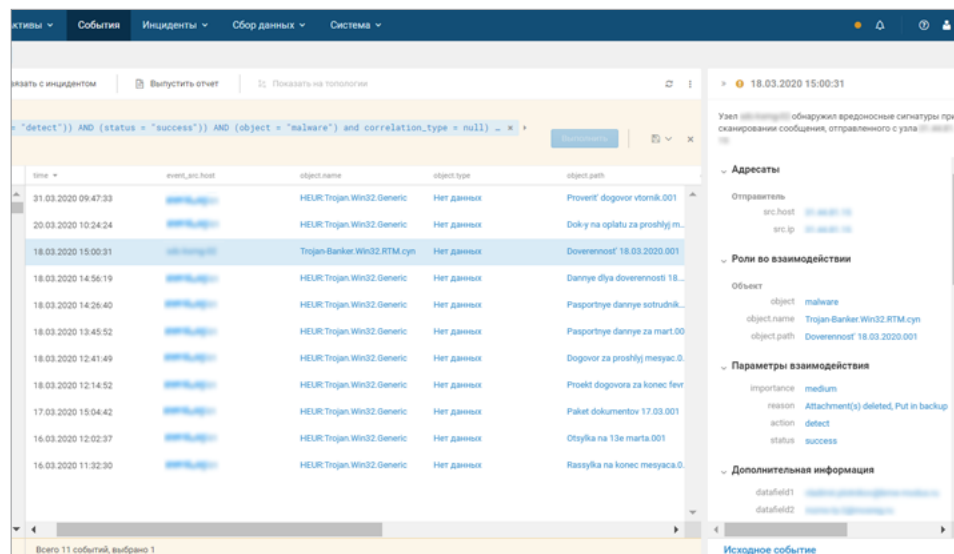


Рисунок 9. Выявление фишинговых рассылок с помощью MaxPatrol SIEM

Аномальное поведение пользователей

В исследовании, посвященном результатам работ по внутреннему тестированию на проникновение, мы говорили, что методы атак во внутренней сети основаны не только на эксплуатации уязвимостей ПО, но и на использовании архитектурных особенностей ОС и механизмов аутентификации, а также на выполнении легитимных действий, предусмотренных функциональностью системы. Легитимные действия, которые позволяют развить вектор атаки, составляют почти половину от всех действий пентестеров. Такие действия иногда сложно отличить от повседневной деятельности пользователей или администраторов, но они могут указывать на скрытое присутствие злоумышленников. Поэтому аномалии в поведении пользователей должны служить поводом для более подробного изучения событий. Примеры событий, на которые стоит обратить внимание сотрудникам службы ИБ, — это попытки выгрузки списков локальных групп или пользователей, создание нового аккаунта сразу после авторизации. В нескольких пилотных проектах SIEM-система фиксировала использование одной учетной записи на нескольких рабочих станциях, что могло означать компрометацию учетных данных. Еще одним признаком потенциальной компрометации учетных данных является работа сотрудника в ночное время.

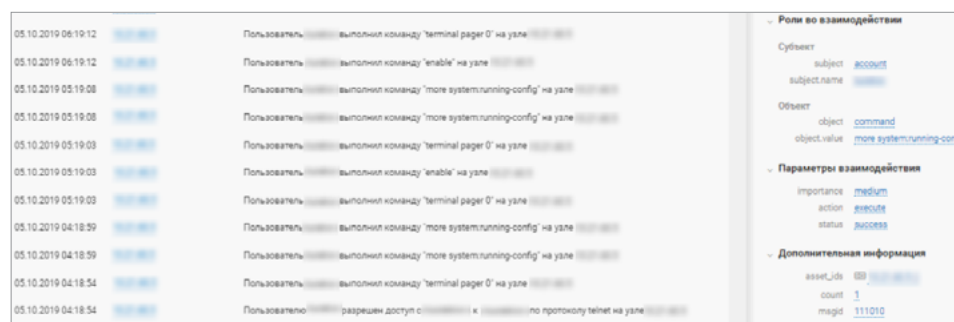


Рисунок 10. Пример инцидента «Работа в ночное время»

Нарушение политик ИБ

Еще одна категория инцидентов — это нарушения политик ИБ. Речь идет о выявлении фактов несоответствия требованиям нормативных документов, таких как PCI DSS, приказ ФСТЭК № 21, а также корпоративным политикам ИБ. Правила, устанавливаемые этими документами, направлены на обеспечение приемлемого уровня защищенности компании. Однако пользователи не всегда строго соблюдают все требования. В половине компаний в ходе пилотных проектов были выявлены нарушения политик ИБ. Так, например, в 39% пилотных проектов были зафиксированы случаи работы программ для удаленного управления компьютером. Эти события могут быть легитимными, например когда инженер технической поддержки удаленно подключается для настройки сервера, а могут указывать на получение доступа злоумышленниками (техника атаки *Remote Access Software*). Как правило, компаниям рекомендуется ограничить список узлов, на которых может использоваться ПО для удаленного доступа.

INC-301
TeamViewer_connection_detect
 Возможно, узел [IP] установил соединение с сервером TeamViewer
 Содержит данные об 1 срабатывании правила корреляции
[TeamViewer_connection_detect](#)

Статус
 Опасность: Средняя
 Статус: Новый
 Ответственный: Не назначен
 Автор:
 Источник инцидента: SIEM
 Обнаружен: 08 октября, 14:59
 Создан: 08 октября, 14:51
 Последнее изменение: Изменено: описание, дата обнаружения, событие, тип 8 октября, 14:51

Параметры
 Категория: Нарушение политик ИБ
 Тип: Установка запрещенного ПО
 Влияние:
 Расположение:

Задачи | **События** | Активы и сети | Атакующие активы | Комментарии

Время	Событие
08 октября 14:59	Возможно, узел [IP] установил соединение с сервером TeamViewer
08 октября 14:54	Обнаружен поток от [IP] к [IP] по протоколу UDP

[Открыть страницу События](#)

Рисунок 11. Инцидент «Выявление работы TeamViewer»

Пример из практики: выполнение политик ИБ

SIEM-система может применяться для проверки выполнения организационных распоряжений в части ИБ. Так, в одной из компаний было необходимо отказаться от определенного ПО, и с помощью SIEM-системы удалось собрать информацию о его использовании. Другой пример — использование решения класса SIEM в ряде организаций для проверки выполнения предписаний по смене паролей.

Заключение

Во всех компаниях происходят инциденты ИБ: выявляются использование вредоносного ПО, события, которые могут свидетельствовать о кибератаке или нарушении политик ИБ. Работы по тестированию на проникновение, выполняемые экспертами Positive Technologies, подтверждают, что в компаниях нередко выявляются следы более ранних атак хакеров, которые не были вовремя замечены службой ИБ. Для обнаружения атак на ранней стадии необходимо знать обо всем, что происходит в инфраструктуре компании. Для этого нужно собирать как можно больше информации о событиях, ведь чем полнее ведется сбор событий и чем больше источников подключено, тем больше шансов своевременно выявить подозрительную активность, принять меры по пресечению атаки и минимизировать негативные последствия.

Большой объем регистрируемых данных требует автоматизированной обработки с помощью таких решений, как SIEM. SIEM-система использует корреляцию, чтобы связывать вместе собранные данные, выявлять шаблоны, указывающие на инцидент. Опыт специалистов экспертного центра безопасности Positive Technologies показывает, что правила корреляции дают отправную точку для обнаружения большинства кибератак², в том числе сложных многоступенчатых APT-атак, а также служат основой для расследования инцидентов. Если дополнительно используется система глубокого анализа трафика (решения класса NTA/NDR), то это позволяет отследить подозрительную активность не только на узлах, но и в сетевом трафике. Стоит принять во внимание, что к расследованию инцидентов следует привлекать квалифицированных экспертов, которые сумеют полностью восстановить цепочку атаки.

---

2. MaxPatrol SIEM благодаря встроенным правилам корреляции позволяет выявлять актуальные техники атак без дополнительной настройки. Кроме того, MaxPatrol SIEM обладает правилами детектирования популярных техник атак (используется классификация MITRE ATT&CK), что позволяет обнаружить активность злоумышленников на ранних этапах.

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/
PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте [ptsecurity.com](#).