EnCase® Cybersecurity

Единый продукт, предназначенный для защиты вашей сети, обнаружения и восстановления критической информации, подвергшейся воздействию полиморфных вирусов

Guidance® SOFTWARE
The World Leader in Digital Investigations™

EnCase® Cybersecurity

Достоинства

- Обнаружение характерных бинарных фрагментов в файлах, предположительно возникающих в ходе самомодификации, с целью выявления полиморфных вирусов и последующего их удаления
- Определение уровня угрозы в конечных точках сети, анализ исполняемого кода, восстановление записей реестра, файлов и процессов для заблаговременного выявления скрытых угроз, а в случае их реализации – восстановления поврежденных данных
- Выполнение анализа вредоносного ПО и централизованное (горячее) восстановление системы без ее остановки
- Заблаговременный аудит критической информации и ее восстановление в случае утечки
- Ранжирование инцидентов в глобальных сетях и борьба с внутренними угрозами
- Расследование нарушений безопасности сетей, действий персонала и сообщений о мошенничестве с сохранением доказательной силы в суде

Главными задачами специалистов служб ИТ-безопасности являются поддержание сети в безопасном состоянии, защита корпоративных данных, заблаговременное выявление сетевых угроз и реагирование на них. Эти задачи решаются круглосуточно и в глобальных масштабах, соответственно масштабам сетей. Для этого необходимы, как минимум, средства выявления и анализа потенциальных угроз, реагирования на них и восстановления в случае их реализации, а также инструменты защиты корпоративных данных, для обеспечения безопасного состояния конечных точек сети.

EnCase Cybersecurity – это многофункциональный программный комплекс, позволяющий специалистам ИТ-безопасности выявлять скрытое вредоносное ПО, включая полиморфные вирусы, а также заблаговременно выявлять угрозы в сетях любого уровня без остановки системы. EnCase Cybersecurity позволяет организации перейти от пассивной (регистрирующей) стратегии безопасности к активной, сконцентрировавшись на своевременном выявлении потенциальных угроз и восстановлении работоспособности системы в случае их реализации, с минимальными затратами времени и средств.

Выявление полиморфного вредоносного ПО

Хакерам давно известно, что вредоносные программы с постоянным кодом (метаморфные) легко поддаются обнаружению по сигнатуре. Соответственно были разработаны новые приемы, с использованием которых вредоносное ПО, например, полиморфный вирус, периодически изменяет свой код, сохраняя при этом исходные возможности. Вследствие этого его обнаружение обычными антивирусными программами, использующими сигнатурный анализ, невозможно.

В пакете EnCase Cybersecurity реализованы оригинальные разработки, дающие преимущество службам ИТ-безопасности в противостоянии атакам корпоративных сетей.

EnCase Cybersecurity позволяет ранжировать признаки скрытых угроз и детально анализировать программный код, используя самые современные алгоритмы сравнения. Всё это позволяет обнаружить и ликвидировать полиморфное ПО и быстро устранить следы его разрушительной деятельности.

Выявление скрытых угроз и минимизация риска в корпоративных сетях

Пакет программ EnCase Cybersecurity обеспечивает надежное обнаружение угроз в конечных точках сети и их устранение в корпоративной сети.

В случае обнаружения неизвестного или подозрительного процесса EnCase Cybersecurity начинает его всесторонний анализ. Средства анализа памяти на основе ядра HBGary Responder Pro дают пользователю возможность подробно проанализировать программный код, чтобы выявить функциональность конкретного процесса, например, способность к самомодификации для уклонения от обнаружения по сигнатуре. Благодаря этому, сотрудники отдела ИТ получают полное представление об угрозе и указания на то, в каких еще частях программного комплекса вредное действие угрозы уже имеет или может иметь место.

Мониторинг сети и устранение последствий реализации угрозы проводятся централизованно и без остановки деятельности организации.

Обнаружение вредоносных программ по следам

Пакет программ EnCase Cybersecurity позволяет обнаруживать и устранять полиморфные и метаморфные вирусы путем сравнительного анализа для определения степени подобия подозрительного бинарного кода сигнатурам уже известных вредоносных программ. Используемый метод основан на сопоставлении вычисленных значений энтропии (степени случайности) для сравниваемых бинарных последовательностей.

В отличии от методов «нечеткого хэширования» для определения степени подобия файлов, в пакете EnCase Cybersecurity реализованы средства экспресс-оценки вредоносных программ «на лету» с заданной достоверностью. При этом сотрудникам отдела ИТ не требуется переносить исходные файлы известных вредоносных программ за пределы начальной точки заражения.

Поддержание безопасного состояния конечных точек сети

Пакет программ EnCase Cybersecurity позволяет использовать реестр ПО «Bit9 Global Software Registry» и заносить в него собственные подтвержденные и неподтвержденные хэши. Эта возможность позволяет специалистам ИТ-безопасности периодически проверять ПО конечных точек сети с использованием миллионов зарегистрированных программ и обеспечивать отсутствие отклонений от безопасного состояния. В случае обнаружения неизвестных файлов или процессов, EnCase Cybersecurity производит глубокий экспресс-анализ угроз, результаты которого позволят специалистам сконцентрироваться на конечных точках с самым высоким уровнем угроз.

Защита конфиденциальных данных организации

Реализованные в пакете EnCase Cybersecurity функции мониторинга внешних и внутренних носителей, позволяют обнаруживать конфиденциальные данные независимо от того, где и каким образом они хранятся в системе – даже после их удаления программными средствами. В случае выявления, специалисты ИТ-безопасности могут произвести физическое удаление конфиденциальных данных из несанкционированных участков сети, чтобы обеспечить их сохранность, защиту и доступность только для уполномоченных пользователей.

Восстановление системы и данных

Пакет программ EnCase Cybersecurity позволяет восстанавливать исходное (неповрежденное) состояние файлов, процессов и параметров реестра, т.е. обеспечивает не только полное устранение сетевых угроз, но и удаление конфиденциальных данных из несанкционированных участков сети. Конкурирующие программы могут обладать механизмами поиска данных, однако ни одна из них не обеспечивает присущей EnCase Cybersecurity полноты восстановления безопасного состояния.

Дополнение к пакету Cybersecurity – усовершенствованные алгоритмы для противодействия неизвестным атакам

Модуль анализа неполного совпадения энтропии «EnCase Cybersecurity Entropy Near Match Analyzer»

В пакете EnCase Cybersecurity использованы разработанные и запатентованные фирмой Guidance Software приемы обнаружения подобия файлов, расположенных на разных участках сети. Оригинальность нашего метода заключается в вычислении энтропии (степени случайности) файла. Это позволяет проводить сравнение и обнаруживать сходство файлов более быстро и точно, чем с помощью традиционного метода хэширования с использованием нечетких вычислений (fuzzy hashing). Данная функция позволяет специалистам ИТ-безопасности обнаруживать полиморфные вирусы после очередных циклов самомодификации и выявлять более старые и более новые версии полиморфного вредоносного ПО.

Принципиально новый метод обнаружения подобия файлов позволяет службам ИТ-безопасности быстро приспосабливаться к новинкам хакеров – полиморфному и метаморфному ПО.

Анализ кода в EnCase Cybersecurity

Сотрудники могут выполнять высокоуровневый экспресс-анализ угроз на основе пользовательских критериев. Как только угроза обнаружена, проводится более глубокий анализ памяти, что позволяет исследовать любой процесс и его функциональность, например, для определения полиморфной природы вредоносной программы.

Сочетание функций анализа угроз и процессов позволяет выявлять неизвестные угрозы.

Модуль Bit9 «EnCase Cybersecurity Bit9 Analyzer»

База данных Bit9 Global Software Registry содержит информацию о метаданных более чем 400 млн файлов, значения хэш-функций более 9 миллионов прикладных программ более чем 20 тысяч производителей, а также значения хэш-функций почти всех известных вредоносных программ. За счет использования этих сведений, модуль EnCase Cybersecurity's Bit9 Analyzer позволяет резко сократить временные затраты и снизить системные требования для проведения антивирусного мониторинга всей системы.

Данный модуль позволяет резко сократить затраты времени на выявление неизвестных ранее угроз, известного вредоносного и несанкционированного ПО.

Возможности

- Мониторинг на уровне диска и оперативной памяти – обеспечивается полный контроль местоположения данных в конечных точках сети
- Запатентованная технология энтропии – обнаружение в системе полиморфного вредоносного ПО после его самомодификации
- Средства выявления и глубокого анализа неизвестных процессов – интеграция с HBGary Responder Professional
- Сравнение состояния конечных точек с безопасным (исходным) состоянием или данными из базы данных «Bit9 Global Software registry» – выявление любых отклонений от безопасного состояния
- Возможность проведения собственного аудита с криминалистически значимыми доказательствами обеспечивает полный контроль ИТ-безопасности (прозрачность) организации
- Сбор и хранение только конфиденциальных данных; отсутствие необходимости архивирования и хранения всего документооборота организации

Сертификаты безопасности для применения в защищенных вычислительных комплексах

Фирма Guidance Software, единственная среди разработчиков ПО для мониторинга и расследования ИТ инцидентов в корпоративных системах, имеет сертификаты Минобороны США (DIACAP), уровня EAL-2 по Основным критериям (стандарт ИСО/МЭК 15408) и FIPS 140-2 (стандарт на средства шифрования). Сертификаты подтверждают безопасность применяемых протоколов в вычислительных комплексах с защитой самого высокого уровня.

www.guidancesoftware.ru

Наши клиенты

Клиенты фирмы Guidance Software – корпорации и государственные органы, в частности, финансовые и страховые компании, промышленность, подрядчики Министерства обороны, фармацевтика, сети розничной торговли. Программный комплекс EnCase® внедрен в более чем 100 компаниях из списка 500 крупнейших корпораций журнала «Fortune» и более чем в половине 50 крупнейших, в том числе: Allstate, Chevron, Ford, General Electric, Honeywell, Mattel, Northrop Grumman, Pfizer, UnitedHealth Group, Viacom и Wachovia.

О компании **Guidance Software (код акций GUID)**

История компании Guidance Software начинается в 1997 году с разработки инновационного программного комплекса для экспертов-криминалистов, работа которых заключалась в поиске доказательств и улик на месте преступления. Это время характеризуется началом распространения поиска и анализа не только физических улик, но и цифровых данных на жестких дисках рабочих машин. Именно компания Guidance Software разработала комплекс EnCase Forensic, который позволял сразу нескольким экспертам работать с цифровыми носителями данных на физическом уровне носителя данных. На протяжении нескольких лет EnCase Forensic уже использовался почти 90% экспертами-криминалистами по всему миру и обладал уникальными возможностями, которые не мог предоставить любой другой продукт.

В 2002 компания выпустила на рынок сетевую версию Encase Forensic для коммерческих и государственных структур под названием Encase Enterprise. Обладая всеми функциями версии для криминалистов Encase Forensic, а также возможностью работы по сети, ЕЕ предоставило организациям проводить всеобъемлющий аудит компьютеров сотрудников и серверов, осуществлять контроль за хранящимися конфиденциальными данными и осуществлять внутренние расследования внутри организации юридически узаконенным способом.

Услугами программного обеспечения EnCase пользуются более 20000 корпоративных и правительственных организаций, и более чем 4000 их сотрудников ежегодно посещают обучающие курсы Guidance Software. Признанное многочисленными судебными органами, а также получившее награды eWEEK's Excellence Award и SC Magazine's Annual Award, программное обеспечение EnCase считается эталоном среди инструментов, используемых для проведения судебных расследований. Среди клиентов Guidance Software половина компаний из списка Fortune 50 и треть из списка Fortune 500. Акции Guidance Software котируются на бирже NASDAQ. Капитализация на начало 2008г. составляет 220 млн. долларов США.