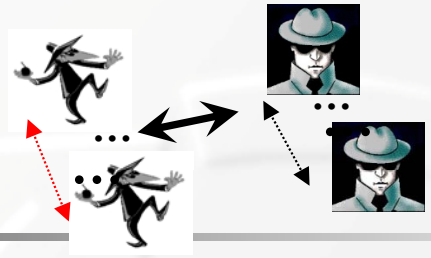


Направления исследований в области Advanced Security Analytics

И.В. Котенко

СПИИРАН

Рускрипто'2018, 22 марта 2018 г.

SIEM-системы

Security information and event management (SIEM) system – система управления информацией и событиями безопасности (система мониторинга и управления инцидентами безопасности).

Основная цель SIEM – повышение ИБ за счет обеспечения возможности в режиме, близком к реальному времени, манипулировать ***информацией о безопасности*** и осуществлять проактивное ***управление инцидентами и событиями безопасности***

«Проактивный» означает «действующий до того, как ситуация станет критической». Предполагается, что проактивное управление инцидентами и событиями безопасности основывается на автоматических механизмах, использующих информацию об «истории» анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга событий к текущему состоянию защищаемой системы

Расширенный список задач, решаемых SIEM-системой

- сбор, обработка и анализ событий безопасности, поступающих в систему из множества гетерогенных источников;
- обнаружение в реальном времени атак и нарушений критериев и политик безопасности;
- оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов;
- анализ и управление рисками информационной безопасности;
- проведение расследований инцидентов;
- обнаружение расхождения критически важных ресурсов и бизнес–процессов с внутренними политиками безопасности и приведение их в соответствие друг с другом;
- выработка и реализация решений по защите информации;
- формирование отчетных документов.

Новые возможности следующего поколения систем мониторинга и управления кибербезопасностью

- **межуровневая корреляция событий безопасности**, поступающих из различных неоднородных источников
- **адаптивная масштабируемая обработка событий**, обеспечивающая управление большими объемами данных о безопасности в реальном или близком к реальному времени
- **прогностический анализ безопасности**, позволяющий осуществлять проактивное обнаружение и предотвращение атак путем принятия соответствующих контрмер **за время, близкое к реальному**
- **высокая доступность и отказоустойчивость сбора данных** о событиях безопасности и доведения решений в условиях распределенности защищаемой инфраструктуры и активного вредоносного и/или непреднамеренного воздействия на каналы связи
- выработка контрмер **в реальном времени**
- возможность построения комплексных систем мониторинга и реагирования, как SOC, или подключения к «ФинЦЕРТ» Банка России или ГосСОПКА (в случае отечественных решений)

Методы корреляции

Сигнатурные методы корреляции событий:

– Правило-ориентированные [R. Sadoddin, A. Ghorbani, 2006],[A. Hanemann, P. Marcu, 2008], [T. Limmer and F. Dressler, 2008]
– Шаблонно-(сценарно-)ориентированные [R. Sadoddin, A. Ghorbani, 2006]
– Граф-ориентированные [A. Muller, 2009],[P. Ning and D. Xu, 2008]
– На основе машины конечных состояний [A.Muller, 2009], [A.A.Ghorbani et al., 2010]
– На основе схожести [M. A. Hasan, 1999], [U. Zurutuza, R. Uribeetxeberria, 2004]
– и др.

Несигнатурные методы корреляции событий:

– Машинного обучения
– Статистические
– На основе прецедентов и др.

Методы машинного обучения:

– Байеса [R. Sadoddin, A. Ghorbani,2006],[A. Muller,2009], [D.W. Guerer et al.,1996]
– Иммунные сети [A. Muller, 2009], [D.W. Guerer et al., 1996]
– Искусственные нейронные сети [A. Muller, 2009],[D.W. Guerer et al., 1996], [H.T. Elshoush and I.M. Osman, 2001] и др.

Моделирование атак

- **Цветные сети Петри [Kumar S., Spafford E.H., 1994; …]:** Каждая сигнатура вторжения определяется как шаблон, который представляет соотношение между событиями и их контекст.
- **Проверка на модели [C.Ramakrishnan and R.Sekar; R.Ritchey and P.Ammann; O.Sheyner; S.Jha and J.Wing; Giannakopoulou, 2011; SMV, NuSMV, SPIN, …]:** Определяется гипотеза (состояние системы), нарушение которой проверяется методом model checking.
- **Экспертные системы [M.Danforth – Java Expert System Shell; Gamal et al., 2011; …]:** Правила – выполнение атакующих действий, факты – состояния системы. Атаки задаются в виде предусловия/постусловия.
- **Логический подход [X.Ou, W.Boyer, M.McQueen, 2009 – Datalog language; …]:** Граф состоит из вершин вывода и вершин фактов. Модель сети – множество высказываний, атаки – правила.
- **Графы атак [Ortalo et al., 1999; Ritchey&Ammann, 2000; Sheyner et al., 2002; Rieke, 2004; Ingols, 2009; …]:** Вершины – состояния системы, дуги – переходы.

Спецификации платформ, уязвимостей, оценок уязвимостей, атак, слабых мест и конфигураций

- **Представление сценариев атак и моделей нарушителей** [Schneier, 1999; Dawkins et al., 2002; Shepard et al., 2005; …]
- **Спецификация платформ, уязвимостей, оценок уязвимостей, атак, слабостей и конфигураций** [NVD; OSVDB; CVE; CVSS; CPE; CCE; CWE; CAPEC; …]
- **Показатели защищенности** [Mell et al., 2007; Jaquith, 2007; Herrmann, 2007; Jansen, 2009; …]
- **Комбинирование графов зависимостей сервисов и графов атак** [Kheir et al., 2009; Kheir et al., 2010; …]
- **Представление атак нулевого дня** [Ingols et al., 2009; Wang et al., 2010; …]
- **Моделирование контрмер** [Kheir et al., 2010; …]

Протоколы для спецификации платформ, уязвимостей, оценок уязвимостей, атак, слабых мест и конфигураций (1/2)

- **Security Content Automation Protocol (SCAP)**
  - Common Vulnerabilities and Exposures (CVE)
  - Common Configuration Enumeration (CCE)
  - Common Platform Enumeration (CPE)
  - eXtensible Checklist Configuration Description Format (XCCDF)
  - Open Vulnerability Assessment Language (OVAL)
  - Common Vulnerability Scoring System (CVSS)
- **Threat Analysis Automation Protocol (TAAP)**
  - Malware Attribute Enumeration & Characterization (MAEC)
  - Common Attack Pattern Enumeration & Classification (CAPEC)
  - Common Platform Enumeration (CPE)
  - Common Weakness Enumeration (CWE)
  - Open Vulnerability and Assessment Language (OVAL)
  - Common Configuration Enumeration (CCE)
  - Common Vulnerabilities and Exposures (CVE).

Протоколы для спецификации платформ, уязвимостей, оценок уязвимостей, атак, слабых мест и конфигураций (2/2)

- **Event Management Automation Protocol (EMAP)**
  - Common Event Expression (CEE)
  - Malware Attribute Enumeration & Characterization (MAEC)
  - Common Attack Pattern Enumeration & Classification (CAPEC).
- **Incident Tracking and Assessment Protocol (ITAP)**
  - Open Vulnerability and Assessment Language (OVAL)
  - Common Platform Enumeration (CPE)
  - Common Configuration Enumeration (CCE)
  - Common Vulnerabilities and Exposures (CVE)
  - Common Vulnerability Scoring System (CVSS)
  - Malware Attribute Enumeration & Characterization (MAEC)
  - Common Attack Pattern Enumeration & Classification (CAPEC)
  - Common Weakness Enumeration (CWE)
  - Common Event Expression (CEE)
  - Incident Object Description Exchange Format (IODEF)
  - National Information Exchange Model (NIEM)
  - Cybersecurity Information Exchange Format (CYBEX).

Основные процессы и модели

Схема методики, реализованной в рамках разработанного программного комплекса

Технология потоковой обработки *CEP*

CEP (Complex Event Processing) – технология оперативной (онлайн) обработки однородных данных, поступающих на узел обработки в виде потока.

Основные свойства CEP:

- **Поток *S*** – это бесконечная последовательность событий
- **Событие** – это кортеж, имеющий предопределенную **схему** (A_1, A_2, ..., A_n)
- **Схема потока** равна схеме события

В технологии выделяют 5 **операторов обработки потоков**: ***map, filter, union, join, aggregate***.

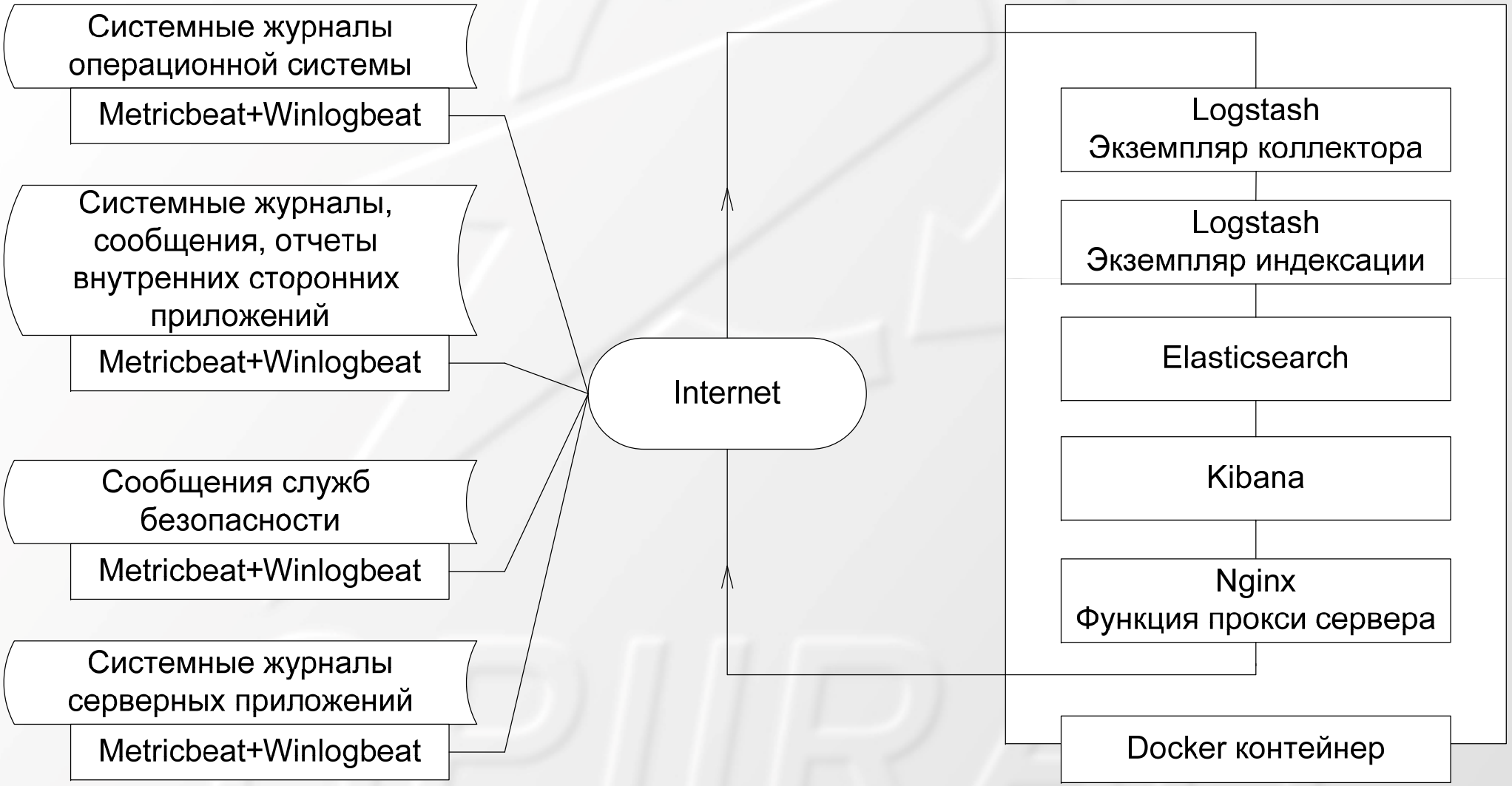
Модульная структура

Платформа включает в себя следующие модули:

1) сбора данных;
2) агрегации данных;
3) нормализации и анализа данных;
4) визуализации и трансляции данных;
5) работы с хранилищем данных

Архитектура:

Архитектура прототипа



Архитектура платформы