Cyber security event processing

Studiengang: MAS Information Technology

Das klassische «Security Information and Event Management (SIEM)» stösst mit den exponentiell wachsenden Logdatenmengen an Grenzen. Die Pflege der Suchmuster und die Analyse der detektierten Ereignisse binden zunehmend Personenressourcen. Neue Ansätze, beyond SIEM auf Basis von «Machine Learning», versprechen neue Aussichten. Wir haben mit dem Bau eines Prototypsystems untersucht, wie der Stand des «Open Source Cyber Security Application Framework», «Apache Metron», ist.

Umfeld

Mit der stetig wachsenden Digitalisierung steigt die Abhängigkeit von Informatik gestützten Produkten und Dienstleistungen. Cyber-Bedrohungen gewinnen immer mehr an Bedeutung. Um auf Unregelmässigkeiten in Informatiksystemen aufmerksam zu werden, hat das Überprüfen von Logeinträgen und Netzwerkverhalten heute erste Priorität. Vorgehensweisen, welche sich von regelbasierten mehr hin zu datengetriebenen Ansätzen mit «Machine Learning» ausrichten, versprechen neue Möglichkeiten. Mit höherer Automatisierung und autonomer Erkennung sollen die künftigen Herausforderungen gemeistert werden können.

Problemstellung

Die Herausforderung liegt darin, auf die relevanten Ereignisse aufmerksam zu werden. Das erfordert das Verknüpfen von komplexen Zusammenhängen bzw. diese technisch abbilden zu können. Erst auf diese Weise eröffnet sich eine Chance, auch fortgeschrittene Angriffe erkennen zu können. Es wird immer wichtiger, die Informationen mit Logik und Kontext zu versehen. Dabei sind Erfahrung und Informationsquellen, wie z. B. von der Melde- und Analysestelle Informationssicherung (MELANI), in der Verknüpfung zum jeweiligen Ereignis wichtig. Um diese Informationen verwalten zu können, benötigen wir eine Tool-Unterstützung, welche über die heute eingesetzten Lösungen hinausgeht.

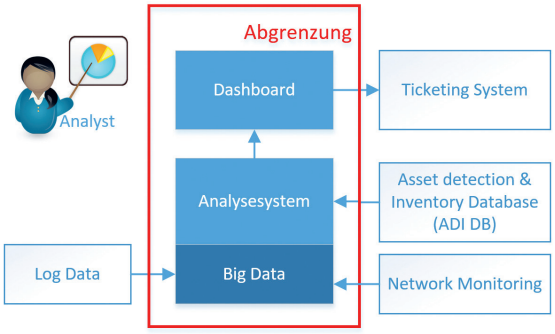

Bild 1: Abgrenzung

Lösungsansatz

Kommerzielle SIEM-Lösungen mit «Machine Learning», häufig wird auch von «Artificial Intelligence» (AI) gesprochen, sind in den letzten paar Jahren von den einschlägigen Herstellern auf den Markt gekommen. In der Open-Source-Welt finden sich erste «Cyber Security Application Frameworks». Wir haben ein solches Prototypsystem einschliesslich darunterliegenden Hadoop Cluster aufgebaut um zu untersuchen, was damit heute bereits möglich ist. Neben den zu verarbeitenden Datenquellen sind für die Einstufung und Zuordnung der Ereignisse weitere Datenlieferanten nötig. Die Asset Detection & Inventory DB beinhaltet Informationen zu Systemen, Schutzobjekteignern und Kontextinformationen zur Ermittlung des Risikowerts. Detektierte Sicherheitsereignisse können auf diese Weise mit einem Risikowert versehen und in der Priorität eingestuft werden.

Schlussbetrachtung

Die untersuchte Open-Source-Lösungen sieht sehr vielversprechend aus, jedoch befindet sie sich noch in einem eher frühen Stadium der Entwicklung. Im Framework sind viele Funktionalitäten vorhanden, doch die Lernkurve für Implementierungs- und Betriebsaufwand stellt sich grösser als erhofft heraus.

Thomas Diener

Thomas Wasser