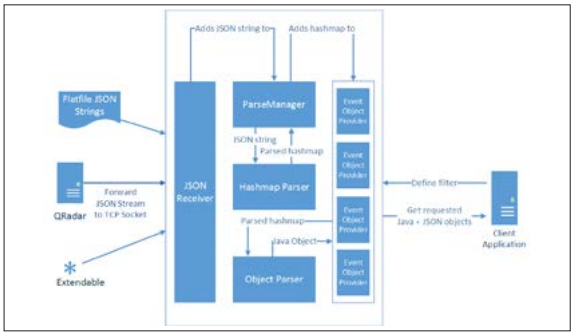
Pascal Langenstein

Pascal Vetsch

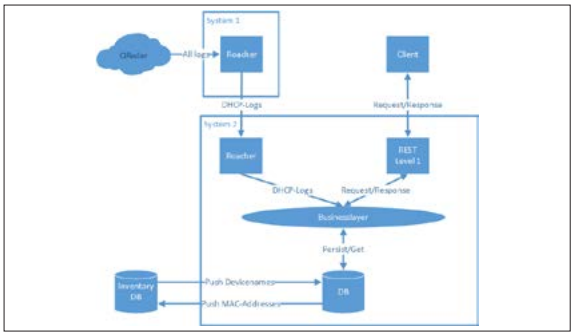
Diplomanden	Pascal Langenstein, Pascal Vetsch
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Sicherheit
Projektpartner	Dr. Marc Stoecklin, IBM Research Zürich, Rüschlikon, ZH

Distributed Security Event Processing System

Verteiltes System zur Verarbeitung, Filterung und Weiterleitung von Sicherheitsevents



Systemübersicht der entwickelten Library



Systemübersicht des Proof of Concept

Screenshot Device Monitoring System

Ausgangslage: IBM hat ein Security Information and Event Management (SIEM)-System namens QRadar®, welches Logs von verschiedenen Quellen entgegennimmt, parst, normalisiert und analysiert. Im neusten Release besteht die Möglichkeit, die normalisierten Logs als JavaScript™ Object Notation (JSON) über das Netzwerk zu exportieren. In dieser Arbeit wird eine Library entwickelt, welche in Forschungsprojekten genutzt werden kann, um einfachen Zugriff auf die Logs von QRadar zu erhalten, ohne diese selber aufgreifen und parsen zu müssen.

Vorgehen/Technologien: Zusammen mit dem Industriepartner wurden Use Cases ausgearbeitet und erste Prototypen entwickelt. Es stellte sich heraus, dass die Flexibilität einen hohen Stellenwert einnehmen muss, aber dennoch die Benutzerfreundlichkeit nicht leiden darf. Um dies zu erreichen, wurde die Library in mehrere Komponenten aufgeteilt, die entweder mit Standardeinstellungen betrieben oder durch die Anwender nach ihren Ansprüchen konfiguriert werden können. Die Projektumgebung für die in Java™ geschriebene Library wurde mit Mercurial, Maven und Jenkins realisiert und die Codequalität mittels SonarQube und Codereviews gewährleistet. Basierend auf der Library wurde das Device Monitoring System als Proof-of-Concept entwickelt. Dieses dient dazu, die Anwendung und Funktionalitäten der Library zu validieren und gleichzeitig die Benutzerfreundlichkeit und Flexibilität zu überprüfen.

Ergebnis: Es wurde eine Library entwickelt, die es dem Benutzer erlaubt, die normalisierten Logs von QRadar zu empfangen und als Java-Objekte weiterzuverarbeiten. Zusätzlich kann der Benutzer eigene Events und Filter definieren, um den gewünschten Output zu erhalten. Weiter ist es möglich, mehrere Instanzen dieser Library als verteiltes System im Netzwerk zu betreiben. Das Device Monitoring System arbeitet mit den geparsten Logs von mehreren Instanzen der Library. Es kann im Netzwerk aktive Geräte erkennen und mit der existierenden Inventardatenbank abgleichen, um fremde Geräte zu identifizieren. Die Library sowie das Device Monitoring System wurden in einer produktiven Umgebung mit realen Netzwerk- und Log-Daten in Zusammenarbeit mit dem IT-Support Team in Betrieb genommen und getestet.