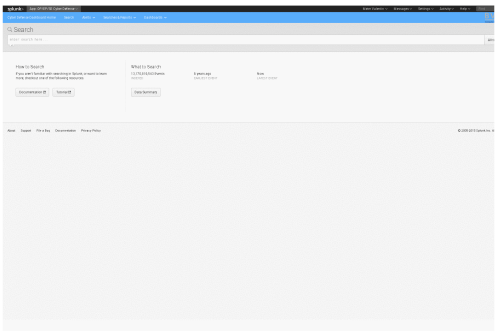

Nicola Grögli


Valentin Meier

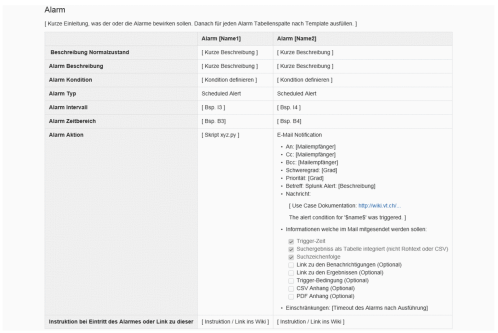
Diplomanden	Nicola Grögli, Valentin Meier
Examinator	Prof. Dr. Andreas Steffen
Experte	Prof. Dr. Andreas Steffen
Themengebiet	Sicherheit
Projektpartner	Bank Vontobel AG, Zürich, ZH

Splunk App für Security Threat Detection & Response

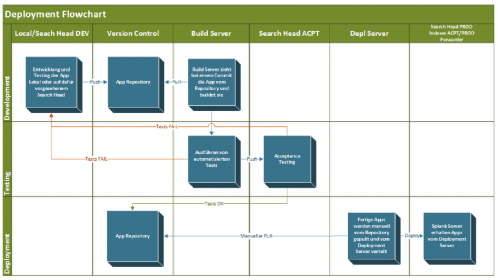
Umsetzung von Security Use Cases mittels Splunk



Übersichtsseite Splunk Suche



Template für die Definition eines Alarms



Deploymentdiagramm für Splunk Apps

Ausgangslage: In dieser Arbeit wurden acht sicherheitsrelevante Use Cases in Splunk umgesetzt. Bei Splunk handelt es sich um eine Datenanalyse Plattform, welche von der Bank Vontobel AG unter anderem als Security Information and Event Management (SIEM) Lösung eingesetzt wird. Es ermöglicht die Aggregation von Daten aus Logs, Datenbanken und weiteren Informationsquellen praktisch in Echtzeit.

Vorgehen/Technologien: Jeder der erwähnten Use Cases beschreibt ein potentielles Sicherheitsrisikos für die Bank Vontobel AG. Zu diesen gehören unter anderem Angriffe über kompromittierte Systeme in der DMZ, Manipulierung von Windows Active Directory Gruppen, Veränderungen an den Registry Autorun Einträgen, Pass-the-Hash Angriffe, Beaconing via HTTP/S und Logins per Honey Token. Für jeden Use Case wurden die relevanten Log Events und Quellen definiert, anschliessend analysiert und auf Basis der Resultate entsprechende Alarme in Splunk eingerichtet. Ebenfalls zum Umfang der Arbeit gehörten das durchführen einer Marktanalyse, eine Anleitung zur Entwicklung von Splunk Apps, sowie ein Alarmierungskonzept der Use Cases.

Ergebnis: Mittels der Marktanalyse konnte festgestellt werden, dass sich die Eigenentwicklung einer Splunk App als Folgearbeit lohnt, da kein Produkt welches bereits auf dem Markt ist, den gewünschten Umfang bietet. Die Anleitung zur Entwicklung der Apps dient als Hilfe dazu. Mit dem Alarmierungskonzept wurde eine Richtlinie geschaffen, welche bei der Implementierung von weiteren Use Cases angewendet werden soll. Dank den umgesetzten Security Use Cases wurde die Wahrscheinlichkeit des Erkennens von Sicherheitsrisiken merklich erhöht. Die Alarme konnten bereits unzulässig manipulierte Active Directory Gruppen, Pass-the-Hash Angriffe und fehlerhafte Netzwerkverbindungen erfolgreich detektieren.