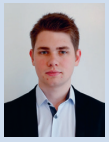


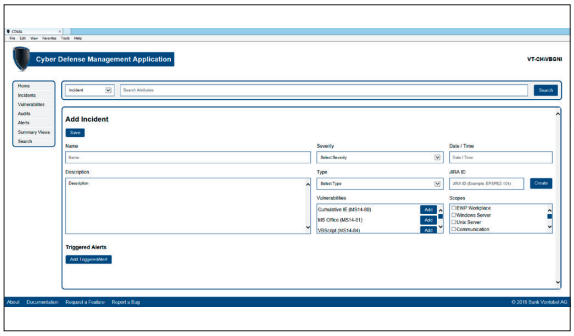
Nicola Grögli

Valentin Meier

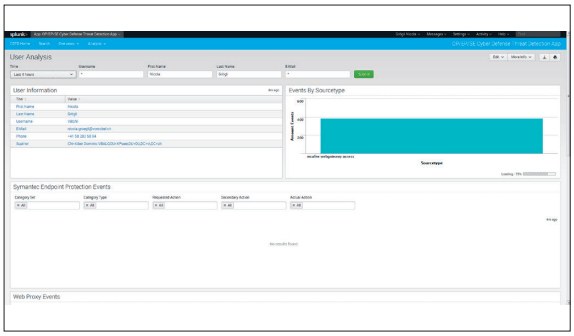
Diplomanden	Nicola Grögli, Valentin Meier
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich, ZH
Themengebiet	Sicherheit
Projektpartner	Bank Vontobel AG, Zürich, ZH

Security Threat Detection & Response

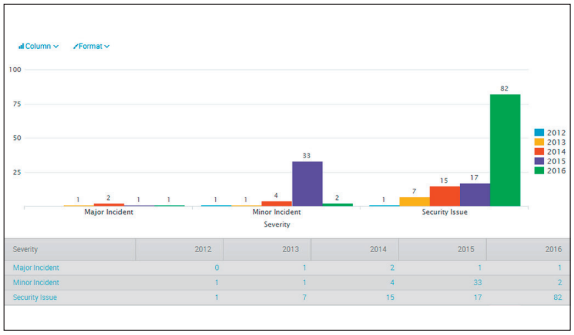
Cyber Defense Threat Detection App in Splunk und Cyber Defense Management Application



Incident Formular CDMA



User Analyse Dashboard CDTD



Severity	2012	2013	2014	2015	2016
Major Incident	0	1	2	1	1
Minor Incident	1	1	4	33	2
Security Issue	1	7	15	17	82

Auswertung Incidents (CDTD und CDMA)

Ausgangslage: Für die Bank Vontobel AG wurden während einer Studienarbeit acht Sicherheitsmechanismen innerhalb eines Security Incident and Event Management Systems (SIEM) umgesetzt, die bösartige Hacker-Aktivitäten alarmieren sollen. Neben diesen acht Use Cases wurden ausserdem diverse Umsysteme eingerichtet, die ebenfalls Alarmierungsfähigkeiten haben. Zusätzlich hat die Bank Vontobel AG weitere Alarme innerhalb des SIEM aufgeschaltet. Durch diese Erweiterungen im Bereich Informationssicherheit werden mehr Vorfälle aufgedeckt, Schwachstellen gefunden, aber auch Fehlalarme ausgelöst. Um diese dennoch effizient zu bewältigen, wurde eine Möglichkeit benötigt, Alarmen nachgehen zu können und entsprechende Nachforschungen anzustellen sowie die aktuelle Lage zu dokumentieren und auszuwerten. Um diesen Anforderungen gerecht zu werden, wurde im Rahmen dieser Bachelorarbeit eine SIEM-App in Splunk erstellt, die die entsprechenden Auswertungen ermöglicht. Zusätzlich wurde eine separate Applikation erstellt, die die Erfassung und Auswertung der aufgetretenen Events, Schwachstellen sowie durchgeführten Audits vereinfacht.

Vorgehen/Technologien: Die Bachelorarbeit wurde in zwei Teile gegliedert. Zuerst wurde die Cyber Defense Threat Detection App (CDTD) für das SIEM erstellt und anschliessend die Webapplikation Cyber Defense Management Application (CDMA), die beim Verwalten der sicherheitsrelevanten Informationen helfen soll. Die CDTD-App wurde innerhalb der bestehenden SIEM-Lösung Splunk eingerichtet. Hierbei wurden Übersichten zu vordefinierten Systemen erstellt. Berücksichtigt wurden dabei die Web Proxies, der Antivirenschutz, das Intrusion Prevention System und die Firewalls. Zusätzlich wurden Analyse-Dashboards erstellt, mit denen man nach Benutzer- oder Systeminformationen suchen kann. Die CDMA wurde primär mittels der Programmiersprache C# und dem .NET Framework entwickelt. Sie gliedert sich in eine Back-End und eine Web Front-End Komponente. Zusätzlich wurde die Applikation an Splunk angebunden, worüber sämtliche Informationen ausgewertet werden können.

Ergebnis: Sowohl die CDTD-App sowie die CDMA konnten erfolgreich umgesetzt werden. Damit stehen der Bank Vontobel AG nun zwei weitere Tools zur Verfügung, die die Überprüfung von potenziellen Vorfällen sowie das Führen einer entsprechenden Dokumentation vereinfacht. Mit diesen beiden Applikationen ist nun ein strukturierteres Vorgehen und Nachführen von Informationen gegeben.