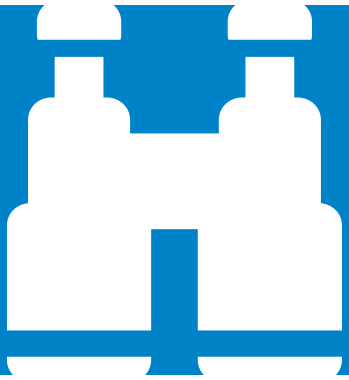
NetUSE AG

NetUSE SIEM Jumpstart

powered by graylog



In 3 Tagen zum Durchblick

Eine sinnvolle Aus- und Bewertung von Ereignissen aus sogenannten Logfiles gehört schon immer zu der Vervollständigung von Sicherheitsstrukturen im IT-Bereich und ist für viele Branchen mittlerweile verpflichtend zu installieren und zu betreiben. Hierfür wird eine Reihe von speziellen Systemen zu einem sogenannten SIEM (Security Information and Event Management) zusammengestellt. Die ersten Erkenntisse werden durch die Anbindung weniger Logquellen erreicht. Für einen Rundumblick sind mehr Logquellen zu integrieren.

Viele SIEM-Projekte scheitern nach wenigen Monaten, weil Ressourcen- und Lizenzbedarf jedes Budget sprengen.

> *Die ersten Ergebnisse werden durch die Anbindung weniger Logquellen generiert. Für einen Rundumblick sind immer mehr Logquellen zu integrieren. Bald ist mehr Hardware oder es sind teure Lizenzen erforderlich und trotzdem geht der Überblick verloren: Die Einbindung verschiedener Ereignissquellen führt zu vielen Fehlalarmen, die eine sinnvolle Arbeit mit dem SIEM-System verhindern.*

Ivo Heinecke, SOC-Spezialist der NetUSE AG.

Überblick gewinnen und behalten

Wir lieben Graylog! Im Laufe von Projekten und dem Betrieb unserer eigenen Plattform haben wir eine Reihe von Best Practices und Tools zusammengestellt. Diese maximieren den Nutzen bei Aufschaltung mehrerer Ereignisquellen durch eine sinnvolle Filterung – damit kommt man mit einer kleineren Ressourcenausstattung sehr viel weiter und sieht auch bei komplexen Logs die relevanten Dinge.

Unser Angebot: in 3 Tagen zum Durchblick

- Sie bekommen von uns anhand Ihrer Abschätzung ein Rezept für die erforderliche Infrastruktur – wo immer sie mögen, ob in Ihrer oder unserer Cloud oder im eigenen Rechenzentrum
- Als Vorbereitung für den Workshop installieren wir Ihre Graylog-Instanz
- Im Workshop integrieren wir mit Ihnen zusammen die ersten Logquellen und implementieren Filter und Alarme. Sie lernen bei der Implementierung, wie das geht
- Wenigen Wochen später schauen wir zusammen, welche Fragen aufgetaucht sind und wo wir gemeinsam optimieren können

Details zum Ablauf und den Voraussetzungen

Ablauf

- Wir ermitteln in einem Call Ihr ungefähres Logvolumen.
- Sie bekommen von uns eine Liste mit Ressourcen-anforderungen und Ports für die Anbindung an Logquellen und den Remote-Zugriff für unsere Experten (Nur für die Workshop-Zeit).
- Zum Workshopzeitpunkt haben wir Ihre Systeme vorbereitet.
- Im Workshop binden Sie gemeinsam mit unseren Experten Logquellen ein, passen das Dashboard an und definieren Alarme.
- Das SIEM läuft und wird mit Logfiles befüllt. Sie können die ersten Erfahrungen sammeln.
- Wir treffen uns zu einem zweiten Termin und schauen für einen halben Tag auf Fragestellungen, Optimierungsmöglichkeiten und weitere Logquellen.
- Optional können Sie uns als dauerhafte Begleitung buchen.

Voraussetzungen

- Zugriff für unsere Experten per SSH und http/https
- Firewallfreischaltungen für Logquellen zum SIEM
- E-Mail-Versand vom SIEM muss möglich sein (Alarme)
- Die Workshopteilnehmer müssen auf das SIEM zugreifen können
- Die Logquellen müssen während des Workshops auf das SIEM eingestellt werden
- Sollen Enterprise-Funktionen eingesetzt werden, muss die entsprechende Lizenz vorliegen

Leistungsumfang

- Installation von Graylog auf den Maschinen des Kunden (Best Practice für ein Cluster)
- Aufbau des Graylog, Verarbeitung erster Nachrichten, Ablage der Nachrichten in Streams und Index Sets
- Einführung in Pipelines, Dashboards, Alerts
- Einbindung der Parser für z.B. Cisco ASA
- Alle Arbeiten erfolgen remote
- Nachtreffen zum Workshop für Anpassungen und Optimierungen

Unser Angebot:
Pauschal einmalig

4.780,- Euro*
zzgl. ges. MwSt.

* inkl. 2 Tage Workshop sowie Zeiten für Vor- bzw. Nachbereitung und Nachbetreuung. Die Arbeiten finden remote statt.

NetUSE AG
NetUSE AG
Dr.-Hell-Straße 6
24107 Kiel
0431 2390-400
info@NetUSE.de
www.NetUSE.de