SCALTEL

SCALTEL
SMART BUILDING

SCALTEL
SNS-SYSTEMS

SCALCOM
E-BUSINESS

BACHELORARBEIT

ADRIAN GAST

TITEL

Threat Hunting- Analyse von Cyber Security Events

Weiterentwicklung der SCALTEL SECURITY Event Management Plattform

BESCHREIBUNG

Die SCALTEL AG betreibt ein Security Operations Center und unterstützt damit ihre mittelständischen Kunden beim Kampf gegen Cyber-Bedrohungen.
Neben den Produkten großer namhafter Hersteller, kommen vor allem in Schnittstellenbereichen, sowie im Bereich des Security Eventmanagements Eigenentwicklungen zum Einsatz.

Ziel der Arbeit ist die Weiterentwicklung der SCALTEL SECURITY Event Management Plattform.

MÖGLICHE SCHWERPUNKTE

- Analyse vorhandener Lösungen am Markt
- Erstellung eines Konzepts zur Automatisierung der Bearbeitung von Cyber Security Events (Weiterentwicklung der SCALTEL SOC Event Management Plattform)
- Erstellung eines Konzepts zur Analyse automatisch geschlossener Events (Automatisch geschlossene Events von Zeit zu Zeit überprüfen)
- Erstellung eines Konzepts zur Auswertung analysierter Events im Hinblick auf False-Positive Raten
- Unterstützung der Analysten durch Anreicherung der Events mit Informationen von externen Quellen

PERSONEN

- Autor
  - Adrian Gast (a.gast@criptext.com)
- Betreuer
  - Prof. Dr. Arnulf Deinzer (arnulf.deinzer@hs-kempten.de)
  - Stefan Jörg (stefan.joerg@scaltel.de)
  - Michael Schrem (michael.schrem@scaltel.de)

KONTAKT

- Scaltel AG
  - www.scaltel.de
- Persönlich
  - Email privat: a.gast@criptext.com
  - Email Hochschule: adrian.gast@stud.hs-kempten.de
  - Email Firma: adrian.gast@scaltel.de