

The SCALTEL logo consists of the word "SCALTEL" in a bold, white, sans-serif font. To the left of the text is a stylized icon of a mountain range with three peaks, also in white. The entire logo is set against a dark blue rectangular background.

SCALTEL

The SCALTEL SMART BUILDING logo features the word "SCALTEL" in a bold, white, sans-serif font, with a stylized mountain range icon to its left. Below "SCALTEL" is the text "SMART BUILDING" in a smaller, white, sans-serif font. The logo is on a dark blue background.

SCALTEL  
SMART BUILDING

The SCALTEL SNS-SYSTEMS logo features the word "SCALTEL" in a bold, white, sans-serif font, with a stylized mountain range icon to its left. Below "SCALTEL" is the text "SNS-SYSTEMS" in a smaller, white, sans-serif font. The logo is on a dark blue background.

SCALTEL  
SNS-SYSTEMS

The SCALCOM E-BUSINESS logo features the word "SCALCOM" in a bold, white, sans-serif font, with a stylized mountain range icon to its left. Below "SCALCOM" is the text "E-BUSINESS" in a smaller, white, sans-serif font. The logo is on a dark blue background.

SCALCOM  
E-BUSINESS

An abstract graphic on a dark grey background. It features a large, faint circle with a smaller circle inside it. A thin white line connects the center of the smaller circle to the top edge of the larger circle. A small white dot is located at the center of the smaller circle.

# 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](http://www.scaltel.de)
- Persönlich
  - Email privat: [a.gast@criptext.com](mailto:a.gast@criptext.com)
  - Email Hochschule: [adrian.gast@stud.hs-kempten.de](mailto:adrian.gast@stud.hs-kempten.de)
  - Email Firma: [adrian.gast@scaltel.de](mailto:adrian.gast@scaltel.de)