Visualisierung von Lagebildinformationen innerhalb eines Security Operating Centers

Vortrag zum Masterseminar-GSM

Gliederung

1. Einleitung
2. Security Operating Center
3. Aktuelle Situation in SOC´s
4. Abgrenzung und Ausblick

Einleitung

- Themenbeschreibung
- Motivation

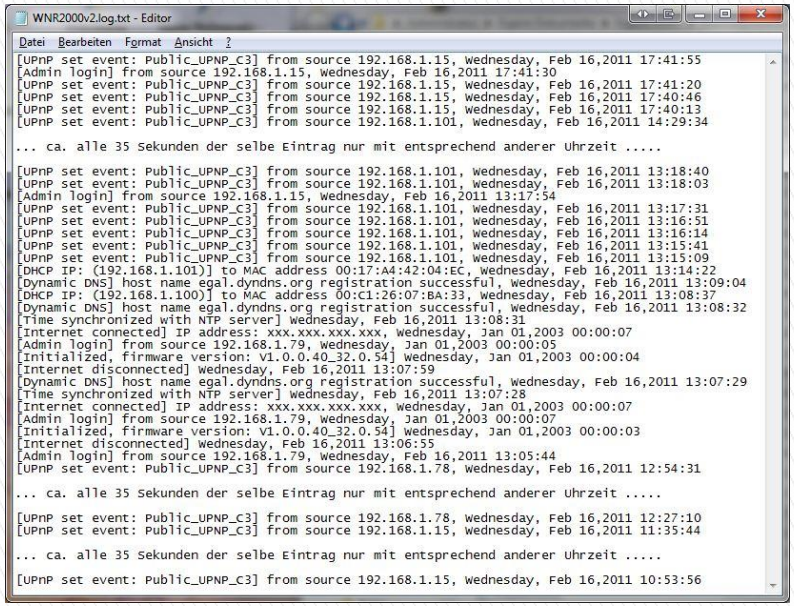
Themenbeschreibung

Ein SOC dient der Gefahrenabwehr von Cyberangriffen. Während meiner Arbeit möchte ich mich damit befassen, zu untersuchen wie das aktuelle Lagebild so visualisiert werden kann, dass es die aktuelle Lage des SOC dem definierten Betrachter[1] klar erkennbar wiedergibt und ihn so bei der Erfüllung seiner Aufgaben unterstützt.

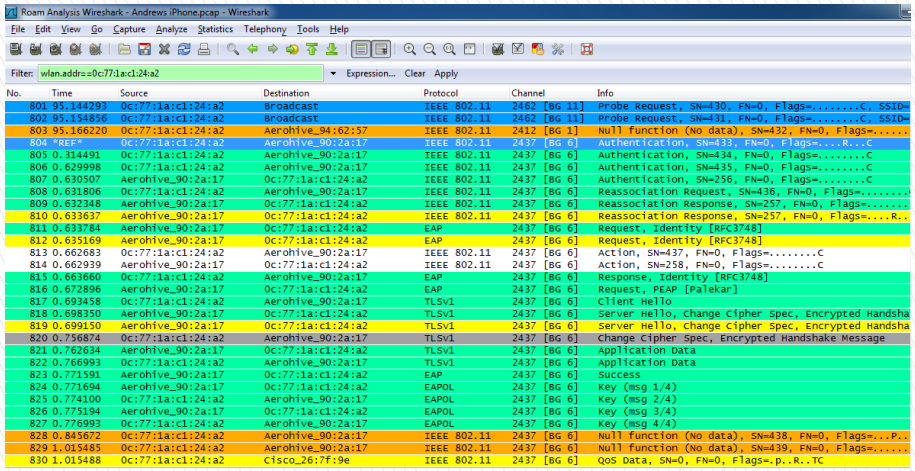
Betreuer: Prof. Dr. Klaus-Peter Kossakowski

[1] Mehrere definierte Benutzerrollen wie z.B. Analyst, Manager

Themenbeschreibung – Darstellung von Daten



[1]



[2]

Übersichtlich?

Themenbeschreibung – Verständnis der Darstellung

[3]

Wie wird das Dargestellte verstanden?

Ist das für jeden gleich verständlich?

Motivation

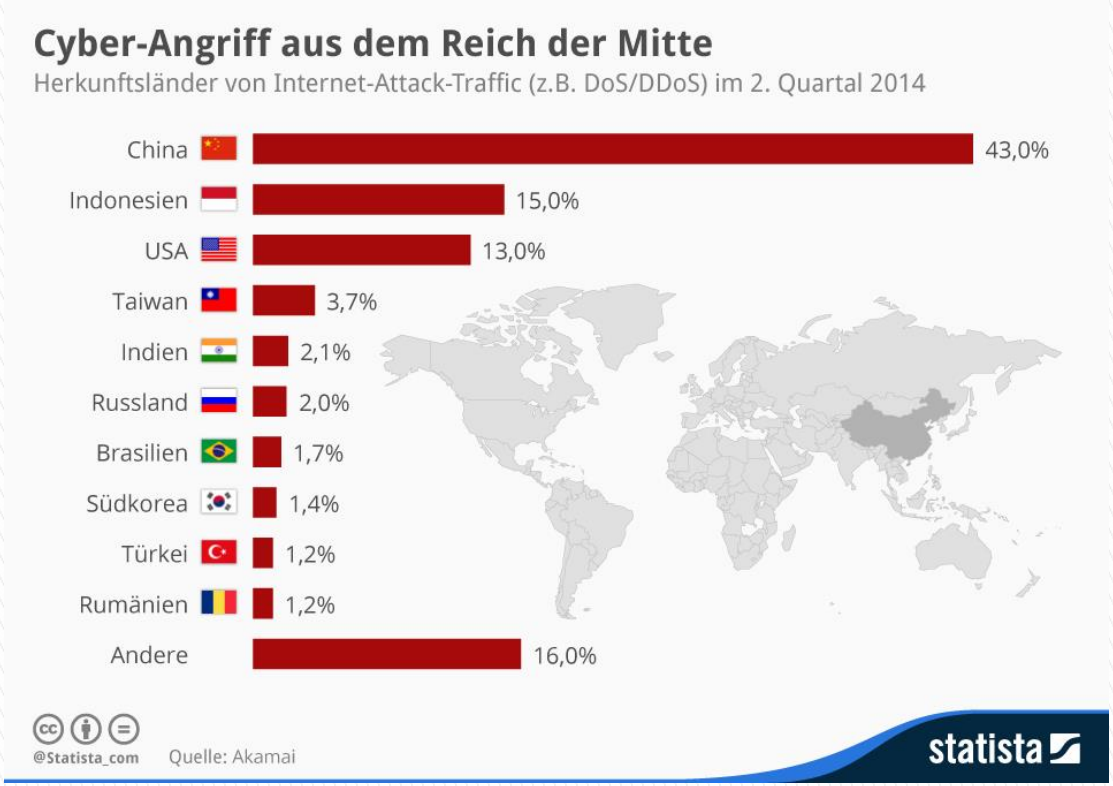
- WP IT-Sicherheit bei Prof. Dr.-Ing Martin Hübner
- Online Recherche zu Masterarbeiten in diesem Themenbereich

Security Operating Center

- Gründe für ein SOC
- Beschreibung
- Untersysteme
- Ausprägung
- Benutzer

[4]

Cybergefahren – Gründe für ein SOC



[5]

Heise-Security (09.12.14)

„Jedes zweite Unternehmen in den letzten drei Jahren Opfer von Angriffen […] Cyber-Straftaten seit 2007 verdoppelt."

[Hei14]

Beschreibung – Was ist ein SOC ?

"A SOC is a team primarily composed of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents." [Zim14]

Beschreibung – die Basisarbeit

Informationen sammeln

- Sensordaten
- Cyber-Intelligence
- News
- Attacken
- Tasks
- uvm.

Informationen analysieren

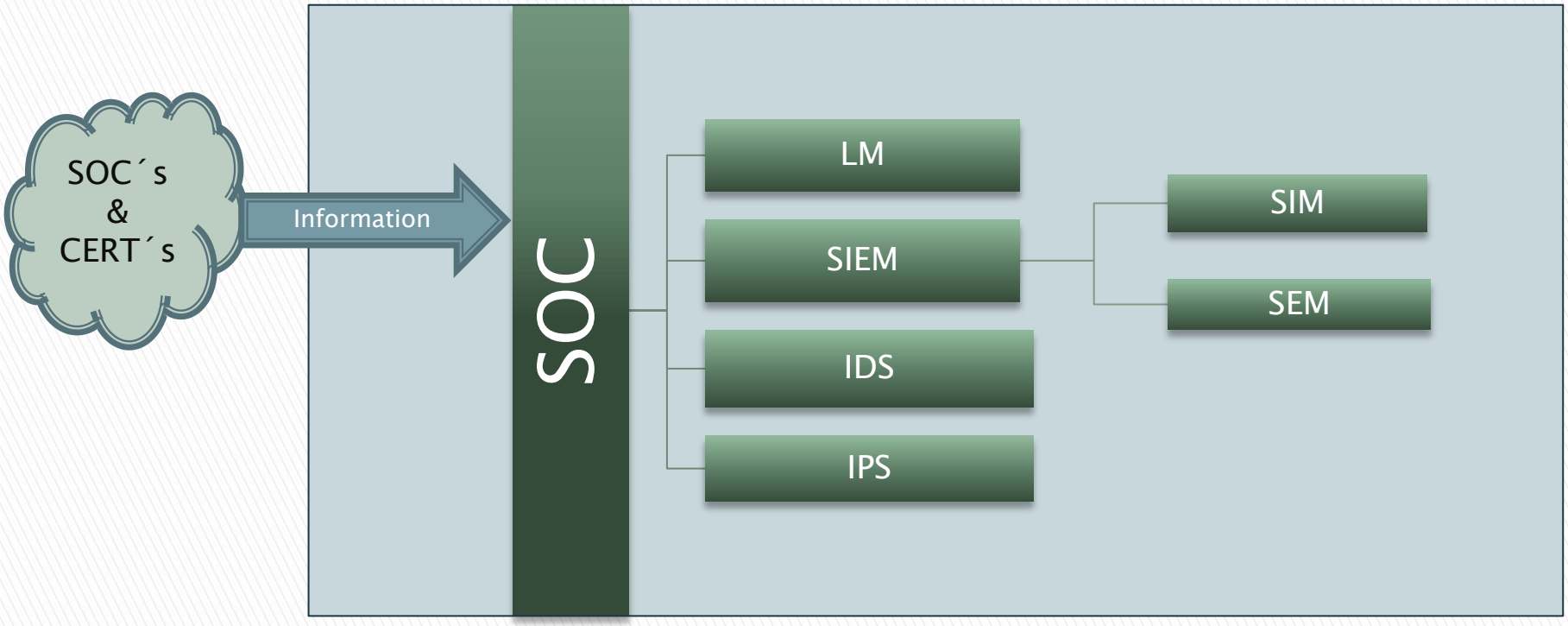
- Recherchieren, plausibilisieren, vorschlagen

Informationen visualisieren

- Aufbereiten der Informationen

OODA-Loop [Zim14]

Untersysteme – Thread Intelligence Feed



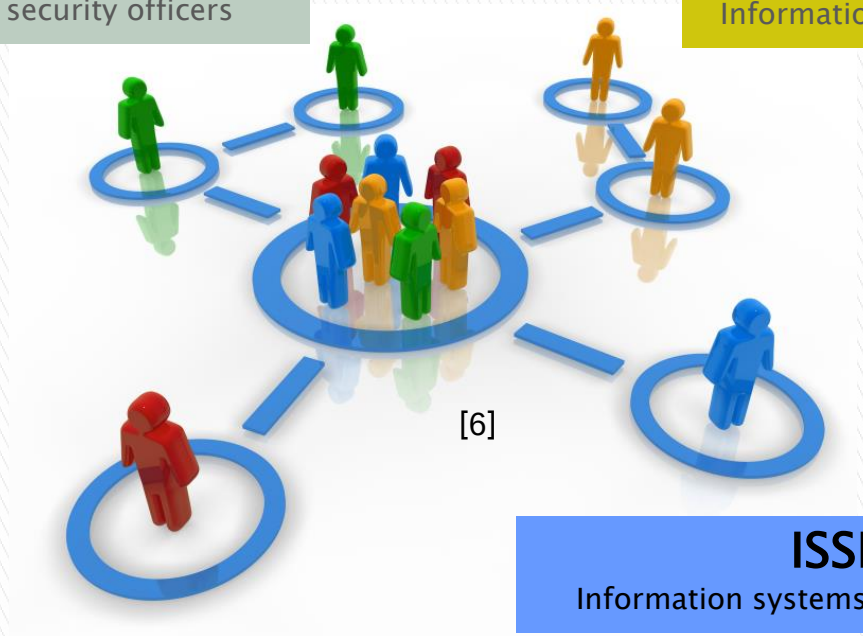
Ausprägungen – Arten von SOC´s

- **Security-Team.** Kleines Sicherheitsteam ohne größere automatisierte incident detection. I.d.R für < 1000 Benutzer oder IP´s
- **Internal distributed SOC.** Integriertes SOC aber mit externer Anbindung an SOC´s. Vorrangig für IT-Security aber weniger CND. Bei 500 – 5.000 Benutzern oder IP´s.
- **Internal centralized SOC.** Vollständiges SOC mit 24/7 Verfügbarkeit. Bei 5.000 – 100.000 Benutzern oder IP´s.
- **Internal combined distr. and centr. SOC.** Kombination aus beiden vorigen SOC´s. Für größere verteilte Netze, 25.000 – 500.000 Benutzer oder IP´s.
- **Coordinating SOC.** Bietet Beratungsleistung an andere Netze bzw SOC´s. Bieten auch Sicherheitsdienstleistungen an untergeordnete SOC´s, wie Threat Intelligence. Besser durch CERT´s.

Personal – Rollen innerhalb eines SOC´s

ISSOs
Information systems security officers

ISSEs
Information systems security engineers



[6]

ISSMs
Information systems security managers

CISOs
Chief information security officer

Aktuelle Situation

- Auf dem Markt gibt es eine Vielzahl kommerzieller SOC-Tools- Anbieter.
- Herstellerspezifische Entwicklungen von Benutzeroberflächen.
- Visualisierungen abhängig vom Produkt.

Beispiele für aktuelle SOC-Tools

[8]

Enterprise Security

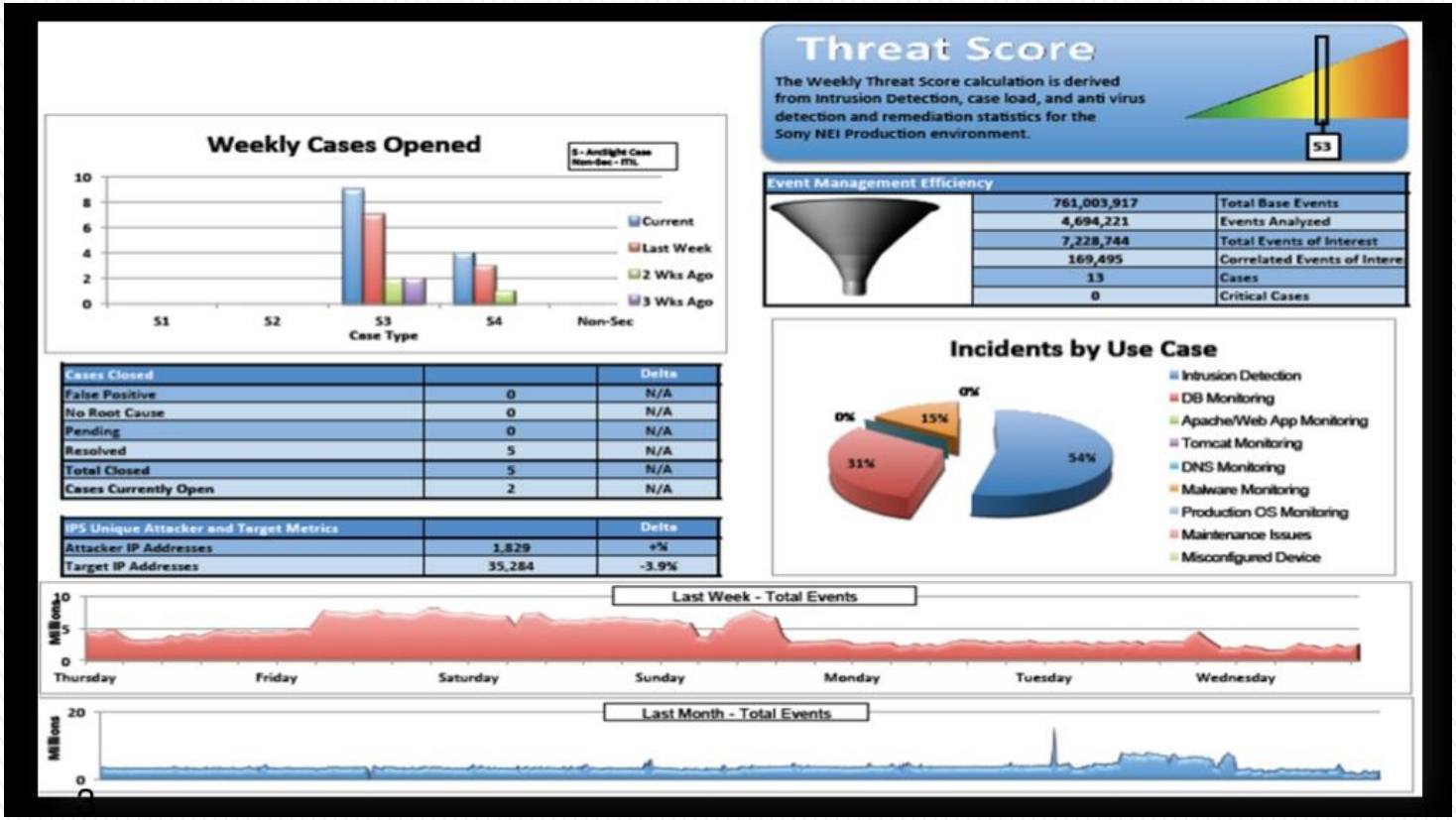
ALIEN VAULT

netIQ

McAfee
An Intel Company

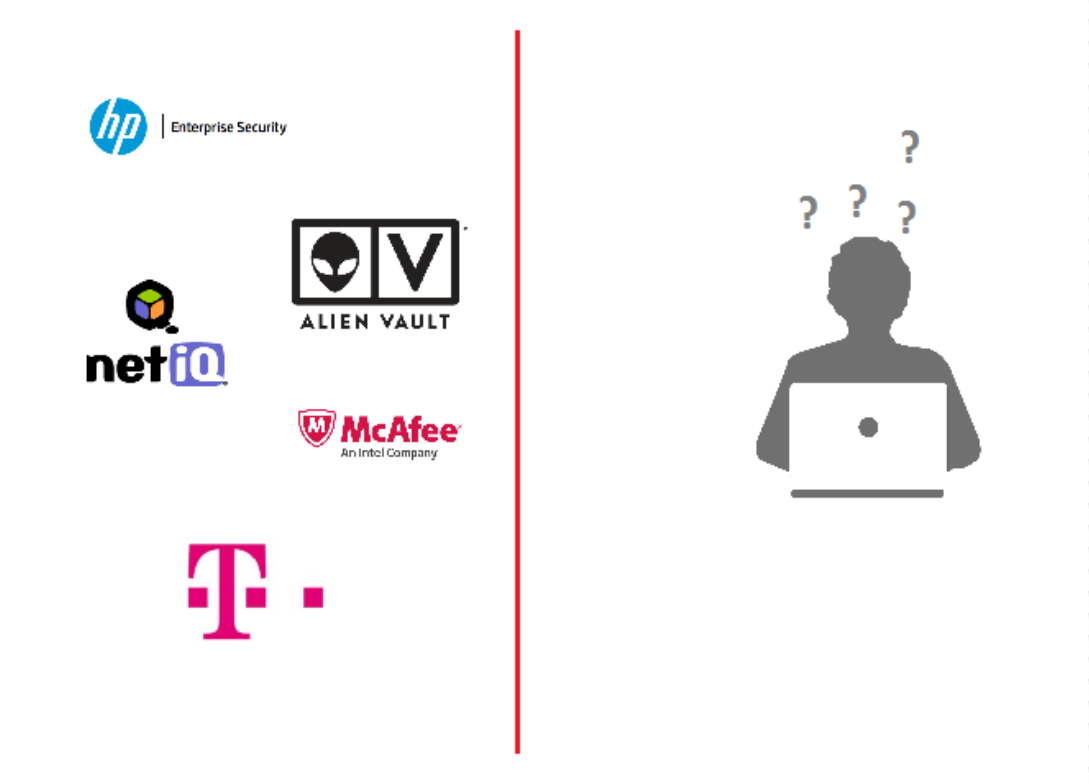
[7]

Beispiele für aktuelle SOC-Tools

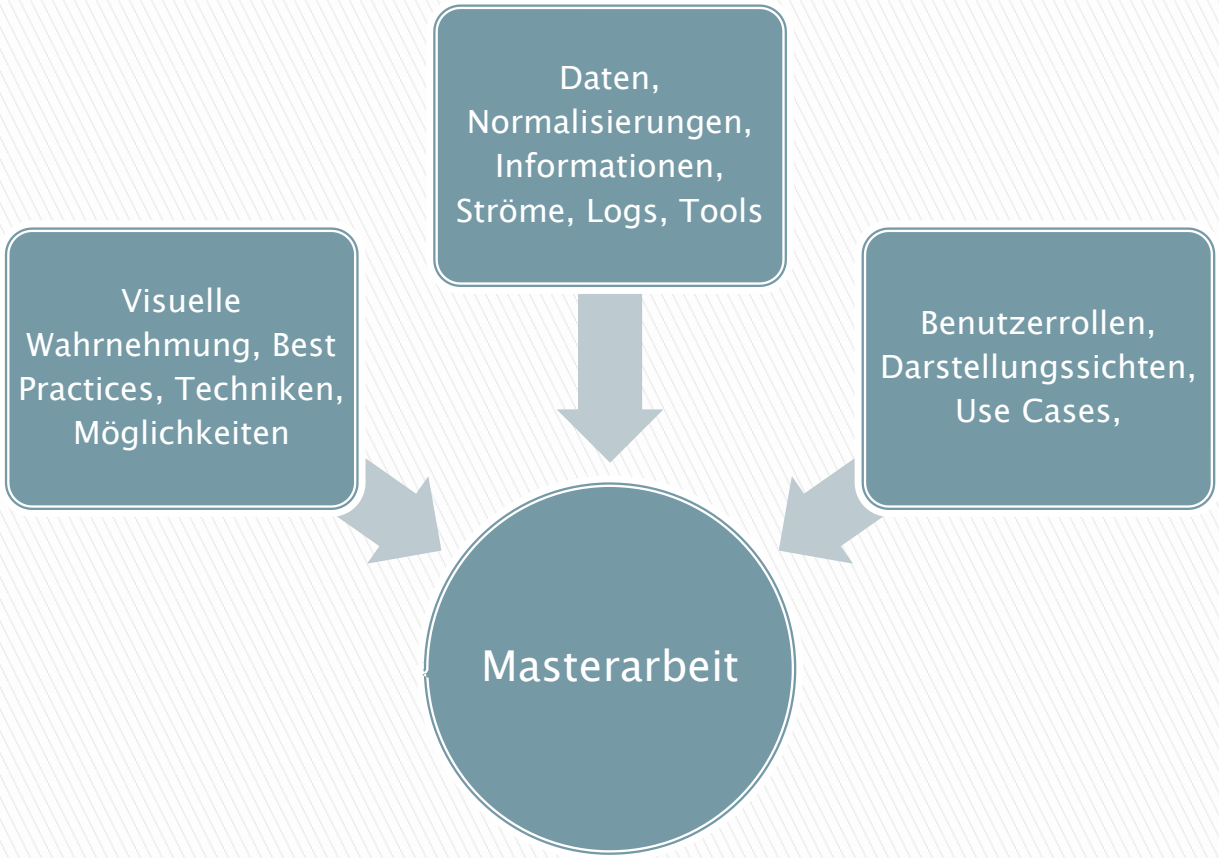


[9]

Abgrenzung und Ausblick



Wie grenzt sich die eigene Arbeit ab ?



Ausblick auf die eigene Arbeit

- Grundlagen guter Visualisierung?
- Wie können Lagedaten aggregiert werden?
- Wie sind diese zu normalisieren?
- rollenbasierte Datendarstellung.

Quellen

[Ali13] ALIENVAULT: *Practitioners Guide to SOC*: 2013. – online verfügbar unter: http://de.slideshare.net/alienvault/practioners-guide-to-soc – Abruf: 2014-12-08

[Hei14] HEISE-SECURITY: *Milliardenschäden für Firmen durch Wirtschaftsspione im Netz*: Heise Security , 09.12.2014. – online verfügbar unter http://www.heise.de/... – Abruf: 2014-12-09

[KKRZ03] KILLCRECE, Georgia; KOSSAKOWSKI, Klaus-Peter; RUEFLE, Robin; ZAJICEK, Mark: *Organizational Models for Computer Security Incident Response Teams (CSIRTs):* Software Engineering Institute, 2003. – online verfügbar unter: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6295 – Abruf: 2014-11-30

[Mai13] MAI, Matthias: *Was SIM und SEM von SIEM unterscheidet* : Computerwoche, 2013. – online verfügbar unter : http://www.computerwoche.de – Abruf: 2014-11-25

[Tel14] TELEKOM: *Advanced Cyber Defense by Telekom – Proaktive Gefahrenabwehr in Echtzeit*: T-Systems International, Frankfurt, 2014.

[Zim14] ZIMMERMANN, Carson: *Ten Strategies of a World-Class Cybersecurity Operations Center:* Mitre, 2014. – ISBN 978-0-692-24310-7 – online verfügbar unter : http://www.mitre.org/sites/default/files/publications – Abruf: 2014-11-03

Buchtip


MITRE
Ten Strategies of a World-Class
Cybersecurity Operations Center
Carson Zimmerman

Bildquellen

[1] http://thomasg.bplaced.net/bilder/router_log.jpg – Abruf: 2014-12-08

[2] http://support.connectblue.com – Abruf: 2014-12-06

[3] https://akihart.wordpress.com/2013/11/15/floodwarning-system-manila/ – Abruf: 2014-12-04

[4] https://www.bsi.bund.de – Abruf: 2014-12-05

[5] https://d28wbuch0jlv7v.cloudfront.net – Abruf: 2014-12-08

[6] http://affiliate-101.com/wp-content/uploads/2014/08/group_user_actions.jpg – Abruf: 2014-12-08

[7] Diverse Firmenlogos von den Firmenwebsites

[8] http://www.compuchannel.net/2009/08/12/netiq-2/ – Abruf: 2014-12-08

[9] http://de.slideshare.net/CERT-GOV-MD/awal-sioc-batrankov?next_slideshow=1 – Abruf: 2014-12-08

FRAGEN?