

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

Einleitung

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 Betrachter¹ 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

Einleitung

Themenbeschreibung – Darstellung von Daten

```
WNR2000v2.log.txt - Editor
Datei Bearbeiten Format Ansicht ?
[UPNP set event: Public_UPNP_C3] from source 192.168.1.15, wednesday, Feb 16,2011 17:41:55
[Admin login] from source 192.168.1.15, wednesday, Feb 16,2011 17:41:30
[UPNP set event: Public_UPNP_C3] from source 192.168.1.15, wednesday, Feb 16,2011 17:41:20
[UPNP set event: Public_UPNP_C3] from source 192.168.1.15, wednesday, Feb 16,2011 17:40:46
[UPNP set event: Public_UPNP_C3] from source 192.168.1.15, wednesday, Feb 16,2011 17:40:13
[UPNP set event: Public_UPNP_C3] from source 192.168.1.101, wednesday, Feb 16,2011 14:29:34
... ca. alle 35 Sekunden der selbe Eintrag nur mit entsprechend anderer Uhrzeit ....
[UPNP set event: Public_UPNP_C3] from source 192.168.1.101, wednesday, Feb 16,2011 13:18:40
[UPNP set event: Public_UPNP_C3] from source 192.168.1.101, wednesday, Feb 16,2011 13:18:03
[Admin login] from source 192.168.1.15, wednesday, Feb 16,2011 13:17:54
[UPNP set event: Public_UPNP_C3] from source 192.168.1.101, wednesday, Feb 16,2011 13:17:31
[UPNP set event: Public_UPNP_C3] from source 192.168.1.101, wednesday, Feb 16,2011 13:16:51
[UPNP set event: Public_UPNP_C3] from source 192.168.1.101, wednesday, Feb 16,2011 13:16:14
[UPNP set event: Public_UPNP_C3] from source 192.168.1.101, wednesday, Feb 16,2011 13:15:41
[UPNP set event: Public_UPNP_C3] from source 192.168.1.101, wednesday, Feb 16,2011 13:15:09
[DHCP IP: (192.168.1.100)] to MAC address 00:17:A4:42:04:1C, wednesday, Feb 16,2011 13:14:22
[Dynamic DNS] host name egal.dyndns.org registration successful, wednesday, Feb 16,2011 13:09:04
[DHCP IP: (192.168.1.100)] to MAC address 00:17:A4:42:04:1C, wednesday, Feb 16,2011 13:08:37
[Dynamic DNS] host name egal.dyndns.org registration successful, wednesday, Feb 16,2011 13:08:32
[Time synchronized with NTP server] wednesday, Feb 16,2011 13:08:31
[Internet connected] IP address: xxx.xxx.xxx.xxx, wednesday, Jan 01,2003 00:00:07
[Admin login] from source 192.168.1.79, wednesday, Jan 01,2003 00:00:05
[Initialized, firmware version: V1.0.0.40_32.0.54] wednesday, Jan 01,2003 00:00:04
[Internet disconnected] wednesday, Feb 16,2011 13:07:59
[Dynamic DNS] host name egal.dyndns.org registration successful, wednesday, Feb 16,2011 13:07:29
[Time synchronized with NTP server] wednesday, Feb 16,2011 13:07:28
[Internet connected] IP address: xxx.xxx.xxx.xxx, wednesday, Jan 01,2003 00:00:07
[Admin login] from source 192.168.1.79, wednesday, Jan 01,2003 00:00:07
[Initialized, firmware version: V1.0.0.40_32.0.54] wednesday, Jan 01,2003 00:00:03
[Internet disconnected] wednesday, Feb 16,2011 13:06:55
[Admin login] from source 192.168.1.79, wednesday, Feb 16,2011 13:05:44
[UPNP set event: Public_UPNP_C3] from source 192.168.1.78, wednesday, Feb 16,2011 12:54:31
... ca. alle 35 Sekunden der selbe Eintrag nur mit entsprechend anderer Uhrzeit ....
[UPNP set event: Public_UPNP_C3] from source 192.168.1.78, wednesday, Feb 16,2011 12:27:10
[UPNP set event: Public_UPNP_C3] from source 192.168.1.15, wednesday, Feb 16,2011 11:35:44
... ca. alle 35 Sekunden der selbe Eintrag nur mit entsprechend anderer Uhrzeit ....
[UPNP set event: Public_UPNP_C3] from source 192.168.1.15, wednesday, Feb 16,2011 10:53:56
```

[1]

Room Analysis Wireshark - Andros iPhone.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: wlan.address==0c77:1a:c1:24:a2 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Channel	Info
801	95.144293	0c77:1a:c1:24:a2	Broadcast	IEEE 802.11	2462 [Bg 1]	Probe Request, SN=430, FN=0, Flags=.....C, SSID=
802	95.154856	0c77:1a:c1:24:a2	Broadcast	IEEE 802.11	2462 [Bg 1]	Probe Request, SN=431, FN=0, Flags=.....C, SSID=
803	95.166220	0c77:1a:c1:24:a2	Aerohive_90:2a:17	IEEE 802.11	2412 [Bg 1]	Null function (No data), SN=432, FN=0, Flags=.....C
804	0.154856	0c77:1a:c1:24:a2	Aerohive_90:2a:17	IEEE 802.11	2437 [Bg 6]	Authentication, SN=433, FN=0, Flags=.....C
805	0.314491	0c77:1a:c1:24:a2	Aerohive_90:2a:17	IEEE 802.11	2437 [Bg 6]	Authentication, SN=434, FN=0, Flags=.....C
806	0.629998	0c77:1a:c1:24:a2	Aerohive_90:2a:17	IEEE 802.11	2437 [Bg 6]	Authentication, SN=435, FN=0, Flags=.....C
807	0.630507	Aerohive_90:2a:17	0c77:1a:c1:24:a2	IEEE 802.11	2437 [Bg 6]	Authentication, SN=256, FN=0, Flags=.....C
808	0.631866	0c77:1a:c1:24:a2	Aerohive_90:2a:17	IEEE 802.11	2437 [Bg 6]	Reassociation Request, SN=436, FN=0, Flags=.....C
809	0.632348	Aerohive_90:2a:17	0c77:1a:c1:24:a2	IEEE 802.11	2437 [Bg 6]	Reassociation Response, SN=257, FN=0, Flags=.....C
810	0.633637	Aerohive_90:2a:17	0c77:1a:c1:24:a2	IEEE 802.11	2437 [Bg 6]	Reassociation Response, SN=257, FN=0, Flags=.....C
811	0.633784	Aerohive_90:2a:17	0c77:1a:c1:24:a2	EAP	2437 [Bg 6]	Request, Identity [RFC3748]
812	0.635169	Aerohive_90:2a:17	0c77:1a:c1:24:a2	EAP	2437 [Bg 6]	Request, Identity [RFC3748]
813	0.662683	0c77:1a:c1:24:a2	Aerohive_90:2a:17	IEEE 802.11	2437 [Bg 6]	Action, SN=437, FN=0, Flags=.....C
814	0.662939	Aerohive_90:2a:17	0c77:1a:c1:24:a2	IEEE 802.11	2437 [Bg 6]	Action, SN=258, FN=0, Flags=.....C
815	0.663660	0c77:1a:c1:24:a2	Aerohive_90:2a:17	EAP	2437 [Bg 6]	Response, Identity [RFC3748]
816	0.672896	Aerohive_90:2a:17	0c77:1a:c1:24:a2	EAP	2437 [Bg 6]	Request, PEAP [Palekar]
817	0.693458	0c77:1a:c1:24:a2	Aerohive_90:2a:17	TLSv1	2437 [Bg 6]	Client Hello
818	0.698350	Aerohive_90:2a:17	0c77:1a:c1:24:a2	TLSv1	2437 [Bg 6]	Server Hello, Change cipher spec, encrypted Handsha
819	0.699150	Aerohive_90:2a:17	0c77:1a:c1:24:a2	TLSv1	2437 [Bg 6]	Server Hello, Change cipher spec, encrypted Handsha
820	0.756874	0c77:1a:c1:24:a2	Aerohive_90:2a:17	TLSv1	2437 [Bg 6]	Change Cipher Spec, Encrypted Handshake Message
821	0.762634	Aerohive_90:2a:17	0c77:1a:c1:24:a2	TLSv1	2437 [Bg 6]	Application Data
822	0.766993	0c77:1a:c1:24:a2	Aerohive_90:2a:17	TLSv1	2437 [Bg 6]	Application Data
823	0.771591	Aerohive_90:2a:17	0c77:1a:c1:24:a2	EAP	2437 [Bg 6]	Success
824	0.771694	Aerohive_90:2a:17	0c77:1a:c1:24:a2	EAPOL	2437 [Bg 6]	Key (msg 1/4)
825	0.774100	0c77:1a:c1:24:a2	Aerohive_90:2a:17	EAPOL	2437 [Bg 6]	Key (msg 2/4)
826	0.775194	Aerohive_90:2a:17	0c77:1a:c1:24:a2	EAPOL	2437 [Bg 6]	Key (msg 3/4)
827	0.776993	0c77:1a:c1:24:a2	Aerohive_90:2a:17	EAPOL	2437 [Bg 6]	Key (msg 4/4)
828	0.845672	0c77:1a:c1:24:a2	Aerohive_90:2a:17	IEEE 802.11	2437 [Bg 6]	Null function (No data), SN=438, FN=0, Flags=.....C
829	1.015485	0c77:1a:c1:24:a2	Aerohive_90:2a:17	IEEE 802.11	2437 [Bg 6]	Null function (No data), SN=439, FN=0, Flags=.....C
830	1.015488	0c77:1a:c1:24:a2	Cisco_26:7f:19e	IEEE 802.11	2437 [Bg 6]	QoS Data, SN=0, FN=0, Flags=p..R..TC

[2]

Übersichtlich?

Einleitung

Themenbeschreibung – Verständnis der Darstellung



Wie wird das Dargestellte verstanden?

Ist das für jeden gleich verständlich?

[3]

RED WARNING	 More than 30mm rain observed in 1 hour and expected to continue in the next 2 hours	 Serious flooding expected in low lying areas	RESPONSE: EVACUATION
GREEN WARNING	 15-30mm (intense) rain observed in 1 hour and expected to continue in the next 2 hours	 Flooding is threatening	RESPONSE: ALERT for possible evacuation
YELLOW WARNING	 7.5-15mm (heavy) rain observed in 1 hour and expected to continue in the next 2 hours	 Flooding is possible	RESPONSE: MONITOR the weather conditions

Einleitung

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

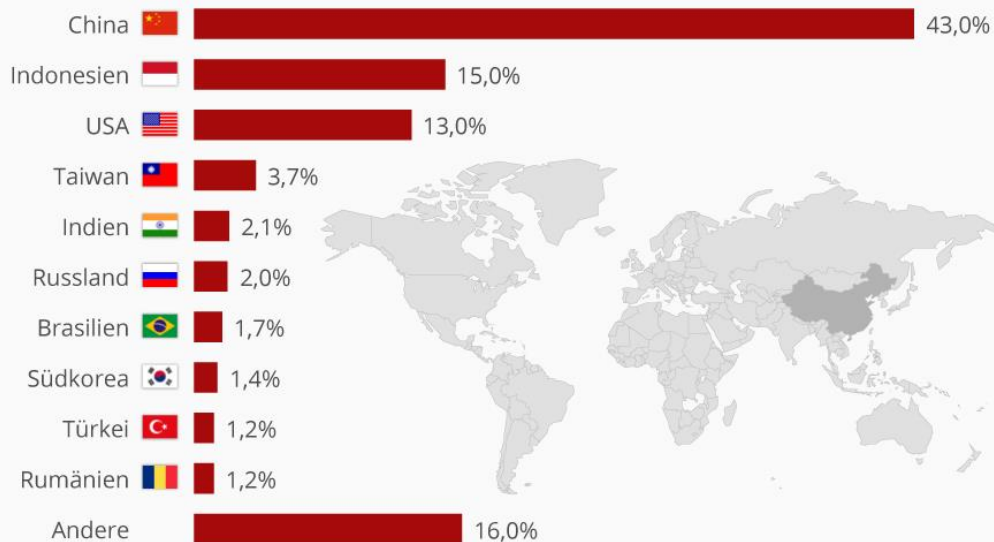


[4]

Cybergefahren – Gründe für ein SOC

Cyber-Angriff aus dem Reich der Mitte

Herkunftsländer von Internet-Attack-Traffic (z.B. DoS/DDoS) im 2. Quartal 2014



Heise-Security (09.12.14)

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

[Hei14]

[5]

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

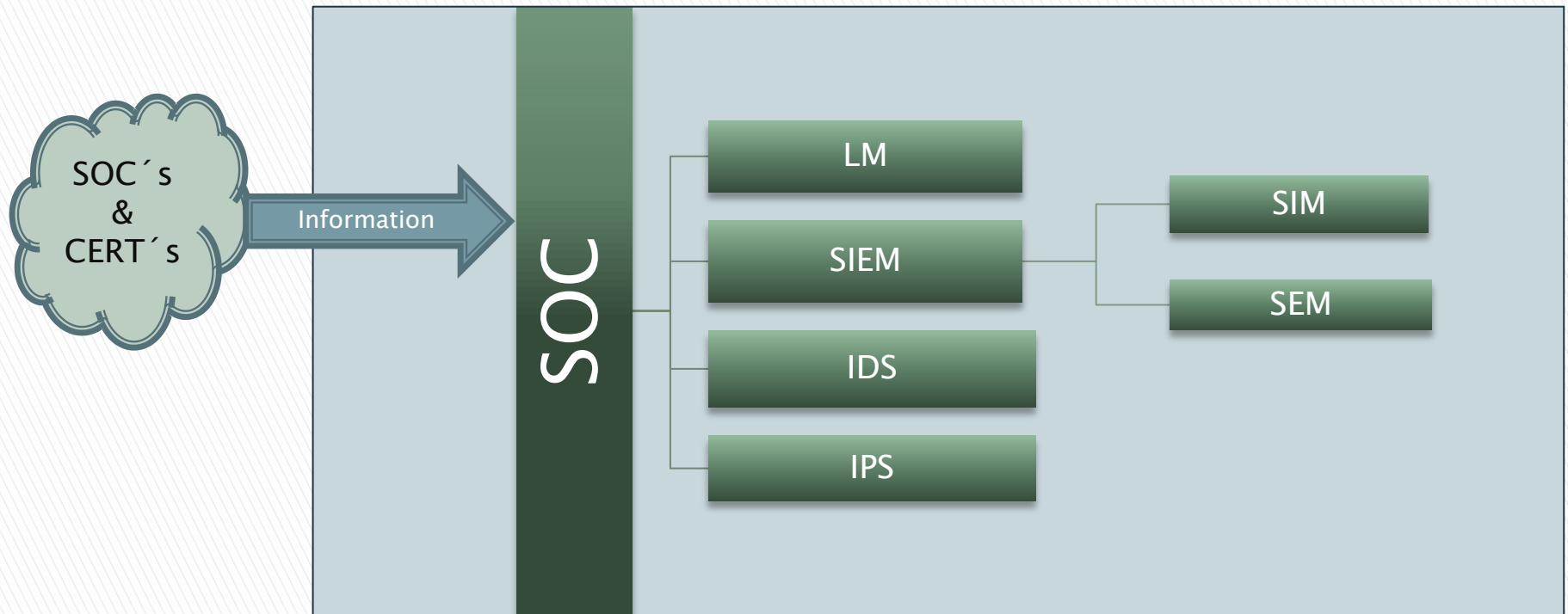
Informationen visualisieren

- 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.

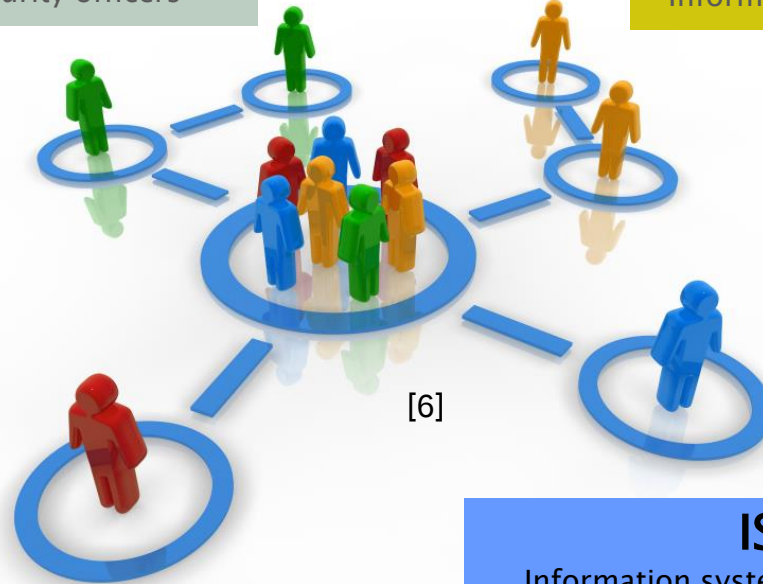
Personal – Rollen innerhalb eines SOC's

ISSOs

Information systems security officers

ISSEs

Information systems security engineers



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.

Aktuelle Situation

Beispiele für aktuelle SOC-Tools



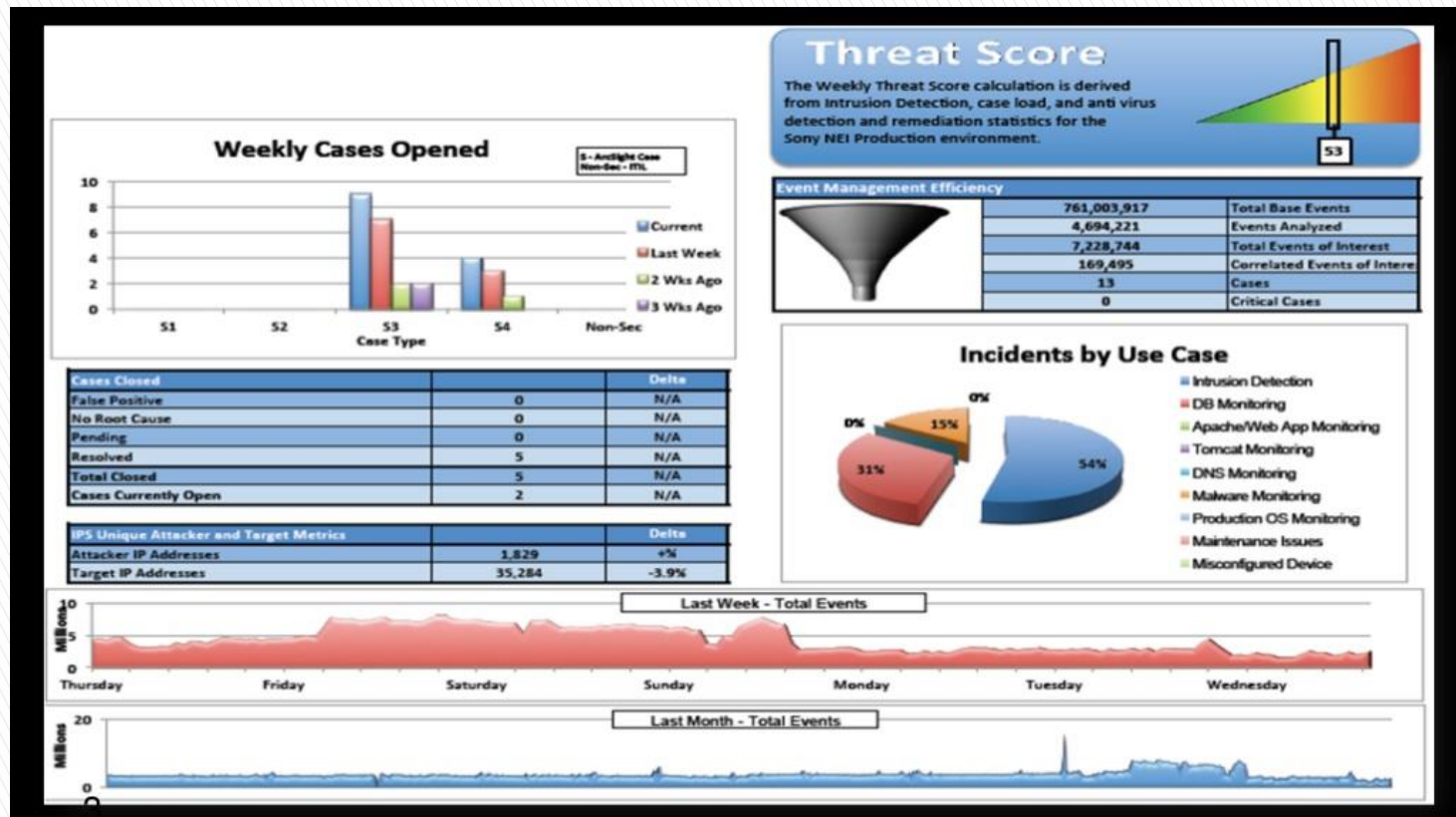
[8]



[7]

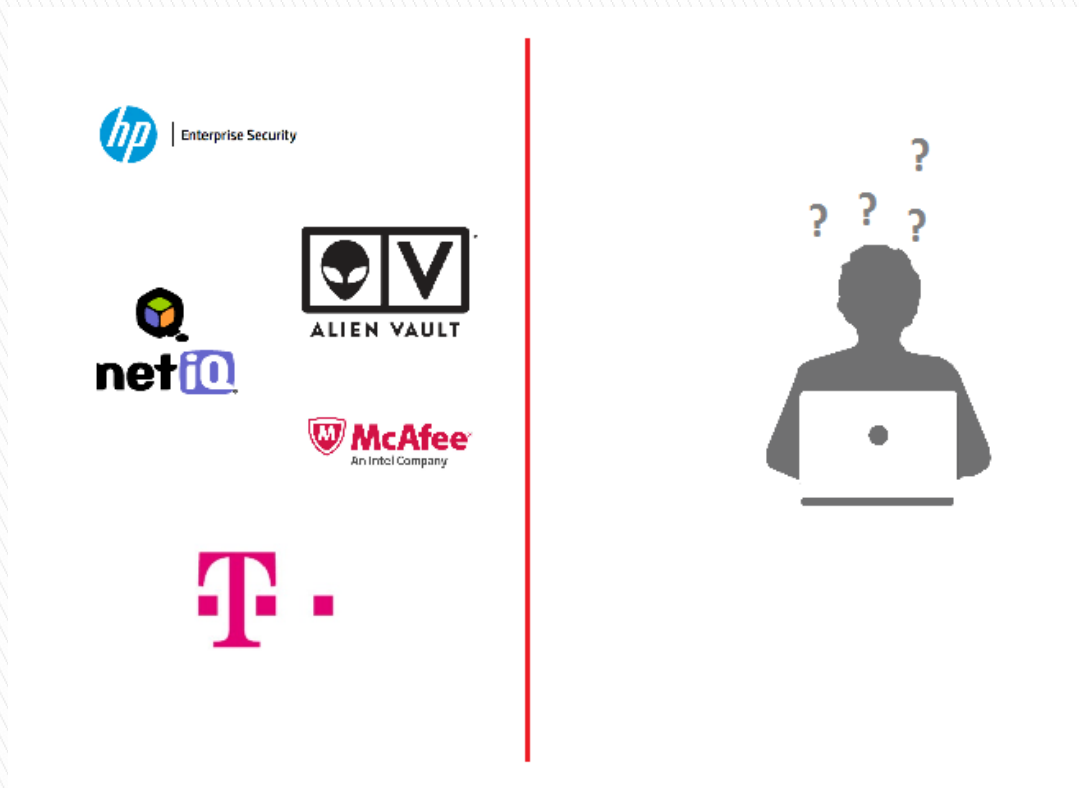
Aktuelle Situation

Beispiele für aktuelle SOC-Tools

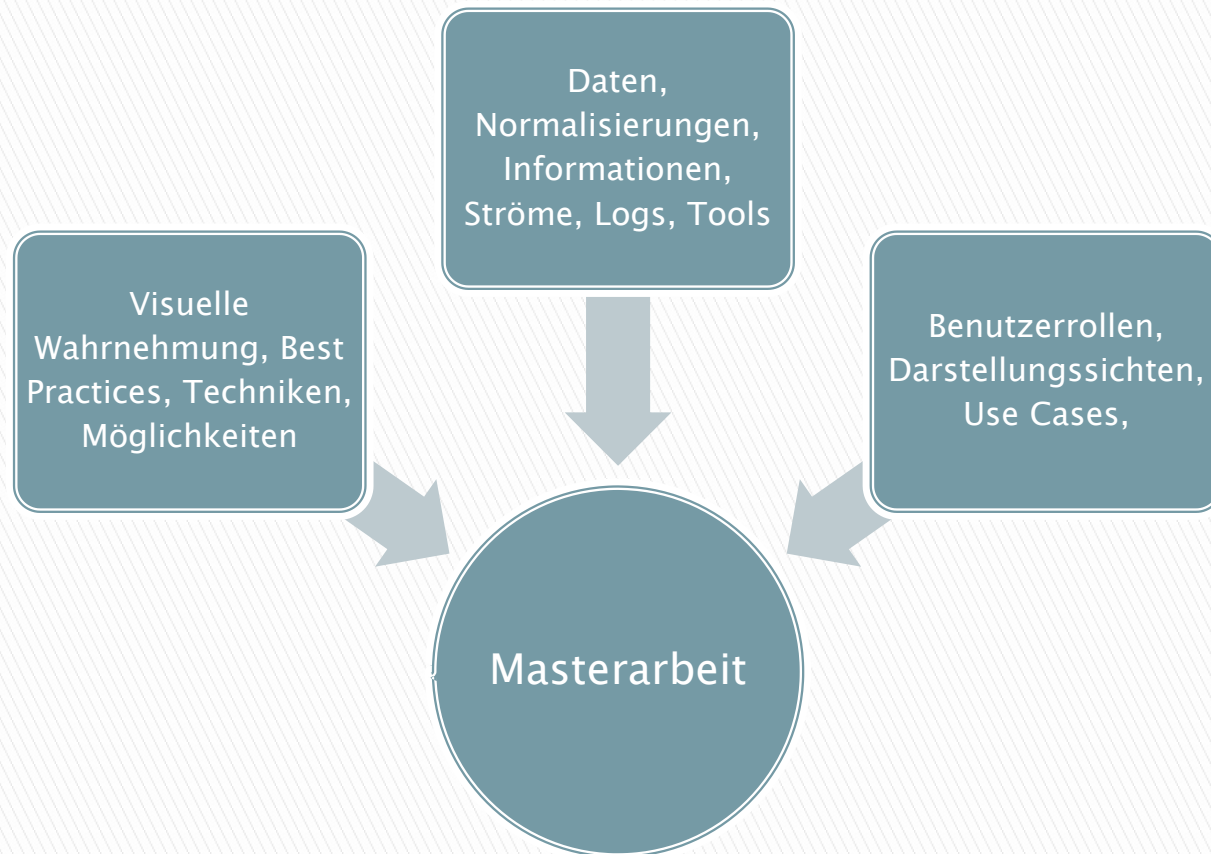


[9]

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



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?