

IT-Security – NETEYE – SIEM

Monitoring für eine unsichere Welt...

BR24

Coronavirus Bayern Sport BR24-Newsletter Wirtschaft Kultur Wissen Netzwelt #Faktenfuchs

DEUTSCHLAND & WELT



15.04.2020, 06:38 Uhr

Cyberkriminalität: Wie Hacker die Corona-Krise nutzen

Die Corona-Pandemie bedroht die Menschen - nicht nur im realen Leben. Mitten im Kampf gegen Covid-19 greifen Kriminelle im Netz an und nutzen Schwachstellen in Computersystemen. Selbst vor Attacken auf Kliniken schrecken sie nicht zurück.

Das Pop-Up, das plötzlich auf dem Bildschirm erscheint, zeigt das Coronavirus. Dort ist zu lesen:

<https://www.br.de/nachrichten/deutschland-welt/cyberkriminalitaet-wie-hacker-die-corona-krise-nutzen,Rw8tgnl>



**Hochzeit für Hacker –
oder wie Covid-19 das
Geschäft mit Cyber Crime
antreibt!**

Die Corona-Krise im Focus von CyberCrime oder warum Geschwindigkeit zählt!



- Hacker haben unglaublich schnell auf die Krise reagiert und haben global unzählige Aktivitäten ausgeführt
- Firmen haben – um ihren Mitarbeiterinnen und Mitarbeitern eine Arbeitskontinuität zu bieten – viele mühsam etablierte Sicherheitsmechanismen abgeschaltet (-> Zugriff von außen auf die Firmen IT muss möglich sein)
- Hacker nutzen dies aus: wenn Sie nicht sehr schnell mit entsprechenden Gegenmaßnahmen wie z.B. Monitoring (wissen was geschieht) reagieren, ist es nur eine Frage der Zeit...



Corona-Krise im Fokus von CyberCrime

Wie die „bösen Jungs“ die Situation schamlos ausnutzen...



Erpresserschreiben auch an Spahn: Hacker greifen in Coronakrise verstärkt Krankenhäuser an

Betrüger und Hacker nutzen angespannte Lage in Krankenhäusern, zeigen interne Behördenberichte. Viele Kliniken sind darauf womöglich nicht vorbereitet.



Jürgen Klöckner



Julian Oik



Britta Rybicki

09.04.2020 - 03:59 Uhr • 1 Kommentar • 14 x geteilt



<https://www.handelsblatt.com/technik/medizin/cyberkriminalitaet-erpresserschreiben-auch-an-spahn-hacker-greifen-in-coronakrise-verstaerkt-krankenhaeuser-an/25726550.html?ticket=ST-234951-Oe6CPI5fzYo2BXIELM2d-an3>

Erpressung



Update: Cyberkriminelle nutzen Corona aus

Die Corona-Krise nimmt Einfluss auf die Methoden von Cyber-Kriminellen. So warnt die Verbraucherzentrale NRW zum Beispiel vor [gefälschten E-Mails der Sparkasse](#), worin Kundinnen und Kunden zur Eingabe ihrer persönlichen Daten aufgefordert werden. Die E-Mail gibt vor, dass die Übermittlung persönlicher Daten an die Sparkasse notwendig sei, um in Zeiten der Corona-Krise auch per Chat mit der Bank in Verbindung bleiben zu können. Über einen Link werden Betroffene auf eine authentisch aussehende Eingabemaske geleitet, die die Daten nach der Eingabe direkt an Betrüger sendet (s. Abbildung).

Umgang mit dem COVID-19-Erreger

18. März 2020 um 07:27



Phishing

Sehr geehrte Kundinnen und Kunden,

Ihre Sicherheit und Gesundheit und auch die unserer Mitarbeiter liegt uns sehr am Herzen.

Vor diesem Hintergrund haben wir uns dafür entschieden, unsere kleineren Filialen

<https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/corona-falschmeldungen.html>

Malware-Kampagne zielt auf Coronavirus-Infos

Facebook Twitter WhatsApp Pocket E-Mail



MalwareHunterTeam @malwrhunterteam · 3. März

"Corona-virus.exe" installer -> "Corona-virus-Map\com.exe"
(2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307) -> different malware samples + decoy viewer.
Has "FiasskHard Work CLIPPER + STEALER" & something (AZO?) w/ C2:
[http://coronavirusstatus\[.\]space/index.php](http://coronavirusstatus[.]space/index.php)



10

84

150



[Diesen Thread anzeigen](#)

Malware

Die täuschend echte, aber Malware-verse

14.03.2020, 19:28 Uhr

Sicherheitsforscher haben
gemacht, bei der Hacker
Coronavirus-Karte verst
Daten.

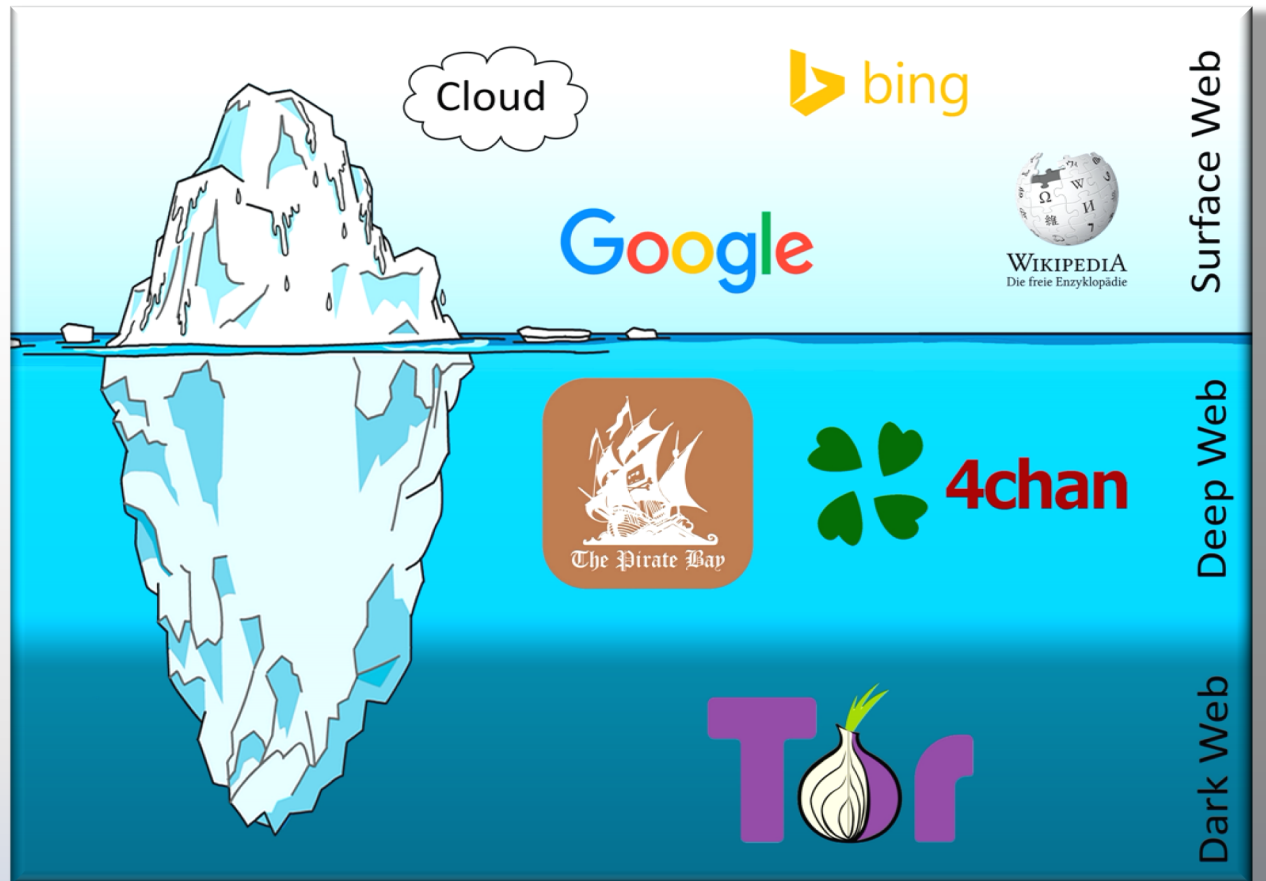
<https://t3n.de/news/malware-kan>

Aktuelle Situation im Überblick

- Firmen und Unternehmen fahren teilweise ihre Schutzschilde herunter, um jedem Mitarbeiter „homeoffice“ zu ermöglichen (Beispiel OWA und VPN)
- Die „bösen Jungs“ reagierten sehr schnell...
- Viele Firmen wissen nicht, was in ihren Netzwerken passiert
- Firewalls und andere, wichtige Geräte (Router, Switches, Server) werden nicht oder nur ungenügend kontrolliert und überwacht
- „Leichtes Spiel“ für Malware aller Art, z.B. für RAT's

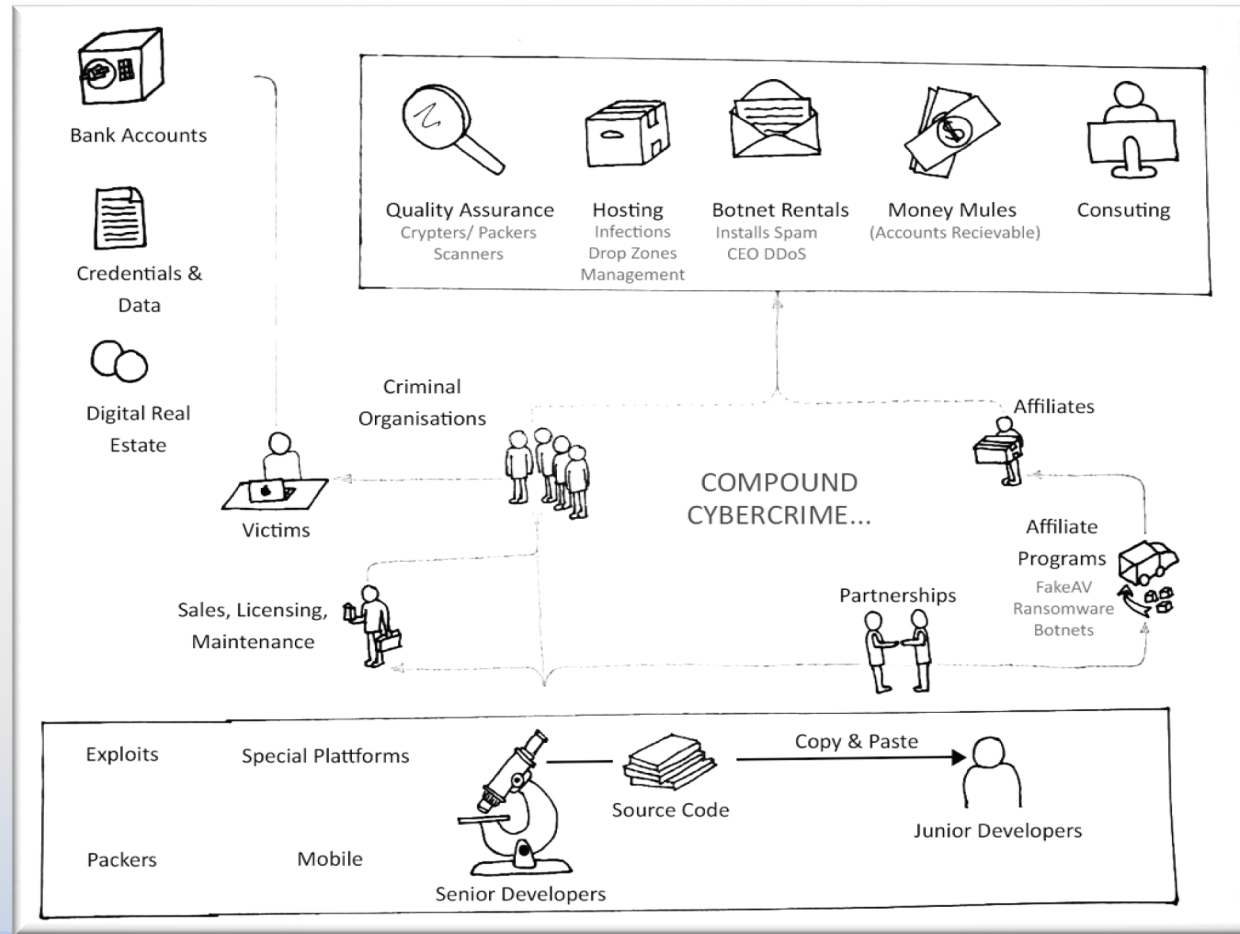


Markt für Informationen aller Art...



Darknet

Industrie für CyberCrime (organisierte Kriminalität)



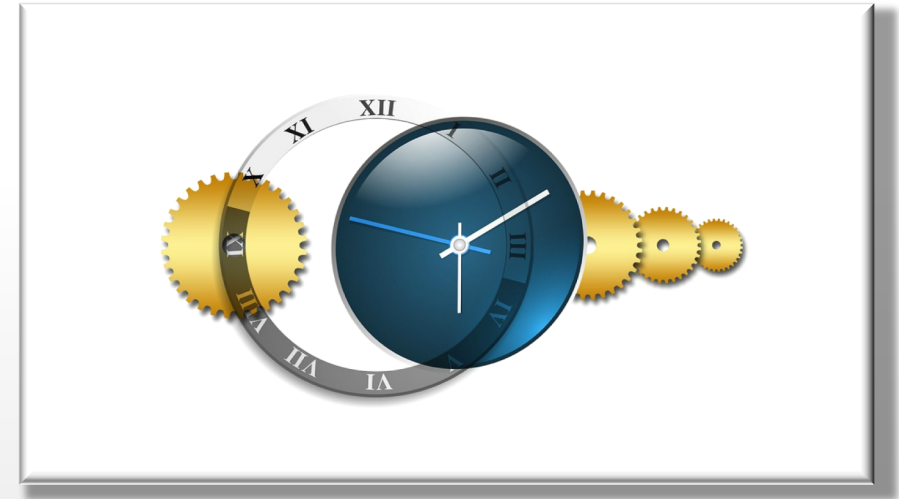
- Für jeden Teilbereich gibt es entsprechende Spezialisten:
- Programmierer
 - Verteiler
 - Akquise von Opfern
 - Geldwäsche
 - Technische Unterstützung
 - Usw.

Wer hier bestehen will, muss schnell sein!



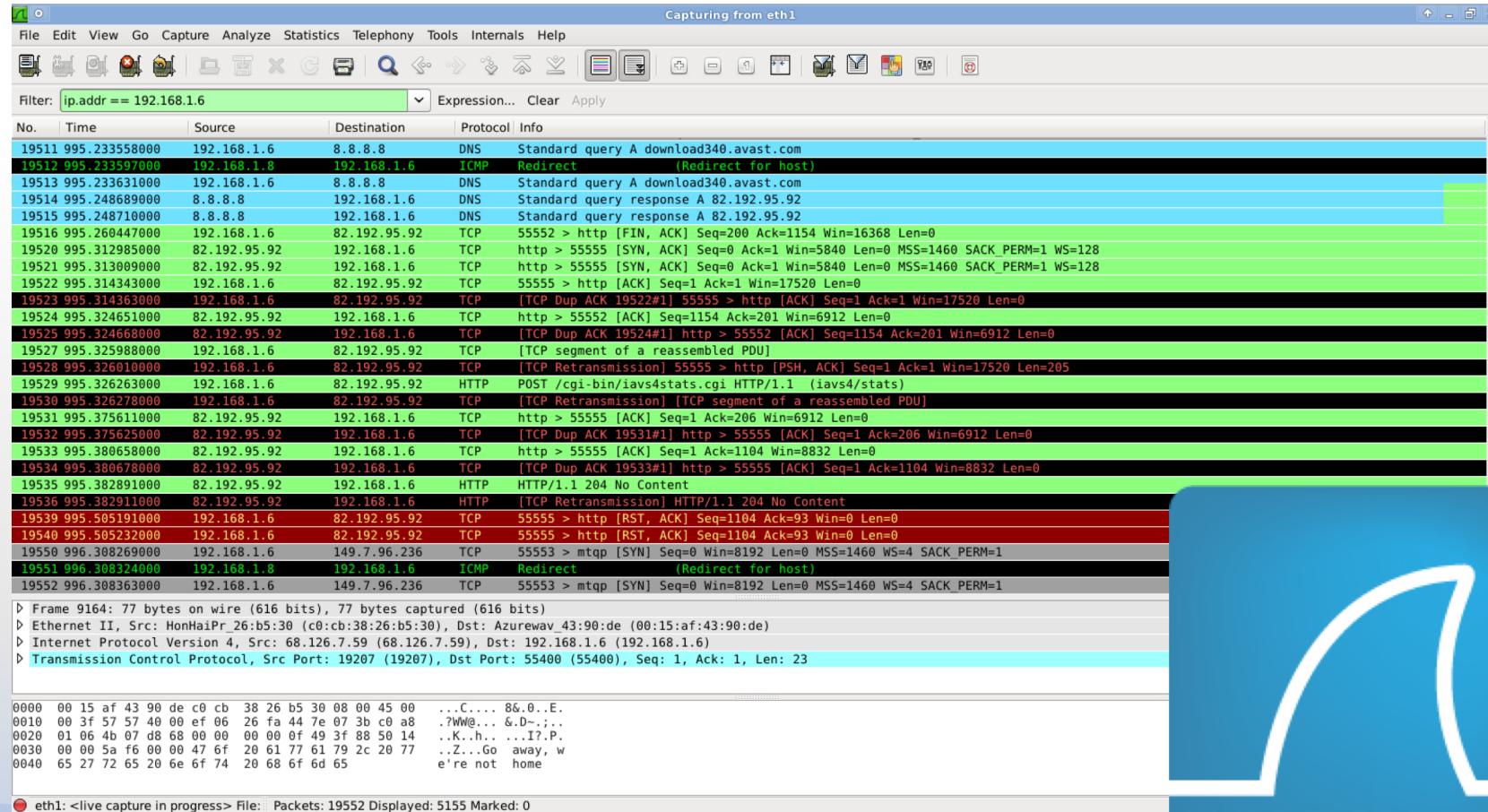
Für die Abwehr notwendig:

- Erkennen
- Reagieren
- Abwehren
- Pro-Aktive Abwehr Strategien entwickeln



Time is security...

Was geschieht in meinem Netzwerk?



The image shows a Wireshark network traffic capture window. The title bar reads "Capturing from eth1". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture, and analysis. The filter bar shows "ip.addr == 192.168.1.6". The packet list pane displays a table of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The packet details pane shows the selected packet (No. 19552) with its Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol details. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
19511	995.233558000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19512	995.233597000	192.168.1.6	192.168.1.6	ICMP	Redirect (Redirect for host)
19513	995.233631000	192.168.1.6	8.8.8.8	DNS	Standard query A download340.avast.com
19514	995.248689000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19515	995.248710000	8.8.8.8	192.168.1.6	DNS	Standard query response A 82.192.95.92
19516	995.260447000	192.168.1.6	82.192.95.92	TCP	55552 > http [FIN, ACK] Seq=200 Ack=1154 Win=16368 Len=0
19520	995.312985000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19521	995.313009000	82.192.95.92	192.168.1.6	TCP	http > 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
19522	995.314343000	192.168.1.6	82.192.95.92	TCP	55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19523	995.314363000	192.168.1.6	82.192.95.92	TCP	[TCP Dup ACK 19522#1] 55555 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
19524	995.324651000	82.192.95.92	192.168.1.6	TCP	http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19525	995.324668000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19524#1] http > 55552 [ACK] Seq=1154 Ack=201 Win=6912 Len=0
19527	995.325988000	192.168.1.6	82.192.95.92	TCP	[TCP segment of a reassembled PDU]
19528	995.326010000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] 55555 > http [PSH, ACK] Seq=1 Ack=1 Win=17520 Len=205
19529	995.326263000	192.168.1.6	82.192.95.92	HTTP	POST /cgi-bin/iavs4stats.cgi HTTP/1.1 (iavs4/stats)
19530	995.326278000	192.168.1.6	82.192.95.92	TCP	[TCP Retransmission] [TCP segment of a reassembled PDU]
19531	995.375611000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19532	995.375625000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19531#1] http > 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0
19533	995.380658000	82.192.95.92	192.168.1.6	TCP	http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19534	995.380678000	82.192.95.92	192.168.1.6	TCP	[TCP Dup ACK 19533#1] http > 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=0
19535	995.382891000	82.192.95.92	192.168.1.6	HTTP	HTTP/1.1 204 No Content
19536	995.382911000	82.192.95.92	192.168.1.6	HTTP	[TCP Retransmission] HTTP/1.1 204 No Content
19539	995.505191000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19540	995.505232000	192.168.1.6	82.192.95.92	TCP	55555 > http [RST, ACK] Seq=1104 Ack=93 Win=0 Len=0
19550	996.308269000	192.168.1.6	149.7.96.236	TCP	55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
19551	996.308324000	192.168.1.6	192.168.1.6	ICMP	Redirect (Redirect for host)
19552	996.308363000	192.168.1.6	149.7.96.236	TCP	55553 > mtqp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

Frame 9164: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
Ethernet II, Src: HonHaiPr_26:b5:30 (c0:cb:38:26:b5:30), Dst: Azurewav_43:90:de (00:15:af:43:90:de)
Internet Protocol Version 4, Src: 68.126.7.59 (68.126.7.59), Dst: 192.168.1.6 (192.168.1.6)
Transmission Control Protocol, Src Port: 19207 (19207), Dst Port: 55400 (55400), Seq: 1, Ack: 1, Len: 23

0000 00 15 af 43 90 de c0 cb 38 26 b5 30 08 00 45 00 ...C....8&0..E.
0010 00 3f 57 57 40 00 ef 06 26 fa 44 7e 07 3b c0 a8 ..?Ww0...&D-;..
0020 01 06 4b 07 d8 68 00 00 00 00 0f 49 3f 88 50 14 ..K...I?P.
0030 00 00 5a f6 00 00 47 6f 20 61 77 61 79 2c 20 77 ..Z...Go away, w
0040 65 27 72 65 20 6e 6f 74 20 68 6f 6d 65 e're not home

eth1: <live capture in progress> File: Packets: 19552 Displayed: 5155 Marked: 0



Was geschieht auf meinen Systemen?

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

A [Icons]

Process	PID	Protocol	L...	Local Port	Re...	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd
TeamViewer....	1708	UDP	DH...	52272	*	*			508	13.718	1.016
TeamViewer....	1708	UDP	DH...	54592	*	*					
TeamViewer....	1708	UDP	DH...	55962	*	*					
TeamViewer....	1708	UDP	DH...	61314	*	*		507	15.719	1.014	
InputDirector....	3912	UDP	DH...	57466	*	*		503	13.188	939	
svchost.exe	996	UDPv6	dhm...	546	*	*		68	13.056		
TmProxy.exe	2864	TCP	dhm...	57821	channel28...	http	ESTABLISHED	1	1.476	2	
TmProxy.exe	2864	TCP	dhm...	57836	channel28...	http	ESTABLISHED				
System	4	TCP	dhm...	57828	dhmucw07...	microsoft-ds	SYN_SENT				
System	4	TCP	dhm...	57829	dhmucw07...	microsoft-ds	SYN_SENT				
TmProxy.exe	2864	TCP	DH...	6999	DHMUCW1...	0	LISTENING				
TmProxy.exe	2864	TCP	DH...	6999	localhost	65382	ESTABLISHED				
chrome.exe	3436	TCP	DH...	57835	localhost	6999	ESTABLISHED				
TmProxy.exe	2864	TCP	DH...	6999	localhost:63...	63403	ESTABLISHED	19	2.211	10	
chrome.exe	3436	TCP	DH...	57831	localhost	6999	ESTABLISHED	1	778	2	
chrome.exe	3436	TCP	DH...	57833	localhost	6999	ESTABLISHED	1	656	2	
TmProxy.exe	2864	TCP	DH...	6999	localhost:57...	57835	ESTABLISHED	38	4.636	22	
TmProxy.exe	2864	TCP	DH...	6999	localhost:57...	57831	ESTABLISHED	92	11.830	57	
chrome.exe	3436	TCP	DH...	57820	localhost	6999	ESTABLISHED	1	1.476	2	
TmProxy.exe	2864	TCP	DH...	6999	localhost:57...	57833	ESTABLISHED	52	6.732	27	
[System Proc...	0	TCP	DH...	6999	localhost:57...	57826	TIME_WAIT	69	8.697	37	
[System Proc...	0	TCP	DH...	6999	localhost:57...	57798	TIME_WAIT	97	11.952	59	
[System Proc...	0	TCP	DH...	6999	localhost:57...	57807	TIME_WAIT	31	5.232	25	
svchost.exe	868	TCP	dhm...	epmap	mucdc01.h...	4485	ESTABLISHED				
mstsc.exe	7748	TCP	dhm...	64351	rotfs01	ms-wbt-server	ESTABLISHED	5	208	6	
mstsc.exe	8924	TCP	dhm...	63929	mucinv01.h...	ms-wbt-server	ESTABLISHED	5	208	5	
mstsc.exe	11256	TCP	dhm...	64729	mucmdt10...	ms-wbt-server	ESTABLISHED	5	329	7	
mstsc.exe	5600	TCP	dhm...	64707	mucev01.h...	ms-wbt-server	ESTABLISHED	5	218	15	

Endpoints: 153 Established: 54 Listening: 30 Time Wait: 14 Close Wait: 4

Die „heilige Zauberwaffe“ gegen
Bedrohungen aller Art

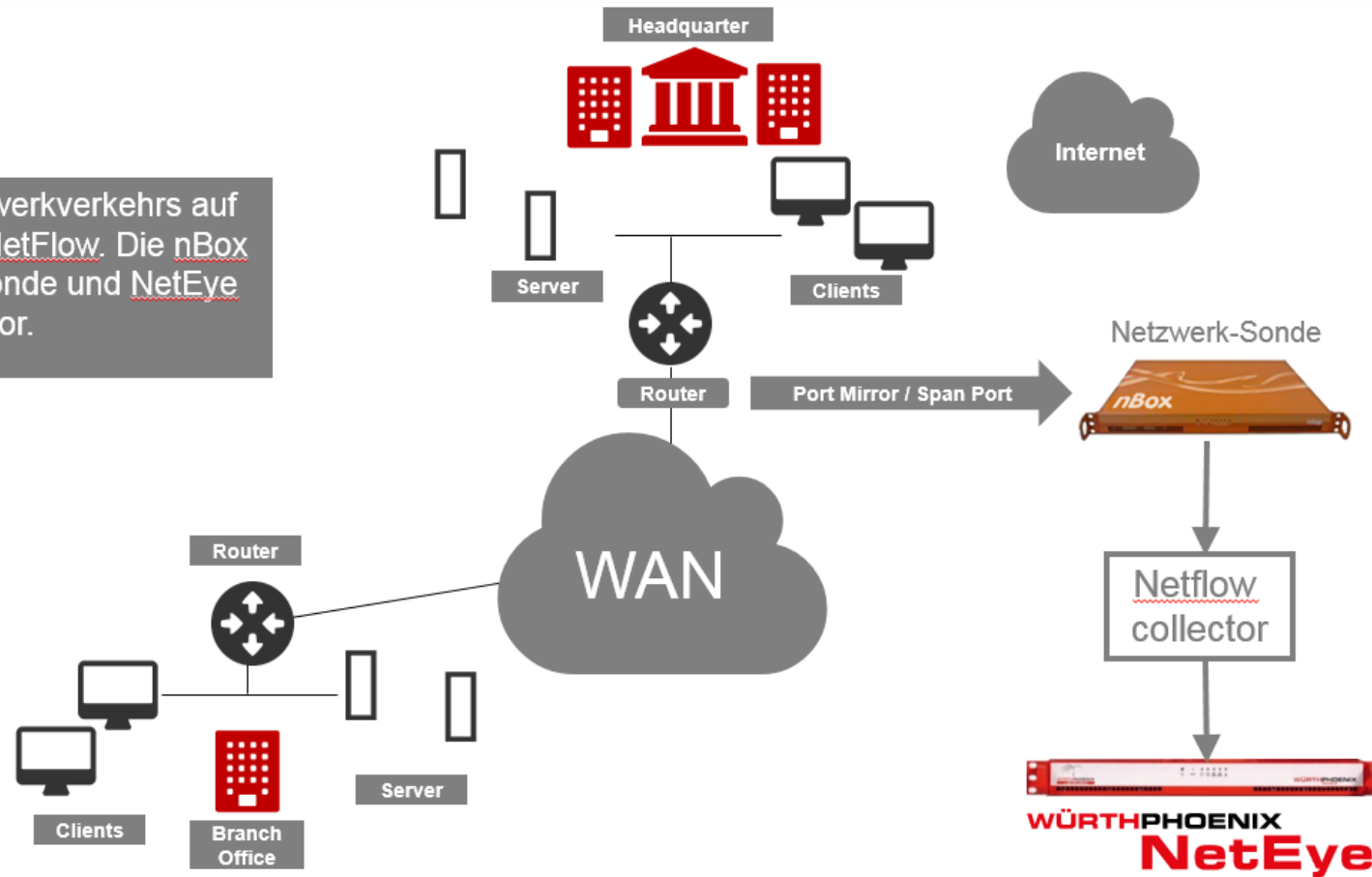


Videmus (wir sehen) lat.

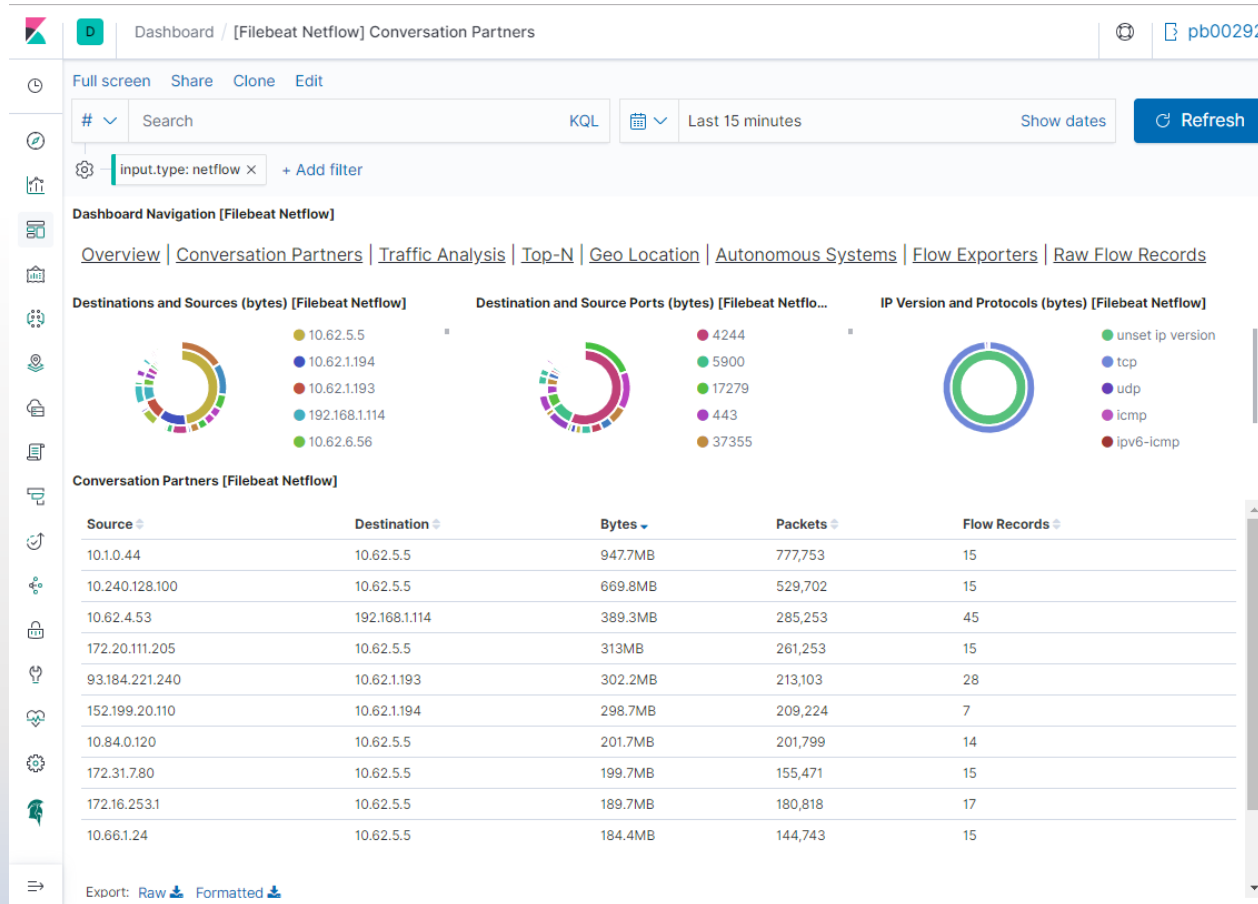
Monitoring

Überwachung des Netzwerkverkehrs

Überwachung des Netzwerkverkehrs auf Applikations-Ebene mit NetFlow. Die nBox fungiert als Netzwerk-Sonde und NetEye als Kollektor.

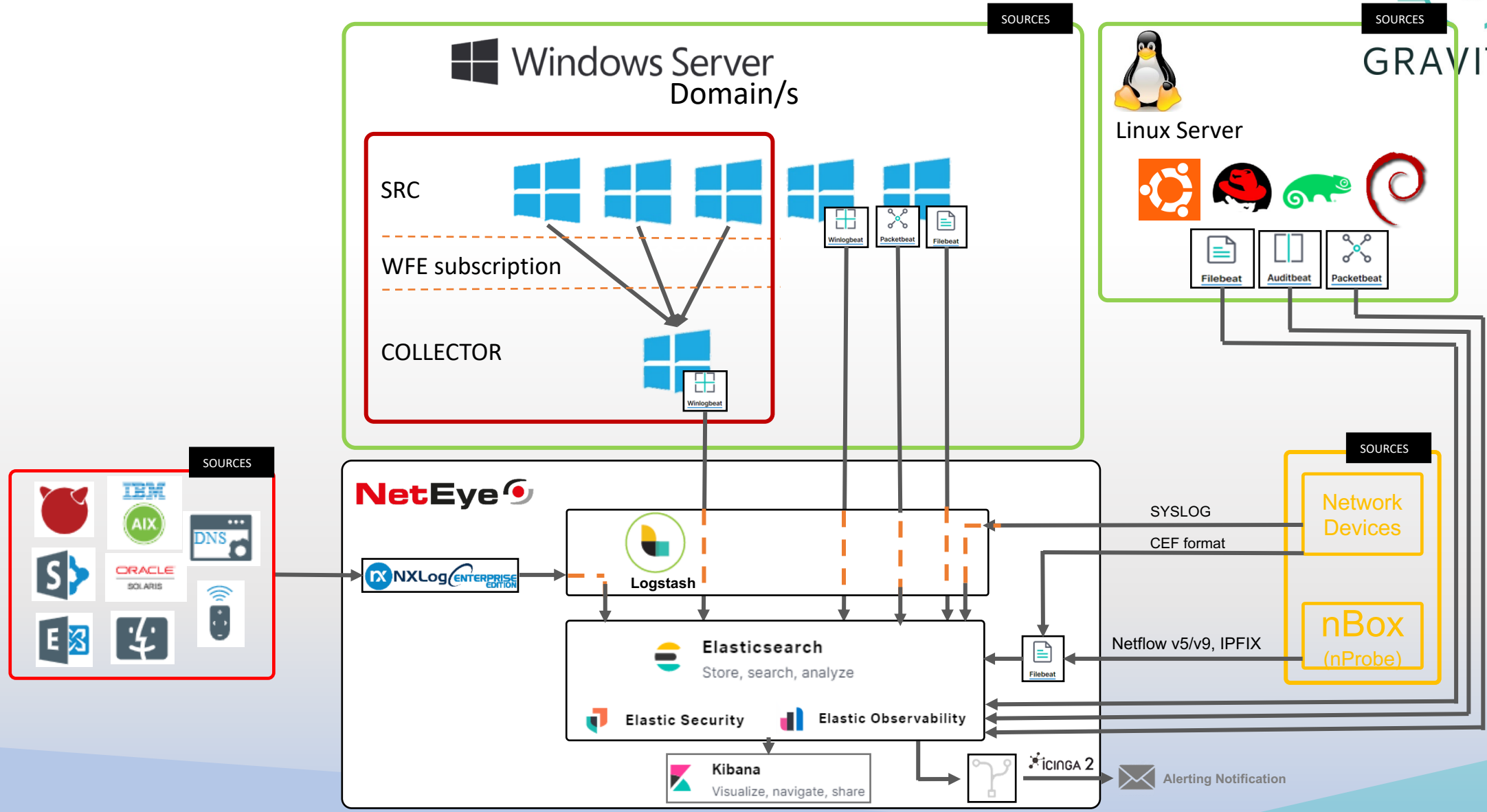


Statistiken zur Überwachung des Netzwerkverkehrs in NetEye



- Analyse des Netzwerkverkehrs basierend auf den verwendeten Protokollen
- Identifikation von Quell- und Ziel-IP-Adresse
- Filter nach Ports TCP/UDP
- Analyse einzelner Pakete

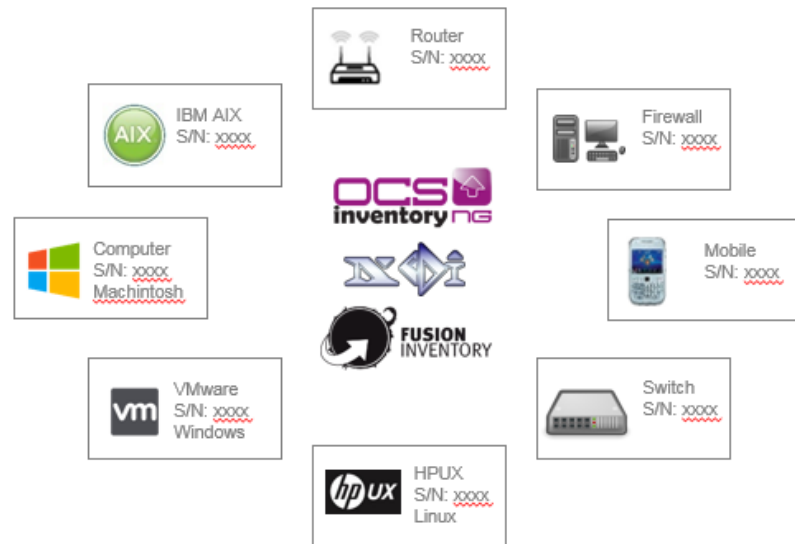
Zusammenführung der erfassten Daten:



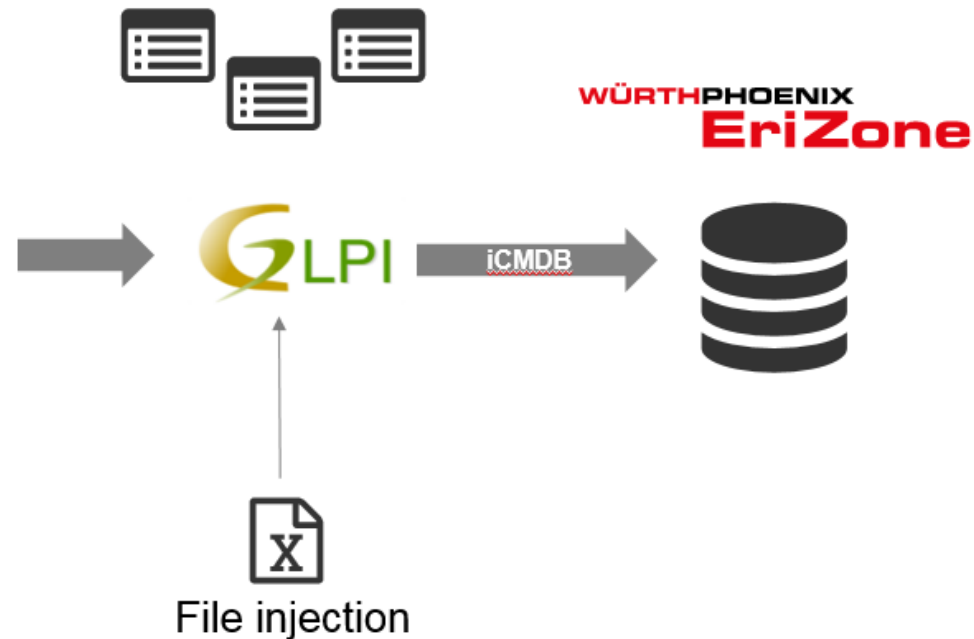
Automatisches Netzwerk Discovery und Asset Management



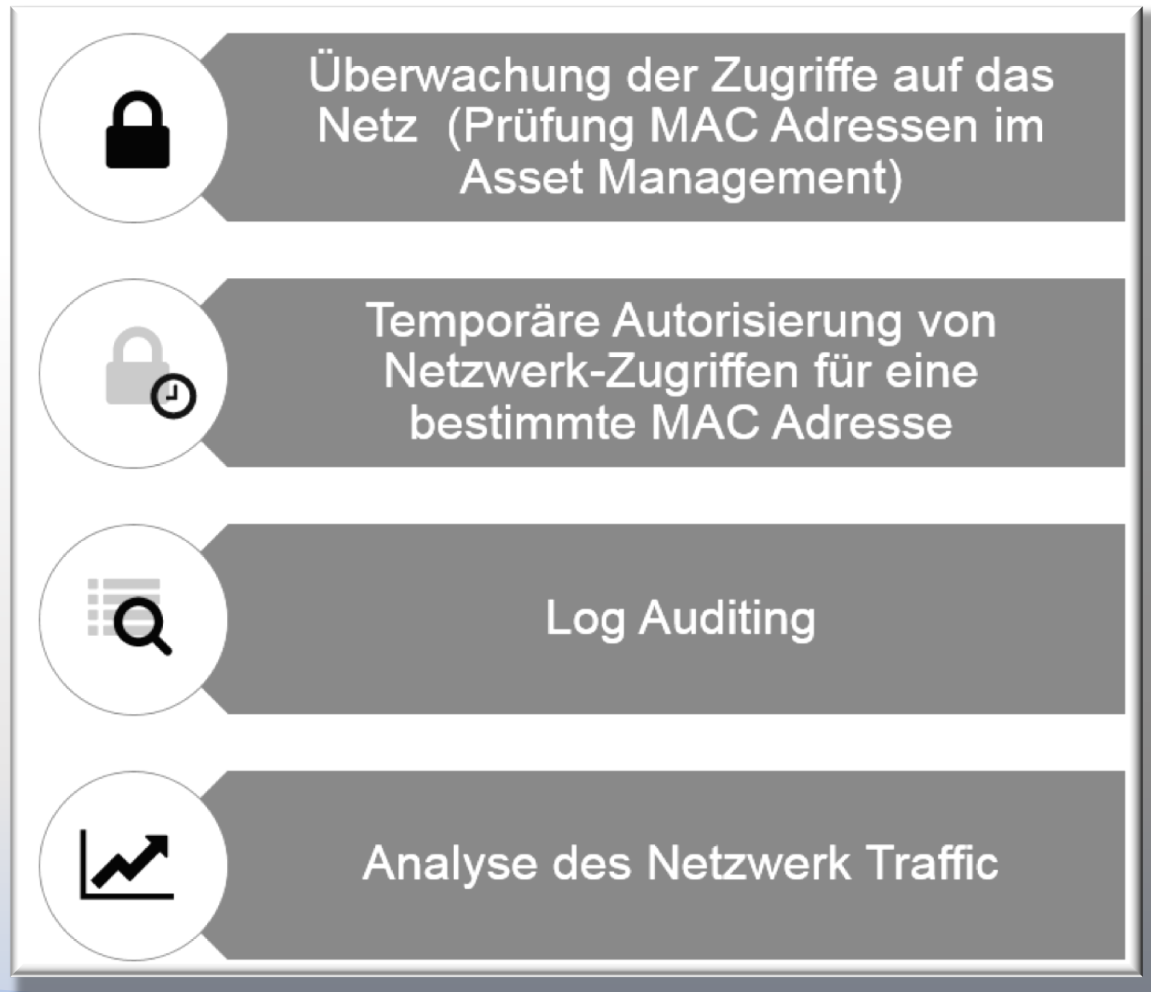
AUTOMATIC DISCOVERY



ASSET MANAGEMENT



Security monitoring mit neteye



SOC / SIEM

Lösungsansätze

- Security Awareness: zu allererst bei den IT Verantwortlichen
- Einsatz leistungsstarker Monitoring Lösungen:
- Überwachung des Netzwerkverkehr, der Firewall und der Geräte im Netzwerk -> Stichwort: SOC, SIEM

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT





GRAVITATE

Ihr Partner für IT-Sicherheit und Monitoring